Command Line Interface Reference, Modes I - Q, StarOS Release 21.28

First Published: 2022-09-29

Last Modified: 2025-05-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

About this Guide

Note The ASR 5000 hardware platform has reached end of life and is not supported in this release. Any references to the ASR 5000 (specific or implied) or its components in this document are coincidental. Full details on the ASR 5000 hardware platform end of life are available at: https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5000-series/eos-eol-notice-c51-735573.html.

This preface describes the *Command Line Interface Reference* and its document conventions.

This reference describes how to use the command line interface (CLI) to interact with the products supported by the StarOS™. The CLI commands are organized by command modes in the code and in this reference. The command modes are presented alphabetically. The description of each command states the command's function, describes its syntax, presents limitations when applicable, and offers an example of its usage.

CLI Command Sections

The following table describes the individual sections in the command descriptions presented in this reference.

Section	Description
Product	The product(s) supporting the CLI command.
Privilege	The user privilege levels having access to the CLI command. For more information on user types and user privileges, refer to the *CLI Administrative Users* section in the *Command Line Interface Overview* chapter.
Mode	The command and configuration mode sequences to the CLI configuration mode for the CLI command. For more information on command modes, refer to the *CLI Command Modes* section in the *Command Line Interface Overview* chapter.

Section	Description
Syntax	The command's syntax. For more information on CLI command syntax, refer to the *CLI Command Syntax* section in the *Command Line Interface Overview* chapter.
	Description of the keyword(s) and variable(s) in the command.
Usage	Information about the command's usage including dependencies and limitations, if any.
Example	Example(s) of the command.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* is a variable representing the desired chassis slot number.

Typeface Conventions	Description
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Command Syntax Conventions	Description
{ keyword or *variable* **}**	Required keyword options and variables are those components that are required to be entered as part of the command syntax. Required keyword options and variables are surrounded by grouped braces { }. For example: **sctp-max-data-chunks { limit** *max_chunks* **| mtu-limit }** If a keyword or variable is not enclosed in braces or brackets, it is mandatory. For example: **snmp trap link-status**
[keyword or *variable* **]**	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by brackets.
|	Some commands support multiple options. These are documented within braces or brackets by separating each option with a vertical bar. These options can be used in conjunction with required or optional keywords or variables. For example: **action activate-flow-detection { intitiation | termination }** or **ip address [count** *number_of_packets* **| size** *number_of_bytes* **]**

Supported Documents and Resources

Related Documentation

The most up-to-date information for this product is available in the product *Release Notes* provided with each software release.

The following related product documents are also available:

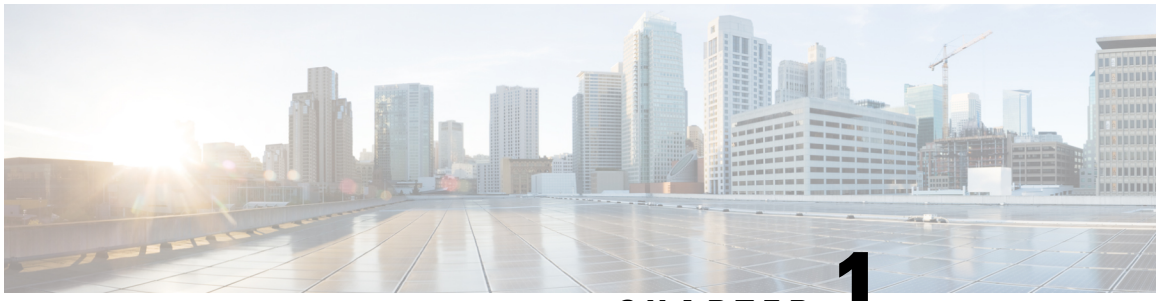
- *AAA Interface Administration and Reference*

- *GTPP Interface Administration and Reference*
- *IPSec Reference*
- Platform-specific System Administration Guides
- Product-specific Administration Guides
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *Statistics and Counters Reference - Bulk Statistics Descriptions*
- *Thresholding Configuration Guide*

Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.



CHAPTER 1

Common Commands

This chapter describes the common commands available in each CLI configuration mode.

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.
```

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

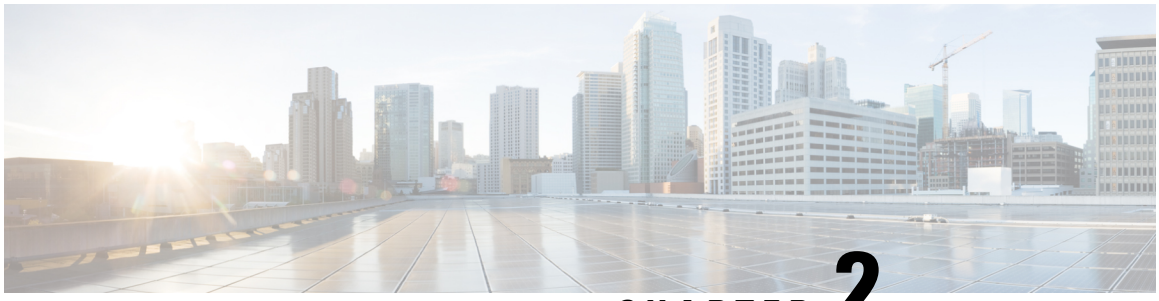
Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description `exit`

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



CHAPTER 2

IFTask Boot-Options Configuration Mode Commands

The iftask boot-options Configuration Mode is used to configure startup configuration parameters on the VPC-DI.

Command Modes

Exec > Global Configuration > IFTask Boot-Options Configuration

configure > iftask boot-options

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-iftask-boot-options)#
```

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

priority

Sets the priority for the boot configuration parameters to take effect on the VPC-DI.

Product

All

Privilege

Administrator

Mode

Exec > Global Configuration > IFTask Boot-Options Configuration

configure > iftask boot-options

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-iftask-boot-options)#
```

Syntax Description

```
priority { cli | cdrom }
```

cli

Sets the CLI-configured boot parameters as priority.

cdrom

Sets the CDROM configuration as priority. If the CDROM configuration is not present, then default boot parameters are applied.

Usage Guidelines

Use this command to set the priority for the boot configuration parameters to take effect on the VPC-DI.

Example

The following command specifies the priority to CDROM for the VPC-DI:

```
priority cdrom
```

sfc

Configures the startup configuration parameters for the Service Function Card (SFC) on the VPC-DI.

Product

All

Privilege

Administrator

Mode

Exec > Global Configuration > IFTask Boot-Options Configuration

configure > iftask boot-options

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-iftask-boot-options)#
```

Syntax Description

`[ no ] sfc { cores [ crypto | mcdma ]` *`percentage`* **`| thread-enable { control | mcdma } }`**

no sfc cores

Disables IFTask cores percentage. This parameter must be enabled for other configured parameters to take effect.

no sfc cores crypto mcdma

Disables crypto cores, percentage, and mcdma cores percentage for SF card.

no sfc thread-enable control mcdma

Disables thread-enable, control, and mcdma SF card parameters.

Note The **no** keyword is not applicable to **priority** because it is mandatory to have a default priority set.

sfc cores [crypto | mcdma] *percentage*

Specifies the cores allocation for crypto or mcdma on the SF card with the percentage of the maximum number of IFTASK cores configured with this CLI. For cores percentage, the limits are checked in iftask.py file. Therefore, any value from 1 to 100 is supported.

sfc cores *percentage*

Specifies the cores allocation for IFTASK in general for crypto or mcdma on the SF card with the percentage of the maximum number of IFTASK cores present in the system. For cores percentage, the limits are checked in iftask.py file. Therefore, any value from 1 to 100 is supported.

thread-enable { control | mcdma }

Enables control thread or mcdma thread.

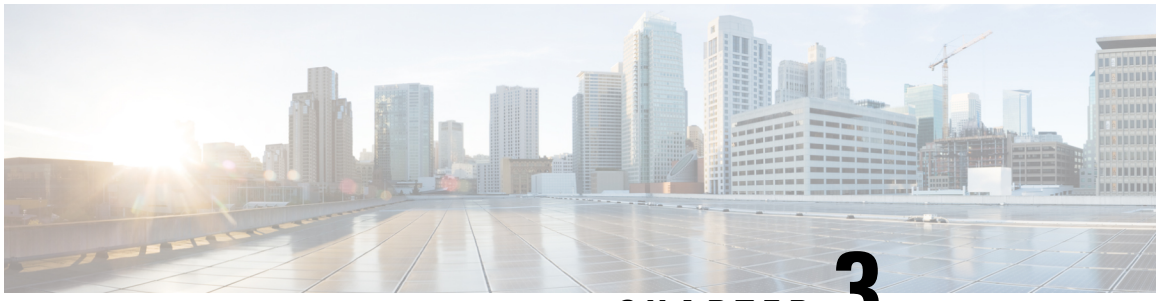
Usage Guidelines

Use this command to configure the startup configuration parameters for the Service Function Card (SFC) on the VPC-DI.

Example

The following command specifies the percentage of cores, crypto cores, and mcdma cores on the SFC card:

```
sfc cores 40 crypto 40 mcdma 40
```



CHAPTER 3

IGMP Profile Configuration Mode Commands

Command Modes

The Internet Group Management Protocol (IGMP) Profile Configuration Mode is used to create and manage the IGMP parameters for an Ethernet interface.

Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

configure > context *context_name* **> ip igmp profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-igmp-profile-<profile_name>)#`

Important Available commands or keywords/variables vary based on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

default ip igmp

Configures default IGMP parameters.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

configure > **context** *context_name* > **ip igmp profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-igmp-profile-<profile_name>)#`

Syntax Description

```
default ip igmp { query | require | robustness |
unsolicited-report-interval | version }
```

Usage Guidelines

Specify the IGMP parameters for the default profile. Refer to the remaining command description in this chapter for additional information.

Example

To apply enable echo mode on this interface, use the following command:

```
bfd echo
```

ip igmp query

Configures the maximum response time for IGMP queries.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

configure > **context** *context_name* > **ip igmp profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-igmp-profile-<profile_name>)#`

Syntax Description

ip igmp query max-response-time *seconds*

max-response-time *seconds*

Specify the maximum number of seconds that the system will wait for an IGMP response as an integer from 1 through 25.

Usage Guidelines

Specify the maximum response time for IGMP queries.

Example

```
ip igmp query max-response-time 10
```

ip igmp require router-alert

Sets the router alert flag to ON in IP IGMP packets.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

configure > context *context_name* **> ip igmp profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-igmp-profile-<profile_name>)#`

Syntax Description **`[ no ] ip igmp require router-alert`**

no

Sets the router alert flag to OFF in IP IGMP packets.

Usage Guidelines Sets the router alert flag to ON in IP IGMP packets.

Example

`ip igmp require router-alert`

ip igmp robustness

Sets the Robustness value in IP IGMP packets. The Robustness variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness variable may be increased. IGMP is robust to packet losses. The Robustness variable should not be set to 1 (one).

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

configure > context *context_name* **> ip igmp profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-igmp-profile-<profile_name>)#`

Syntax Description **`ip igmp robustness`** *`value`*

value

Sets the robustness value as an integer from 1 through 10. Default: 2

Usage Guidelines Sets the robustness value in IP IGMP packets.

Example

`ip igmp robustness 7`

ip igmp unsolicited-report-interval

Sets the Unsolicited Report Interval which is the time between repetitions of a host's initial report of membership in a group.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

configure > context *context_name* **> ip igmp profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-igmp-profile-<profile_name>)#`

Syntax Description

`ip igmp unsolicited-report-interval` *`seconds`*

seconds

Specifies the number of seconds between repetitions of a host's initial report of membership in a group as an integer from 1 through 25. Default: 10

Usage Guidelines

Set the Unsolicited Report Interval which is the time between repetitions of a host's initial report of membership in a group.

Example

```
ip igmp unsolicited-report-interval 15
```

ip igmp version

Sets the IGMP version to be supported by this interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

configure > context *context_name* **> ip igmp profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-igmp-profile-<profile_name>)#`

Syntax Description

`ip igmp version { v1 | v2 | v3 }`

v1 | v2 | v3

Specifies the IGMP Version number:

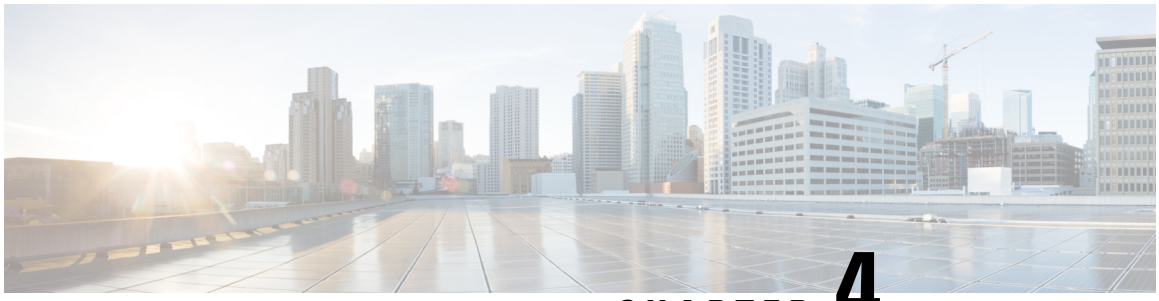
- **v1:** Version 1, RFC 1112
- **v2**: Version 2, RFC 2236
- **v3**: Version 3, RFC 4604

Usage Guidelines

Set the IGMP version to be supported by this interface.

Example

```
ip igmp version v2
```



CHAPTER 4

IKEv2 Security Association Configuration Mode Commands

The IKEv2 Security Association Configuration Mode is used to configure a Security Association (SA) at the outset of an IPSec session. A security association is the collection of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. In normal bi-directional traffic, the flows are secured by a pair of security associations.

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

default

Sets the default properties for the selected parameter.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

default { encryption | group | hmac | lifetime | prf }

Set the defaults for the following parameters:

- **encryption**: Default algorithm for the IKEv2 IKE SA is AES-CBC-128.
- **group**: Default Diffie-Hellman group is Group 2.
- **hmac**: Default IKEv2 IKE SA hashing algorithm is SHA1-96.
- **lifetime**: Default lifetime for SAs derived from this transform-set is 86400 seconds.
- **prf**: Default PRF for the IKEv2 IKE SA is SHA1.

Usage Guidelines

Configure default parameters for the IKEv2 IKE SA transform-set.

Example

Use the following configuration to set the default encryption algorithm:

```
default encryption
```

encryption

Configures the appropriate encryption algorithm and encryption key length for the IKEv2 IKE security association. AES-CBC-128 is the default.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

encryption { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc | null }
default encryption

3des-cbc

Data Encryption Standard Cipher Block Chaining encryption applied to the message three times using three different cypher keys (triple DES).

aes-cbc-128

Advanced Encryption Standard Cipher Block Chaining with a key length of 128 bits.

aes-cbc-256

Advanced Encryption Standard Cipher Block Chaining with a key length of 256 bits.

des-cbc

Data Encryption Standard Cipher Block Chaining. Encryption using a 56-bit key size. Relatively insecure.

null

Configures no IKEv2 IKE Security Association Encryption Algorithm. All IKEv2 IPsec Child Security Association protected traffic will be sent in the clear.

Note USE OF THIS ALGORITHM FOR IKE_SA ENCRYPTION IS A VIOLATION OF RFC 4306. THIS ALGORITHM SHOULD ONLY BE USED FOR TESTING PURPOSES.

Usage Guidelines

IKEv2 requires a confidentiality algorithm to be applied in order to work.

In cipher block cryptography, the plaintext is broken into blocks usually of 64 or 128 bits in length. In cipher block chaining (CBC) each encrypted block is chained into the next block of plaintext to be encrypted. A randomly-generated vector is applied to the first block of plaintext in lieu of an encrypted block. CBC provides confidentiality, but not message integrity.

Because RFC 4307 calls for interoperability between IPSec and IKEv2, the IKEv2 confidentiality algorithms must be the same as those configured for IPSec in order for there to be an acceptable match during the IKE message exchange. Because of RFC4307, in IKEv2, there is no viable NULL option, it is available for testing only.

Example

The following command configures the encryption to be aes-cbc-128:

```
encryption aes-cbc-128
```

group

Configures the appropriate key exchange cryptographic strength by applying a Diffie-Hellman group. Default is Group 2.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

group { 1 | 2 | 5 | 14 }
default group

1

Configures crypto strength at the Group 1 level. Lowest security.

2

Configures crypto strength at the Group 2 (default) level. Medium security.

This is the default setting for this command.

5

Configures crypto strength at the Group 5 level. Higher security.

14

Configures crypto strength at the Group 14 level. Highest security

Usage Guidelines

Diffie-Hellman groups are used to determine the length of the base prime numbers used during the key exchange process in IKEv2. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group upon which the prime numbers are based.

Group 1 provides 768 bits of keying strength, Group 2 provides 1024 bits, Group 5 provides 1536 bits and Group 14 provides 2048 bits of encryption strength.

Configuring a DH group also enables Perfect Forward Secrecy, which is disabled by default.

Example

This command configures crypto strength at the Group 14 level. Highest security group 14:

default group

hmac

Configures the IKEv2 IKE SA integrity algorithm. Default is SHA1-96.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

hmac { aes-xcbc-96 | md5-96 | sha1-96 | sha2-256-128 | sha2-384-192 | sha2-512-256 }
default hmac

aes-xcbc-96

HMAC-AES-XCBC uses a 128-bit secret key and produces a 128-bit authenticator value.

md5-96

HMAC-MD5 uses a 128-bit secret key and produces a 128-bit authenticator value.

sha1-96

HMAC-SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value. This is the default setting for this command.

sha2-256-128

HMAC-SHA-256 uses a 256-bit secret key and produces a 128-bit authenticator value.

sha2-384-192

HMAC-SHA-384 uses a 384-bit secret key and produces a 192-bit authenticator value.

sha2-512-256

HMAC-SHA-512 uses a 512-bit secret key and produces a 256-bit authenticator value.

Usage Guidelines

IKEv2 requires an integrity algorithm be configured in order to work.

A keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity. A hash takes a message of any size and transforms it into a message of a fixed size: the authenticator value. This is truncated and transmitted. The authenticator value is reconstituted by the receiver and the first truncated bits are compared for a 100 percent match.

Example

This command configures HMAC value md5-96:

hmac md5-96

lifetime

Configures the lifetime of a security association (SA) in seconds.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

`lifetime` *`sec`*
`default lifetime`

lifetime *sec*

Sets the value of the timeout parameter in seconds as an integer from 60 through 86400. Default: 86400

Usage Guidelines

The secret keys that are used for various aspects of a configuration should only be used for a limited amount of time before timing out. This exposes a limited amount of data to the possibility of hacking. If the SA expires, the options are then to either close the SA and open an new one, or renew the existing SA.

Example

The following command sets the lifetime timeout to 120 seconds:

`lifetime 120`

prf

Selects one of the HMAC integrity algorithms to act as the IKE Pseudo-Random Function. A PRF produces a string of bits that an attacker cannot distinguish from random bit string without knowledge of the secret key. The default is SHA1.

Product

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context *context_name* **> ikev2-ikesa transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

Syntax Description

prf { aes-xcbc-128 | md5 | sha1 | sha2-256 | sha2-384 | sha2-512 } default prf

aes-xcbc-128

Configure IKEv2 IKE Security Association Pseudo Algorithm to be AES-XCBC-128.

md5

MD5 uses a 128-bit secret key and produces a 128-bit authenticator value.

sha1

SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value.

SHA-1 is considered cryptographically stronger than MD5, but it takes more CPU cycles to compute.

This is the default setting for this command.

sha2-256

PRF-HMAC-SHA-256 uses a 256-bit secret key.

sha2-384

PRF-HMAC-SHA-384 uses a 384-bit secret key.

sha2-512

PRF-HMAC-SHA-512 uses a 512-bit secret key.

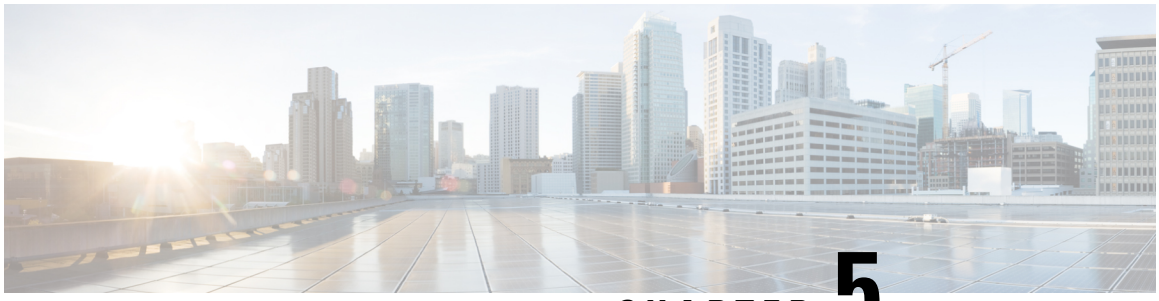
Usage Guidelines

This command generates keying material for all the cryptographic algorithms used in both the IKE_SA and the CHILD_SAs.

Example

This configuration sets the PRF to be value sha2-256:

```
prf sha2-256
```



CHAPTER 5

IMEI Profile Configuration Mode

Essentially, an IMEI profile is a template which groups a set of device-specific commands that may be applicable to one or more IMEIs. The same IMEI profile can be associated with multiple IMEI ranges and multiple operator policies.

An SGSN supports a total of 1000 IMEI profile configurations.

Command Modes

The IMEI profile configuration mode defines a set of parameters controlling the SGSN behavior when a Request is received from a device in the specified IMEI (International Mobile Equipment Identity) range. An IMEI profile is a key element in the Operator Policy feature and an IMEI profile is not used or valid unless it is associated with an IMEI range and this association is specified in an operator policy (see the *Operator Policy Configuration Mode Commands* chapter elsewhere in the *Command Line Interface Reference*).

Exec > Global Configuration > IMEI Profile Configuration

configure > imei-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-imei-profile-profile_name)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

associate

Associate an APN remap table with this IMEI profile.

Note that an APN remap table can be associated with an IMEI profile before the table has actually been created/configured.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > IMEI Profile Configuration

configure > imei-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-imei-profile-profile_name)#`

Syntax Description

associate apn-remap-table *table_name*
no associate apn-remap-table

no

Disables the configured remap table association.

table_name

Define the name of an APN remap table that is to be associated with this IMEI profile for call routing based in IMEI.

Usage Guidelines

Use this command to associate an APN remap table with this IMEI profile. With such an association, it is possible to override an APN call-routing based on an IMEI.

For example, with the APN exceptions defined in an APN remap table (refer to the *APN Remap Table Configuration Mode* chapter), a blank APN or an incorrect APN could be overriden. So during PDP Activation for in incoming call, the call could be rerouted based on an IMEI in the range defined for the IMEI profile.

Example

Associate the APN remap table 'remapHO' (remaps all calls with blank APNS to the head-office) to this IMEI profile:

associate apn-remap-table *remapHO*

blacklist

Blacklist all mobile devices that fit the IMEI definitions associated with this IMEI profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > IMEI Profile Configuration

configure > imei-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-imei-profile-profile_name)#`

Syntax Description

`blacklist`
`remove blacklist`

remove

Including this keyword with the command, removes the blacklist command from the IMEI profile configuration.

Usage Guidelines

Blacklists subscribers whose devices bear IMEI that match the defined IMEI range for this profile.

Example

Use this command to black list all subscribers with IMEI that fall within the range set for this IMEI profile:

`blacklist`

description

Define a descriptive string relevant to the specific APN profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > IMEI Profile Configuration

configure > imei-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-imei-profile-profile_name)#`

Syntax Description

`description` *`description`*
`remove description`

remove

Removes the configured description from this APN profile.

description

Enter an alphanumeric string of 1 to 100 alphanumeric characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotes (").

Usage Guidelines Define information that identifies this particularly APN profile.

Example

Indicate that this IMEI profile *IMEIprof1* is to be used for customers in the United Kingdom and that the profile:

```
description "IMEIprof1 defines routing actions based on IMEI for customers in the UK."
```

direct-tunnel

Instruct the SGSN to enable/disable a direct tunnel between the RNC and the GGSN based on the IuPS service configuration.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IMEI Profile Configuration

configure > imei-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-imei-profile-profile_name)#
```

Syntax Description

```
direct-tunnel check-iups-service
no direct-tunnel
```

no direct-tunnel

This command instructs the SGSN to disable the direct tunnel function between the GGSN and the RNC.

Usage Guidelines Direct tunnel is enabled by default on the GGSN and often on the RNC. This leaves it to the SGSN's configuration to actually enable or disable a direct tunnel.

With the SGSN, the options for configuring a direct tunnel are complex -- enable/disable on the basis of APNs, or RNCs, or GGSNs, or on the basis of the IMEI range. Refer to the *SGSN Administration Guide* for configuration details.

Example

Assuming the IuPS service configuration has enabled DT for associated RNCs, then use this command to enable DT from the RNC to the GGSN associated with this IMEI profile:

```
direct tunnel check-iups-service
```

ggsn-address

Identify the target GGSN for traffic being managed by this IMEI profile.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IMEI Profile Configuration

configure > imei-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-imei-profile-profile_name)#`

Syntax Description **ggsn-address** *IPv4/IPv6_address*

IPv4/IPv6_address

Enter the IP address of the target GGSN. Enter the address in either standard IPv4 dotted decimal format or in standard IPv6 colon notation format.

Usage Guidelines Use this command to define the IP address of the target GGSN to be associated with this IMEI profile.

Example

The following command identifes the address of the GGSN associated with this IMEI profile as 209.165.200.225

ggsn-address *209.165.200.225*

ignore-pdp-data-inactivity

On executing this command the SGSN ignores PDP Data Inactivity configuration under the APN profile for one or more matching IMEIs.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IMEI Profile Configuration

configure > imei-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-imei-profile-profile_name)#`

Syntax Description
ignore-pdp-data-inactivity
remove ignore-pdp-data-inactivity

remove

This command is used to disable or remove the option to ignore PDP data inactivity from the IMEI profile.

Usage Guidelines

The SGSN supports options to configure PDP Data Inactivity detection duration and actions to be performed on timeout under the APN-Profile. The following configurable actions are supported under APN-Profile in case of PDP Data Inactivity detection in the PDP context:

1. De-activate all PDPs of the subscriber
2. De-activate all PDPs of the bundle (all linked PDPs)
3. Detach the subscriber. This action is triggered when:
   - Data in-activity is detected for all PDPs
   - Data in-activity is detected for any of the PDPs

On the Detection of the PDP Data Inactivity, depending on the configuration option the SGSN either de-activates the PDP or detaches the subscriber.

The **ignore-pdp-data-inactivity** CLI is added to provide an option under the IMEI-Profile to ignore PDP Data Inactivity configuration for one or more IMEIs. On configuring this CLI, the SGSN ignores the application of in-activity configuration (configured in the APN-Profile) for a specified set of IMEI's.

Note The IMEI range or set of IMEI's are mapped to specific IMEI-Profile using the CLI configuration option under Operator-policy.

Example

Use this command to ignore PDP Data Inactivity configuration under the APN profile for one or more matching IMEIs.

ignore-pdp-data-inactivity

pdp-activate

This command enables the operator to configure the SGSN to reject Secondary PDPActivation Requests from the UE based on IMEI range.

Product

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > IMEI Profile Configuration

configure > **imei-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-imei-profile-profile_name)#
```

Syntax Description

[remove] pdp-activate { drop | restrict } secondary-activation access-type { gprs | umts }

remove

Removes the configured value and returns the pdp-activate configuration to the default 'not configured' state.

drop

This keyword causes the GSN to ignore the Request.

restrict

This keyword instructs the SGSN to reject Secondary PDP Activation Requests.

access-type { gprs | umts }

This keyword instructs the SGSN to ignore or reject Secondary PDP Activation Requests on the basis of the UE's access network type:

- **gprs** : from a 2G network.
- **umts** : from a 3G network.

Usage Guidelines

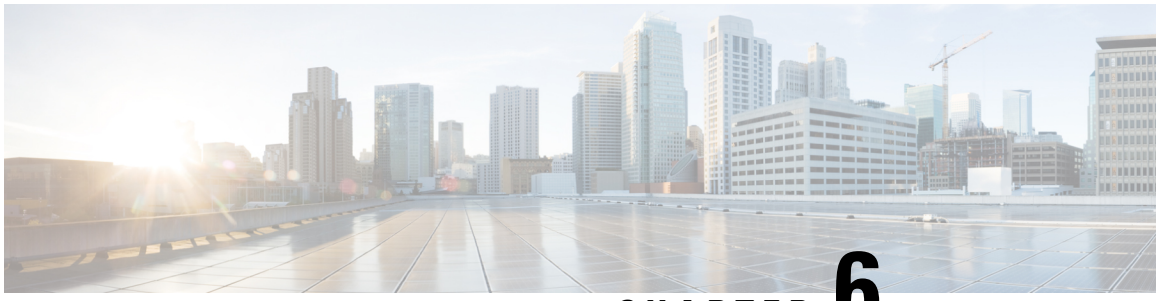
The SGSN administrator can use this command to configure the IMEI profile in the operator policy to either ignore or reject Secondary PDP Activation Requests from UEs based on an IMEI range and UE access-type.

Restricting secondary PDP activation based on the IMEI (in the IMEI profile) takes precedence over secondary PDP activation that might be configured in the call control profile.

Example

Enable rejection of Secondary PDP Activation Requests for 2G callers:

```
pdp-activate restrict secondary-activation access-type gprs
```



CHAPTER 6

IMEI-TAC-Group Configuration Mode Commands

The IMEI-TAC-Group Configuration Mode provides access to the commands used to configure the IMEI-TAC values and ranges included in the IMEI-TAC groups. These IMEI-TAC values and ranges are used as the selection criteria for operator policy selection based on IMEI-TAC. For details about this functionality, refer to the *Operator Policy Selection Based on IMEI-TAC* chapter in the *MME Administration Guide*.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > IMEI-TAC-Group

configure > lte-policy > imei-tac-group*group_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(imei-tac-group)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

tac

Confitures individual TAC (type allocation code) values to be included in a IMEI-TAC group which will be used as criteria for operator policy selection.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > IMEI-TAC-Group

configure > lte-policy > imei-tac-group*group_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(imei-tac-group)#
```

Syntax Description

`[ no ] tac` *`tac_value`* **`[`** *`tac_value tac_value +`* **`]`**

no

Removes the identified TAC from the IMEI-TAC group configuration.

tac_value

Specifies the 8-digit number that identifies a specific "type allocation code". When entering more than one TAC, simply use a space between each TAC. Additional TAC values can be added at any time after the IMEI-TAC group is configured.

Usage Guidelines

Use this command to enter one or more individual TAC (type allocation code) values to the IMEI-TAC group. Up to 500 unique IMEI-TAC values can be included in an IMEI-TAC group.

The TAC, the first eight digits of the 15-digit IMEI or 16-digit IMEI-SV, identifies the equipment manufacturer, the wireless device type and the model number (if there is one); for example, TAC of 35201906 identifies an Apple iPhone 5S.

Example

The following command adds four IMEI-TAC to an IMEI-TAC group:

```
tac 31441551 77777777 87650506 87654321
```

tac-range

Defines a range of IMEI-TAC values to be included in a IMEI-TAC group which will be used as criteria for operator policy selection.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > IMEI-TAC-Group

configure > lte-policy > imei-tac-group*group_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(imei-tac-group)#
```

Syntax Description

`[ no ] tac-range from` *`start_tac_value`* **`to`** *`end_tac_value`*

no

Removes the identified TAC range from the IMEI-TAC group configuration.

start_tac_value* to *end_tac_value

tac_value - Specifies the 8-digit number that identifies a specific "type allocation code". The **start** TAC is the first TAC in the range. The **end** TAC is the last TAC in the range.

Usage Guidelines

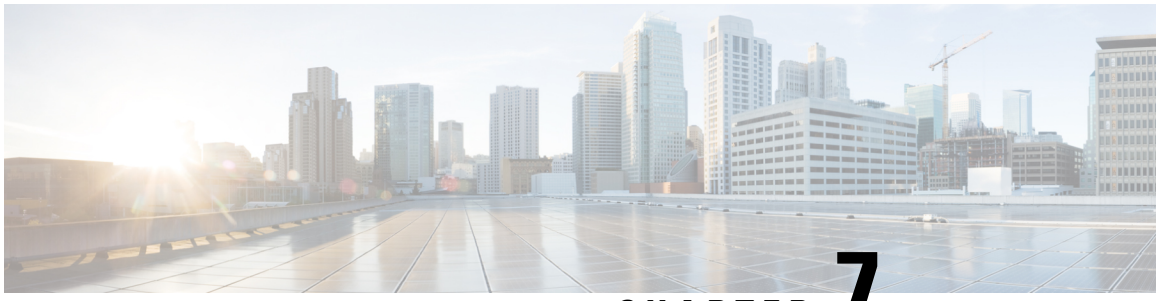
Use this command to enter up to 20 IMEI-TAC value ranges. Ranges can be overlapping.

The TAC, the first eight digits of the 15-digit IMEI or 16-digit IMEI-SV, identifies the equipment manufacturer, the wireless device type and the model number (if there is one); for example, TAC of 35201906 identifies an Apple mobile phone. Defining ranges would enable carriers to select operator policies for call handling based on multiple device types.

Example

The following command defines a TAC range to be added to the IMEI-TAC group:

```
tac-range from 23456789 to 23456889
```



CHAPTER 7

IMS Authorization Service Configuration Mode Commands

The IMS Authorization Service Configuration Mode enables to configure IP Multimedia Subsystem (IMS) authorization services to manage policy control functions and Gx interface support.

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

p-cscf discovery

This command defines the method of Proxy-Call Session Control Function (P-CSCF) discovery to be used.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
p-cscf discovery { table { 1 | 2 } [ algorithm { ip-address-modulus |
msisdn-modulus | round-robin } ] | diameter-configured }
[ default | no ] p-cscf discovery
```

default

Sets the P-CSCF discovery to default parameter.

no

Removes/deletes configured parameters for P-CSCF discovery.

table { 1 | 2 }

Specifies that which P-CSCF table is to be used to obtain the primary and secondary P-CSCF addresses. Total 2 tables can be configured for P-CSCF discovery.

algorithm { ip-address-modulus | msisdn-modulus | round-robin }

Specifies the algorithm to select the row from the P-CSCF table to be used for P-CSCF discovery.

- **ip-address-modulus**: This algorithm divides the IP address, in binary, of the subscriber by the number of rows in the table, and the remainder is used as an index into the specified table to select the row.
- **msisdn-modulus**: This algorithm divides the MSISDN value, in binary without the leading "+", of the subscriber by the number of rows in the table, and the remainder is used as an index in the specific table to select the row.
- **round-robin**: This algorithm rotates all rows in the active table for selection of the row in round-robin way. If no algorithm is specified this is the default behavior.

Default: **round-robin**

diameter-configured

This option enables the table number and algorithm specified by the **diameter host-select table** configuration in Policy Control Configuration mode.

Usage Guidelines

Use this command to configure the table and row selection methods to select IP address/host address for P-CSCF discovery.

Example

The following command specifies **table 1** with **round-robin** algorithm to select the rows with IP address for P-CSCF discovery.

```
p-cscf discovery table 1 algorithm round-robin
```

p-cscf table

This command adds/appends rows with primary and/or secondary IPv4/IPv6 addresses to a P-CSCF discovery table with precedence for P-CSCF discovery.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

In releases prior to 18:

p-cscf table { 1 | 2 } row-precedence *precedence_value* **{ address** *ipv4_address* **| ipv6-address** *ipv6_address* **} [secondary { address** *ipv4_address* **| ipv6-address** *ipv6_address* **}] [weight** *value* **]**
no p-cscf table { 1 | 2 } row-precedence *precedence_value*

In 18 and later releases:

p-cscf table { 1 | 2 } row-precedence *precedence_value* **{ ipv4-address** *ipv4_address* **[ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address* **] } [secondary { ipv4-address** *ipv4_address* **[ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address* **] } [weight** *value* **]**
no p-cscf table { 1 | 2 } row-precedence *precedence_value*

no

Removes/deletes configured row with precedence in specified table for P-CSCF discovery address.

{ 1 | 2 }

Specifies which P-CSCF table is to be used to add/append the primary and secondary P-CSCF addresses. Two tables can be configured for P-CSCF discovery address.

row-precedence *precedence_value*

This keyword adds/appends the row with the specified row-precedence to the P-CSCF address table.

In 8.1 and later releases, *precedence_value* must be an integer from 1 through 128, and a maximum of 128 rows can be added to a table.

In release 8.0, *precedence_value* must be an integer from 1 through 100, and a maximum of 16 rows can be added to a table.

secondary

Specifies the secondary IPv4/IPv6 address to be entered in P-CSCF table rows.

address *ip_address*

Specifies the primary and/or secondary IPv4 address for P-CSCF discovery table. This keyword, if used with **secondary** keyword, specifies the secondary IPv4 address.

Important This keyword is available only in releases prior to 18. In 18 and later releases, this keyword is concealed and is replaced with **ipv4-address** to support the PDN type v4v6 request for VoLTE setup.

ip_address must be entered in IPv4 dotted-decimal notation.

ipv4-address *ipv4_address*

Specifies the primary and/or secondary IPv4 address for P-CSCF discovery table. This keyword, if used with **secondary** keyword, specifies the secondary IPv4 address.

ipv4_address must be entered in IPv4 dotted-decimal notation.

Important This keyword is available in 18 and later releases to support the PDN type v4v6 request for VoLTE setup.

In releases prior to 18, the P-CSCF configuration accepts only one primary and one secondary P-CSCF IP addresses – both IPv4 and IPv6 addresses per row in the P-CSCF address table. Two IP addresses are not sufficient enough to address the requirement with PDN type v4v6 request for VoLTE setup. Hence, in release 18, the P-CSCF configuration has been enhanced to allow users to configure a maximum of two IPv4 addresses (primary/secondary) and two IPv6 addresses (primary/secondary) per P-CSCF table row.

ipv6-address *ipv6_address*

Specifies the primary and/or secondary IPv6 address for P-CSCF discovery table. This keyword, if used with **secondary** keyword, specifies the secondary IPv6 address.

ipv6_address must be entered in IPv6 colon-separated-hexadecimal notation.

In releases prior to 18, the P-CSCF configuration accepts only one primary and one secondary P-CSCF IP addresses – both IPv4 and IPv6 addresses per row in the P-CSCF address table. Two IP addresses are not sufficient enough to address the requirement with PDN type v4v6 request for VoLTE setup. Hence, in release 18, the P-CSCF configuration has been enhanced to allow users to configure a maximum of two IPv4 addresses (primary/secondary) and two IPv6 addresses (primary/secondary) per P-CSCF table row.

weight *value*

This keyword designates weight to a row-precedence relative to other row-precedences configured under this table, Default value is 1. *value* must be an integer from 1 through 10.

Within the IMS Authorization configuration, the P-CSCF address is selected based on round robin fashion. This feature allows the customer to perform P-CSCF selection based on weight factor.

With this CLI option, the user can configure and add weight (in the scale of 1 to 10) to each row, and the rows are selected based on weighted round-robin. That is, the row with higher weight parameter is selected more number of times than the row with less number of weights.

Usage Guidelines

Use this command to add rows with primary and/or secondary IP addresses for P-CSCF discovery. The row is added with the specified row-precedence.

In releases prior to 17.0, IMSA will select the servers if requested server address type and selected row server-address type are the same. Otherwise, it will return NULL. In 17.0 and later releases, P-CSCF server selection algorithm is modified such that the P-CSCF server selection happens based on UE-requested server-type.

The operator can add/remove rows to the table that is not currently selected by the **diameter host-select table** command in Policy Control Configuration Mode.

In releases prior to 18, the look-up and forwarding of P-CSCF server information from P-CSCF table to the session manager were performed by IMS Authorization (IMSA) server only during the setup. In 18 and later releases, whenever IMSA receives a Modify Bearer request with P-CSCF Address request indication, then the list of P-CSCF IP addresses are sent to the session manager through Modify Bearer Response message.

This look-up and forwarding functionality works even when the call is with the Local Policy (LP) engine during the time the Modify Bearer Request is triggered.

Example

The following command adds a row in **table 2** with primary IP address *209.165.200.228*, secondary IP address as *209.165.200.232*, and row-precedence value as *20* for P-CSCF discovery.

```
p-cscf table 2 row-precedence 20 address 209.165.200.228 secondary
209.165.200.232
```

policy-control

This command enters the Policy Control Configuration mode for Diameter Policy Control Application (DPCA) to configure Diameter authorization and policy control parameter for IMS authorization.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] policy-control
```

no

Disables the pre-configured policy control parameters for IMS authorization in this IMS authorization service.

use-pcscf-config-from-imsa

Specifies to use the P-CSCF configuration from IMSA in Local Policy.

Usage Guidelines

Use this command to enter the Policy Control Configuration Mode to configure the policy control parameters for Diameter authorization and charging policy in IMS Authorization Service.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-imsa-dpca)#

Policy Control configuration commands are described in the *Policy Control Configuration Mode Commands* chapter.

qos-update-timeout

This command is obsolete in release 11.0 and later releases. This command sets the Quality of Service update timeout for a subscriber in IMS authorization service.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-imsa-service)#

Syntax Description

qos-update-timeout *timeout_duration*
no qos-update-timeout

no

Disables the pre-configured QoS update timeout parameter in this IMS authorization service.

timeout_duration

Specifies the duration of timeout in seconds as an integer from 0 through 3600.

Default: 60

Usage Guidelines

Use this command to set the maximum time to wait for a subscriber to initiate the update QoS procedure in IMS authorization service.

Example

The following command sets the QoS update timeout to *90* seconds.

qos-update-timeout 90

reauth-trigger

This command specifies the trigger events to initiate re-authorization for a subscriber in IMS authorization service.

Important This command now moved to Policy Control Config mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default ] reauth-trigger { all | { an-gw-change | bearer-loss |
bearer-recovery | plmn-change | policy-failure | qos-change | rat-change
 | sgsn-change | tft-change | tft-delete } + }
```

Default

Sets the pre-configured Re-authorization trigger to default value.

all

Sets the IMS authorization service to initiate re-authorization process for a subscriber on all events listed in this command.

an-gw-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber whose access network gateway changed.

bearer-loss

Sets the IMS authorization service to initiate re-authorization process for a subscriber on loss of bearer or service.

bearer-recovery

Sets the IMS authorization service to initiate re-authorization process for a subscriber when a bearer or service recovered after loss of bearer or service.

default-bearer-qos-change

Sets the IMS authorization service to initiate re-authorization process when QoS is changed and DEFAULT_EPS_BEARER_QOS_CHANGE event triggered for the default EPS bearer context of a subscriber in LTE network.

plmn-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Public Land Mobile Network (PLMN) of subscriber.

policy-failure

Sets the IMS authorization service to initiate re-authorization process for a subscriber on failure of credit and charging policy for subscriber.

qos-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Quality of Service level/rating of subscriber.

rat-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Radio Access Type (RAT) of subscriber node.

sgsn-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in SGSN for subscriber node.

tft-change

Sets the IMS authorization service to initiate re-authorization process for a subscriber on change in Traffic Flow Template (TFT) of subscriber session.

tft-delete

Sets the IMS authorization service to initiate re-authorization process for a subscriber when Traffic Flow Template (TFT) of subscriber session is deleted by a system administrative user.

Usage Guidelines

Use this command to set the triggers to initiate QoS re-authorization process for a subscriber in IMS authorization service.

Example

The following command sets the re-authorization trigger to **bearer-loss**, so that re-authorization of subscriber session is initiated on loss of bearer.

```
reauth-trigger bearer-loss
```

signaling-flag

This command specifies whether a request for a PDP context dedicated to signaling (for IMS sessions) should be granted or denied.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
signaling-flag { deny | permit }
default signaling-flag
```

default

Sets the signaling flag to default mode of deny.

deny

Denies the request for a signaling PDP context for IMS session and keeps signaling co-existed with other traffic on PDP contexts. Default: Enabled

permit

Permits the request for a signaling PDP context for IMS session and a separate signaling context activated. Default: Disabled

Usage Guidelines

Use this command to allow or deny the activation of a dedicated PDP context for signaling. The user equipment (UE) may indicate that the PDP context should be dedicated for IP multimedia (IM) signaling by setting the IP Multimedia Core Network (IM-CN) signaling flag in the Protocol Configuration Options (PCO).

The **deny** option causes the system to inform the UE that the PDP context will not be dedicated for IM signaling and signaling will co-exist with other traffic on PDP context.

The **permit** option is used to activate the signaling context for signal traffic and the other traffic uses other PDP context for traffic with the following destinations:

- Towards the DHCP and DNS servers for the IMS domain
- Towards the P-CSCF(s)

The UE is not trusted to follow these restrictions, and the system monitors and restricts the traffic from the dedicated PDP context. The **signaling-flow class-map** command is used to configure the restrictions.

Example

The following command denies the request for a signaling PDP context for IMS session.

```
default signaling-flag
```

signaling-flow

This command specifies the packet filters and policy servers for bandwidth control and singling context enforcement that define the traffic that is allowed through the dedicated signaling context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
signaling-flow permit server-address ipv4/ipv6_address [ server-port { port_num
 | range start_port to end_port } ] [ description STRING ]
no signaling-flow permit server-address ipv4/ipv6_address [ server-port {
port_num | range start_port to end_port } ]
```

no

Disables the signaling flow option configured with this command.

server-address *ipv4/ipv6_address*

The server address refers to the destination IP address in uplink packets, and the source IP address in downlink packets.

ipv4/ipv6_address is an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation and can be used with a subnet mask.

A maximum of 16 signaling server addresses can be configured per IMS Authorization service.

server-port { *port_num* | range *start_port* to *end_port* }

Specifies the TCP/UDP port number(s) of the server to be used for communication.

port_num must be an integer from 1 through 65535.

range *start_port* **to** *end_port* provides the option to configure the range of ports on server for communication.

start_port must be an integer from 1 through 65535 but lesser than *end_port*, and *end_port* must be an integer from 1 through 65535 but greater than *start_port*.

description *STRING*

Specifies the customized description for configured signaling server as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Traffic that matches any instance of the signaling-flow command will be forwarded via the signaling PDP context. In addition, the policy server gives policy gates to use for the signaling PDP context.

Example

The following command sets the packet filter server address to *209.165.200.228* with port number *1234* for packet filtering.

```
signaling-flow server-address 209.165.200.228 server-port 1234
```

traffic-policy

This command specifies the action on packets which do not match any policy gates in the general purpose PDP context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context *context_name* **> ims-auth-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
traffic-policy general-pdp-context no-matching-gates direction { downlink
 | uplink } { forward | discard }
default traffic-policy general-pdp-context no-matching-gates direction {
 downlink | uplink }
```

default

Sets the default traffic policy for packets without any policy gate match in general purpose PDP context.

By default packets which do not have any matching policy gate are forwarded.

no-matching gates

Applies traffic policy for packets which do not match any policy gate.

direction { downlink | uplink }

Specifies the direction of traffic to apply this traffic policy in general PDP context.

downlink: Specifies the traffic from system to MN. Default is set to forward.

uplink: Specifies the traffic from MN to system. Default is set to forward.

forward

Forwards the packets which do not match any policy gates. Default: Enabled

discard

Discards the packets which do not match any policy gates. Default: Disabled

Usage Guidelines

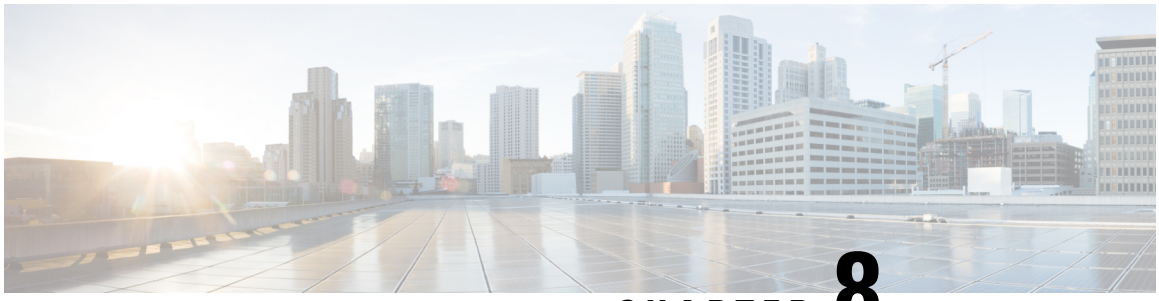
This command provides configuration on traffic policy applied on packets which are not matching any policy gate in general PDP context. Packets can either be forwarded or discarded on the basis of operator's configuration.

This command needs to be configured once for downlink and once for uplink separately.

Example

The following command discards uplink packets which do not match any policy gate in general purpose PDP context.

```
traffic-policy general-pdp-context no-matching-gates direction uplink
discard
```



CHAPTER 8

IMSI Group Configuration Mode Commands

The IMSI Group Configuration Mode provides commands to configure discrete list and range of International Mobile Subscriber Identity (IMSI) numbers.

Command Modes

Exec > Global Configuration > IMSI Group Configuration

configure > imsi-group *group_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-imsi-group)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

imsi

This command configures the discrete list of IMSI numbers.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > IMSI Group Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-imsi-group)#
```

Syntax Description

imsi mcc *mcc_value* **mnc** *mnc_value* **msin** *msin_value*
no imsi mcc *mcc_value* **mnc** *mnc_value* **msin** *msin_value*

no

Deletes the specified IMSI numbers.

mcc ***mcc_value***

Specifies the mobile country code (MCC) portion of the IMSI identifier. *mcc_value* is a three digit number between 0 and 999.

mnc ***mcc_value***

Specifies the mobile network code (MNC) portion of the IMSI identifier. *mnc_value* is a two or three digit number between 0 and 999.

msin ***msin_value***

Specifies the Mobile Subscriber Identification Number (MSIN) of the IMSI identifier. This keyword allows up to 500 MSINs to be configured per group. *value* is 9 or 10 digit MSIN.

Usage Guidelines

Use this command to specify the discrete list of IMSI numbers (Combination of discrete and range line is 20 per group).

Example

The following command configures the MCC as *334*, MNC as *456* and MSIN as *123456789*:

```
imsi mcc 334 mnc 456 msin 123456789
```

range

This command configures the range of IMSI numbers.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > IMSI Group Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-imsi-group)#
```

Syntax Description

range mcc *mcc_value* **mnc** *mnc_value* **msin first** *start_range* **last** *end_range*
no range mcc *mcc_value* **mnc** *mnc_value* **msin first** *start_range* **last** *end_range*

no

Deletes the specified IMSI numbers.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the IMSI identifier. *mcc_value* is a three digit number between 0 and 999.

mnc *mcc_value*

Specifies the mobile network code (MNC) portion of the IMSI identifier. *mnc_value* is a two or three digit number between 0 and 999.

msin first *start_range* last *end_range*

Specifies the Mobile Subscriber Identification Number (MSIN) prefix range. *start_range* and *end_range* are 9 or 10 digit MSIN numbers.

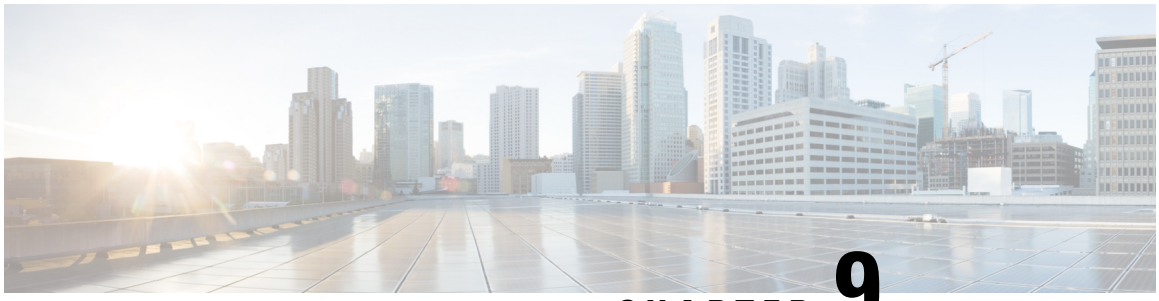
Usage Guidelines

Use this command to configure the IMSI range.

Example

The following command configures the MCC as *334*, MNC as *456* and MSIN range as *123456789* and *234567890*:

```
range mcc 334 mnc 456 msin first 123456789 last 234567890
```



CHAPTER 9

IMS Sh Service Configuration Mode Commands

PDIF to communicate with the HSS server. HSS server is used for MAC address validation in the IKEv2 exchanges to set up SAs and for storing part of the user profile.SCM to communicate with the HSS server. HSS server is used for retrieval and update of call feature parameters and call restriction data.

Command Modes The IMS Sh Interface Configuration Mode is used to configure various Diameter parameters in order for:

Exec > Global Configuration > Context Configuration > IMS Sh Interface Configuration

configure > context *context_name* **> ims-sh-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ims-sh-service)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

diameter

This command configures Diameter parameters.

Product PDIF

SCM

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > IMS Sh Interface Configuration

configure > **context** *context_name* > **ims-sh-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ims-sh-service)#
```

Syntax Description

```
diameter { dictionary { custom1 | standard | endpoint string }
default diameter { dictionary | endpoint }
no diameter endpoint
```

no

Removes previously configured endpoint.

default

Configures parameters to the default value.

dictionary

Specifies the dictionary to use.

- **custom1**: A custom dictionary
- **standard**: The standard dictionary

Important SCM uses only the standard dictionary.

endpoint *string*

Selects an endpoint to use in the configuration.

string must be the endpoint name, and must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage Guidelines

The Diameter endpoint contains information on the peer names and IP addresses and port, and the local IP address to use for Diameter.

You can have more than one Diameter endpoint configured on the chassis and the ims-sh-service needs to know which Diameter endpoint to use. This command is to select the appropriate Diameter endpoint, even if only one has been configured.

Example

The following example selects a diameter endpoint *diam1:*

```
diameter endpoint diam1
```

failure-handling

This command configures the action to take in the event of an HSS server request failure.

Product

PDIF

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Sh Interface Configuration

configure > context *context_name* **> ims-sh-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ims-sh-service)#
```

Syntax Description

`[ default ] failure-handling { profile-update-request | user-data-request } { { diameter-result-code` *`result_code`* **`[ to` *`result_code`* **`] } | timeout } action { continue | retry-and-terminate | terminate } } }`

default

Resets configuration for the specified keyword to the default setting.

profile-update-request

Configures failure-handling as a result of a profile update request error.

user-data-request

Configures failure-handling as a result of a user data request.

diameter-result-code *result_code* [to *result_code*]

The Result-Code data field contains a space representing errors. Diameter provides the following classes of errors, all identified by the thousands digit in the decimal notation:

- 3xxx (Protocol Errors)
- 4xxx (Transient Failures)
- 5xxx (Permanent Failure)

result_code specifies either a result code value (**diameter-result-code** *3001*) or a range of result code values (**diameter-result-code** *3000* **to** *9999*) to which the failure-handling applies.

action

Configures the action to take depending on the diameter-result-code:

- Continue the session
- Retry and then terminate
- Terminate the session

request-timeout action

Configures the action to take as a result of a request timeout error:

- Continue the session
- Retry and then terminate
- Terminate the session

Usage Guidelines Configures all failure-handling parameters.

Example

The following command configures profile-update-request failure-handling using a result-code configuration with the terminate session option:

failure-handling profile-update-request diameter-result-code *3005* **to** *3600***action terminate**

request

Configures application request timeout.

Product PDIF

SCM

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > IMS Sh Interface Configuration

configure > context *context_name* **> ims-sh-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ims-sh-service)#`

Syntax Description

request timeout *secs*
[no | default] request timeout

no

Disables a configured timeout request.

default

Default: 300 seconds

Resets configuration to the default setting.

request timeout *secs*

Configures the request timeout in seconds.

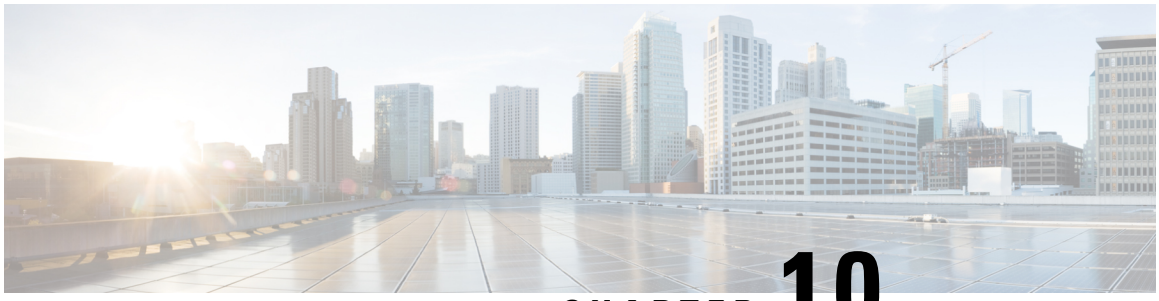
secs must be an integer from 1 through 300.

Usage Guidelines Specifies the session request timeout period in seconds after which the request is deemed to have failed.

Example

The following example configures the default timeout request of 300 seconds:

```
default request timeout
```



CHAPTER 10

IPMS Client Configuration Mode Commands

Important This is a license enabled external application support. For more information on this product, refer to the *IPMS Installation and Administration Guide*.

Command Modes

The IPMS Client Configuration Mode is used to enable the Intelligent Packet Monitoring System (IPMS) client service on an Access Gateway and to set basic service-wide options in a context.

Exec > Global Configuration > Context Configuration > IPMS Configuration

configure > context *context_name* **> ipms**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-ipms)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

export keys

Enables the encryption key export in specific key exchange events to IPMS server from IPMS-enabled AGW.

Important This is a license enabled customer specific command.

Product IPMS

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPMS Configuration

configure > context *context_name* **> ipms**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-ipms)#
```

Syntax Description

no

Removes the configured source IP address from this context for IPMS client communication with IPMS server.

ikev2

Enables the security association (SA) key export for Internet Key Exchange (IKEv2) protocol to IPMS server.

Usage Guidelines Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.

Example

The following command assigns the IP address *10.2.3.4* to the IPMS client service in context to communicate with IPMS server. This is the IP address allocated for IPMS client service on chassis.

```
source address 10.2.3.4
```

heartbeat

Configures the IPMS heartbeating between the IPMS-enabled AGW and the IPMS server.

Product IPMS

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPMS Configuration

configure > context *context_name* **> ipms**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-ipms)#
```

Syntax Description

```
heartbeat period dur [ permitted-failure no_of_failures ]
[ no | default ] heartbeat
```

default

Configures the heartbeat period and permitted number of failures to the default values of 10 seconds and 1 failure respectively.

no

Disables/removes the configured heartbeat period and permitted number of failures.

period *dur*

Specifies the periodicity (in seconds) between heartbeat messages as an integer from 1 through 3600. Default: 10

permitted-failure *no_of_failures*

Specifies the number of errors/failures allowed before declaring an IPMS server as dead/unreachable as an integer from 1 through 10. Default: 1

Usage Guidelines

Use this command to configure the heartbeat message periodicity and permissible failure of heartbeat message response before declaring an IPMS server as dead or unreachable. When an IPMS server is declared down an SNMP trap is sent.

Example

Following command configures the heartbeat message periodicity to *5* second and number of failures allowed as *3* to determine an IPMS server as dead.

```
heartbeat period 5 permitted-failure 3
```

server

Configures the IPMS server address and ports on which the IPMS client on an IPMS-enabled AGW communicates. This is the IP address and port range of the IPMS server.

Product

IPMS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPMS Configuration

configure > context *context_name* **> ipms**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-ipms)#
```

Syntax Description

server address *ip_address* [**seconary**] [**start-port** *start_port* [**end-port** *end_port*]][**secondary**]
no server address *ip_address*

no

Removes the configured IPMS server IP address and port range from this context.

address *ip_address*

Specifies the IP address of the IPMS server to which the IPMS client service communicates in IPv4 dotted-decimal notation.

A maximum of 4 IPMS severs can be configured with this command in one context.

[start-port *start_port*[end-port *end_port*]]

Default: 45001 source port

45005 end port

Specifies the range of UDP ports on which IPMS client communicates with the IPMS server.

start-port *start_port*: Specifies starting port number as an integer from 1 through 65535 that is less than *end_port*, if end-port is specified.

end-port *end_port*: Specifies is the end port number as an integer from 1 through 65535 that is more than *start_port*.

secondary

The secondary keyword is used to configure the specified server address as secondary IP address on the IPMS client interface.

Usage Guidelines

Use this command to configure/remove the IPMS servers. Up to 4 different IPMS servers can be configured with this command. UDP port number can also be configured with this command. IPMS client will search for this IP address to push the event and traffic logs.

Example

The following command configures IPMS server having IP address *209.165.201.4* in the IPMS client service export the event and traffic logs for intelligent packet monitoring functionality. It also specifies the UDP port range from *48000* to *48005* for communication.

```
server address 209.165.201.4 start-port 48000 end-port 48005
```

source

Configures the source address of the IPMS client in this context to communicate with the IPMS server. This is the IP address for IPMS client on the chassis.

Product

IPMS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPMS Configuration

configure > context *context_name* **> ipms**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-ipms)#
```

Syntax Description

source address *ip_address*

address *ip_address*

Specifies the IP address of the IPMS client on the AGW in this context. This is the address which is bound to the IPMS client service in this context.

ip_address is expressed in IPv4 dotted-decimal notation.

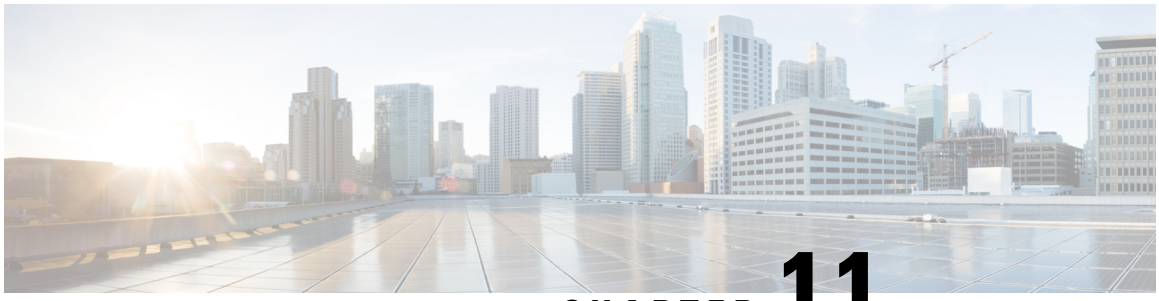
Usage Guidelines

Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.

Example

The following command assigns the IP address *209.165.201.4* to the IPMS client service in context to communicate with IPMS server. This is the IP address allocated for IPMS client service on chassis.

```
source address 209.165.201.4
```



CHAPTER 11

IPNE Endpoint Configuration Mode Commands

Command Modes

The IPNE Endpoint Configuration Mode provides the commands to configure the parameters for an IPNE Endpoint in an IPNE Service.

Exec > Global Configuration > Context Configuration > IPNE Service Configuration > IPNE Endpoint Configuration

configure > context *context_name* **> ipne-service** *ipne_service_name* **> ipne-endpoint**

Entering the above command sequence results in the following prompt:

```
[ context_name]host_name (config-ipne-endpoint)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

bind

This command binds the IPNE client socket to the IPNE endpoint.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPNE Service Configuration > IPNE Endpoint Configuration

configure > context *context_name* **> ipne-service** *ipne_service_name* **> ipne-endpoint**

Entering the above command sequence results in the following prompt:

```
[ context_name]host_name (config-ipne-endpoint)#
```

Syntax Description **`[ no ] bind { ipv4-address | ipv6-address }`** *ip_address*

no

When included as a command prefix, the system removes the bind address from the IPNE endpoint configuration.

ipv4-address | ipv6-address

Identifies whether the bind address uses IPv4 or IPv6 format.

ip_address

Enter either an IPv4 dotted-decimal address or an IPv6 colon-separated hexadecimal notation

Usage Guidelines The **bind** command defines the IP address of the IPNE client socket as the local address.

Example

Use a command similar to the following to bind the IPNE client socket to the IPNE endpoint.

```
bind ipv4-address 209.165.200.225
```

peer

Identifies the MINE server as a peer for the IPNE endpoint.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPNE Service Configuration > IPNE Endpoint Configuration

configure > context *context_name* **> ipne-service** *ipne_service_name* **> ipne-endpoint**

Entering the above command sequence results in the following prompt:

```
[ context_name]host_name (config-ipne-endpoint)#
```

Syntax Description **`[ no ] peer { ipv4-address | ipv6-address }`** *ip_address*

no

Removes the peer address from the IPNE endpoint configuration.

ipv4-address | ipv6-address

Informs the system of the format of the peer address.

ip_address

Enter either an IPv4 dotted-decimal address or an IPv6 colon-separated hexadecimal notation.

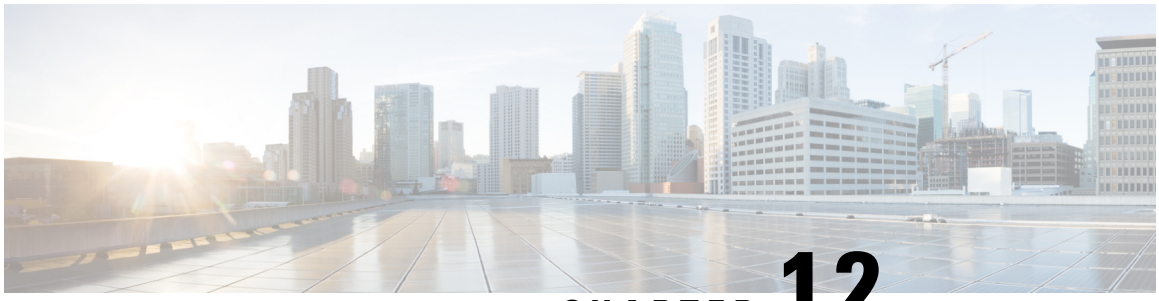
Usage Guidelines

Use the **peer** command to configure a MINE server IP address as the peer for the IPNE endpoint.

Example

Enter an IPv4 address for the MINE server:

```
peer ipv4-address 209.165.201.1
```



CHAPTER 12

IPNE Service Configuration Mode Commands

Command Modes

The IPNE Service Configuration Mode is used to configure and manage the IPNE Service.

Exec > Global Configuration > Context Configuration > IPNE Service Configuration

configure > context *context_name* **> ipne-service** *ipne_service_name*

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

ipne-endpoint

Creates and configures an IPNE endpoint and enters the IPNE endpoint configuration mode. An IPNE endpoint is a combination of a local IPP address, a peer address and, optionally, a port.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPNE Service Configuration

configure > context *context_name* **> ipne-service** *ipne_service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] ipne-endpoint`

no

Causes the system to delete the IPNE endpoint configuration from the IPNE service configuration.

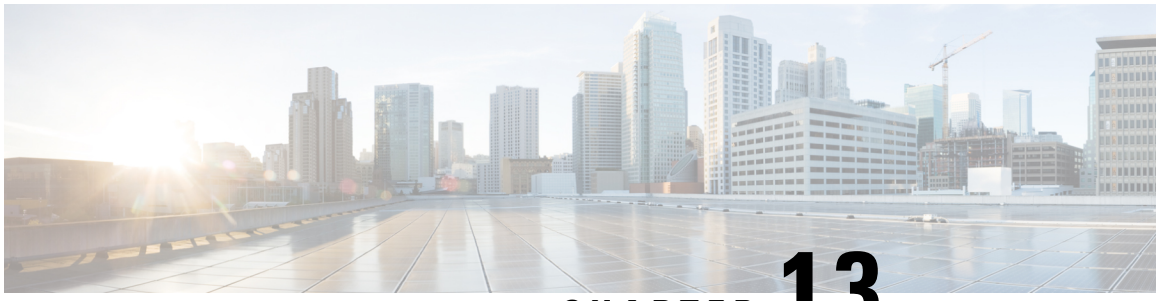
Usage Guidelines

Use this command to create an IPNE endpoint and to enter the IPNE endpoint sub-configuration mode.

Example

Use the following command to access commands to configure the IPNE endpoint:

```
ipne-endpoint
```



CHAPTER 13

IP Pool Management Policy Configuration Mode Commands

Command Modes

The IP Pool Management Policy Configuration Mode is used to configure and manage the IP Pool management policies.

Exec > Global Configuration > Context Configuration > IP Pool Management Policy Configuration

configure > context *context_name* **> ip-pool-mgmt-policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[ context_name]host_name (config-ip-pool-mgmt-policy)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

user-plane-group

Use this command to associate IP Pools to UP Group.

Product

CUPS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IP Pool Management Policy Configuration

configure > context *context_name* **> ip-pool-mgmt-policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[ context_name]host_name (config-ip-pool-mgmt-policy)#
```

Syntax Description

user-plane-group *group_name* **{ ip-address-pool-name** *ipv4_pool_name* **| ipv6-address-pool-name** *ipv6_pool_name* **}**

group_name

Specifies the UP Group name and must be a string of size 1-31.

ipv4_pool_name

Specifies the IPv4 address pool name and must be a string of size 1-31.

ipv6_pool_name

Specifies the IPv6 address pool name and must be a string of size 1-31.

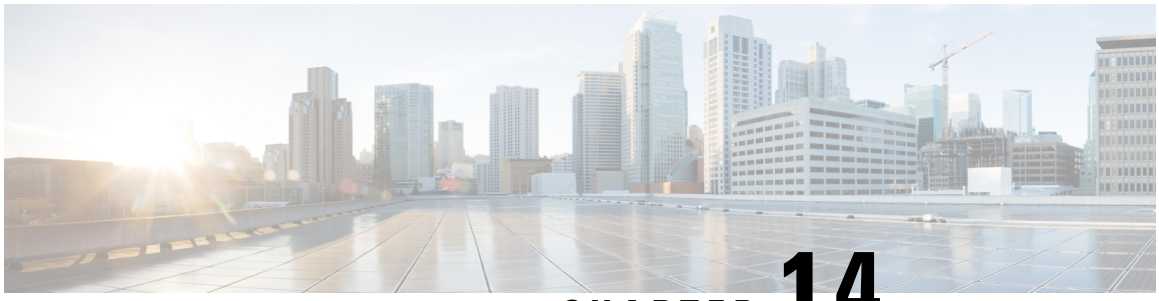
Usage Guidelines

Use this command to configure multiple UP Groups, and UP Group-specific IP pools for an APN.

Example

The following command adds *v4-pool* and *v6-pool* to a UP Group named *G1*:

```
user-plane-group G1 ip-address-pool-name v4-pool ipv6-address-pool-name
v6-pool
```



CHAPTER 14

IPSec Transform Set Configuration Mode Commands

The IPSec Transform Set Configuration Mode is used to configure IPSec security parameters. There are two core protocols, the Authentication Header (AH) and Encapsulating Security Payload (ESP). AH may be considered redundant as ESP can provide the same authentication services that AH does.

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-context-vrf)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

encryption

Configures the appropriate IPSec ESP encryption algorithm and encryption key length. AES-CBC-128 is the default.

Product

ePDG

PDIF

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

encryption { 3des-cbc | aes-128-gcm-128 | aes-cbc-128 | aes-128-gcm-64 | aes-128-gcm-96 | aes-256-gcm-128 | aes-256-gcm-64 | aes-256-gcm-96 | aes-cbc-256 | des-cbc | null }
default encryption

3des-cbc

Data Encryption Standard Cipher Block Chaining encryption applied to the message three times using three different cypher keys (triple DES).

aes-128-gcm-128

IKEv2 Child Security Association IPsec ESP Algorithm is AES-GCM-128 with 128-bit ICV (Integrity Check Value). HMAC algorithm with this encryption algorithm should be None.

aes-128-gcm-64

IKEv2 Child SA (Security Association) IPsec ESP Algorithm is AES-GCM-128 with 64-bit ICV. HMAC algorithm with this encryption algorithm should be None.

aes-128-gcm-96

IKEv2 Child SA IPsec ESP Algorithm to be AES-GCM-128 with 96-bit ICV. HMAC algorithm with this encryption algorithm should be None.

aes-256-gcm-128

IKEv2 Child SA IPsec ESP Algorithm is AES-GCM-256 with 128-bit ICV. HMAC algorithm with this encryption algorithm should be None.

aes-256-gcm-64

IKEv2 Child SA IPsec ESP Algorithm is AES-GCM-256 with 64-bit ICV. HMAC algorithm with this encryption algorithm should be None.

aes-256-gcm-96

IKEv2 Child SA IPsec ESP Algorithm is AES-GCM-256 with 96-bit ICV. HMAC algorithm with this encryption algorithm should be None.

aes-cbc-128

Advanced Encryption Standard Cipher Block Chaining with a key length of 128 bits. This is the default setting for this command.

aes-cbc-256

Advanced Encryption Standard Cipher Block Chaining with a key length of 256 bits.

des-cbc

Data Encryption Standard Cipher Block Chaining. Encryption using a 56-bit key size. Relatively insecure.

null

The NULL encryption algorithm represents the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.

default

Sets the default IPSec ESP algorithm to AES-CBC-128.

Usage Guidelines

AES-GCM (Advanced Encryption Standard-Galois Counter Mode) is a block cipher mode of operation that uses universal hashing over a binary Galois field to provide authenticated encryption (RFC 5288). It uses mechanisms that are supported by a well-understood theoretical foundation, and its security follows from a single reasonable assumption about the security of the block cipher. StarOS supports these AEAD (Authenticated Encryption with Associated Data) algorithms for improved IPsec performance when using OpenSSL to process ESP packets.

Important The AEAD algorithms are only supported on virtualized platforms. They are not supported on ASR 5x00 hardware.

In cipher block cryptography, the plaintext is broken into blocks usually of 64 or 128 bits in length. In cipher block chaining (CBC) each encrypted block is chained into the next block of plaintext to be encrypted. A randomly generated vector is applied to the first block of plaintext in lieu of an encrypted block. CBC provides confidentiality, but not message integrity.

Because RFC 4307 calls for interoperability between IPSec and IKEv2, the IKEv2 confidentiality algorithms must be the same as those configured for IPsec in order for there to be an acceptable match during the IKE message exchange. In IKEv2, there is no NULL option.

Example

The following command configures the encryption to be the default aes-cbc-128:

```
default encryption
```

esn

Enables support for the use of 64-bit Extended Sequence Numbers (ESNs) in ikev2 Encapsulating Security Payload (ESP) and Authentication Header (AH) packets. The ESN transform is included in an ikev2 proposal used in the negotiation of IKE SAs as part of the IKE_SA_INIT exchange.

Product

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

esn

Usage Guidelines

Use this command to enable support for the use of 64-bit ESNs for ikev2. The ESN transform is included in an ikev2 proposal used in the negotiation of IKE SAs as part of the IKE_SA_INIT exchange.

The ESN transform has the following meaning:

- A proposal containing one ESN transform with value 0 means "do not use extended sequence numbers".
- A proposal containing one ESN transform with value 1 means "use extended sequence numbers".
- A proposal containing two ESN transforms with values 0 and 1 means "I support both normal and extended sequence numbers, you choose". This case is only allowed in requests; the response will contain only one ESN transform.

In most cases, the exchange initiator will include either the first or third alternative in its SA payload. The second alternative is rarely useful for the initiator: it means that using normal sequence numbers is not acceptable (so if the responder does not support ESNs, the exchange will fail with NO_PROPOSAL_CHOSEN.

Enabling the **esn** command is the equivalent of sending ESN Transform = 0 and 1; support both 32-bit and 64-bit sequence numbers. If the **esn** command is not enabled, support only 32-bit sequence numbers (default behavior).

Including the ESN transform is mandatory when creating ESP or AH SAs.

For additional information, see the *IPSec Reference*.

Important ESN is only supported on ASR 5500 and ASR 9000 Virtualized Services Modules (VSMs). It is not supported on the ASR 5000 or VPC-SI.

Example

The following command enables support for 64-bit ESNs in ikev2 ESP and AH packets:

esn

group

Configures the appropriate key exchange cryptographic strength and activate Perfect Forward Secrecy by applying a Diffie-Hellman group.

Product

ePDG

PDIF

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-context-vrf)#`

Syntax Description

```
group { 1 | 2 | 5 | 14 | none }
default group
```

default group

Configures the default crypto strength to be **none** and disables Perfect Forward Secrecy.

1

Configures crypto strength at the Group 1 level. Lowest security.

2

Configures crypto strength at the Group 2 level. Medium security.

5

Configures crypto strength at the Group 5 level. Higher security.

14

Configures crypto strength at the Group 14 level. Highest security.

none

Applies no group and disables Perfect Forward Secrecy. This is the default.

default

Sets the default Diffie-Hellman group algorithm to none. This also deactivates PFS.

Usage Guidelines

Diffie-Hellman groups are used to determine the length of the base prime numbers used during the key exchange process. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group upon which the prime numbers are based.

Group 1 provides 768 bits of keying strength, Group 2 provides 1024 bits, Group 5 provides 1536 bits and Group14 2048 bits. Selecting a group automatically activates Perfect Forward Secrecy. The default value is none, which disables PFS

Example

This command configures security at Group 2 and activates PFS:

```
group 2
```

hmac

Configures the IPsec ESP integrity algorithm using a Hash-based Message Authentication Code (HMAC).

Product

ePDG

PDIF

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

```
hmac { aes-xcbc-96 | md5-96 | none| null | sha1-96 | sha2-256-128 |
sha2-384-192 | sha2-512-256 }
default hmac
```

default hmac

Sets the default IPSec hashing algorithm to SHA1-96.

aes-xcbc-96

AES-XCBC-96 uses a 128-bit secret key and produces a 128-bit authenticator value.

md5-96

MD5-96 uses a 128-bit secret key and produces a 128-bit authenticator value.

none

Sets the IPsec hashing algorithm to none. Used with OpenSSL AEAD algorithms.

null

Configures the HMAC value to be null. The NULL encryption algorithm represents the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.

sha1-96

SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value. This is the default setting for this command.

sha2-256-128

HMAC-SHA-256 uses a 256-bit secret key and produces a 128-bit authenticator value.

sha2-384-192

HMAC-SHA-384 uses a 384-bit secret key and produces a 192-bit authenticator value.

sha2-512-256

HMAC-SHA-512 uses a 512-bit secret key and produces a 256-bit authenticator value.

Usage Guidelines

HMAC is an encryption technique used by IPsec to make sure that a message has not been altered.

A keyed-Hash-based Message Authentication Code (HMAC), is a type of message authentication code that is calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity. A hash takes a message of any size and transforms it into a message of a fixed size: the authenticator value. This is truncated to 96 bits and transmitted. The authenticator value is reconstituted by the receiver and the first 96 bits are compared for a 100 percent match.

Example

The following command configures the default HMAC value (SHA1-96):

```
default hmac
```

mode

Configures the security of IP datagrams based on header placement. Tunnel mode applies security to a completely encapsulated IP datagram, while Transport does not. Default is Tunnel mode.

Product

ePDG

PDIF

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context *context_name* **> ipsec transform-set** *set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

```
mode { transport | tunnel }
default mode
```

transport

In Transport mode, the IPSec header is applied only over the IP payload, not over the IP header in front of it. The AH and/or ESP headers appear between the original IP header and the IP payload, as follows:

Original IP header, IPSec headers (AH and/or ESP), IP payload (including transport header).

Transport mode is used for host-to-host communications and is generally unsuited to PDIF traffic.

tunnel

In Tunnel mode, the original IP header is left intact, so a complete IP datagram is encapsulated, forming a virtual tunnel between IPSec-capable devices. The IP datagram is passed to IPSec, where a new IP header is created ahead of the AH and/or ESP IPSec headers, as follows:

New IP header, IPSec headers (AH and/or ESP), old IP header, IP payload.

Tunnel mode is used for network-to-network communications (secure tunnels between routers) or host-to-network and host-to-host communications over the Internet.

This is the default setting for this command.

default mode

Sets the default IPSec Mode to Tunnel.

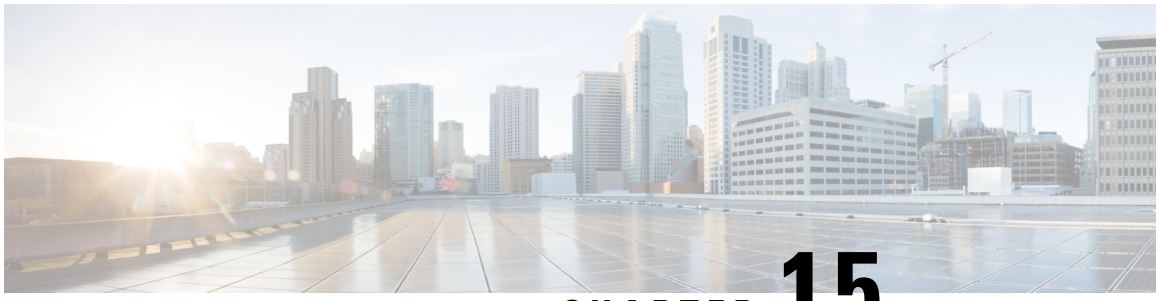
Usage Guidelines

IPSec modes are closely related to the function of the two core protocols, the Authentication Header (AH) and Encapsulating Security Payload (ESP). Both of these protocols provide protection by adding to a datagram a header (and possibly other fields) containing security information. The choice of mode does not affect the method by which each generates its header, but rather, changes what specific parts of the IP datagram are protected and how the headers are arranged to accomplish this.

Example

The following command configures the default Tunnel mode:

```
default mode
```



CHAPTER 15

IPSG RADIUS Snoop Configuration Mode Commands

The IP Services Gateway (IPSG) RADIUS Snoop Configuration Mode is used to create and configure IPSG services within the current context. The IPSG RADIUS Snoop Mode configures the system to inspect RADIUS accounting requests on the way to the RADIUS accounting server and extract user information.

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-snoop**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ipsg-service-radius-snoop)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

bind

This command allows you to configure the service to accept data on any interface configured in the context. Optionally, you can also configure the system to limit the number of sessions processed by this service.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-snoop**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-snoop)#
```

Syntax Description

bind [max-subscribers *max_sessions* **]**
no bind

no

If previously configured, deletes the binding configuration for the service.

max-subscribers *max_sessions*

Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

In StarOS 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.

In StarOS 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.

Usage Guidelines

Use this command to initiate the service and begin accepting data on any interface configured in the context.

Example

The following command prepares the system to receive subscriber sessions on any interface in the context and limits the sessions to *10000*:

```
bind max-subscribers 10000
```

connection authorization

This command allows you to configure the RADIUS authorization password that must be matched by the RADIUS accounting requests "snooped" by this service.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-snoop**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-snoop)#
```

Syntax Description

connection authorization [encrypted] password *password*
no connection authorization

no

Deletes the RADIUS connection authorization configuration from the current IPSG RADIUS snoop service.

[encrypted] password *password*

- **encrypted**: Specifies that the received RADIUS authorization password is encrypted.
- **password** *password*: Specifies the password that must be matched by incoming RADIUS accounting requests.

  In StarOS 12.2 and later releases, *password* with encryption must be an alphanumeric string of 1 through 132 characters, and without encryption an alphanumeric string of 1 through 63 characters.

  In StarOS 12.1 and earlier releases, *password* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

RADIUS accounting requests being examined by the IPSG RADIUS snoop service are destined for a RADIUS Accounting Server. Since the "snoop" service does not terminate user authentication, the user password is unknown.

Use this command to configure the authorization password that the RADIUS accounting requests must match in order for the service to examine and extract user information.

Example

The following command sets the RADIUS authorization password that must be matched by the RADIUS accounting requests "snooped" by this service. The password is encrypted, and the password used in this example is "*secret*".

```
connection authorization encrypted password secret
```

profile

This command allows you to configure the service to use APN or subscriber profile.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-snoop**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-snoop)#
```

Syntax Description

```
profile { APN | subscriber }
default profile
```

default

Configures this command with its default setting.

APN

Specifies the service to support APN configuration required to enable Gx support.

subscriber

Specifies the service to support subscriber profile lookup.

Usage Guidelines

Use this command to set the service to support APN profiles (supporting Gx through the enabling of **ims-auth-service**) or for basic subscriber profile lookup.

Example

The following command specifies to use the subscriber profile:

```
profile subscriber
```

radius

This command allows you to specify the RADIUS accounting servers where accounting requests are sent after being "inspected" by this service.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-snoop**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-snoop)#
```

Syntax Description

radius { accounting server *ipv4_address* **[port** *port_number* **| source-context** *context_name* **] | dictionary { 3gpp2 | 3gpp2-835 | custom***XX* **| standard | starent | starent-835 | starent-vsa1 | starent-vsa1-835 } }**
[no] radius accounting server *ipv4_address* **[port** *port_number* **| source-context** *context_name* **]**

no

Removes the RADIUS accounting server identifier from this service.

radius accounting server *ipv4_address*

Specifies the IP address of a RADIUS accounting server where accounting requests are sent after being "snooped" by this service in IPv4 dotted-decimal notation.

Up to 16 addresses can be configured.

port *port_number*

Specifies the port number of the RADIUS Accounting Server where accounting requests are sent after being "snooped" by this service.

port_number must be an integer from 1 through 65535.

Default: 1813

source-context *context_name*

Specifies the source context where RADIUS accounting requests are received.

context_name must be an alphanumeric string of 1 through 79 characters.

If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

dictionary { 3gpp2 | 3gpp2-835 | custom *XX* | standard | starent | starent-835 | starent-vsa1 | starent-vsa1-835 }

Specifies what dictionary to use. The possible values are described in the following table:

Dictionary	Description
3gpp	This dictionary consists not only of all of the attributes in the standard dictionary, but a of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, but a of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, but a of the attributes specified in IS-835.
custom*XX*	These are customized dictionaries. For information on custom dictionaries, please cont Cisco account representative. *XX* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RF
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorp additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionar master-set of all of the attributes in all of the dictionaries supported by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and inco additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionar master-set of all of the attributes in all of the -835 dictionaries supported by the systen
starent-vsa1	This dictionary consists not only of the 3gpp2 dictionary, but also includes Starent Net vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-by VSA Type field in order to support certain RADIUS applications. The one-byte limit a support for only 256 VSAs (0–255). This is the default dictionary.
starent-vsa1-835	This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent N vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-by VSA Type field in order to support certain RADIUS applications. The one-byte limit a support for only 256 VSAs (0–255). This is the default dictionary.

Usage Guidelines Use this command to specify the RADIUS Accounting Servers where accounting requests are sent after being snooped by this service.

Example

The following command specifies the IP address (*209.165.200.228*) of a RADIUS Accounting Server whose accounting requests are to be "snooped", and the source context (*aaa_ingress*) where the requests are received on the system:

```
radius accounting server 209.165.200.228 source-context aaa_ingress
```

sess-replacement

This command allows you to enable/disable session replacement.

Important This command is not supported in this release. The Session Replacement feature is under development for future use.

Product IPSG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

configure > **context** *context_name* > **ipsg-service** *service_name* **mode radius-snoop**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-snoop)#
```

Syntax Description

```
sess-replacement { with-diff-acct-sess-id | with-diff-ip | with-diff-key
 }
{ default | no } sess-replacement
```

default

Configures this command with its default setting.

Default: Disabled.

no

If previously configured, deletes the configuration.

with-diff-acct-sess-id

Specifies to replace current session when a new session request comes with same IP address and same user name/IMSI but different accounting session ID.

with-diff-ip

Specifies to replace current session when a new session request comes with same user name/IMSI but different IP address.

with-diff-key

Specifies to replace current session when a new session request comes with same IP address but different user name/IMSI.

Usage Guidelines

Use this command to enable/disable session replacement. By default, session replacement is disabled.

Example

The following command enables session replacement specifying to replace the current session when a new session request comes with same user name/IMSI but different IP address:

```
sess-replacement with-diff-ip
```

setup-timeout

This command allows you to configure the timeout value for IPSG session setup attempts.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-snoop**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-snoop)#
```

Syntax Description

setup-timeout *setup_timeout*
default setup-timeout

setup_timeout

Specifies the period of time (in seconds) the IPSG session setup is allowed to continue before the setup attempt is terminated.

setup_timeout must be an integer from 1 through 1000000.

Default: 60

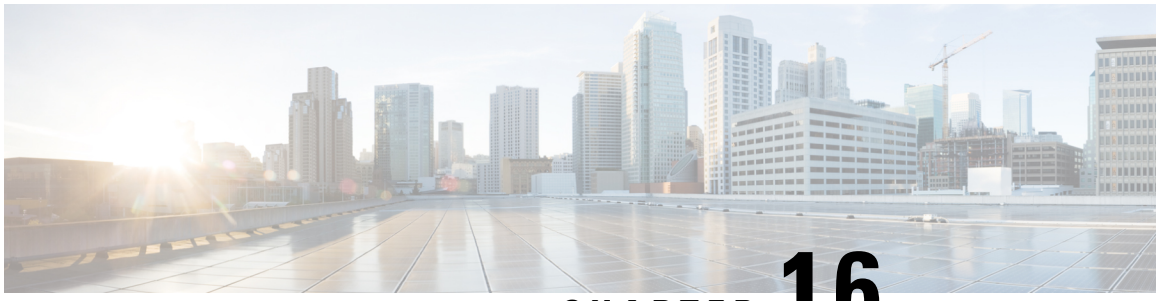
Usage Guidelines

Use this command to prevent IPSG session setup attempts from continuing without termination.

Example

The following command configures the session setup timeout setting to *20* seconds:

```
setup-timeout 20
```



CHAPTER 16

IPSG RADIUS Server Configuration Mode Commands

The IP Services Gateway (IPSG) RADIUS Server Configuration Mode is used to create and configure IPSG RADIUS Server/eWAG services in the current context. This mode enables configuring the system to receive RADIUS accounting requests as if it is a RADIUS accounting server, and reply after accessing those requests for subscriber information.

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

accounting-context

This command allows you to specify the GTPP accounting context.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

accounting-context *context_name*
no accounting-context

no

If previously configured, removes the accounting context configuration.

context_name

Specifies name of the GTPP accounting context.

context_name must be an alphanumeric string of 1 through 79 characters in length.

Usage Guidelines

Use this command to specify the GTPP accounting context.

Example

The following command specifies to use the GTPP accounting context *context12* for the eWAG service:

accounting-context *context12*

associate sgtp-service

This command allows you to associate an SGTP service with the current eWAG service.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

associate sgtp-service *sgtp_service_name* **[context** *sgtp_context_name* **]**
no associate sgtp-service

no

If previously configured, removes the service association from the configuration.

sgtp-service *sgtp_service_name*

Specifies name of the SGTP service to associate with this service.

sgtp_service_name must be the name of an SGTP service, and must be an alphanumeric string of 1 through 63 characters in length.

context *sgtp_context_name*

Specifies name of the context in which the SGTP service is configured.

sgtp_context_name must be the name of the context, and must be an alphanumeric string of 1 through 63 characters in length.

If a context is not specified, the current context is used.

Usage Guidelines

Use this command to associate an SGTP service with the IPSG service. This enables the GTP functionality for eWAG supporting GTP-C (GTP Control Plane) messaging and GTP-U (GTP User Data Plane) messaging between eWAG and GGSN over the Gn' interface.

Important Any change to this configuration will result in restart of the eWAG service.

Example

The following command associates an SGTP service named *service1*, configured in the context named *context2*, with the IPSG service:

associate sgtp-service *service1* **context** *context2*

bind

This command allows you to bind the current IPSG/eWAG service to a logical AAA interface, and specify the number of subscriber sessions allowed.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

```
bind accounting-proxy address ipv4_address [ max-subscribers max_sessions |
port port_number | source-context source_context ]
bind address ipv4_address [ disconnect-message [ src-port source_port_number ]
 | max-subscribers max_sessions | port port_number | source-context source_context
 ]+
bind authentication-proxy address ipv4_address [ acct-port port_number |
auth-port port_number | max-subscribers max_sessions | source-context
source_context ]
no bind
```

no

If previously configured, removes the binding for the service.

bind accounting-proxy address *ipv4_address* [max-subscribers *max_sessions* | port *port_number* | source-context *source_context*]

- **accounting-proxy address** *ipv4_address* : Specifies the IP address of the interface where accounting proxy requests are received by this service in IPv4 dotted-decimal notation.
- **max-subscribers** *max_sessions*: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

  In StarOS 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.

  In StarOS 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.
- **port** *port_number*: Specifies the port number of the interface where accounting requests are received by this service.

  port_number must be an integer from 1 through 65535.

  Default: 1813
- **source-context** *source_context*: Specifies the source context where RADIUS accounting requests are received.

  source_context must be an alphanumeric string of 1 through 79 characters.

  This keyword should be configured if the source of the RADIUS requests is in a different context than the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

bind address *ipv4_address* [disconnect-message [src-port *source_port_number*] | max-subscribers *max_sessions* | port *port_number* | source-context *source_context*]+

- **address** *ipv4_address* : Specifies the IP address of the interface where accounting requests are received by this service in IPv4 dotted-decimal notation.
- **disconnect-message [src-port** *source_port_number* **]**: Specifies to send RADIUS disconnect message to the configured RADIUS accounting client in call failure scenarios.

  src-port *source_port_number*: Specifies the port number to which the disconnect message must be sent.

  source_port_number must be an integer from 1 through 65535.
- **max-subscribers** *max_sessions*: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

  In StarOS 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.

  In StarOS 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.
- **port** *port_number*: Specifies the port number of the interface where accounting requests are received by this service.

  port_number must be an integer from 1 through 65535.

  Default: 1813
- **source-context** *source_context*: Specifies the source context where RADIUS accounting requests are received.

  source_context must be an alphanumeric string of 1 through 79 characters.

  This keyword should be configured if the source of the RADIUS requests is in a different context than the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

bind authentication-proxy address *ipv4_address* [acct-port *port_number* | auth-port *port_number* | max-subscribers *max_sessions* | source-context *source_context*]

- **authentication-proxy address** *ipv4_address* : Specifies the IP address of the interface where authentication proxy requests are received by this service in IPv4 dotted-decimal notation.

Important Enabling authentication proxy also enables accounting proxy.

- **acct-port** *port_number*: Specifies the port number of the interface where accounting proxy requests are received by this service.

  port_number must be an integer from 0 through 65535.

  Default: 1813
- **auth-port** *port_number*: Specifies the port number of the interface where authentication proxy requests are received by this service.

  port_number must be an integer from 0 through 65535.

  Default: 1812

- **max-subscribers** *max_sessions*: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

  In StarOS 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.

  In StarOS 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.

- **source-context** *source_context*: Specifies the source context where RADIUS accounting requests are received.

  source_context must be an alphanumeric string of 1 through 79 characters.

  This keyword should be configured if the source of the RADIUS requests is in a different context then the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

- +: Indicates that more than one of the preceding options may be specified in a single command.

Usage Guidelines

Use this command to bind the IPSG RADIUS Server/eWAG service to a logical AAA interface and specify the number of allowed subscriber sessions. If the AAA interface is not located in this context, configure the **source-context** parameter.

Use the accounting and authentication proxy settings to enable RADIUS proxy server functionality on the IPSG. These commands are used when the NAS providing the RADIUS request messages is incapable of sending them to two separate devices. The IPSG in RADIUS Server mode proxies the RADIUS request and response messages while performing the user identification task in order to provide services to the session.

Example

The following command binds the service to a AAA interface with and IP address of *209.165.200.228* located in the source context named *aaa_ingress*:

```
bind address 209.165.200.228 source-context aaa_ingress
```

connection authorization

This command allows you to configure the RADIUS authorization password that must be matched by the RADIUS accounting requests received by the current IPSG service.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

```
connection authorization [ encrypted ] password password
no connection authorization
```

no

Deletes the RADIUS authorization from the current IPSG RADIUS Server service.

[encrypted] password *password*

- **encrypted**: Specifies that the RADIUS authorization password is encrypted.
- **password** *password*: Specifies the password that must be matched by incoming RADIUS accounting requests.

  In StarOS 12.2 and later releases, *password* with encryption must be an alphanumeric string of 1 through 132 characters, and without encryption an alphanumeric string of 1 through 63 characters.

  In StarOS 12.1 and earlier releases, *password* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

The IPSG RADIUS server service does not terminate RADIUS user authentication so the user password is unknown.

Use this command to configure the authorization password that the RADIUS accounting requests must match in order for the service to examine and extract user information.

Example

The following command sets the RADIUS authorization password that must be matched by the RADIUS accounting requests sent to this service. The password is encrypted, and the password used in this example is "*secret*".

```
connection authorization encrypted password secret
```

gtp max-contexts-per-imsi

This command allows you to configure multiple primary contexts having the same IMSI number.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

gtp max-contexts-per-imsi *max_value* **min-nsapi** *min_nsapi_value*
default gtp max-contexts-per-imsi

default

Configures this command to disable use of multiple primary contexts. Only one PDP context per user is allowed.

max-contexts-per-imsi: 1

min-nsapi: 15

max-contexts-per-imsi *max_value*

Specifies the limit for the maximum number of contexts per IMSI.

max_value must be an integer from 1 through 11.

min-nsapi *min_nsapi_value*

Specifies the range of NSAPI values to be assigned to different PDP context of the same subscriber.

*min_nsapi_value*must be an integer from 5 through 15.

Usage Guidelines

Use this command to configure the maximum number of contexts per IMSI, and the range of NSAPI values to be assigned to different PDP context.

Example

The following command configures the maximum contexts per IMSI to 5 and specify the range of values NSAPI valie to 7.

```
gtp max-contexts-per-imsi 5 min-nsapi 7
```

gtp peer-ip-address

This command allows you to configure GGSN IP address under the eWAG service.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

```
gtp peer-ip-address ipv4_address
no gtp peer-ip-address
```

no

Deletes the configuration, if previously configured.

gtp peer-ip-address *ipv4_address*

Specifies the GGSN IP address.

ipv4_address

Usage Guidelines

Use this command to configure the GGSN IP address under the eWAG service.

This command replaces the hidden mode command **[no] ggsn-ip-address** *ipv4_address*

Example

The following command configures the GGSN IP address *209.165.200.228* under the current eWAG service.

```
gtp peer-ip-address 209.165.200.228
```

ip

This command enables you to configure IP parameters for the current eWAG service.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

```
ip { gnp-qos-dscp | qos-dscp } qci { { { 1 | 2 | 3 | 4 | 9 } | { 5 | 6 |
 7 | 8 } allocation-retention-priority { 1 | 2 | 3 } } { af11 | af12 |
af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be
 | ef | pt } } +
default ip { gnp-qos-dscp | qos-dscp }
no ip { gnp-qos-dscp | qos-dscp } qci { { 1 | 2 | 3 | 4 | 9 } | { 5 | 6
| 7 | 8 } allocation-retention-priority { 1 | 2 | 3 } } +
```

default

Configures this command, for specified option, with default setting for all QoS Class Identifier (QCI) values.

- QCI-based DSCP map:
  - **qci 1**: **ef**
  - **qci 2**: **ef**
  - **qci 3**: **af11**
  - **qci 4**: **af11**
  - **qci 5**: **ef**
  - **qci 6**: **ef**
  - **qci 7**: **af21**
  - **qci 8**: **af21**

- **qci 9**: **be**

- ARP-based DSCP map for interactive class:
  - **qci 5 allocation-retention-priority 1**: **ef**
  - **qci 5 allocation-retention-priority 2**: **ef**
  - **qci 5 allocation-retention-priority 3**: **ef**
  - **qci 6 allocation-retention-priority 1**: **ef**
  - **qci 6 allocation-retention-priority 2**: **ef**
  - **qci 6 allocation-retention-priority 3**: **ef**
  - **qci 7 allocation-retention-priority 1**: **af21**
  - **qci 7 allocation-retention-priority 2**: **af21**
  - **qci 7 allocation-retention-priority 3**: **af21**
  - **qci 8 allocation-retention-priority 1**: **af21**
  - **qci 8 allocation-retention-priority 2**: **af21**
  - **qci 8 allocation-retention-priority 3**: **af21**

no

Resets configured value for specified QCI with its default setting.

gnp-qos-dscp

Specifies, for uplink direction, the DiffServ Code Point marking to be used for sending packets of a particular 3GPP QoS class.

qos-dscp

Specifies, for downlink direction, the DiffServ Code Point marking to be used for sending packets of a particular 3GPP QoS class.

qci { 1 | 2 | 3 | 4 | 9 }

Specifies the QCI attribute of QoS.

- **1**: QCI 1 attribute of QoS
- **2**: QCI 2 attribute of QoS
- **3**: QCI 3 attribute of QoS
- **4**: QCI 4 attribute of QoS
- **9**: QCI 9 attribute of QoS

qci { 5 | 6 | 7 | 8 } allocation-retention-priority { 1 | 2 | 3 }

Specifies the QCI attribute of QoS with ARP.

- **5**: QCI 5 attribute of QoS
- **6**: QCI 6 attribute of QoS
- **7**: QCI 7 attribute of QoS
- **8**: QCI 8 attribute of QoS

allocation-retention-priority { 1 | 2 | 3 }: Specifies the ARP.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | pt

Specifies the Per-Hop Forwarding Behavior (PHB) to use.

- **af11**: Assured Forwarding 11 PHB
- **af12**: Assured Forwarding 12 PHB
- **af13**: Assured Forwarding 13 PHB
- **af21**: Assured Forwarding 21 PHB
- **af22**: Assured Forwarding 22 PHB
- **af23**: Assured Forwarding 23 PHB
- **af31**: Assured Forwarding 31 PHB
- **af32**: Assured Forwarding 32 PHB
- **af33**: Assured Forwarding 33 PHB
- **af41**: Assured Forwarding 41 PHB
- **af42**: Assured Forwarding 42 PHB
- **af43**: Assured Forwarding 43 PHB
- **be**: Best Effort Forwarding PHB
- **ef**: Expedited Forwarding PHB
- **pt**: Pass Through (do not modify the ToS)

Usage Guidelines

Use this command to configure IP parameters for the eWAG service.

Example

The following command specifies to configure the DiffServ Code Point marking to be used for sending packets specifying QCI as 1 and Assured Forwarding 11 PHB:

```
ip gnp-qos-dscp qci 1 af11
```

map ue-mac-to-imei

This command allows you to map the UE MAC received in the Calling-Station-Id RADIUS attribute to IMEIsV in order to forward it in the GTP CPC message to the GGSN.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ipsg-service-radius-server)#`

Syntax Description

`[ default | no ] map ue-mac-to-imei`

default

If previously configured, disables mapping of UE MAC address to IMEIsV IE of GTP message in order to forward it to GGSN.

Default: Mapping is disabled.

no

If previously configured, disables mapping of UE MAC address to IMEIsV IE of GTP message in order to forward it to GGSN.

Usage Guidelines

Use this command to enable or disable mapping of UE MAC address to IMEIsV IE of GTP message in order to forward it to GGSN.

overlapping-ip-address

This command allows you to enable or disable overlapping of IP addresses which enables multiple users to use the same IP address.

Product

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ipsg-service-radius-server)#`

Syntax Description

`[ default | no ] overlapping-ip-address`

default

If previously configured, disables IPSG support of overlapping IP addresses.

Using overlapping IP addresses is disabled by default.

no

If previously configured, disables IPSG support of overlapping IP addresses.

Usage Guidelines

Use this command to enable or disable overlapping IP addresses for subscribers on different networks that are independent of each other.

Example

The following command enables IPSG overlapping of IP addresses:

```
overlapping-ip-address
```

plmn id

This command allows you to configure Public Land Mobile Network (PLMN) identifier for the current eWAG service.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

```
plmn id mcc mcc_number mnc mnc_number
no plmn id
```

no

If previously configured, deletes the PLMN ID configuration.

mcc *mcc_number*

Specifies the mobile country code (MCC) part of the PLMN identifier for the eWAG service.

mcc_number must be a three-digit number ranging from 200 to 999.

mnc *mnc_number*

Specifies the mobile network code (MNC) part of the PLMN identifier for the eWAG service.

mnc_number must be a two- or three-digit number ranging from 00 to 999.

Usage Guidelines Use this command to configure the location-specific mobile network identifiers included in the Routing Area Identity (RAI) field of the PDP Create Request messages sent to the GGSN.

Important Any change to this configuration will result in restart of the eWAG service.

Example

The following command configures the PLMN identifier for the eWAG service as MCC *333* and MNC *99*:

```
plmn id mcc 333 mnc 99
```

profile

This command allows you to configure the IPSG/eWAG service to use APN or subscriber profile.

Important In release 14.0, eWAG service uses only the APN profile. In release 15.0, ReWAG uses the APN profile and DeWAG uses the subscriber profile. Whereas, the IPSG service uses both APN and subscriber profiles.

Product eWAG

IPSG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

```
profile { APN [ default-apn apn_name ] | subscriber }
default profile
```

default

Configures this command with its default setting.

Default: **APN**

APN

Specifies to use APN profile for the service.

default-apn *apn_name*

Important This option is supported only for the eWAG service.

Specifies the default APN to be used for the eWAG service.

apn_name must be the name of an APN, it must be an alphanumeric string of 1 through 62 characters in length, and can consist only of the alphabetic characters (A–Z and a–z), digits (0–9), dot (.), and the hyphen (-).

subscriber

Important This option is supported only for the IPSG RADIUS Server service, and in release 15.0 for DeWAG service. For the DeWAG service, this command must be configured with the **subscriber** option. This is because DeWAG will operate based on subscriber template profile selection only for connecting users. If the APN profile selection is configured, the DeWAG service will not be started.

Specifies to use subscriber profile for the service.

Usage Guidelines

Use this command to set the service to support APN profiles (supporting Gx through the enabling of **ims-auth-service**) or for basic subscriber profile lookup.

For the DeWAG service, this command must be configured with the **subscriber** option. This is because DeWAG will operate based on subscriber template profile selection only for connecting users. If the APN profile selection is configured, the DeWAG service will not be started.

Example

The following command specifies to use the subscriber profile:

```
profile subscriber
```

radius accounting

This command allows you to specify the IP address and shared secret of the RADIUS accounting client from which RADIUS accounting requests are received. The RADIUS client can be either the access gateway or the RADIUS accounting server depending on which device is sending accounting requests.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

radius accounting { client { *ipv4_address* | *ipv4_address/mask* } [encrypted] key *key* [acct-onoff [aaa-context *aaa_context_name*] [aaa-group *aaa_server_group_name*] [clear-sessions] +] [dictionary *dictionary*] [disconnect-message [release-on-acct-stop *acct_stop_wait_timeout*] [dest-port *destination_port_number*] + | interim create-new-call | validate-client-ip }
no radius accounting { client { *ipv4_address* | *ipv4_address/mask* } | interim create-new-call | validate-client-ip }
default radius accounting { interim create-new-call | validate-client-ip }

no

If previously configured, removes the specified configuration.

ipv4_address* | *ipv4_address/mask

Specifies the IP address, and optionally subnet mask of the RADIUS client from which RADIUS accounting requests are received.

ipv4_address/*ipv4_address/mask* must be in IPv4 dotted-decimal notation.

A maximum of 16 IP addresses can be configured.

[encrypted] key *key*

- **encrypted**: Specifies that the shared key between the RADIUS client and this service is encrypted.
- **key** *key*: Specifies the shared key between the RADIUS client and this service.

  In StarOS 12.2 and later releases, *key* with encryption must be an alphanumeric string of 1 through 236 characters, and without encryption an alphanumeric string of 1 through 127 characters. Note that *key* is case sensitive.

  In StarOS 12.1 and earlier releases, *key* must be an alphanumeric string of 1 through 127 characters and is case sensitive.

acct-onoff [aaa-context *aaa_context_name*] [aaa-group *aaa_server_group_name*] [clear-sessions] +

Important In release 12.3 and earlier releases, this option is applicable only to the IPSG Proxy Mode.

Important In release 14.0 and later releases, this option is applicable to the IPSG Proxy and Server Modes.

Specifies to proxy accounting On/Off messages to AAA server.

- **aaa-context** *aaa_context_name*: Specifies the context to find AAA server groups. If not specified, by default, the AAA context will be the source context.

  aaa_context_name must be the name of a AAA context, and must be an alphanumeric string of 1 through 79 characters.

- **aaa-group** *aaa_server_group_name*: Specifies the AAA server group. If not specified, by default, the AAA server group will be *default*.

  aaa_server_group_name must be the name of AAA server group, and must be an alphanumeric string of 1 through 63 characters.

- **clear-sessions**: Specifies to clear eWAG or IPSG sessions on receiving accounting On/Off messages.
- **+**: Indicates that more than one of the preceding options may be specified in a single command.

dictionary *dictionary*

Specifies the dictionary to use.

Important In this release, eWAG supports only the **starent-vsa1** dictionary.

dictionary can be one of the following.

Dictionary	Description
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, all of the attributes specified in IS-835.
custom*X*	These are customized dictionaries. For information on custom dictionaries, please your Cisco account representative. *X* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, a 2869.
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type This dictionary is the master-set of all of the attributes in all of the dictionaries su by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary incorporates additional Starent Networks VSAs by using a two-byte VSA Type This dictionary is the master-set of all of the attributes in all of the -835 dictiona supported by the system.
starent-vsa1	This dictionary consists not only of the 3GPP2 dictionary, but also includes Star Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary a one-byte wide VSA Type field in order to support certain RADIUS applicatio one-byte limit allows support for only 256 VSAs (0–255). This is the default dic **Important** In StarOS 12.0 and later releases, no new attributes can be added to the **starent-** dictionary. If there are new attributes to be added, you can only add them to the dictionary. For more information, please contact your Cisco account representat

Dictionary	Description
starent-vsa1-835	This dictionary consists not only of the 3GPP2-835 dictionary, but also includes Sta Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary sup a one-byte wide VSA Type field in order to support certain RADIUS applications. T one-byte limit allows support for only 256 VSAs (0–255). This is the default diction

Important For information on the specific dictionary to use for your deployment contact your Cisco account representative.

disconnect-message [release-on-acct-stop *acct_stop_wait_timeout*] [dest-port *destination_port_number*]

Specifies to send RADIUS disconnect message to the configured RADIUS accounting client in call failure scenarios.

- **release-on-acct-stop** *acct_stop_wait_timeout*: Specifies to wait for the accounting stop request after sending the Packet of Disconnect (PoD) to the client for the specified time. This keyword is disabled by default.

  acct_stop_wait_timeout must be an integer from 10 through 300 seconds. This indicates the time to wait to clear the call in case IPSG does not receive any accounting stop for the subscriber after sending the PoD.

  This keyword is configured on a per RADIUS accounting client basis and not for the entire service.

- **dest-port** *destination_port_number*: Specifies the port number to which the disconnect message must be sent.

  destination_port_number must be an integer from 1 through 65535.

interim create-new-call

Important This option does not apply to the IPSG Proxy Mode.

Specifies to create a new session upon receipt of a RADIUS interim message.

Default: Disabled

validate-client-ip

Specifies to enable the ipsgmgr to validate RADIUS accounting messages from different configured RADIUS client IP address, and forward requests to the session manager.

Default: The RADIUS client IPs are validated.

Usage Guidelines

Use this command to configure the communication parameters for the RADIUS client from which RADIUS accounting requests are received.

Example

The following command configures the service to communicate with a RADIUS client with an IP address of *209.165.200.228* and an encrypted shared secret of *key1234*:

```
radius accounting client 209.165.200.228 encrypted key key1234
```

radius dictionary

This command allows you to specify the RADIUS dictionary for the current IPSG/eWAG service.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

radius dictionary *dictionary_name*
default radius dictionary

default

Specifies to use the default dictionary.

Default: **starent-vsa1**

dictionary *dictionary_name*

Specifies the dictionary to use.

Important In 15.0 and later releases, for DeWAG use the **starent** dictionary.

dictionary_name must be one of the following.

Dictionary	Description
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, all of the attributes specified in IS-835.

Dictionary	Description
custom*XX*	These are customized dictionaries. For information on custom dictionaries, please co your Cisco account representative. *XX* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and 2869.
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type fiel This dictionary is the master-set of all of the attributes in all of the dictionaries suppo by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary an incorporates additional Starent Networks VSAs by using a two-byte VSA Type fiel This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.
starent-vsa1	This dictionary consists not only of the 3GPP2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary sup a one-byte wide VSA Type field in order to support certain RADIUS applications. T one-byte limit allows support for only 256 VSAs (0–255). This is the default dictio
starent-vsa1-835	This dictionary consists not only of the 3GPP2-835 dictionary, but also includes Sta Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary sup a one-byte wide VSA Type field in order to support certain RADIUS applications. T one-byte limit allows support for only 256 VSAs (0–255). This is the default dictio

Important For information on the specific dictionary to use for your deployment contact your Cisco account representative.

Usage Guidelines Use this command to specify the RADIUS dictionary to use for the IPSG RADIUS Server/eWAG service.

Example

The following command specifies to use the *custom10* RADIUS dictionary:

```
radius dictionary custom10
```

respond-to-non-existing-session

Configures the IPSG service to respond to Radius Accounting-Stop messages even if a session does not exist.

Product IPSG

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ipsg-service-radius-server)#`

Syntax Description

[default | no] respond-to-non-existing-session

default

Configures this command with its default setting.

Default: Disabled. IPSG service drops packets containing the Radius Accounting-Stop message if the session does not exist.

no

If previously enabled, disables the configuration.

Usage Guidelines

Use this command to enable/disable the IPSG service to respond to Radius Accounting-Stop messages with a Radius Accounting-Response message for non-existing sessions.

sess-replacement

This command allows you to enable/disable the Session Replacement feature for eWAG and IPSG services.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ipsg-service-radius-server)#`

Syntax Description

```
sess-replacement { with-diff-acct-sess-id | with-diff-ip | with-diff-key
 [ with-diff-acct-sess-id ] }
{ default | no } sess-replacement
```

default

Configures this command with its default setting.

Default: Disabled.

no

If previously configured, deletes the configuration.

with-diff-acct-sess-id

Specifies to replace current session when a new session request comes with same IP address and same user name/IMSI but different accounting session ID.

with-diff-ip

Specifies to replace current session when a new session request comes with same user name/IMSI but different IP address.

with-diff-key [with-diff-acct-sess-id]

Specifies to replace current session when a new session request comes with same IP address but different user name/IMSI.

For IPSG, you can also use a combination of replacement options of different key and different account session ID.

Usage Guidelines

Use this command to enable/disable the Session Replacement feature. By default, the Session Replacement feature is disabled.

Example

The following command enables session replacement specifying to replace the current session when a new session request comes with same user name/IMSI but different IP address:

```
sess-replacement with-diff-ip
```

setup-timeout

This command allows you to configure a timeout for session setup attempts for the current IPSG/eWAG service.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

setup-timeout *setup_timeout_seconds*
default setup-timeout

default

Configures this command with its default setting.

Default: 60 seconds

setup_timeout_seconds

Specifies the time period, in seconds, for which a session setup attempt is allowed to continue before being terminated.

setup_timeout_seconds must be an integer from 1 through 1000000.

Usage Guidelines

Use this command to configure a timeout for IPSG/eWAG session setup attempts.

Example

The following command configures the timeout for session setup attempts to *30* seconds:

```
setup-timeout 30
```

w-apn

This command allows you to configure the W-APNs that can be connected through DeWAG, and the default-gateway IP addresses to be used by the UEs for connecting to the W-APN network.

Product

eWAG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context *context_name* **> ipsg-service** *service_name* **mode radius-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

Syntax Description

w-apn *apn_name* **default-gw** *ipv4/ipv6_address/maskbits* **+**
no w-apn *apn_name*

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 (-).

This value is compared against the subscribed APN returned by the AAA server or locally configured APN in the subscriber-template configuration to find the default-gateway IP address to be used in DHCP signaling packets.

default-gw *ipv4/ipv6_address/maskbits*

Specifies the IP address of the default gateway to be used by UE for W-APN access.

You can configure a maximum of four default gateways per W-APN. Multiple default-gateways are possible as the APN can have different pools of different subnet with different default-gateway IP addresses.

ipv4/ipv6_address/maskbits must be an IPv4/IPv6 address and subnet-mask, for example 192.168.1.1/24.

This value should be in the same subnet as that of UE allocated IP address from GGSN for the W-APN. GGSN does not supply subnet-mask along with IP address. Therefore, the identification of whether GGSN-allocated IP address is in same subnet or not is done with the help of configured "/maskbits". This default-gateway value is sent to the UE as default-gateway IP address using "Router" option in DHCP-OFFER message. The maskbits is sent to the UE as subnet-mask using the "Subnet Mask" option in DHCP-OFFER message.

Usage Guidelines

Use this command to configure the list of W-APN names that can be connected through DeWAG and the default-gateway IP addresses to be used by UE for connecting to the W-APN network. During DHCP signaling the configured default-gateway value will be notified to UE as the router. This command also configures the subnet-mask to be used for the respective default-gateway IP address in order to find the network prefix of the default-gateway.

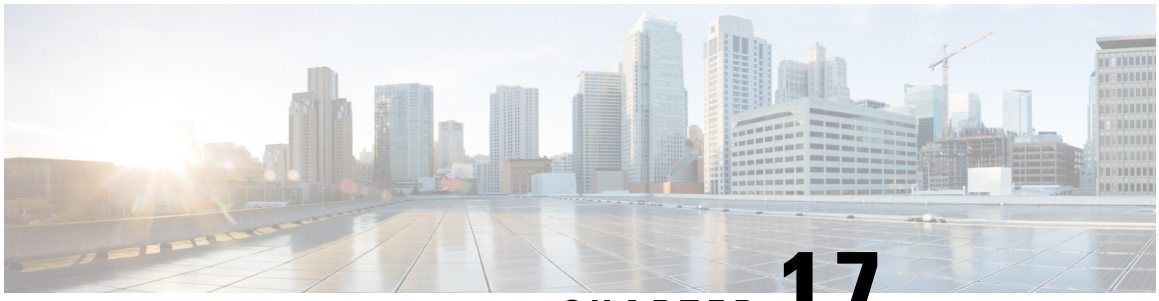
Note that DeWAG will be acting as 'default-gateway' for the UE in its connected network.

Important This command can be configured a maximum of four times to configure four different APNs and the corresponding default-gateways.

Example

The following command configures an APN named *apn123* with the default gateway IP address and mask *209.165.201.0/27*:

```
w-apn apn123 default-gw 209.165.201.0/27
```



CHAPTER 17

IPSP Configuration Mode Commands

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

Command Modes

The IPSP Configuration Mode is used to configure properties for the IP Pool Sharing Protocol (IPSP). System-based HA services use IPSP during an offline-software upgrade to avoid the assignment of duplicate IP addresses to sessions while allowing them to maintain the same address, and to preserve network capacity

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration > IP Pool Sharing Protocol Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast > pool-share-protocol { primary** *ip_address* **| secondary** *ip_address* **}**

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

dead-interval

Configures the retry time to connect to the remote system for the IP Pool Sharing Protocol.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration > IP Pool Sharing Protocol Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast > pool-share-protocol { primary** *ip_address* **| secondary** *ip_address* **}**

Syntax Description

dead-interval *seconds*
[no | default] dead-interval

no

Disables the dead interval. On loss of connectivity to the remote system, no retries are attempted and the remote system is marked dead immediately on failure.

default

Resets the dead interval to the default of 3600 seconds.

seconds

Default: 3600 seconds

The amount of time in seconds to wait before retrying the remote system. *seconds* must be an integer from 25 through 259200.

Usage Guidelines

Use this command to set the amount of time to wait before retrying to connect with the remote system for the IP pool sharing protocol.

Example

Use the following command to set the interval to 180 seconds (3 minutes):

dead-interval 180

reserved-free-percentage

This command is used to set the amount of free addresses reserved for use on the primary HA.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration > IP Pool Sharing Protocol Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast > pool-share-protocol { primary** *ip_address* **| secondary** *ip_address* **}**

Syntax Description

reserved-free-percentage *value*
default reserved-free-percentage

value

Default: 100

value specifies the percentage of free addresses reserved for the use on the primary HA for IP pool sharing during upgrade. It must be an integer from 0 through 100.

Usage Guidelines

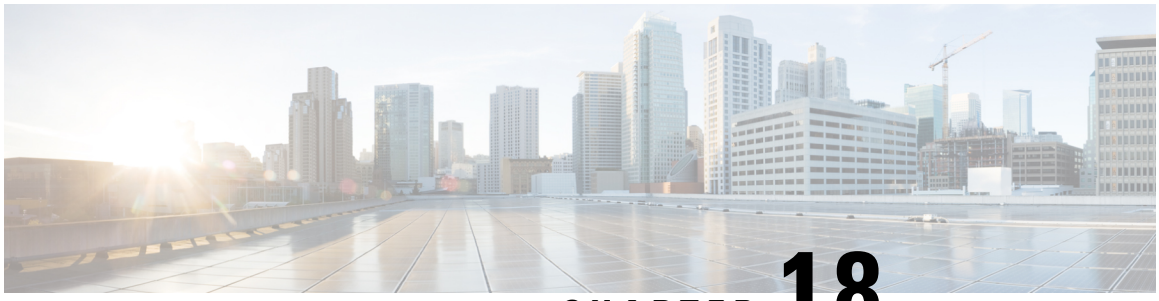
This command is used with **pool-sharing-protocol active mode** on the primary HA. Before using this command, **pool-sharing-protocol** in the Ethernet Interface Configuration Mode must be configured.

For more information, refer to the *Ethernet Interface Configuration Mode Commands* chapter in this guide.

Example

To reserve 40 percent of free addresses in primary HA for IP pool sharing, enter the following command:

```
reserved-free-percentage 40
```



CHAPTER 18

IPv6 ACL Configuration Mode Commands

The IPv6 Access Control List Configuration Mode is used to create and manage IPv6 access privileges.

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

deny/permit (by source IP address masking)

Used to filter subscriber sessions based on the IPv6 address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

{ deny | permit } [log] *source_address source_wildcard*
after { deny | permit } [log] *source_address source_wildcard*
before { deny | permit } [log] *source_address source_wildcard*
no { deny | permit } [log] *source_address source_wildcard*

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.

- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

Usage Guidelines Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rules as it does not require a rule for each source and destination pair.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Example

The following command defines two rules with the second logging filtered packets:

```
permit 2001:4A2B::1f3F
deny log 2001:4A2B::1f3F
```

The following sets the insertion point to before the first rule defined above:

```
before permit 2001:4A2B::1f3F
```

The following command sets the insertion point after the second rule defined above:

```
after deny log 2001:4A2B::1f3F
```

The following deletes the first rule defined above:

```
no permit 2001:4A2B::1f3F
```

deny/permit (any)

Used to filter subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
{ deny | permit } [ log ] any
after { deny | permit } [ log ] any
before { deny | permit } [ log ] any
no { deny | permit } [ log ] any
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

any

Indicates all packets will match the filter regardless of source and/or destination.

Usage Guidelines

Define a catch all rule to place at the end of the list of rules.

Important It is suggested that any rule which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines two rules with the second logging filtered packets:

```
permit any
deny log any
```

The following sets the insertion point to before the first rule defined above:

```
before permit any
```

The following command sets the insertion point after the second rule defined above:

```
after deny log any
```

The following deletes the first rule defined above:

```
no permit any
```

deny/permit (by host IP address)

Used to filter subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
{ deny | permit } [ log ] host source_host_address
after { deny | permit } [ log ] host source_host_address
before { deny | permit } [ log ] host source_host_address
no { deny | permit } [ log ] host source_host_address
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

Usage Guidelines

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines two rules with the second logging filtered packets:

```
permit host 2001:4A2B::1f3F
deny log host 2001:4A2B::1f3F
```

The following sets the insertion point to before the first rule defined above:

```
before permit host 2001:4A2B::1f3F
```

The following command sets the insertion point after the second rule defined above:

```
after deny log host 2001:4A2B::1f3F
```

The following deletes the first rule defined above:

```
no permit host 2001:4A2B::1f3F
```

deny/permit (by source ICMP packets)

Used to filter subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

{ deny | permit } [log] icmp { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [*icmp_type* [*icmp_code*]]

after { deny | permit } [log] icmp { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [*icmp_type* [*icmp_code*]]

before { deny | permit } [log] icmp { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [*icmp_type* [*icmp_code*]]

no { deny | permit } [log] icmp { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [*icmp_type* [*icmp_code*]]

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 hexadecimal-colon-separated notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 hexadecimal-colon-separated notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type is an integer from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type is an integer from 0 through 255.

Usage Guidelines

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk.

The IP filtering allows flexible controls for pairs of individual hosts or groups by IP masking which allows the filtering of entire subnets if necessary.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines two rules with the second logging filtered packets:

```
permit icmp host 2001:4A2B::1f3F4 any 168
deny log icmp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410 168 11
```

The following sets the insertion point to before the first rule defined above:

```
before permit icmp host 2001:4A2B::1f3F any 168
```

The following command sets the insertion point after the second rule defined above:

```
after deny log icmp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
168 11
```

The following deletes the first rule defined above:

```
no permit icmp host 2001:4A2B::1f3F any 168
```

deny/permit (by IP packets)

Used to filter subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > **context** *context_name* > **ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

{ deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol*num***]**

after { deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol*num*]
before { deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol*num*]
no { deny | permit } [log] ip { *source_address source_wildcard* | any | host *source_host_address* } { *dest_address dest_wildcard* | any | host *dest_host_address* } [fragment] [protocol*num*]

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: indicates the rule, when matched, drops the corresponding packets.
- **permit**: indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

fragment

Indicates packet filtering is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.

num can be any integer ranging from 0 to 255.

Usage Guidelines

Block IP packets when the source and destination are of interest.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines two rules with the second logging filtered packets:

```
permit ip host 2001:4A2B::1f3F any fragment
deny log ip 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
```

The following sets the insertion point to before the first rule defined above:

```
before permit ip host 2001:4A2B::1f3F any fragment
```

The following command sets the insertion point after the second rule defined above:

```
after deny log ip 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
```

The following deletes the first rule defined above:

```
no permit ip host  2001:4A2B::1f3F any fragment
```

deny/permit (by TCP/UDP packets)

Used to filter subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
{ deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard |
any | host source_host_address } [ eq source_port | gt source_port | lt source_port
 | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address
 } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ] }
after { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard
 | any | host source_host_address } [ eq source_port | gt source_port | lt source_port
 | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address
 } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ] }
before { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard
 | any | host source_host_address } [ eq source_port | gt source_port | lt source_port
 | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address
 } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ] }
no { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard
| any | host source_host_address } [ eq source_port | gt source_port | lt source_port
 | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address
 } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ] }
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

tcp | udp

Specifies the filter is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Filter applies to TPC packets.
- **udp**: Filter applies to UDP packets.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an integer from 0 through 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be configured to an integer from 0 through 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be configured to an integer from 0 through 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be configured to an integer from 0 through 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.

- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be configured to an integer from 0 through 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be configured to an integer from 0 through 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer from 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be configured to an integer from 0 through 65535.

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines four rules with the second and fourth rules logging filtered packets:

```
permit tcp host 2001:4A2B::1f3F any
deny log udp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
permit tcp host 2001:4A2B::1f3F gt 1023 any
```

The following sets the insertion point to before the first rule defined above:

```
before permit tcp host 2001:4A2B::1f3F any
```

The following command sets the insertion point after the second rule defined above:

```
after deny log udp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
```

The following deletes the third rule defined above:

```
no permit tcp host 2001:4A2B::1f3F gt 1023 any
```

readdress server

Alter the destination address and port number in TCP or UDP packet headers to redirect packets to a different server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

readdress server *redirect_address* **[port** *port_number* **] { tcp | udp } { {** *source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { {** *dest_address dest_wildcard* **any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dst_port* **] }**

after readdress server *redirect_address* **[port** *port_no* **] { tcp | udp } { {** *source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { {** *dest_address dest_wildcard* **any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dst_port* **] }**

before readdress server *redirect_address* **[port** *port_no* **] { tcp | udp } { {** *source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { {** *dest_address dest_wildcard* **any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dst_port* **] }**

no readdress server *redirect_address* **[port** *port_number* **] { tcp | udp } { {** *source_address source_wildcard* **| any | host** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **] } { {** *dest_address dest_wildcard* **any | host** *dest_host_address* **} [eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dst_port* **] }**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

redirect_address

The IP address to which the IP packets are redirected. TCP or UDP packet headers are rewritten to contain the new destination address. This must expressed in IPv6 colon-separated-hexadecimal notation.

port *port_number*

The number of the port at the redirect address where the packets are sent. TCP or UDP packet headers are rewritten to contain the new destination port number.

tcp | udp

Specifies the redirect is to be applied to the IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an integer from 0 through 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be configured to an integer from 0 through 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be configured to an integer from 0 through 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be configured to an integer from 0 through 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be configured to an integer from 0 through 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be configured to an integer from 0 through 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer from 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be configured to an integer from 0 through 65535.

Usage Guidelines

Use this command to define a rule that redirects packets to a different destination address. The TCP and UDP packet headers are modified with the new destination address and destination port.

Important

The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the server at *fe80::c0a8:a04*, UDP packets coming from any host with a destination of any host are matched:

```
readdress server fe80::c0a8:a04 udp any any
```

The following sets the insertion point to before the rule defined above:

```
before readdress server fe80::c0a8:a04 udp any any
```

The following deletes the rule defined above:

```
no readdress server fe80::c0a8:a04 udp any any
```

redirect context (by IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect context context_id [ log ] source_address source_wildcard
after redirect context context_id [ log ] source_address source_wildcard
before redirect context context_id [ log ] source_address source_wildcard
no redirect context context_id [ log ] source_address source_wildcard
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

Specifies the context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

Filters by the IP address(es) from which the packet originated. This option filters all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

Filters packets for a group of addresses specified in conjunction with the *source_address* option.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

Usage Guidelines Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23* and the source IP and wildcard of *2002::c6a2:1600* and *2002::c6a2:1600*:

```
redirect context 23 2002::c6a2:1600 2002::c6a2:1600
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 2002::c6a2:1600 2002::c6a2:1600
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 2002::c6a2:1600 2002::c6a2:1600
```

The following deletes the first rule defined above:

```
no redirect context 23 2002::c6a2:1600 2002::c6a2:1600
```

redirect context (any)

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > **context** *context_name* > **ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect context context_id [ log ] any
after redirect context context_id [ log ] any
```

before redirect context *context_id* **[log] any**
no redirect context *context_id* **[log] any**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage Guidelines

Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important It is suggested that any rule which is added to be a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23* and any source IP:

```
redirect context 23 any
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 any
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 any
```

The following deletes the first rule defined above:

```
no redirect context 23 any
```

redirect context (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > **context** *context_name* > **ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect context context_id [ log ] host source_ip_address
after redirect context context_id [ log ] host source_ip_address
before redirect context context_id [ log ] host source_ip_address
no redirect context context_id [ log ] host source_ip_address
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23* and a host IP address of *fe80::c0a8:c80b*:

```
redirect context 23 host fe80::c0a8:c80b
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 host fe80::c0a8:c80b
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 host fe80::c0a8:c80b
```

The following deletes the first rule defined above:

```
no redirect context 23 host fe80::c0a8:c80b
```

redirect context (by source ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**
after redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**
before redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**
no redirect context *context_id* **[log] icmp {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [** *icmp_type* **[** *icmp_code* **]]**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. Type is an integer from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered type is an integer from 0 through 255.

Usage Guidelines

Define a rule to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23*, and ICMP packets coming from the host with the IP address *2002::c6a2:6419*:

```
redirect context 23 icmp host 2002::c6a2:6419
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 icmp host 2002::c6a2:6419
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 icmp host 2002::c6a2:6419
```

The following deletes the first rule defined above:

```
no redirect context 23 icmp host 2002::c6a2:6419
```

redirect context (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect context context_id [ log ] ip { source_address source_wildcard | any |
host source_host_address } { dest_address dest_wildcard | any | host dest_host_address
 } [ fragment ] [ protocol num ]
after redirect context context_id [ log ] ip { source_address source_wildcard |
any | host source_host_address } { dest_address dest_wildcard | any | host
dest_host_address } [ fragment ] [ protocol num ]
```

before redirect context *context_id* **[log] ip {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**
no redirect context *context_id* **[log] ip {** *source_address source_wildcard* **| any | host** *source_host_address* **} {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [fragment] [protocol** *num* **]**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.

num is an integer from 0 through 255.

Usage Guidelines Block IP packets when the source and destination are of interest.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23*, and IP packets coming from the host with the IP address *2002::c6a2:6419*, and fragmented packets for any destination are matched:

```
redirect context 23 ip host 2002::c6a2:6419 any fragment
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 ip host 198.162.100.25 any fragment
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 ip host 2002::c6a2:6419 any fragment
```

The following deletes the first rule defined above:

```
no redirect context 23 ip host 2002::c6a2:6419 any fragment
```

redirect context (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product All

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect context context_id [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port
 | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host
 dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ]
}
after redirect context context_id [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port
 | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host
 dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ]
}
before redirect context context_id [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port
 | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host
 dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ]
}
no redirect context context_id [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port
 | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host
 dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ]
}
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an integer from 0 through 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be configured to an integer from 0 through 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be configured to an integer from 0 through 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be configured to an integer from 0 through 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be configured to an integer from 0 through 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be configured to an integer from 0 through 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer from 0 through 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be configured to an integer from 0 through 65535.

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the context with the context ID of *23*, and UDP packets coming from any host are matched:

```
redirect context 23 udp any
```

The following sets the insertion point to before the rule defined above:

```
before redirect context 23 udp any
```

The following command sets the insertion point after the rule defined above:

```
after redirect context 23 udp any
```

The following deletes the rule defined above:

```
no redirect context 23 udp any
```

redirect css delivery-sequence

This is a restricted command. In StarOS 9.0 and later, this command is obsoleted.

redirect css service (any)

Used to redirect subscriber sessions based on any packet received with Content Service Steering (CSS) enabled. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect css service svc_name [ log ] any
after redirect css service svc_name [ log ] any
before redirect css service svc_name [ log ] any
no redirect css service svc_name [ log ] any
```

after

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definitions which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the CSS service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be a string of 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage Guidelines

Define a catch all rule definitions to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important It is suggested that any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important A maximum of 16 rule definitions can be configured per ACL.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service with the name *css-svc1* and any source IP:

```
redirect css service css-svc1 any
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 any
```

The following command sets the insertion point after the second rule definitions above:

```
after redirect css service css-svc1 any
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 any
```

redirect css service (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect css service svc_name [ log ] host source_host_address
after redirect css service svc_name [ log ] host source_host_address
before redirect css service svc_name [ log ] host source_host_address
no redirect css service svc_name [ log ] host source_host_address
```

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be an alphanumeric string of 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service with the name *css-svc1* and a host IP address of *fe80::c0a8:c80b*:

```
redirect css service css-svc1 host fe80::c0a8:c80b
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 host fe80::c0a8:c80b
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 host fe80::c0a8:c80b
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 host fe80::c0a8:c80b
```

redirect css service (by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect css service *svc_name* **[log] icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [***icmp_type* **[** *icmp_code* **]]**
after redirect css service *svc_name* **[log] icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [***icmp_type* **[** *icmp_code* **]]**
before redirect css service *svc_name* **[log] icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [***icmp_type* **[** *icmp_code* **]]**
no redirect css service *svc_name* **[log] icmp { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [***icmp_type* **[** *icmp_code* **]]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured charging services.

svc_name must be an alphanumeric string of 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type is an integer from 0 through 255.

Usage Guidelines

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service named *css-svc1*, and ICMP packets coming from the host with the IP address *2002::c6a2:6419*:

```
redirect css service css-svc1 icmp host 2002::c6a2:6419
```

The following sets the insertion point to before the first rule definition above:

before redirect css service css-svc1 icmp host 2002::c6a2:6419

The following command sets the insertion point after the second rule definition above:

after redirect css service css-svc1 icmp host 2002::c6a2:64195

The following deletes the first rule definition above:

no redirect css service css-svc1 icmp host 2002::c6a2:6419

redirect css service (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax Description

redirect css service *svc_name* **[log] ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
after redirect css service *svc_name* **[log] ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
before redirect css service *svc_name* **[log] ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
no redirect css service *svc_name* **[log] ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be an alphanumeric string of 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage Guidelines

Block IP packets when the source and destination are of interest.

Important A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service named *css-svc1*, and IP packets coming from the host with the IP address *2002::c6a2:6419*, and fragmented packets for any destination are matched:

```
redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```

redirect css service (by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect css service *svc_name* **[log]** *source_address source_wildcard*
after redirect css service *svc_name* **[log]** *source_address source_wildcard*
before redirect css service *svc_name* **[log]** *source_address source_wildcard*
no redirect css service *svc_name* **[log]** *source_address source_wildcard*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be an alphanumeric string of 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

Usage Guidelines Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Important A maximum of 16 rule definitions can be configured per ACL.

Example

The following command defines a rule definition to redirect packets to a CSS service named *css-svc1*:

```
redirect css service css=svc1 2002::c6a2:6419
```

redirect css service (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect css service svc_name [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port
 | lt source_port | neq source_port | range start_source_port end_source_port ] } {
{ dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt
dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
after redirect css service svc_name [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port
 | lt source_port | neq source_port | range start_source_port end_source_port ] } {
{ dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt
dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
after redirect css service svc_name [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port
 | lt source_port | neq source_port | range start_source_port end_source_port ] } {
{ dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt
dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
no redirect css service svc_name [ log ] { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } [ eq source_port | gt source_port
 | lt source_port | neq source_port | range start_source_port end_source_port ] } {
{ dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt
dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured charging services.

svc_name must be an alphanumeric string of 1 through 15 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an integer from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be configured to an integer from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be configured to an integer from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be configured to an integer from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.

start_source_port is the initial port in the range and *end_source_port* is the final port in the range.

Both *start_source_port* and *end_source_port* can be configured to an integer from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be configured to an integer from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be configured to an integer from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be configured to an integer from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered.

start_dest_port is the initial port in the range and *end_dest_port* is the final port in the range.

Both *start_dest_port* and *end_dest_port* can be configured to an integer from 0 to 65535

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service named *css-svc1*, and UDP packets coming from any host are matched:

```
redirect css service css-svc1 udp any
```

The following sets the insertion point to before the rule definition above:

```
before redirect css service css-svc1 udp any
```

The following command sets the insertion point after the rule definition above:

```
after redirect css service css-svc1 udp any
```

The following deletes the rule definition above:

```
no redirect css service css-svc1 udp any
```

redirect css service (for downlink, any)

Used to redirect subscriber sessions based on any packet received in the downlink (from the Mobile Node) direction. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect css service svc_name [ log ] downlink any
after redirect css service svc_name [ log ] downlink any
before redirect css service svc_name [ log ] downlink any
no redirect css service svc_name [ log ] downlink any
```

after

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be an alphanumeric string of 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage Guidelines Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important It is suggested that any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important A maximum of 16 rule definitions can be configured per ACL.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the CSS service with the name *css-svc1* and any source IP:

```
redirect css service css-svc1 downlink any
```

The following sets the insertion point to before the first rule definition above:

```
before redirect service css-svc1 downlink any
```

The following command sets the insertion point after the second rule definition above:

```
after redirect service css-svc1 downlink any chgsvc1 downlink any
```

The following deletes the first rule definition above:

```
no redirect service css-svc1 downlink any
```

redirect css service (for downlink, by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address in the downlink (from the Mobile Node) direction.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect css service *svc_name* **[log] downlink host** *source_host_address*
after redirect css service *svc_name* **[log] downlink host** *source_host_address*
before redirect css service *svc_name* **[log] downlink host** *source_host_address*
no redirect css service *svc_name* **[log] downlink host** *source_host_address*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be an alphanumeric string of 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *css-svc1* and a host IP address of *fe80::c0a8:c80b*:

```
redirect service css-svc1 downlink host fe80::c0a8:c80b
```

The following sets the insertion point to before the first rule definition above:

```
before redirect service css-svc1 downlink host fe80::c0a8:c80b
```

The following command sets the insertion point after the second rule definition above:

```
after redirect service css-svc1 downlink host fe80::c0a8:c80b
```

The following deletes the first rule definition above:

```
no redirect service css-svc1 downlink host fe80::c0a8:c80b
```

redirect css service (for downlink, by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets in the downlink (from the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect css service svc_name [ log ] downlink icmp { any | host
source_host_address | source_address source_wildcard } { any | host dest_host_address
| dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]
after redirect css service svc_name [ log ] downlink icmp { any | host
source_host_address | source_address source_wildcard } { any | host dest_host_address
```

```
| dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]
before redirect css service svc_name [ log ] downlink icmp { any | host
source_host_address | source_address source_wildcard } { any | host dest_host_address
| dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]
no redirect css service svc_name [ log ] downlink icmp { any | host
source_host_address | source_address source_wildcard } { any | host dest_host_address
| dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]
```

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be an alphanumeric string of 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value from 0 through 255.

Usage Guidelines

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *css-svc1*, and ICMP packets coming in the downlink (from the Mobile Node) direction from the host with the IP address *2002::c6a2:6419*:

```
redirect css service css-svc1 downlink icmp host 2002::c6a2:6419
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 downlink icmp host 2002::c6a2:6419
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 downlink icmp host 2002::c6a2:6419
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 downlink icmp host 2002::c6a2:6419
```

redirect css service (for downlink, by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets in the downlink (from the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect css service *svc_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
after redirect css service *svc_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
before redirect css service *svc_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**
no redirect css service *svc_name* **[log] downlink ip { any | host** *source_host_address* **|** *source_address source_wildcard* **} { any | host** *dest_host_address* **|** *dest_address dest_wildcard* **} [fragment]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be a string of 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage Guidelines

Block IP packets when the source and destination are of interest.

Important A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *css-svc1*, and downlink IP packets coming from the host with the IP address *2002::c6a2:6419*, and fragmented packets for any destination are matched:

```
redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any fragment
```

The following sets the insertion point to before the first rule definition above:

before redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any fragment

The following command sets the insertion point after the second rule definition above:

after redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any fragment

The following deletes the first rule definition above:

no redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any fragment

redirect css service (for downlink, by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source in the downlink (from the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax Description

redirect css service *svc_name* **[log] downlink** *source_address source_wildcard*
after redirect css service *svc_name* **[log] downlink** *source_address source_wildcard*
before redirect css service *svc_name* **[log] downlink** *source_address source_wildcard*
no redirect css service *svc_name* **[log] downlink** *source_address source_wildcard*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be an alphanumeric string of 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

Usage Guidelines Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Important A maximum of 16 rule definitions can be configured per ACL.

Example

The following command defines a rule definition to redirect packets to a charging service named *css-svc1*:

```
redirect css service css-svc1 donwlink fe80::c0a8:a04
```

redirect css service (for downlink, by TCP/UDP packets)

Used to redirect subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the downlink (from the Mobile Node) direction.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > **context** *context_name* > **ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect css service svc_name [ log ] downlink { tcp | udp } { { source_address
 source_wildcard | any | host source_host_address } [ eq source_port | gt source_port
 | lt source_port | neq source_port | range start_source_port end_source_port ] } {
{ dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt
dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
after redirect css service svc_name [ log ] downlink { tcp | udp } { {
source_address source_wildcard | any | host source_host_address } [ eq source_port |
gt source_port | lt source_port | neq source_port | range start_source_port
end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address }
[ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port
 end_dest_port ] }
after redirect css service svc_name [ log ] downlink { tcp | udp } { {
source_address source_wildcard | any | host source_host_address } [ eq source_port |
gt source_port | lt source_port | neq source_port | range start_source_port
end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address }
[ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port
 end_dest_port ] }
no redirect css service svc_name [ log ] downlink { tcp | udp } { {
source_address source_wildcard | any | host source_host_address } [ eq source_port |
```

gt *source_port* **| lt** *source_port* **| neq** *source_port* **| range** *start_source_port end_source_port* **] } { { ***dest_address dest_wildcard* **| any | host** *dest_host_address* **}** **[eq** *dest_port* **| gt** *dest_port* **| lt** *dest_port* **| neq** *dest_port* **| range** *start_dest_port end_dest_port* **] }**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be an alphanumeric string of 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.

- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.

start_source_port is the initial port in the range and *end_source_port* is the final port in the range.

Both *start_source_port* and *end_source_port* can be configured to an integer value from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered.

start_dest_port is the initial port in the range and *end_dest_port* is the final port in the range.

Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *css-svc1*, and UDP packets coming from any host are matched:

```
redirect css service css-svc1 downlink udp any
```

The following sets the insertion point to before the rule definition above:

```
before redirect css service css-svc1 downlink udp any
```

The following command sets the insertion point after the rule definition above:

```
after redirect css service css-svc1 downlink udp any
```

The following deletes the rule definition above:

```
no redirect css service css-svc1 downlink udp any
```

redirect css service (for uplink, any)

Used to redirect subscriber sessions based on any packet received in the uplink (to the Mobile Node) direction. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect css service svc_name [ log ] uplink any
after redirect css service svc_name [ log ] uplink any
before redirect css service svc_name [ log ] uplink any
no redirect css service svc_name [ log ] uplink any
```

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be an alphanumeric string of 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage Guidelines

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

Important It is suggested that any rule definition which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

Important A maximum of 16 rule definitions can be configured per ACL.

Important Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *css-svc1* and any source IP:

```
redirect css service css-svc1 uplink any
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 uplink any
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 uplink any
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 uplink any
```

redirect css service (for uplink, by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address in the uplink (to the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect css service *svc_name* **[log] uplink host** *source_host_address*
after redirect css service *svc_name* **[log] uplink host** *source_host_address*
before redirect css service *svc_name* **[log] uplink host** *source_host_address*
no redirect css service *svc_name* **[log] uplink host** *source_host_address*

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

after

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must ben alphanumeric string of 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

Usage Guidelines

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service with the name *css-svc1* and a host IP address of *fe80::c0a8:c80b*:

```
redirect service css-svc1 uplink host fe80::c0a8:c80b
```

The following sets the insertion point to before the first rule definition above:

```
before redirect service css-svc1 uplink host fe80::c0a8:c80b
```

The following command sets the insertion point after the second rule definition above:

```
after redirect service css-svc1 uplink host fe80::c0a8:c80b
```

The following deletes the first rule definition above:

```
no redirect service css-svc1 uplink host fe80::c0a8:c80b
```

redirect css service (for uplink, by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets in the uplink (to the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect css service *svc_name* **[log] uplink icmp { any | host** *source_host_address* | *source_address source_wildcard* **} { any | host** *dest_host_address* | *dest_address dest_wildcard* **} [** *icmp_type* **[** *icmp_code* **]]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the **show css service all** command to display the names of all configured CSS services.

svc_name must be an alphanumeric string of 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value from 0 through 255.

Usage Guidelines

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important A maximum of 16 rule definitions can be configured per ACL. Also note that "redirect" rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and ICMP packets in the uplink (to the Mobile Node) direction from the host with the IP address *198.162.100.25*:

```
redirect css service chgsvc1 uplink icmp host 198.162.100.25
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service chgsvc1 uplink icmp host 198.162.100.25
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service chgsvc1 uplink icmp host 198.162.100.25
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink icmp host 198.162.100.25
```

redirect css service (for uplink, by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets in the uplink (to the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect css service *svc_name* **[log] uplink ip { any | host** *source_host_address* **| source_address source_wildcard } { any | host** *dest_host_address* **| dest_address dest_wildcard } [fragment]**
after redirect css service *svc_name* **[log] uplink ip { any | host** *source_host_address* **| source_address source_wildcard } { any | host** *dest_host_address* **| dest_address dest_wildcard } [fragment]**
before redirect css service *svc_name* **[log] uplink ip { any | host** *source_host_address* **| source_address source_wildcard } { any | host** *dest_host_address* **| dest_address dest_wildcard } [fragment]**
no redirect css service *svc_name* **[log] uplink ip { any | host** *source_host_address* **| source_address source_wildcard } { any | host** *dest_host_address* **| dest_address dest_wildcard } [fragment]**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

svc_name must be a string of 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage Guidelines

Block IP packets when the source and destination are of interest.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and uplink IP packets going to the host with the IP address *198.162.100.25*, and fragmented packets for any destination are matched:

```
redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following sets the insertion point to before the first rule definition above:

```
redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service chgsvc1 uplink ip host 198.162.100.25 any
fragment
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

redirect css service (for uplink, by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source in the uplink (to the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect css service *svc_name* **[log] uplink** *source_address source_wildcard*

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

svc_name must be a string of 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Usage Guidelines

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Example

The following command defines a rule definition to redirect packets to a charging service named *chgsvc1*:

```
redirect css service chgsvc1 uplink 1:1:1:1:1:1:1:1
```

redirect css service (for uplink, by TCP/UDP packets)

Used to redirect subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the uplink (to the Mobile Node) direction.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect css service *svc_name* **[log] uplink { tcp | udp } { {** *source_address source_wildcard* **| any |** *source_host_address* **} [eq** *source_port* **| gt** *source_port* **| lt** *source_port* **| neq** *source_port* **| range** *start_source_port end_source_port* **] } { {** *dest_address dest_wildcard* **| any | host** *dest_host_address* **} [eq** *dest_port* **| gt**

dest_port **|** **lt** *dest_port* **|** **neq** *dest_port* **|** **range** *start_dest_port end_dest_port* **] }**
after redirect css service *svc_name* **[log] uplink { tcp | udp } { {** *source_address source_wildcard* **|** **any** **|** *source_host_address* **} [eq** *source_port* **|** **gt** *source_port* **|** **lt** *source_port* **|** **neq** *source_port* **|** **range** *start_source_port end_source_port* **] } { {** *dest_address dest_wildcard* **|** **any** **|** **host** *dest_host_address* **} [eq** *dest_port* **|** **gt** *dest_port* **|** **lt** *dest_port* **|** **neq** *dest_port* **|** **range** *start_dest_port end_dest_port* **] }**
before redirect css service *svc_name* **[log] uplink { tcp | udp } { {** *source_address source_wildcard* **|** **any** **|** *source_host_address* **} [eq** *source_port* **|** **gt** *source_port* **|** **lt** *source_port* **|** **neq** *source_port* **|** **range** *start_source_port end_source_port* **] } { {** *dest_address dest_wildcard* **|** **any** **|** **host** *dest_host_address* **} [eq** *dest_port* **|** **gt** *dest_port* **|** **lt** *dest_port* **|** **neq** *dest_port* **|** **range** *start_dest_port end_dest_port* **] }**
no redirect css service *svc_name* **[log] uplink { tcp | udp } { {** *source_address source_wildcard* **|** **any** **|** *source_host_address* **} [eq** *source_port* **|** **gt** *source_port* **|** **lt** *source_port* **|** **neq** *source_port* **|** **range** *start_source_port end_source_port* **] } { {** *dest_address dest_wildcard* **|** **any** **|** **host** *dest_host_address* **} [eq** *dest_port* **|** **gt** *dest_port* **|** **lt** *dest_port* **|** **neq** *dest_port* **|** **range** *start_dest_port end_dest_port* **] }**

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

no

Removes the rule definition which exactly matches the options specified.

css service *svc_name*

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the **show active-charging service all** command to display the names of all configured charging services.

svc_name must be a string of 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

range *start_source_port end_source_port*

Specifies that all source TCP ports within a specific range are to be filtered.

start_source_port is the initial port in the range and *end_source_port* is the final port in the range.

Both *start_source_port* and *end_source_port* can be configured to an integer value from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

range *start_dest_port end_dest_port*

Specifies that all destination TCP ports within a specific range are to be filtered.

start_dest_port is the initial port in the range and *end_dest_port* is the final port in the range.

Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Example

The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and UDP packets coming from any host are matched:

```
redirect css service chgsvc1 uplink udp any
```

The following sets the insertion point to before the rule definition above:

```
before redirect css service chgsvc1 uplink udp any
```

The following command sets the insertion point after the rule definition above:

```
after redirect css service chgsvc1 uplink udp any
```

The following deletes the rule definition above:

```
no redirect css service chgsvc1 uplink udp any
```

redirect nexthop (by IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > **context** *context_name* > **ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **}** **[log]** *source_address source_wildcard*
after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log]** *source_address source_wildcard*

before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log]** *source_address source_wildcard*
no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log]** *source_address source_wildcard*

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alpha and/or numeric string from 1 to 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

Usage Guidelines

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at *192.168.10.4*, the context with the context ID of *23* and the source IP and wildcard of *198.162.22.0* and *0.0.0.31*:

```
redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following sets the insertion point to before the first rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following command sets the insertion point after the second rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

redirect nexthop (any)

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**
after redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**
before redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**
no redirect nexthop *nexthop_addr* **{ context** *context_id* **| interface** *interface_name* **} [log] any**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alpha and/or numeric string from 1 to 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

Usage Guidelines

Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important It is suggested that any rule which is added to be a catch all should also have the **log** option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at *192.168.10.4*, the context with the context ID of *23* and any source IP:

```
redirect nexthop 192.168.10.4 context 23 any
```

The following sets the insertion point to before the first rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 any
```

The following command sets the insertion point after the second rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 any
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 any
```

redirect nexthop (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect nexthop nexthop_addr { context context_id | interface interface_name }
[ log ] host source_ip_address
after redirect nexthop nexthop_addr { context context_id | interface interface_name
 } [ log ] host source_ip_address
before redirect nexthop nexthop_addr { context context_id | interface
interface_name } [ log ] host source_ip_address
no redirect nexthop nexthop_addr { context context_id | interface interface_name
 } [ log ] host source_ip_address
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alpha and/or numeric string from 1 to 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

Usage Guidelines

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at *192.168.10.4*, the context with the context ID of *23* and a host IP address of *192.168.200.11*:

```
redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following sets the insertion point to before the first rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following command sets the insertion point after the second rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```

redirect nexthop (by source ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect nexthop nexthop_addr { context context_id | interface interface_name }
[ log ] icmp { source_address source_wildcard | any | host source_host_address } {
 dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code
] ]
after redirect nexthop nexthop_addr { context context_id | interface interface_name
 } [ log ] icmp { source_address source_wildcard | any | host source_host_address
} { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code
 ] ]
before redirect nexthop nexthop_addr { context context_id | interface
interface_name } [ log ] icmp { source_address source_wildcard | any | host
source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [
 icmp_type [ icmp_code ] ]
no redirect nexthop nexthop_addr { context context_id | interface interface_name
 } [ log ] icmp { source_address source_wildcard | any | host source_host_address
} { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code
 ] ]
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alpha and/or numeric string from 1 to 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

icmp_code

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value from 0 through 255.

Usage Guidelines

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at *fe80::c0a8:a04*, the context with the context ID of *23*, and ICMP packets coming from the host with the IP address *2002::c6a2:64195*:

```
redirect nexthop fe80::c0a8:a04 context 23 icmp host 2002::c6a2:6419
```

The following sets the insertion point to before the first rule defined above:

```
before redirect nexthop fe80::c0a8:a04 context 23 icmp host 2002::c6a2:6419
```

The following command sets the insertion point after the second rule defined above:

```
after redirect nexthop fe80::c0a8:a04 context 23 icmp host 2002::c6a2:6419
```

The following deletes the first rule defined above:

```
no redirect nexthop fe80::c0a8:a04 context 23 icmp host 2002::c6a2:6419
```

redirect nexthop (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect nexthop nexthop_addr { context context_id | interface interface_name }
[ log ] ip { source_address source_wildcard | any | host source_host_address } {
dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol
 num ]
```

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 through 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

protocol *num*

Indicates that the packet filtering is to be applied to a specific protocol number.

num can be an integer from 0 through 255.

Usage Guidelines Block IP packets when the source and destination are of interest.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

redirect nexthop (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context *context_name* **> ipv6 access-list** *ipv6_acl_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

Syntax Description

```
redirect nexthop nexthop_addr { context context_id | interface interface_name }
[ log ] { tcp | udp } { { source_address source_wildcard | any | host
source_host_address } [ eq source_port | gt source_port | lt source_port | neq
source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq
 dest_port | gt dest_port | lt dest_port | neq dest_port ] }
after redirect nexthop nexthop_addr { context context_id | interface interface_name
 } [ log ] { tcp | udp } { { source_address source_wildcard | any | host
source_host_address } [ eq source_port | gt source_port | lt source_port | neq
source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq
 dest_port | gt dest_port | lt dest_port | neq dest_port ] }
before redirect nexthop nexthop_addr { context context_id | interface
interface_name } [ log ] { tcp | udp } { { source_address source_wildcard | any |
```

host *source_host_address* **}** **[** **eq** *source_port* **|** **gt** *source_port* **|** **lt** *source_port* **|** **neq** *source_port* **]** **}** **{** **{** *dest_address dest_wildcard* **|** **any** **|** **host** *dest_host_address* **}** **[** **eq** *dest_port* **|** **gt** *dest_port* **|** **lt** *dest_port* **|** **neq** *dest_port* **]** **}**
no redirect nexthop *nexthop_addr* **{** **context** *context_id* **|** **interface** *interface_name* **}** **[** **log** **]** **{** **tcp** **|** **udp** **}** **{** **{** *source_address source_wildcard* **|** **any** **|** **host** *source_host_address* **}** **[** **eq** *source_port* **|** **gt** *source_port* **|** **lt** *source_port* **|** **neq** *source_port* **]** **}** **{** **{** *dest_address dest_wildcard* **|** **any** **|** **host** *dest_host_address* **}** **[** **eq** *dest_port* **|** **gt** *dest_port* **|** **lt** *dest_port* **|** **neq** *dest_port* **]** **}**

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.

nexthop *nexthop_addr*

The IP address to which the IP packets are redirected.

context *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the **show context all** command to display context names and context IDs.

interface *interface_name*

The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 through 79 characters.

log

Default: packets are not logged.

Indicates all packets which match the redirect are to be logged.

tcp | udp

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

source_address

The IP address(es) form which the packet originated.

This option is used to filter all packets from a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source_wildcard* parameter.

source_wildcard

This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule applies to all packets.

host

Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

eq *source_port*

Specifies a single, specific source TCP port number to be filtered.

source_port must be configured to an integer value from 0 to 65535.

gt *source_port*

Specifies that all source TCP port numbers greater than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

lt *source_port*

Specifies that all source TCP port numbers less than the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

neq *source_port*

Specifies that all source TCP port numbers not equal to the one specified are to be filtered.

source_port must be configured to an integer value from 0 to 65535.

dest_address

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

dest_wildcard

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

Important The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

eq *dest_port*

Specifies a single, specific destination TCP port number to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

gt *dest_port*

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

lt *dest_port*

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

neq *dest_port*

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

dest_port must be configured to an integer value from 0 to 65535.

Usage Guidelines

Block IP packets when the source and destination are of interest but for only a limited set of ports.

Important The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that "redirect" rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at *fe80::c0a8:a04*, the context with the context ID of *23*, and UDP packets coming from any host are matched:

```
redirect nexthop fe80::c0a8:a04 context 23 udp any
```

The following sets the insertion point to before the rule defined above:

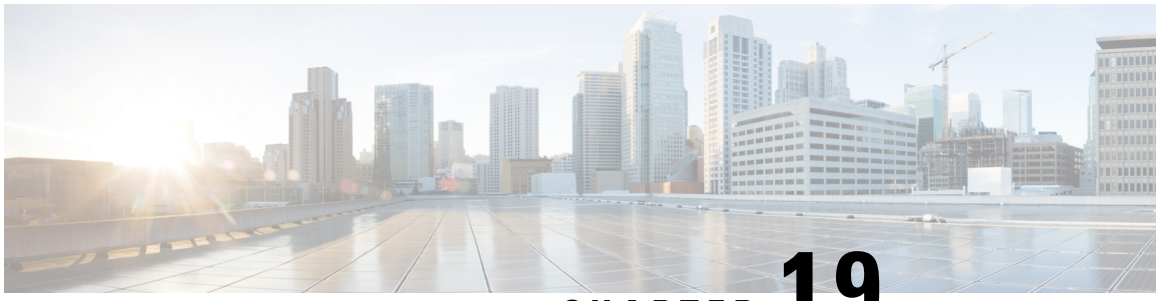
```
before redirect nexthop fe80::c0a8:a04 context 23 udp any
```

The following command sets the insertion point after the rule defined above:

```
after redirect nexthop fe80::c0a8:a04 context 23 udp any
```

The following command deletes the first rule defined above:

```
no redirect nexthop fe80::c0a8:a04 context 23 udp any
```



CHAPTER 19

IPv6 to IPv4 Tunnel Interface Configuration Mode Commands

The IPv6 to IPv4 Tunnel Interface Configuration Mode is used to create and manage the IP interface for addresses, address resolution options, etc.

Command Modes

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration

configure > context *context_name* **> interface** *interface_name* **tunnel > tunnel-mode ipv6ip**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-if-tunnel-ipv6ip)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

destination address

Configures the destination of the tunnelled packets for a manual tunnel.

Product All

Privilege Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration

configure > context *context_name* **> interface** *interface_name* **tunnel > tunnel-mode ipv6ip**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-ipv6ip)#
```

Syntax Description

destination address *address*

no destination address

no

Removes configuration for the specified keyword.

address

Specifies the IP address of the destination device. *address* must be specified in IPv4 dotted decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to configure the IP address of the destination end of the tunnel.

Example

The following command sets the destination address for packets on this tunnelled interface to *209.165.200.228*:

```
destination address 209.165.200.228
```

mode

Configures the mode of IPv6 to IPv4 tunneling. The default is set to manual mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration

configure > context *context_name* **> interface** *interface_name* **tunnel > tunnel-mode ipv6ip**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-ipv6ip)#
```

Syntax Description

mode { 6to4 | manual }

default mode

6to4

Configures automatic IPv6-to-IPv4 (6to4) tunnels as specified in RFC 3056.

manual

Configures point-to-point manual IPv6-to-IPv4 tunnels by specifying the IPv4 address of the tunnel remote end.

default

Resets the mode of IPv6-to-IPv4 tunneling to manual mode.

Usage Guidelines

There can be only one IPv6-to-IPv4 tunnel possible in a context. Once an IPv6-to-IPv4 tunnel is configured, all subsequent tunnels will be configured as manual tunnels.

Example

The following command configures the mode to IPv6-to-IPv4 (*6to4*).

```
mode 6to4
```

The following command configures the mode to *6to4*.

```
mode manual
```

source

Configures the source of tunneled packets.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration

configure > context *context_name* **> interface** *interface_name* **tunnel > tunnel-mode ipv6ip**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-ipv6ip)#
```

Syntax Description

```
source { address ip_address | interface interface_name }
no source { address | interface }
```

address *ip_address*

Specifies the IPv4 address to use as the source address of the tunnel.

ip_address must be expressed in IPv4 dotted-decimal notation.

interface *interface_name*

Specifies the name of a non-tunnel IPv4 interface, whose address is used as the source address of the tunnel. *interface* must be an alphanumeric string of 1 through 79 characters.

no source { address | interface }

Removes configuration for the specified keyword.

Usage Guidelines

Configures the source IPv4 address of the tunnel by either specifying the IP address (host address) or by specifying another configured non-tunnel IPv4 interface. The source address must be an existing interface address before it is used. State of source address will affect the operational state of the tunnel.

Example

The following command configures the source address of the tunnel.

```
source address 209.165.200.228
```

The following command specifies the source interface as *testsource1*.

```
source interface testsource1
```

tos

Configures the type of service (TOS) settings of the outer IPv4 header of the tunneled packets.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration

configure > context *context_name* **> interface** *interface_name* **tunnel > tunnel-mode ipv6ip**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-ipv6ip)#
```

Syntax Description

```
tos { copy | value tos_value }
default tos
```

copy

Copies the DC octet of the IPv6 packet to the TOS octet of IPv4 packet.

default

Configures default setting for the specified keyword.

value *tos_value*

Configures the raw TOS value ranging from 0 to 255. The default is 0.

Usage Guidelines

Sets the TOS parameter to be used in the tunnel transport protocol or copies the TOS value from the original IPv6 DC byte to the TOS value of the encapsulating IPv4 header.

Example

The following command sets the tos value to *1*:

```
tos value 1
```

ttl

Configures the TTL (Time to live) value of the outer IPv4 header of the tunneled packets.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration

configure > context *context_name* **> interface** *interface_name* **tunnel > tunnel-mode ipv6ip**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-ipv6ip)#
```

Syntax Description

ttl value *ttl_value*

default

Configures default setting for the specified keyword.

value *ttl_value*

ttl_value is an integer from 1 through 255. The default is 16.

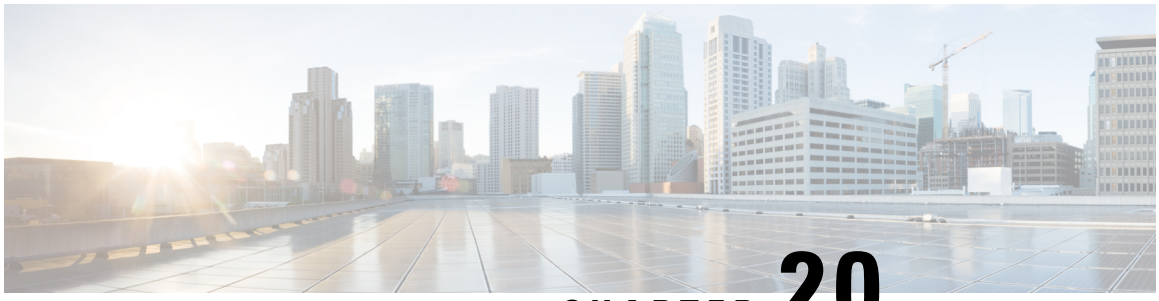
Usage Guidelines

Configures the TTL parameter to be used in the tunnel transport protocol.

Example

The following command sets the TTL value to *25*.

```
ttl value 25
```



CHAPTER 20

IP VRF Context Configuration Mode Commands

The IP VRF Context Configuration Mode is used to create and manage the Virtual Routing and Forwarding (VRF) context instance for BGP/MPLS VPN, GRE, IPSec tunneling or service interfaces for virtual routing, addresses, address resolution options, etc.

Command Modes

Exec > Global Configuration > Context Configuration > IP VRF Context Configuration

configure > context *context_name* **> ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

associate l2-mapping-table

Associates a global QoS-to-Level 2 mapping table with this VRF.

Product

ePDG

HSGW

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IP VRF Context Configuration

configure > context *context_name* **> ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

associate l2-mapping-table { name *table_name* **| system-default }**
no associate l2-mapping-table

no

Disassociates an existing L2 mapping table from this VRF.

name *table_name*

Specifies the name of an existing internal table from which to map QoS to L2 values.

table_name is an alphanumeric string of 0 through 80 characters.

system-default

Associates the system-default table with this VRF. This is useful if the base-context has a different explicit mapping.

Usage Guidelines

Use this command to associates a global QoS-to-Level 2 mapping table with this VRF.

Internal-QoS will be mapped to an actual L2 value (either or both of 802.1p/MPLS) using a per-VRF based table.

Important If an l2-mapping-table association is made at both the VRF and VPN level, the VRF level takes precedence.

The mapping table is configured via the Global Configuration mode **qos l2-mapping-table** command.

Example

The following command associates this VRF with Qos-to-L2 mapping table *vrf10*.

associate l2-mapping-table name vrf10

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.

ip aggregate-address

Specifies an IPv4 address/mask for aggregating frame routes in the VRF.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IP VRF Context Configuration

configure > context *context_name* **> ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

```
ip aggregate-address ipv4_address/mask [summary-only]
no ip aggregate-address ipv4_address/mask
```

no

Deletes the specified IPv4 aggregate address.

ipv4_address/mask

Specifies the IP address and mask in IPv4 CIDR dotted-decimal notation.

[summary-only]

When this option is configured, the constituent routes are removed from the VRF.

Usage Guidelines Use this command to configure aggregate framed-routes in a VRF. It enables inserting an aggregate-address in a VRF and its advertisement in the routing domain if at least one constituent framed-route exists in that

VRF. By default, the constituent routes will also be present along with the aggregate address. However, if the summary-only option is configured, the constituent routes will be removed from the VRF. Up to 32 aggregate addresses can be configured in a VRF.

Example

The following example sets an IPv4 aggregate address for the VFR:**ip aggregate-address 209.165.201.0/27**

ip guarantee

Enables and disables local switching of framed route packets.

Product

GGSN

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ip guarantee framed-route local-switching

no

Disables local switching of framed route packets.

framed-route local-switching

Enables local switching of framed route packets. By default, this functionality is disabled.

Usage Guidelines

Use this command to enable and disable local switching of framed route packets. This functionality will be applicable only when there are some NEMO/framed route sessions in a context.

Example

The following command enables local switching of framed route packets:

```
ip guarantee framed-route local-switching
```

ip maximum-routes

This command configures the maximum number of routes in an IP VRF routing table configured in this context.

Important This command should only be used for framed or NEMO (Network Mobility) routes of the VRF.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IP VRF Context Configuration

configure > context *context_name* **> ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

ip maximum-routes *max_routes*
no ip maximum-routes

no

Disables the configured maximum routes in specific IP VRF context.

max_routes

Sets the maximum number of routes in a specific IP VRF context.

max_routes must be an integer from 1 through 32768 or 65536 (release 17.0+).

Usage Guidelines

Use this command to configure the maximum number of routes in a particular VRF routing table. When the number of routes in the VRF is more than the maximum limit configured, a critical log is generated indicating that the number of routes is over the limit. Once the number of routes in the VRF goes under the limit, a **clear log** is generated.

The maximum routes configured using this command will be sent to the threshold configuration logic for appropriate action. For more information on threshold configuration, refer to descriptions of the **threshold route-service** and **threshold poll route-service interval** commands in the *Global Configuration Mode Commands* chapter.

Example

The following command sets *1000* routes as a maximum limit for specific VRF context:

```
ip maximum-routes 1000
```

mpls map-dscp-to-exp

This command maps the final differentiated services code point (DSCP) bit value in the IP packet header to the final Experimental (EXP) bit value in the MPLS header for incoming traffic.

Important This command has been deprecated beginning with Release 15.0.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IP VRF Context Configuration

configure > context *context_name* **> ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

[no] mpls map-dscp-to-exp dscp *dscp_bit_value* **exp** *exp_bit_value*

no

Disables the configured DSCP bit value mapping to the EXP bit value from a specific IP VRF context.

dscp *dscp_bit_value*

Specifies the final DSCP bit value which is to map with the final EXP bit value in MPLS header for incoming traffic.

dscp_bit_value specifies the value of DSCP bit values separated in eight groups and represented with integers from 0 through 7.

The default representation of DSCP value in eight groups is given in the following table:

DSCP Marking Value	DSCP Map Group
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

exp *exp_bit_value*

Specifies the final EXP bit value in MPLS header to which the final DSCP bit value 0 to 7 (represented in eight values) coming from incoming traffic will be mapped.

exp_bit_value is the value of EXP bit in MPLS header and must be an integer between 0 through 7.

Usage Guidelines

Use this command to map the final DSCP value coming from incoming IP traffic to a final EXP value in MPLS header. This mapping determines the QoS and service parameters to which the packet is assigned.

Example

The following command maps the DSCP value *3* (24 to 31) to EXP bit *3* in MPLS header:

```
mpls map-dscp-to-exp dscp 3 exp 3
```

mpls map-exp-to-dscp

Maps incoming the Experimental (EXP) bit value in MPLS header to the internal differentiated services code point (DSCP) bit value in IP packet headers for outgoing traffic.

Important This command has been deprecated beginning with Release 15.0.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IP VRF Context Configuration

configure > context *context_name* **> ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax Description

`[ no ] mpls map-exp-to-dscp exp` *`exp_bit_value`* **`dscp`** *`dscp_bit_value`*

no

Disables the configured EXP bit value mapping to DSCP bit value from specific IP VRF context.

exp *exp_bit_value*

Specifies the incoming EXP bit value in MPLS header to which the internal DSCP bit value 0 to 7 (represented in 8 values) in IP traffic will be mapped.

exp_bit_value is the value of the EXP bit in an MPLS header and must be an integer from 0 through 7.

dscp *dscp_bit_value*

Maps the DSCP bit value with the incoming EXP bit value in an MPLS header.

dscp_bit_value specifies the value of the DSCP bit values separated in eight groups and represented with integers between 0 through 7.

The default representation of DSCP value in eight groups is given in the following table:

DSCP Marking Value	DSCP Map Group
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

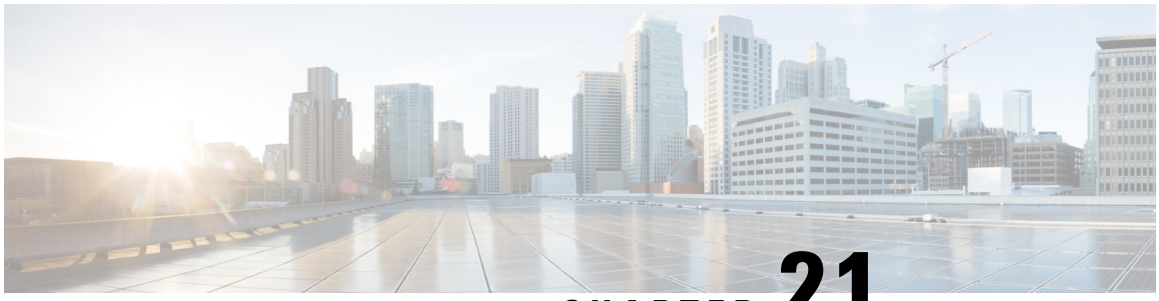
Usage Guidelines

Use this command to map the incoming EXP bit value in MPLS headers to the DSCP bit value in IP traffic. This mapping determines the QoS and service parameters to which the packet is assigned.

Example

The following command maps the EXP bit value *4* to DSCP value *6* (48 to 55) in IP header:

```
mpls map-exp-to-dscp exp 4 dscp 6
```



CHAPTER 21

ISAKMP Configuration Mode Commands

Modification(s) to an existing ISAKMP policy configuration will not take effect until the related security association has been cleared. Refer to the **clear crypto security-association** command described in the *Exec Mode (A–C) Commands* chapter for more information.

Command Modes

The ISAKMP Configuration Mode is used to configure Internet Security Association Key Management Protocol (ISAKMP) policies that are used to define Internet Key Exchange (IKE) security associations (SAs).

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > context *context_name* **> isakmp policy** *policy_number*

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

authentication

Configures the ISAKMP policy authentication mode.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > context *context_name* **> isakmp policy** *policy_number*

Syntax Description

```
authentication preshared-key
[ default | no ] authentication
```

default authentication

Restores the default setting of this parameter. This command is enabled by default.

no authentication

Disables the preshared key authentication mode.

preshared-key

Specifies that the policy will be authenticated through the use of the pre-shared key.

Usage Guidelines

When the system is configured to use ISAKMP-type crypto maps for establishing IPSec tunnels, this command is used to indicate that the policy will be authenticated through the use of the pre-shared key configured in the ISAKMP crypto map.

Example

The following command sets policy authentication mode to use a pre-shared key:

```
authentication preshared-key
```

encryption

Configures the encryption protocol to use to protect subsequent IKE SA negotiations.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > context *context_name* **> isakmp policy** *policy_number*

Syntax Description

```
encryption { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc }
[ default | no ] encryption
```

default encryption

Restores the default setting of this parameter.

no encryption

Removes a previously configured encryption type.

3des-cbc

Specifies that the encryption protocol is Triple Data Encryption Standard (3DES) in chain block (CBC) mode.

aes-cbc-128

Specifies that the encryption protocol is Advanced Encryption Standard (AES) in CBC mode with a 128-bit key.

aes-cbc-256

Specifies that the encryption protocol is Advanced Encryption Standard (AES) in CBC mode with a 256-bit key.

des-cbc

Specifies that the encryption protocol is DES in CBC mode. This is the default setting.

Usage Guidelines

Once the D-H exchange between the system and the security gateway has been successfully completed, subsequent IKE SA negotiations will be protected using the protocol specified by this command.

Example

The following command sets the IKE encryption method to 3des-cbc:

```
encryption 3des-cbc
```

group

Configures the Oakely group (also known as the Diffie-Hellman [D-H] group) in which the D-H exchange occurs.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > context *context_name* **> isakmp policy** *policy_number*

Syntax Description

```
group { 1 | 2 | 5 }
[ default | no ] group
```

default group

Restores the default setting of this parameter.

no group

Removes a previously configured group.

{ 1 | 2 | 5 }

Default: **1**

Specifies the number of the Oakley group. The following groups are allowed:

- **1**: Enables Oakley Group 1 using a 768-bit modp as defined in RFC 2409.
- **2**: Enables Oakley Group 2, using a 1024-bit modp as defined in RFC 2409.
- **5**: Enables Oakley Group 5, using a 1536-bit modp as defined in RFC 3526.

Usage Guidelines

Specifies the Oakley group that determine the length of the base prime numbers that are used during the key exchange process.

Example

The following command sets the group to 5 which specifies 1536-bit base prime numbers:

```
group 5
```

hash

Configures the IKE hash protocol to use during IKE SA negotiations.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator\

Command Modes

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > **context** *context_name* > **isakmp policy** *policy_number*

Syntax Description

```
hash { md5 | sha1 }
[ default | no ] hash
```

default

Restores the default setting of this parameter.

no

Removes a previously configured hash algorithm.

md5

Specifies that the hash protocol is Message Digest 5 truncated to 96 bits.

sha1

Specifies that the hash protocol is Secure Hash Algorithm-1 truncated to 96 bits. This is the default setting for this command.

Usage Guidelines

Use this command to configure the hash algorithm used during key negotiation.

Example

Set the hash algorithm to Message-Digest 5 by entering the following command:

```
hash md5
```

lifetime

Configures the lifetime of the IKE Security Association (SA).

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

configure > context *context_name* **> isakmp policy** *policy_number*

Syntax Description

```
lifetime seconds
default lifetime
```

default lifetime

Restores the default setting of this parameter.

seconds

Default: 86400

The number of seconds for the SA to live. *seconds* must be an integer from 60 to 86400.

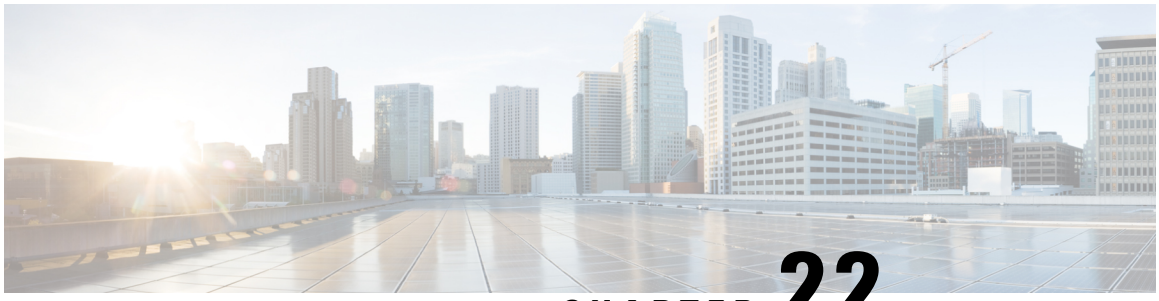
Usage Guidelines

Use this command to set the time that an ISAKMP SA will be valid. The lifetime is negotiated with the peer and the lowest configured lifetime duration is used.

Example

The following command sets the SA lifetime to 100 seconds:

lifetime *100*



CHAPTER 22

IuPS Service Configuration Mode Commands

Command Modes

The IuPS Service configuration mode is used to define properties for the IuPS service which controls the Iu-PS interface connections to Radio Network Controllers (RNCs) of the UMTS Terrestrial Radio Access Network (UTRAN).

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

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

Note From R15.0 onwards, License Control is implemented on all Network Sharing related commands.

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

access-protocol

This command configures the access protocol parameters for the IuPS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

access-protocol sccp-network *sccp_net_id*
no access-protocol sccp-network

no

Removes a previously configured access protocol value.

sccp-network *sccp_net_id*

Specifies the Signaling Connection Control Part (SCCP) for this IuPS service to use.

sccp_net_id must be an integer from 1 to 16.

Usage Guidelines

Use this command to configure access protocol parameters for the current IuPS service.

Example

The following command specifies that the current Iu-PS service should use SCCP *1*:

```
access-protocol sccp-network 1
```

associate

This command associates a configured DSCP marking template with this IuPS service and associated Iu interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

associate dscp-template downlink *dscp_template_name*
no associate dscp-template downlink

no

Removes a previously configured association.

dscp_template_name

Specifies a DSCP marking template that was previously configured with the commands in the DSCP Template configuration mode.

dscp_template_name- Enter an alphanumeric string of 1 to 64 characters, including dots (.), dashes (-), and forward slashes (/), to identify a unique instance of a DSCP marking template.

Usage Guidelines

Use this command to associate a specific DSCP marking template with this IuPS service and associated Iu interface. The DSCP template provides a mechanism for differentiated services code point (DSCP) marking of control packets and signaling messages at the SGSN's M3UA level on the Iu interface. This DSCP marking enables the SGSN to perform classifying and managing of network traffic and to determine quality of service (QoS) for the interface to the IP network.

Example

The following command associates a DSCP marking template named *dscptemp1* with the Iu interface:

```
associate dscp-template downlink dscptemp1
```

The following command disassociates a previously associated DSCP marking template named *template4* with this IuPS service configuration:

```
no associate dscp-template downlink
```

blockedlist-timeout-gtpu-bind-addresses

This command specifies the time period that a GTP-U bind address (loopback address) will not be used (is blacklisted) in RAB-Assignment requests after a RAB assignment request, with that GTP-U bind address, has been rejected by an RNC with the cause - Unspecified Error. This is a failure at the RNC's GTP-U IP interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

In releases prior to StarOS 21.26:

```
blacklist-timeout-gtpu-bind-addresses seconds
default blacklist-timeout-gtpu-bind-addresses
no blacklist-timeout-gtpu-bind-addresses
```

From StarOS 21.26 and later releases:

```
blockedlist-timeout-gtpu-bind-addresses seconds
default blockedlist-timeout-gtpu-bind-addresses
no blockedlist-timeout-gtpu-bind-addresses
```

no

Disables the Blockedlisting timeout configuration.

default

Resets the blockedlist time to 60 seconds.

seconds

Number of seconds that the GTP-U bind (loopback) address will not be used in a RAB-Assignment request.

seconds : Must be an integer from 1 to 1800.

Usage Guidelines

Use this command to configure the blockedlist period.

Example

In releases prior to StarOS 21.26:

The following command specifies a 15 minutes (*460 seconds*) blacklist period.

blacklist-timeout-gtpu-bind-addresses 460

From StarOS 21.26 and later releases:

The following command specifies a 15 minutes (*460 seconds*) blacklist period.

blockedlist-timeout-gtpu-bind-addresses 460

empty-cr

This command allows the operator to determine how empty Connection Request messages will be handled.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

empty-cr procedure reject
[default | no] empty-cr procedure reject

default | no

Using either **default** or **no** with the command disables the rejection function and returns the system to the default behavior, which is to ignore receipt of the empty CRs.

Usage Guidelines

Use this command to enable/disable the procedure for handling empty (not containing dataparameters) Connection Request (CR) messages.

This feature can be used in the following scenario: During 4G to 3G handovers, some Connection Requests from mobile subscribers might be ignored by the SGSN, even though their UE would display that the WCDMA was available. The RNC would send an SCCP Connection Request (CR) over the Iu interface to the SGSN. Normally, this message contains a RANAP message and GMM, but according to 3GPP and ITU Q.713 standards, it is permissible to send an SCCP CR without any data parameters. In such a situation, normally the SGSN would ignore these SCCP CR messages, because without these data parameters the SGSN would be unable to derive the DeMux key which is the basis for determining the Session Manager instance to be used for a subscriber. Using this feature allows the SGSN to send a Reject to the mobile subscriber when an "empty" SCCP CR is sent from their UE.

Fields have been added to the output of the following CLI show commands to track the receipt and rejection of Connect Request (CR) messages:

- show gmm-sm statistics
- show gmm-sm statistics verbose

Example

The following command enables the empty CR handling procedure:

empty-cr procedure reject

The following command disables the empty CR handling procedure:

default empty-cr procedure reject

force-authenticate consecutive-security-failure

Disable/enable authentication when the MS/UE security fails and configures the procedures and frequency for authentication

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax Description

force-authenticate consecutive-security-failure { inter-sgsn-rau | local-messages count *frequency* **| non-local-messages count** *frequency* **}**
[default | no] force-authenticate consecutive-security-failure { inter-sgsn-rau | local-messages | non-local-messages }

default

Resets the values to defaults. Forced authentication is enabled for all the types of event procedures with the default values for determining frequency for authentication.

no

Disables the specified authentication configuration.

inter-sgsn-rau

Default: enabled

Enables/disables authentication for inter-SGSN RAU.

The SGSN does not remember previous inter-SGSN-RAU failures for a P-TMSI/RAI because the SGSN clears all contexts on the occurrence of an inter-SGSN-RAU security failure. So the next inter-SGSN-RAU can only be authenticated forcefully if it comes before the previous context is cleared. This type of forced authentication is enabled by default because this type of failure is fairly common.

local-messages count *frequency*

Default: 5

Enables/ disables authentication for local messages (such as local RAUs, Service Requests, Detach Requests, etc) . Consecutive security failures is fairly rare for local messages so the default count frequency is fairly

high, 5. Setting the count frequency enables the feature and sets the number of consecurity local message security failures that must occur prior t o authentication being forced.

frequency: Enter an integer from 1 to 10.

non-local-messages count *count*

Default: 1

Enables/ disables authentication for non-local messages (such as inter-RAT RAUs and all types of attaches) . Consecutive security failures for non-local messages is fairly common so the default count frequency is 1. Setting the count frequency enables the feature and sets the number of consecurity non-local message security failures that must occur prior t o authentication being forced.

frequency: Enter an integer from 1 to 10.

Usage Guidelines

GMM authentication is optional for UMTS. When GMM authentication is skipped, the SGSN and the MS continue to re-use the latest keys exchanged during the most recent GMM authentication procedure. This can result in the SGSN and the MS going out of sync with the CK and IK currently in use. If a mismatch occurs when the MS continues to use the correct parameters (e.g., cksn or P-TMSI signature) in the next Iu and if the SGSN skips authentication on the Iu, then, usually, the security mode will timeout or be rejected because the MS will not be able to decipher or perform an integrity check on the network messages. This scenario results in a lot of useless signaling in the network. This command allows the operator to enable a forced GMM authentication that will either resolve this type of problem or avoid it. As well, the operator can configure a frequency of authentication that best meets their needs.

Example

The following command enables forced authentication after every *3rd* local message security failure:

```
force-authenticate consecutive-security-failure local-messages count 3
```

gtpu

This commands configures parameters for the GTP user (GTP-U) dataplane.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
gtpu { bind ip_addr | echo-interval seconds | max-retransmissions number |
retransmission-timeout seconds | sync-echo-with-peer }
no gtpu { bind address ip_addr | echo-interval | max-retransmissions |
retransmission-timeout | sync-echo-with-peer }
```

```
default gtpu { echo-interval | max-retransmissions | retransmission-timeout
 | sync-echo-with-peer }
```

no

Removes the configured parameter value.

default

Sets the specified parameter to its default setting.

bind address *ip_addr*

This command binds the specified IP address to the Iu-PS GTP-U endpoint.

ip_addr: Must be an IP v4 IP address in dotted decimal notation.

echo-interval *seconds*

Default: 60

Configures the rate, in seconds, at which GTP-U echo packets are sent to the UTRAN over the Iu-PS interface.

seconds : Must be an integer from 60 through 3600.

max-retransmissions *number*

Default: 5

Configures the maximum number of transmission retries for GTP-U packets.

number : Must be an integer from 0 through 15.

retransmission-timeout *seconds*

Default: 5

Configures the retransmission timeout for GTPU packets in seconds.

seconds : Must be an integer from 1 through 20.

sync-echo-with-peer

This keyword is applicable to the SGSN only.

This keyword enables the SGSN to synchronize path management procedures with the peer after a GTP service restart recovery.

After GTP service recovery, the SGSN restarts the timers for GTP echo transmission, hence a drift in echo request transmission time (from the pre-recovery time) can occur causing the SGSN to be out of sync with the peer. By using this keyword, when the SGSN receives the first Echo Request (GTPC or GTPU) from the peer after the GTP service restart, in addition to replying with an ECHO Response, the SGSN transmits an ECHO Request to the peer and the SGSN restarts the timers associated with the path management procedures. This causes the path management procedure at SGSN to synchronize with the peer node.

Default: Enabled

Usage Guidelines

Use this command to configure GTP-U parameters for the Iu-PS interface.

Example

The following command binds the IP address *192.168.0.10* to the Iu-PS interface for communication with the UTRAN:

```
gtpu bind address 192.168.0.10
```

inter-rnc-procedures

This command enables the processing of SRNS relocation when the source RNC is behaving as the target RNC

Product

SGSN

Insert product and tag this paragraph appropriately.

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
[ no ] inter-rnc-procedures [ source-rnc-as-target-rnc |
use-old-location-info ]
```

no

Disables SRNS relocation when the source RNC is behaving as the target RNC. This is the default behavior.

source-rnc-as-target-rnc

Configures the SGSN to complete SRNS relocation when the source RNC is behaving as the target RNC. For example, in the case of a Femtocell-to-Femtocell handoff - the femtocell gateway may act both as the source and target RNC to the femtocells, although from the SGSN's perspective it is the same RNC.

use-old-location-info

Selects and uses the old values of LAC, RAC and SAC for S-CDRs and ULI information sent to the GGSN during an intra-SRNS procedure.

Usage Guidelines

Use this command to enable/disable SRNS relocation when the source RNC is behaving as the target RNC.

Example

Enter this command to enable SRNS relocation for those scenarios where the source RNC is behaving as the target RNC.

```
inter-rnc-procedures source-rnc-as-target-rnc
```

iu-hold-connection

Defines the type and duration of the Iu hold connection.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
iu-hold-connection [ always | requested-by-ms ] [ hold-time seconds ]
default iu-hold-connection
no iu-hold-connection
```

default

Resets the Iu hold connection parameters to requested-by-ms and 100 second duration.

no

Removes the configuration information for the specified Iu hold connection parameter.

always

Specifies that there is always to be an Iu hold connection procedure.

requested-by-ms

Specifies that there is only an Iu hold connection procedure if requested by the MS/UE.

This is the default setting for Iu-hold-connection.

hold-time *time*

This variable configures the interval (in seconds) that the SGSN holds the Iu connection.

time: must be an integer from 1 to 3600.

time: must be an integer from 10 to 3600.

Important It is recommended to use a minimum value of "10" seconds. If a value less than "10" seconds is used, more collisions may be observed. If the minimum value of "1" is set, after a re-load, INTRA-RAU (with unknown ptmsi, old-rai known) will be released in "1" second if the Identity Rsp does not come within "1" second.

Default is 100.

Usage Guidelines Define the amount of time the Iu connection will be held open.

Example

Instruct the SGSN to hold the Iu connection open for 120 seconds

```
iu-hold-connection always hold-time 120
```

iu-recovery

Important This command has been deprecated and is no longer available.

Product SGSN

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

iu-release-complete-timeout

Configures the SGSN's timer for waiting for an Iu Release Complete message from the RNC.

Product SGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
iu-release-complete-timeout time
default iu-release-complete-timeout
```

default

Resets the timer to its default setting.

time

This variable defines the amount of time (in seconds) that the SGSN waits to receive an 'Iu Release Complete' message from the RNC.

Default: 10.

time: Must be an integer from 1 to 60.

Usage Guidelines Configure the number of seconds that the SGSN waits to receive the Iu Release Complete message.

Example

Set the SGSN to wait 20 seconds for Iu-Release-Complete:

```
iu-release-complete-timeout 20
```

loss-of-radio-coverage ranap-cause

This command sets the detection cause included in the Iu Release message. This command is unique to releases 9.0 and higher.

Product SGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
loss-or-radio-coverage ranap-cause cause_number
default loss-of-radio-coverage ranap-cause
```

default

This keyword resets the configuration to the default cause ID number.

ranap-cause *cause_number*

This number identifies the reason the SGSN has detected, from Iu Release messages, for the loss of radio coverage (LORC). This value is included in the IE messages the SGSN sends to either the GGSN or the GGSN and the peer SGSN to indicate LORC state. The range of reasons is a part of the set defined by 3GPP 25413.

cause_number : Must be an integer from 1 to 512.

Default: 46 (MS/UE radio connection lost)

Usage Guidelines By defining a cause code, the SGSN knows to detect the LORC state of the mobile from Iu Release messages it receives for the subscriber. This configuration also instructs the SGSN to include the defined cause code for the LORC state in the IE portion of various messages sent to the GGSN and optionally the peer SGSN.

This command is one of the two commands required to enable the SGSN to work with the GGSN and, optionally the peer SGSN, to implement the Overcharging Protection feature (see the *SGSN Overview* in the *SGSN Administration Guide* for feature details. The other command needed to implement the Overcharging

Protection feature is the **gtp private extension** command explained in the *SGSN APN Policy Configuration Mode* chapter of the *Command Line Interface Reference*.

Example

Use the following command to set the cause code to indicate that there are no radio resources available in the target cell, cause *53*.

```
loss-or-radio-coverage ranap-cause 53
```

mbms

This command is in development for future use so the command and keywords that you might see are **not** currently supported.

network-sharing cs-ps-coordination

Enables/disables the SGSN service to perform a CS-PS coordination check.

Important With the release of 15.0, both 2G and 3G MOCN functionality is license controlled and the license is required to use all previously available network sharing SGSN configuration commands. For additional information, contact your Cisco Account Representative.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
network-sharing cs-ps-coordination [ homer | roamer ]
default network-sharing cs-ps-coordination
no network-sharing cs-ps-coordination
```

default

Including this keyword resets the SGSN service to allow the check to be performed.

no

Disables this CS-PS coordination checking for this IuPS service.

homer

Enables checking for CS-PS co-ordination for homers (UEs registered in the home network) only.

roamer

Enables checking for CS-PS co-ordination for roamers (UEs from outside the home network) only.

Usage Guidelines

Use this command to facilitate the network sharing functionality. With this command, the SGSN can be instructed to perform a check to determine if CS-PS coordination is needed.

3GPP TS 25.231 section 4.2.5 describes the functionality of the SGSN to handle CS-PS (circuit-switching/packet-switching) coordination for attached networks not having a Gs-interface. In compliance with the standard, the SGSN rejects an Attach in a MOCN configuration with cause 'CS-PS coordination required', after learning the IMSI, to facilitate the RNC choosing the same operator for both CS and PS domains.

Example

Use the following syntax to disable the CS-PS coordination check:

```
no network-sharing cs-ps-coordination
```

Use the following command to enable the CS-PS coordination check only for UEs from outside the home network:

```
no network-sharing cs-ps-coordination roamer
```

network-sharing failure-code

Configure the reject cause code to included in network-sharing Reject messages.

Important With the release of 15.0, both 2G and 3G MOCN functionality is now license controlled and the license is required to use all previously available network sharing SGSN configuration commands. For additional information, contact your Cisco Account Representative.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

network-sharing failure *failure_code*
default network-sharing failure

default

Resets the SGSN service to use the default cause code,14 (GPRS services not allowed in this PLMN).

failure_code

Enter one of the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state

- 111 - Protocol error, unspecified

Usage Guidelines Use this command to determine which failure code will be included in Reject messages sent by the SGSN when there is a network-sharing failure.

Example

Use the following syntax to indicate that roaming is not allowed (*#13*) as the cause for the network-sharing failure:

```
network-sharing failure 13
```

network-sharing non-shared

This command allows non-shared area access when network-sharing is enabled.

Product SGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
network-sharing non-shared
[ default | no ] network-sharing non-shared
```

default

Resets the default to disable non-shared access.

Usage Guidelines When non-shared area access is enabled, the SGSN sends the selected-plmn value in Attach/RAU accept if LAI is having one of the selected-plmn and "selected-plmn" or "Redirect-attempt flag" IEs are not included in the request message.

Example

Disable non-shared area access if it has already been configured:

```
no network-sharing non-shared
```

network-sharing stop-redirect-reject-cause

Enables the operator to disable the default behavior which sends Redirection Indication IE in RANAP Reject messages when reject is due to GMM cause #17 (network failure) related to System Failure or Unexpected

Data value MAP errors from the HLR. This change of the default behavior would only be applicable to 3G Roamers.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

network-sharing stop-redirect-reject-cause network-failure
{ default | no } network-sharing stop-redirect-reject-cause

default

Instructs the SGSN to use the default behavior and send redirect indication in Attach Reject or RAU Reject if reject is due to GMM cause 'network failure' which resulted from one of the MAP errors unexpected data value or system failure.

no

Disables this function and returns to the default behavior.

Usage Guidelines

With this command, the operator would change the SGSN's default behavior (complies with 3GPP Release 11) for roaming subscribers and send Redirection Complete IE in Attach and RAU Reject messages when the reject is due to GMM cause #17 (network failure) in response to receiving System Failure or Unexpected Data value MAP errors from the HLR

Example

Configure the SGSN to send Redirect Indication IE in RANAP reject messages:

default network-sharing stop-redirect-reject-cause

plmn

Configures the PLMN (public land mobile network) related parameters for the IuPS service. This command is appicable to releases 8.1 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

plmn id mcc *mcc_num* **mnc** *mnc_num* **[network-sharing common-plmn mcc** *mcc_num* **mnc** *mnc_num* **[plmn-list mcc** *mcc_num* **mnc** *mnc_num* **[mcc** *mcc_num* **mnc** *mnc_num***+]]]**
no plmn id

no

Removes the PLMN ID from the configuration.

id

Creates a PLMN configuration instance based on the PLMN ID (comprised of the MCC and MNC). In accordance with TS 25.413, the SGSN supports up to 32 PLMN configurations for shared networks.

mcc *mcc_num*

Specifies the mobile country code (MCC) portion of the PLMN's identifier.

mcc_num: The PLMN MCC identifier and can be configured to any integer value between 100 and 999.

mnc *mnc_num*

Specifies the mobile network code (MNC) portion of the PLMN's identifier.

mnc_num: The PLMN MNC identifier and can be configured to any 2-digit or 3-digit value between 00 and 999.

network-sharing common-plmn mcc *mcc_num* mnc *mnc_num*

When network sharing is employed, this set of keywords is required to define the PLMN Id of the common PLMN. The common PLMN is usually not the same as the local PLMN.

Important With the release of 15.0, both 2G and 3G MOCN functionality is now license controlled and the license is required to use all previously available network sharing SGSN configuration commands. For additional information, contact your Cisco Account Representative.

plmn-list mcc *mcc_num* mnc *mnc_num*

When network sharing is employed and more than two PLMNs are available, then use the **plmn-list** keyword to begin a list of all additional PLMNs.

Usage Guidelines

Use this command to configure the PLMN associated with the SGSN. There can only be one PLMN associated with an SGSN unless one of the following features is enabled and configured: network sharing or multiple PLMN.

For network sharing, use of the **network-sharing** keywords make it possible to identify more than one PLMN. Including the PLMN identified initially. None have precedence. They are all treated equally but they must each be unique. In a MOCN configuration, the PLMN list will not be used as there would only be one local PLMN.

For multiple PLMN support, the SGSN can support up to 8 Iu-PS configurations for PLMNs. These Iu-PS service configurations must be associated with the SGSN via the **ran-protocol** command in the SGSN Service configuration mode.

Example

Use the following command to identify a PLMN by the MCC *313* and MNC *23* and instruct the SGSN to perform network sharing with a single *common PLMN* identified by MCC *404* and MNC *123*:

```
plmn id mcc 313 mnc 23 network-sharing common-plmn mcc 404 mnc 123
```

rab-assignment-response-timeout

Configures the RAB assignment timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

rab-assignment-response-timeout *time*
default rab-assignment-response-timeout

default

Resets the timer to its default setting.

time

This variable configures the amount of time (in seconds) that the SGSN waits to receive a RAB assignment from the RNC.

time: must be an integer from 1 to 60.

Default: 8.

Usage Guidelines

This command defines time the SGSN waits for the completion of the RAB assignment procedure.

Example

Change the timer setting to *11* seconds.

```
rab-assignment-response-timeout 11
```

radio-network-controller

This command creates an instance of an RNC configuration to associate with the IuPS service for the SGSN. This command is only available in release 8.0; use the **rnc** command for releases 8.1 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

radio-network-controller id *rnc_id* **mcc** *mcc_num* **mnc** *mnc_num*
no radio-network-controller id *rnc_id* **mcc** *mcc_num* **mnc** *mnc_num*

no

Removes the configuration information for the specified RNC.

id *rnc_id*

Define the instance number of the RNC configuration.

rnc_id : Must be an integer from 0 to 4095.

mcc *mcc_num*

Specifies the mobile country code (MCC).

mcc_num : Must be an integer between 100 and 999.

mnc *mnc_num*

Specifies the mobile network code (MNC).

mnc_num : Must be an integer between 00 and 999.

Usage Guidelines

Use this command to configure information for the IuPS service to use to contact specific RNCs.

This command also provides access to the RNC configuration mode.

Example

The following command creates or accesses RNC configuration instance *#1* with MCC of *131* and MNC of *22*:

```
radio-network-controller id 1 mcc 131 mnc 22
```

rai-skip-validation

Enable or disable if validation checks are done to verify the MCC and MNC fields received in the old RAI IE in Attach/RAU Requests.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

`[ no ] rai-skip-validation`

no

Disables skipping the validation of the old RAI MCC/MNC fields and enables the default behavior to validate.

Usage Guidelines

This command configures the SGSN to enable or disable rejection of RAU requests with invalid MCC/MNC values in the old RAI field. By default, this configuration is disabled allowing the default behavior to validate the old RAI MCC/MNC fields.

This command also impacts the PTMSI attaches where the old RAI field is invalid. If the OLD RAI field is invalid and if the validation is enabled, the identity of the MS is requested directly from the MS instead of the peer SGSN.

Validation checks are done per 3GPP TS 24.008 for the MCC/MNC fields of the old RAI IE in Attach/RAU Requests. RAU requests with invalid MCC/MNC values in the old RAI field are rejected. For Attach requests with invalid MCC/MNC values in the old RAI field, the identity of the MS is retrieved directly from the MS instead of sending an identity request to the peer Node where the MS identity is derived from the valid old-RAI.

Example

Use this command to configure rejection of RAU requests with invalid MCC/MNC values in the old RAI field:

`no rai-skip-validation`

relocation-alloc-timeout

This command defines the amount of time the SGSN waits for a Relocation Request message.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

relocation-alloc-timeout *timeout_value*
default relocation-alloc-timeout

default

Resets the configuration to a 5 second wait time.

timeout_value

Time in seconds that the SGSN waits to receive a Relocation Request message.

timeout_value : Must be an integer from 1 to 60.

Default : 5 seconds.

Usage Guidelines

Use this command to configure the number of seconds the SGSN will wait for a Relocation Request message to be received. This timeout needs to be set with sufficient time so that SRNS procedure aborts can be avoided if the peer fails to respond in a timely fashion in the case of a hard handoff.

Example

The following command sets the wait time to *10* seconds.

relocation-alloc-timeout 10

relocation-complete-timeout

This command specifies the maximum time for the SGSN to wait for a Relocation Completion from the core network.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

relocation-complete-timeout *timeout_value*
default relocation-complete-timeout

default

Resets the configuration to a 5 second wait time.

timeout_value

Time in seconds that the SGSN waits for relocation to be completed.

timeout_value : Must be an integer from 1 to 60.

Default : 5 seconds.

Usage Guidelines

Use this command to configure the number of seconds the SGSN will wait for a relocation to be completed. This timeout needs to be set with sufficient time so that SRNS procedure aborts can be avoided if the peer fails to respond in a timely fashion in the case of a hard handoff.

Example

The following command sets the wait time for *10* seconds.

```
relocation-complete-timeout 10
```

reset

Defines the configuration specific to the RESET procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
reset { ack-timeout time | guard-timeout time | max-retransmissions retries
 | sgsn-initiated }
default reset { ack-timeout | guard-timeout | max-retransmissions |
sgsn-initiated }
no reset sgsn-initiated
```

default

Returns to the default settings for the Reset procedure.

no

Removes the SGSN-initiated reset procedure from the configuration.

ack-timeout *time*

Configures the interval (in seconds) for which the SGSN waits for RESET-ACK from the RNC.

time must be an integer from 5 to 60.

Default: 20.

guard-timeout

Configures the interval (in seconds) after which the SGSN sends RESET-ACK to the RNC.

time must be an integer from 5 to 60.

Default : 10

max-retransmissions

Configures maximum retries for RESET message.

retries must be an integer from 0 to 2.

Default: 1.

sgsn-initiated

Enables SGSN initiated RESET procedure.

Default: disabled.

Usage Guidelines

Configures the parameters that determine a RESET.

Example

Use the following to have the SGSN initiate the RESET procedure:

```
reset sgsn-initiated
```

rnc

This command creates or accesses an instance of an RNC (radio network controller) configuration.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

rnc id *rnc_id*
no rnc id *rnc_id*

no

Removes the configuration information for the specified RNC.

id *rnc_id*

Set the identification number of the RNC configuration instance.

rnc_id : Must be an integer from 0 to 4095 for 8.1 releases. Must be an integer from 0 to 65535 for releases 9.0 and higher.

Usage Guidelines

Use this command to configure information for the IuPS service to use to contact specific RNCs.

This command also provides access to the RNC configuration mode.

Example

The following command creates an RNC configuration instance *#3442*:

```
rnc id 3442
```

security-mode-complete-timeout

This command configures the security mode timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

security-mode-complete-timeout *time*
default security-mode-complete-timeout

default

Resets the timer configuration to the default settings.

time

Configures the interval (in seconds) the SGSN waits for the security mode from the MS to complete.

time must be an integer from 1 to 60.

Default is 5

Usage Guidelines

Use this command to configure the timer that determines how long the SGSN waits for a Security Mode Complete message from the MS (mobile station).

Example

Instruct the SGSN to wait *7* seconds:

```
security-mode-complete-timeout 7
```

service-request-follow-on

Instructs the SGSN not to release an Iu immediately.

Product

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
[ default | no ] service-request-follow-on
```

default

Resets the configuration to the default, this function is enabled.

no

Disables this function so that Iu is released without waiting for the Iu-Hold-Timer to expire.

Usage Guidelines

For an Iu established as the result of a Service Request (signaling), the SGSN, by default, waits for the Iu-Hold-Timer to expire.

Use this command with the 'no' prefix to disable this function.

Use this command with the 'default' prefix or without any prefix if the configuration was modified previously with by **no service-request-follow-on**.

Example

Disable this function to wait for the Iu-Hold-Timer to expire:

no service-request-follow-on

Enable this function if it was previously disabled:

service-request-follow-on

srns-context-response-timeout

This command configures the SGSN context response timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

srns-context-response-timeout *time*
default srns-context-response-timeout

default

Resets the timer configuration to the default setting.

time

Configures the interval (in seconds) for which the SGSN waits for an SRNS Context Request message.

time must be an integer from 1 to 60.

Default: 5.

Usage Guidelines

Configures the time to wait before the SGSN sends a response to the SRNS Context-Request message.

Example

Configure the SGSN to wait *7* seconds for an SRNS Context-Request response:

srns-context-response-timeout 7

tigoc-timeout

This command configures the TigOc interval.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

tigoc-timeout *time*
default tigoc-timeout

default

Resets the timer configuration to the default setting.

time

This command sets the time in seconds.

time : Must be an integer from 1 to 60.

Default: 5.

Usage Guidelines

Define the amount of time that the SGSN ignores any overload messages for TigOc interval after receiving one overload message from the RNC.

Example

Use the following command to change the default TigOc interval to *4* seconds:

tigoc-timeout 4

tintc-timeout

This command configures the TinTc interval..

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

tintc-timeout *time*
default tintc-timeout

default

Resets the timer configuration to the default setting.

time

Set the number of seconds to wait.

time : Must be an integer from 1 to 60.

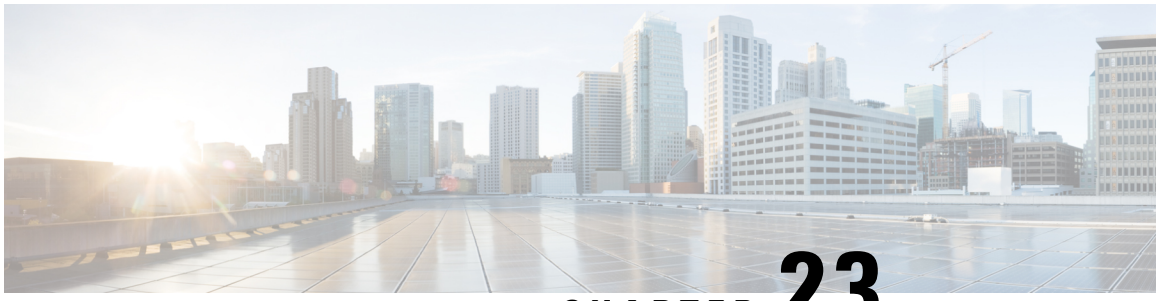
Default: 30.

Usage Guidelines

Define *4* as the number of seconds that the SGSN waits before decrementing (by one) the traffic level of the RNC.

Example

```
tintc-timeout 4
```



CHAPTER 23

LAC Service Configuration Mode Commands

The LAC Service Configuration Mode is used to create and manage L2TP services within contexts on the system. L2TP Access Concentrator (LAC) services facilitate tunneling to peer L2TP Network Servers (LNSs).

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

allow

This command configure the system to allow different attributes in the LAC Hostname Attribute Value Pair (AVP) and Called-Number AVP for L2TP messages exchanged between LAC and LNS.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
allow { aaa-assigned-hostname | called-number value apn | calling-number
 value imsi }
default allow { aaa-assigned-hostname | called-number value apn }
no allow { aaa-assigned-hostname | called-number value apn | calling-number
 }
```

no

Disable the configured attribute and returns to the behavior that uses the LAC-Service name as the HostName AVP.

aaa-assigned-hostname

When enabled if AAA assigns a valid Tunnel-Client-Auth-ID attribute for the tunnel, it is used as the HostName AVP in the L2TP tunnel setup message.

This keyword works in conjunction with the **local-hostname** *hostname* keyword applied via the **tunnel l2tp** command in APN Configuration mode.

When Tunnel parameters are not received from the RADIUS Server, Tunnel parameters configured in an APN are considered for the LNS peer selection. When APN configuration is selected, the local-hostname configured with the **tunnel l2tp** command in the APN for the LNS peer will be used as an LAC Hostname.

called-number value apn

Configures the system to send the APN name in the Called-Number AVP as a part of ICRQ message sent to the LNS. If this keyword is not configured, Called-Number AVP will not be included in ICRQ message sent to the LNS.

calling-number value imsi

Configures the system to allow the IMSI to be used as Calling-Number as a part of ICRQ message sent to the LNS. If this keyword is not configured, then MSISDN will be used as Calling-Number.

Important This is a customer-specific keyword available for PDSN. Please contact your local Cisco sales representative for more information.

Usage Guidelines

Use this command to configure the attribute for the HostName AVP for L2TP messages exchanged between LAC and LNS.

LAC Hostname will be different for the subscribers corresponding to the different corporate APNs. In the absence of a AAA assigned HostName, the LAC-Service name is used as HostName. By default the LAC-Service name is used as the HostName AVP.

Example

The following command enables the use of the value of Tunnel-Client-Auth-ID attribute for the HostName AVP:

```
allow aaa-assigned-hostname
```

Use the following command to reset the behavior so that the LAC-Service uses the LAC-Service name as the HostName AVP:

```
no allow aaa-assigned-hostname
```

bind

This command assigns a local end point address to the LAC service in the current context.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

bind *ip_address* **[max-subscribers]**
no bind *ip_address*

no

Unassign, or unbind, the local end point to the LAC service.

ip_address

This must be a valid IP address entered using IPv4 dotted-decimal notation.

max-subscribers

The maximum number of subscribers that can use the endpoint for this LAC service. Must be an integer from 1 to 2500000.

Usage Guidelines

Use this command to bind a local end point IP address to the LAC service.

Example

The following command binds the local end point IP address *209.165.200.234* to the LAC service in the current context:

```
bind 209.165.200.234
```

The following command removes the binding of the local end point to the LAC service:

```
no bind
```

data sequence-number

Enables data sequence numbering for sessions that use the current LAC service. Data sequence numbering is enabled by default.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description `[ no ] data sequence-number`

no

Disables data sequence numbering for sessions.

Usage Guidelines An L2TP data packet header has an optional data sequence numbers field. The data sequence number may be used to ensure ordered delivery of data packets. This command is used to re-enable or disable the use of the data sequence numbers for data packets.

Example

Use the following command to disable the use of data sequence numbering:

```
no data sequence-number
```

Use the following command to re-enable data sequence numbering:

```
data sequence-number
```

default

This command sets the specified LAC service parameter to its default value or setting.

Product GGSN

PDSN

P-GW

SAEGW

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
default { data sequence-number | hide-attributes | keepalive-interval |
load-balancing | local-receive-window | max-retransmission |
max-session-per-tunnel | max-tunnel-challenge-length | max-tunnels |
proxy-lcp-authentication | retransmission-timeout-first |
retransmission-timeout-max | trap all | tunnel-authentication }
```

data sequence-number

Enables data sequence numbering for sessions.

hide-attributes

Disables hiding attributes in control messages sent from the LAC to the LNS.

keepalive-interval

Sets the interval for send L2TP Hello keepalive if there is no control or data transactions to the default value of 60 seconds.

load-balancing

Sets the load balancing algorithm to be used when many LNS peers have been configured to the default of round robin.

local-receive-window

Sets the window size to be used for the local side for the reliable control transport to the default of 16.

max-retransmission

Sets the maximum number of retransmissions to the default of 5.

max-session-per-tunnel

Sets the maximum number of sessions per tunnel at any point in time to the default of 512.

max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge to the default of 16 bytes.

max-tunnels

Sets the maximum number of tunnels for this service to the default of 32000.

proxy-lcp-authentication

Sets sending of proxy LCP authentication parameters to the LNS to the default state of enabled.

retransmission-timeout-first

Sets the first retransmit interval to the default of 1 second.

retransmission-timeout-max

Sets the maximum retransmit interval to the default of 8 seconds.

trap all

Generates all supported SNMP traps.

tunnel-authentication

Sets tunnel authentication to the default state of enabled.

Usage Guidelines

Use the default command to set LAC service parameters to their default states.

Example

Use the following command to set the keep alive interval to the default value of 60 seconds:

```
default
keepalive-interval
```

Use the following command to set the maximum number of sessions per tunnel to the default value of 512:

```
default max-session-per-tunnel
```

hide-attributes

Enables hiding certain attributes (such as proxy-auth-name and proxy-auth-rsp) in control messages sent from the LAC to the LNS. The LAC hides such attributes only if tunnel authentication is enabled between the LAC and the LNS.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] hide-attributes
```

no

Disable hiding attributes.

Usage Guidelines

Use this command to hide certain attributes from control messages when tunnel authentication is enabled between the LAC and the LNS.

Example

The following command enables hiding attributes:

```
hide-attributes
```

keepalive-interval

This command specifies the amount of time to wait before sending a Hello keep alive message.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

keepalive-interval *seconds*
no keepalive-interval

no

Disables the generation of Hello keepalive messages on the tunnel.

seconds

Default: 60

The number of seconds to wait before sending a Hello keepalive message. The number can be configured to an integer from 30 to 2147483648.

Usage Guidelines

Use this command to set the amount of time to wait before sending a Hello keepalive message or disable the generation of Hello keep alive messages completely. A keepalive mechanism is employed by L2TP in order to differentiate tunnel outages from extended periods of no control or data activity on a tunnel. This is accomplished by injecting Hello control messages after a specified period of time has elapsed since the last data or control message was received on a tunnel. As for any other control message, if the Hello message is not reliably delivered then the tunnel is declared down and is reset. The transport reset mechanism along with the injection of Hello messages ensures that a connectivity failure between the LNS and the LAC is detected at both ends of a tunnel.

Example

Use the following command to set the Hello keepalive message interval to *120* seconds:

```
keepalive-interval 120
```

Use the following command to disable the generation of Hello keepalive messages:

```
no keepalive-interval
```

load-balancing

Configures how LNSs are selected for this LAC service.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`load-balancing { balanced | prioritized | random }`

balanced

LNS selection is made without regard to prioritization, but in a sequential order that balances the load across the total number of LNS nodes available.

prioritized

LNS selection is made based on the priority assigned in the Tunnel-Preference attribute. An example of this method is three LNS nodes, with preferences of 1, 2, and 3 respectively. In this example, the RADIUS server always tries the tunnel with a preference of 1 before using any of the other LNS nodes.

random

Default: Enabled

LNS selection is random in order, wherein the RADIUS server does not use the Tunnel-Preference attribute in determining which LNS to select.

Usage Guidelines

Use this command to configure the load-balancing algorithm that defines how the LNS node is selected by the LAC when there are multiple peer LNSs configured in the LAC service.

Example

The following command sets the LAC service to connect to LNSs in a sequential order;

`load-balancing balanced`

The following command sets the LAC service to connect to LNSs according to the priority assigned through the Tunnel-Preference attribute:

`load-balancing prioritized`

local-receive-window

Specifies the number of control messages the remote peer LNS can send before waiting for an acknowledgement.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

local-receive-window *integer*

integer

Default: 4

Specifies the number of control messages to send before waiting for an acknowledgement. The number can be configured to an integer from 1 to 256.

Usage Guidelines

Use this command to set the size of the control message receive window being offered to the remote peer LNS. The remote peer LNS may send the specified number of control messages before it must wait for an acknowledgment.

Example

The following command sets the local receive window to *10* control messages:

```
local-receive-window 10
```

max-retransmission

Sets the maximum number of retransmissions of a control message to a peer before the tunnel and all sessions within it are cleared.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-retransmission *integer*

integer

Default: 5

Specifies the maximum number of retransmissions of a control message to a peer. This value must be an integer from1 through 10.

Usage Guidelines

Each tunnel maintains a queue of control messages to be transmitted to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. If no peer response is detected after the number of retransmissions set by this command, the tunnel and all sessions within are cleared.

Use this command to set the maximum number of retransmissions that the LAC service sends before closing the tunnel and all sessions within. it.

Example

The following command sets the maximum number of retransmissions of a control message to a peer to *7*:

```
max-retransmissions 7
```

max-session-per-tunnel

Sets the maximum number of sessions that can be facilitated by a single a tunnel at any time.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-sessions-per-tunnel *integer*

integer

Default: 512

The maximum number of sessions expressed as an integer from 1 through 65535.

Usage Guidelines

Use this command to set the maximum number of sessions you want to allow in a tunnel.

Example

The following command sets the maximum number of sessions in a tunnel to *5000*:

```
max-sessions-per-tunnel 5000
```

max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge in bytes.The challenge is used for tunnel authentication purposes during tunnel creation.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-tunnel-challenge-length *bytes*

bytes

Default: 16

Specifies the maximum length (in bytes of the tunnel challenge. This must be an integer from 4 through 32.

Usage Guidelines

Use this command to set the maximum length (in bytes) for the tunnel challenge that is used during tunnel creation.

Example

The following command sets the maximum length of the tunnel challenge to *32* bytes:

```
max-tunnel-challenge-length 32
```

max-tunnels

The maximum number of tunnels that the current LAC service can support.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-tunnels *integer*

integer

Default: 32000

The maximum number of tunnels expressed as an integer from 1 through 32000.

Usage Guidelines

Use this command to set the maximum number tunnels that this LAC service can support at any on time.

Example

Use the following command to set the maximum number of tunnels for the current LAC service to *20000*:

```
max-tunnels 20000
```

peer-lns

Adds a peer LNS address for the current LAC service. Up to eight peer LNSs can be configured for each LAC service.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

peer-lns *ip_address* **[encrypted] secret** *secret* **[crypto-map** *map_name* **{ [encrypted] isakmp-secret** *secret* **}] [description** *text* **] [preference** *integer* **]**
no peer-lns *ip_address*

no peer-lns *ip_address*

Deletes the peer LNS at the IP address specified by *ip_address*. *ip_address* must be entered in IPv4 dotted-decimal notation.

ip_address

The IP address of the peer LNS for the current LAC service. *ip_address* must be entered in IPv4 dotted-decimal notation.

[encrypted] secret *secret*

Designates the secret which is shared between the current LAC service and the peer LNS. *secret* must be an alphanumeric string of 1 through 256 characters that is case sensitive.

encrypted secret *secret*: Specifies that encryption should be used when communicating the secret with the peer LNS.

crypto-map *map_name* { [encrypted] isakmp-secret *secret* }

map_name is the name of a crypto map that has been configured in the current context. *map_name* must be an alphanumeric string of 1 through 127 characters that is case sensitive.

isakmp-secret *secret*: The pre-shared key for IKE. *secret* must be an alphanumeric string of 1 through 127 characters that is case sensitive.

encrypted isakmp-secret *secret*: 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.

description *text*

Specifies the descriptive text to use to describe the specified peer LNS. *text* must be an alphanumeric string of 0 through 79 characters.

preference *integer*

This sets the priority of the peer LNS if multiple peer LNSs are configured. *integer* must be an integer from 1 through 128.

Usage Guidelines

Use this command to add a peer LNS address for the current LAC service.

Example

The following command adds a peer LNS to the current LAC service with the IP address of *10.10.10.100*, sets encryption on, specifies the shared secret to be *1b34nnf5d*, and sets the preference to *3*:

```
peer-lns 10.10.10.100 encrypted secret 1b34nnf5d preference 3
```

The following command removes the peer LNS with the IP address of *209.165.200.244* for the current LAC service:

```
no peer-lns 209.165.200.244
```

proxy-lcp-authentication

Enables and disables the sending of proxy LCP authentication parameters to the LNS.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] proxy-lcp-authentication
```

no

Disables the sending of proxy LCP authentication parameters to the LNS.

proxy-lcp-authentication

Default: Enabled

Enables the sending of proxy LCP authentication parameters to the LNS.

Usage Guidelines Use this feature in situations where the peer LNS does not understand the proxy LCP Auth AVPs that the system sends and does not do an LCP renegotiation and tears down the call.

Example

Use the following command to disable the sending of proxy LCP authentication parameters to the LNS;

```
no proxy-lcp-authentication
```

Use the following command to re-enable the sending of proxy LCP authentication parameters to the LNS:

```
proxy-lcp-authentication
```

retransmission-timeout-first

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. This command sets the initial timeout for retransmission of control messages.

Product GGSN

PDSN

P-GW

SAEGW

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **retransmission-timeout-first** *integer*

integer

Default: 1

The amount of time to wait (in seconds) before sending the first control message retransmission. This must be an integer from 1 through 100.

Usage Guidelines Use this command to set the initial timeout before retransmitting control messages to the peer.

Example

The following command sets the initial retransmission timeout to *3* seconds:

```
retransmission-timeout-first 3
```

retransmission-timeout-max

Configures maximum amount of time between two retransmission of control messages.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

retransmission-timeout-max *integer*

integer

Default: 8

integer is the maximum time (in seconds) to wait before retransmitting control messages expressed as e an integer from 1 through 100.

Usage Guidelines

Use this command to set the maximum amount of time that can elapse before retransmitting control messages.

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval.

Example

The following command sets the maximum retransmission time-out to *10* seconds:

```
retransmission-timeout-max 10
```

single-port-mode

This command enables/disables the L2TP LAC service always to use standard L2TP port 1701 as source port for all L2TP control and data packets originated from LAC node.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] single-port-mode

default

Default: Enabled

Sets this command to its default state of disabled. By default single source port configuration for L2TP LAC packets is disabled.

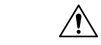
no

Disables the configured single source port configuration from this LAC service.

Usage Guidelines

Use this command to enable or disable the single port mode for L2TP LAC service.

If this feature is enabled, then L2TP LAC service will always use standard L2TP port 1701 as source port for all L2TP control/data packets originated from LAC (instead of the default scheme in which each L2TPMgr uses a dynamic source port). L2TPMgr instance 1 will handle all L2TP calls for the service.



Caution Changing this configuration, while the service is already running, will cause restart of the service.

Example

The following command enables the LAC service to use port 1701 as source port for all L2TP control and data packets:

single-port-mode

snoop framed-ip-address

When enabled, this feature allows the LAC to detect IP Control Protocol (IPCP) packets exchanged between the mobile node and the LNS and extract the framed-ip-address assigned to the mobile node. The address will be reported in accounting start/stop messages and displayed for subscriber sessions.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] snoop framed-ip-address

default

Disabled.

no

Disables the feature. Accounting start/stop will occur before the PPP session is established and the framed IP address field will be reported as 0.0.0.0.

Usage Guidelines

This feature is available to address simple IP roaming scenarios. If this feature is enabled, the Accounting Start will be sent only after the framed-ip-address is detected. If the framed-ip-address is not detected within 16 seconds, an Accounting Start will be sent for the session with the 0.0.0.0 address. If the session is disconnected during the detection attempt, Accounting Start/Stop will be sent for the session. If the session renegotiates IPCP, an Accounting Stop will be generated with a framed-ip-address from the old session, and an Accounting Start will be generated with an IP address for the new session. IPv6 address detection is not supported.

Important When this feature is enabled and the show subscribers all command is invoked, the framed-IP-address is displayed for the PDSN Simple IP subscriber in the output display.

trap

This command generates SNMP traps.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] trap all
```

no

Disables SNMP traps.

Usage Guidelines

Use this command to enable/disable all supported SNMP traps.

Example

To enable all supported SNMP traps, enter the following command:

```
trap all
```

tunnel selection-key

Enables the creation of tunnels between an L2TP service and an LNS server on the basis of a key received from AAA server.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
tunnel selection-key { none | tunnel-client-auth-id | tunnel-server-auth-id
 }
default tunnel selection-key
```

default

Disables the creation of tunnel between LAC service and LNS based on a key value received from AAA server.

none

Default: Enabled

This keyword disables the creation of multiple tunnels between a pair of LAC service and LNS server. LAC will not make use of the key to choose a tunnel with LNS in this setup.

tunnel-client-auth-id

Default: Disabled

This keyword enables the creation of tunnels between LAC service and an LNS server on the basis of domain attribute "Tunnel-Client-Auth-ID" value received from AAA server.

tunnel-server-auth-id

Default: Disabled

This keyword enables the creation of tunnels between LAC service and an LNS server on the basis of domain attribute "Tunnel-Server-Auth-ID" value received from AAA server.

Usage Guidelines

Use this command to enable or disable the creation of additional L2TP tunnels between LAC service and LNS server on the basis of "Tunnel-Client-Auth-ID" or "Tunnel-Server-Auth-ID" attribute value received from AAA Server in Access-Accept message. This value of attribute is treated as a key for tunnel selection and creation.

When the LAC needs to establish a new L2TP session, it first checks for an existing L2TP tunnel with the peer LNS based on the value of the key configured. If no such tunnel exists for the key, it will create a new tunnel with the LNS.

The default configuration has the selection-key as **none**. Hence, LAC will not make use of key to choose a tunnel with LNS in default setup.

The maximum number of sessions, as configured via the **max-sessions-per-tunnel** command, is applicable for each tunnel created through this command. By default, each tunnel supports 512 sessions.

If the LAC service needs to establish a new tunnel for a new L2TP session with LNS and the tunnel create request fails because maximum tunnel creation limit is reached, LAC will try other LNS addresses received from AAA server in Access-Accept message for the APN/subscriber. If all available peer-LNS are exhausted, LAC service will reject the call.

Example

The following command enables the use of "Tunnel-Server-Auth-ID" attribute value received from AAA Server in Access-Accept message as a key for tunnel selection and creation:

```
tunnel selection-key tunnel-server-auth-id
```

tunnel-authentication

Enables tunnel authentication. When tunnel authentication is enabled, a configured shared secret is used to ensure that the LAC service is communicating with an authorized peer LNS. The shared secret is configured by the **peer-lns** command in the LAC Service Configuration mode, the **tunnel l2tp** command in the Subscriber Configuration mode, or the **Tunnel-Password** attribute in the subscribers RADIUS profile.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] tunnel-authentication

no

Disables tunnel authentication.

Tunnel authentication is enabled by default.

Usage Guidelines

Disable or enable the usage of secrets to authenticate a peer LNS when setting up a tunnel.

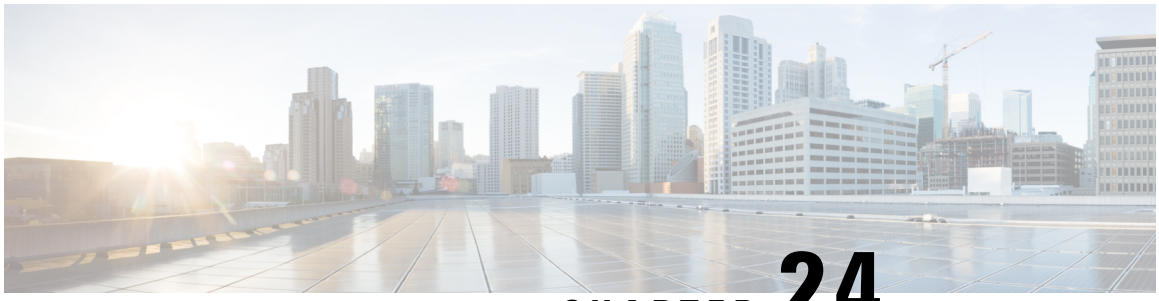
Example

To disable tunnel authentication, use the following command:

no tunnel-authentication

To re-enable tunnel authentication, use the following command:

tunnel-authentication



CHAPTER 24

Line Configuration Mode Commands

The Line Configuration Mode is used to manage the terminal line characteristics for output formatting.

Command Modes

Exec > Global Configuration > Line Configuration

configure > line

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-line)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

length

Configures the output for the display's length (number of rows).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Line Configuration

configure > line

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-line)#
```

Syntax Description **`[ default ] length`** *`number`*

default

Restores the default value for the number of rows (length) that will be displayed in the output.

number

Specifies the number of rows (lines) of output that can be displayed on the terminal. *number* must be 0 or an integer from 5 through 512, where the special value 0 implies an infinite number of rows.

Usage Guidelines Use this command to set the display terminal's output length other than the default. The special infinite value (0) is typically used when logging the output of a session from a remote machine since this will result in no pagination of output.

Example

The following command sets the length of the display to *33* rows.

```
length 33
```

width

Configures the output for the displays width (number of characters in a single row).

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Line Configuration

configure > line

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-line)#
```

Syntax Description **`[ default ] width`** *`number`*

default

Restores the default value for the number of characters in a single row (width) that will be displayed in the output on the terminal.

number

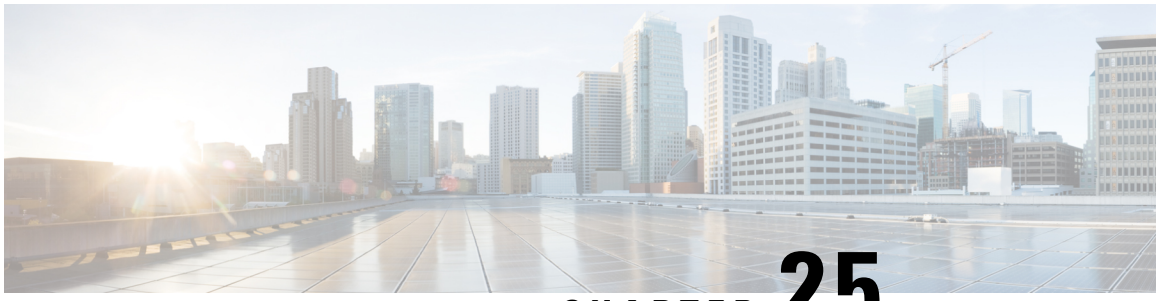
Specifies the number of characters in a single row that can be displayed on the terminal. *number* must be an integer from 5 through 512.

Usage Guidelines Use this command to set the display terminal's output width other than the default.

Example

The following command sets the width of the display to *75* characters.

```
width 75
```



CHAPTER 25

Link Configuration Mode Commands

Command Modes

The Link configuration mode defines the MTP3 link parameters for a specific link in a linkset of an SS7 routing domain instance.

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

arbitration

This command configures link arbitration.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

```
arbitration { active | passive }
no arbitration
```

no

Removes the arbitration configuration for the link.

active

The SSCOP initiates the transmission of PDUs.

passive

The SSCOP waits to receive PDUs.

Usage Guidelines

Sets the configuration to initiate transmission of PDUs.

Example

```
arbitration active
```

mtp2-aerm-emergency-threshold

Configure the alignment error rate monitor (AERM) emergency threshold value. This command is only available for a lowspeed-narrowband link-type.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp2-aerm-emergency-threshold *value*
default mtp2-aerm-emergency-threshold

default

Resets the parameter to the default value of 1.

value

value : Enter an integer from 1 to 50. Default: 1.

Usage Guidelines

This command sets the emergency threshold for the MTP2 alignment error rate monitor.

Example

Set the emergency AERM threshold to 17:

mtp2-aerm-emergency-threshold *17*

mtp2-aerm-normal-threshold

Configure the alignment error rate monitor (AERM) normal threshold value. This command is only available for a lowspeed-narrowband link-type.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp2-aerm-normal-threshold *value*
default mtp2-aerm-normal-threshold

default

Resets the parameter to the default value of 4.

value

value : Enter an integer from 4 to 100. Default: 4.

Usage Guidelines

This command sets the normal threshold for the MTP2 alignment error rate monitor.

Example

Set the normal AERM threshold to 55:

mtp2-aerm-normal-threshold *55*

mtp2-eim-decrement

Configure the errored interval monitor (EIM) emergency decrement value. This command is only available for a highspeed-narrowband link-type.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp2-eim-decrement *value*
default mtp2-eim-decrement

default

Resets the parameter to the default value of 11.

value

value : Enter an integer from 1 to 63. Default: 11.

Usage Guidelines

This command sets the emergency decrement value for the EIM.

Example

Reset the EIM emergency decrement to 1:

```
default mtp2-eim-decrement
```

mtp2-eim-increment

Configure the errored interval monitor (EIM) emergency increment value. This command is only available for a highspeed-narrowband link-type.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

```
mtp2-eim-increment value
default mtp2-eim-increment
```

default

Resets the parameter to the default value of 198.

value

value : Enter an integer from 1 to 1023. Default: 198.

Usage Guidelines

This command sets the emergency increment value for the EIM.

Example

Set the EIM emergency increment to 2:

```
mtp2-eim-increment 2
```

mtp2-eim-threshold

Configure the errored interval monitor (EIM) emergency threshold value. This command is only available for a highspeed-narrowband link-type.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp2-eim-threshold *value*
default mtp2-eim-threshold

default

Resets the parameter to the default value of 794.

value

value : Enter an integer from 1 to 65535. Default: 794.

Usage Guidelines

This command sets the emergency threshold value for the EIM.

Example

Set the EIM emergency threshold to 154:

mtp2-eim-threshold *154*

mtp2-error-correction

Configure the error correction method to be used. This command is only available for lowspeed or highspeed narrowband link-types.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp2-error-correction { basic | preventive-cyclic-retransmission }
default mtp2-error-correction

default

Resets the parameter to the default value.

basic

Basic error correction (BEC) is a positive / negative acknowledgement method that uses backwards retransmission. This method is best for links with less than 30 ms one-way propagation delays.

preventtive-cyclic-retransmission

PCR is recommended for links with 125 ms, or higher, propagation delays.

Usage Guidelines Set the method of MTP2 layer error correct to be used on the link.

Example

Set error correction for a link with 15 ms propagaion delay::

```
mtp2-error-correction basic
```

mtp2-lssu-len

This command sets the length of the link status signal unit (LSSU) which carries link status information used to manage link alignment and indicate the status of the signaling points to each other. This command is only available for lowspeed or highspeed narrowband link-types.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

```
mtp2-lssu-len #_octets
default mtp2-lssu-len
```

default

Using this keyword with the command resets the length to the default of 1 octet.

#_octets

Sets the number of octets for the length of the LSSU.

#_octets: Must be either 1 or 2.

Usage Guidelines Use this command to define the maximum amount of link status information that is to be shared between signaling points.

Example

You can use the following command to set the LSSU length to 2 octets - the maximum length:

mtp2-lssu-len *2*

mtp2-max-outstand-frames

This command sets the maximum number of outstanding packets to be sent by the link manager (linkmgr) - applicable for both high speed (HSL) and low speed (LSL) narrowband links.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp2-max-outstand-frames *#_bytes*
default mtp2-max-outstand-frames

default

Using this keyword with the command resets number of packets to the default of 7 bytes.

#_bytes

Sets the maximum number of packets sent by the linkmgr that can be allowed to be outsanding.

#_bytes: Must be an integer from 5 to 10.

Usage Guidelines

The linkmgr (MTP2) sends data at a higher rate, than the narrowband (NB) E1 link speed, when in congestion and performing retransmission. This can lead to more congestion leading to more time taken for the link to come out of congestion. If using a value of 10 during congestion, then linkmgr pumps data at a rate higher than 2.5 mbps. To avoid this problem, a lower value is usually considered optimal. This configuration holds good for both HSL and LSL.

Example

Use the following command to reset the default number of outstanding packets sent by the LinkMgr:

default mtp2-max-outstand-frames

Set the maximum number of oustanding packets the linkmgr can send to 6:

mtp2-max-outstand-frames *6*

mtp2-suerm-threshold

Configure the signal unit error rate monitor (SUERM) threshold. This command is only available for lowspeed-narrowband link-types.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp2-suerm-threshold *value*
default mtp2-suerm-threshold

default

Resets the parameter to the default value.

value

Defines the threshold for number of bad frames

value: Enter an integer from 64 to 1023. Default is 64.

Usage Guidelines

Sets the threshold for link monitoring of bad frames.

Example

Set a new link monitoring bad frames (SEURM) threshold of 256:

mtp2-suerm-threshold *256*

mtp3-discard-priority

Configure MTP3 message discard priority.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp3-discard-priority *priority*
default mtp3-discard-priority

default

Resets the priority to the default value.

priority

priority: must be an integer between 0 and 3.

Default is 0.

Usage Guidelines

Use this command to manage MTP3 messaging.

Example

mtp3-discard-priority *2*

mtp3-max-slt-try

Configure maximum number of times to retry SLT (signaling link test).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp3-max-slt-try *retries*
default mtp3-max-slt-try

default

Resets the number of retries to the default value.

retries

retries: must be an integer between 1 to 65535.

Default is 10.

Usage Guidelines Use this command to troubleshoot MTP3 link mismatch.

Example

```
mtp3-max-slt-try 35
```

mtp3-msg-priority

Configures the priority for sending MTP3 management messages.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

```
mtp3-msg-priority priority
default mtp3-msg-priority
```

default

Resets the number of priority to the default value.

priority

priority: must be an integer from 0 to 3.

Default: 0

Usage Guidelines Use this command to set the priority for sending MTP3 management messages.

Example

Use the following to set the message priority to 3:

```
mtp3-msg-priority 3
```

mtp3-msg-size

Configures the size of messages from layer 3 to layer 2.

Product SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp3-msg-size *size*
default mtp3-msg-size

default

Resets the the size to the default value which is 4096 (for q.2140) or 272 (for MTP2)

size

size: must be an integer from 1 to 272 for high-speed or low-speed narrowband SS7 links.

size: must be an integer from 1 to 4096 for ATM broadband links.

Usage Guidelines

Use this command to set the maximum message size, in bytes.

Example

Use this command to set the MTP3 message size to 4096 bytes:

mtp3-msg-size *4096*

mtp3-p1-qlen

Configure the size for the MTP3 p1 queue length.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp3-p1-qlen *size*
default mtp3-p1-qlen

default

Resets the number of size of the priority 1 queue to the default value.

size

size: integer from 1 to 65535. Size should be less than MTP3 p2 qlen and p3 qlen.

Default: 1024

Usage Guidelines Use this command to configure the queue length threshold for raising the congestion priority to level 1.

Example

Use this command to set the queue length priority to 128:

mtp3-p1-qlen *128*

mtp3-p2-qlen

Configure the size of the priority 2 queue.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#`

Syntax Description

mtp3-p2-qlen *size*
default mtp3-p2-qlen

default

Resets the number of size of the priority 2 queue to the default value.

size

size: integer from 1 to 65535. Size should be less than MTP3 p3 qlen and greater than p1 qlen.

Default: 1024

Usage Guidelines Use this command to configure the queue length threshold for raising the congestion priority to level 2.

Example

Use this command to set the queue length threshold to 256:

mtp3-p2-qlen *256*

mtp3-p3-qlen

Configure the size of the priority 3 queue.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp3-p3-qlen *size*
default mtp3-p3-qlen

default

Resets the number of size of the priority 3 queue to the default value.

size

size: integer from 1 to 65535. Size should be greater than MTP3 p1 qlen and p2 qlen .

Default: 1024

Usage Guidelines

Use this command to configure the queue length threshold for raising the congestion priority to level 3.

Example

mtp3-p3-qlen *1024*

mtp3-test-pattern

Configures the character string for the test message.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

mtp3-test-pattern *pattern*
default mtp3-test-pattern

default

Resets the pattern to the default value.

pattern

pattern: 1 to 15 alphanumeric characters.

Default: SGSN-ORIGINATED

Usage Guidelines

Use this command to define a test pattern string for the signalling link test match (SLTM).

Example

mtp3-test-pattern *TEST1-HomeOffice*

priority

Configures the MTP3 Link Priority.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

priority *pri_value*
no priority

no

Removes the priority configuration.

pri_value

pri_value: 0 represents highest priority and 15 represents the lowest priority.

Usage Guidelines

Use this command to configure the link priority within the MTP3 link set.

Example

priority *2*

signaling-link-code

Configures the signaling link code (SLC).

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#`

Syntax Description

signaling-link-code *code*
no signaling-link-code

no

Removes the SLC configuration.

code

code: integer from 0 to 15.

Usage Guidelines Use this command to uniquely identify the signaling link to be used for MTP3 management messages.

Example

`signaling-link-code 4`

sscf-nni-n1

Configures the SSCF NNI N1. This command is only available for ATM-broadband link-types.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > **ss7-routing-domain** *domain_id* **variant** *var_type* > **linkset id** *linkset_id* > **link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

sscf-nni-n1 *value*
no sscf-nni-n1

default

Removes the sscf-nni-n1 configuration.

value

value: integer from 1 to 65535.

Default: 1000

Usage Guidelines

Use this command to identify the network-to-node interface (NNI) between the MTP3 and SSCOP layers.

Example

sscf-nni-n1 *4064*

sscop-max-cc

Configure the maximum value for the SSCOP connection control (CC) state variable. his command is only available for ATM-broadband link-types.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > **ss7-routing-domain** *domain_id* **variant** *var_type* > **linkset id** *linkset_id* > **link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

sscop-max-cc *value*
no sscop-max-cc

default

Removes the sscop-max-cc configuration.

value

value: integer from 1 to 65535.

Default: 4

Usage Guidelines Use this command as part of the configuration responsible for managing the SSCOP connection. This command sets the number of times retries.

Example

sscop-max-cc *256*

sscop-max-pd

Configures the maximum acceptable value for the SSCOP state variable VT(PD). his command is only available for ATM-broadband link-types.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-linkset-linkset_id-link-link_id)#`

Syntax Description

sscop-max-pd *value*
no sscop-max-pd

default

Removes the **sscop-max-pd** configuration.

value

value: integer from 1 to 65535.

Default: 500

Usage Guidelines Use this command to define the maximum number of data PDUs transmitted between POLL PDUs.

Example

sscop-max-pd *2500*

sscop-max-stat

Configures the maximum number of elements included in a status PDU. his command is only available for ATM-broadband link-types.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

sscop-max-stat *value*
no sscop-max-stat

default

Removes the **sscop-max-stat** configuration.

value

value: integer from 3 to 65535. This parameter should be an odd integer greater than or equal to 3.

Defaultz; 67

Usage Guidelines

Received in response to a POLL PDU, the STAT PDU includes information about the number of SD PDUs that have been received.

Example

sscop-max-stat *56000*

timeout

This command enables configuration of an array of signaling and flow control timers - for MTP, SSCF, and SSCOP.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id* **> link id** *link_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

Syntax Description

[no] timeout *timer timer_value*

no

Adding **no** to the **timeout** command removes the timer configuration.

timer timer_value

Select the timer and enter a value from the range.

For timers having different ranges for highspeed and lowspeed links or for different variants, the appropriate ranges will be displayed based on the link-type configured.

Important Currently, the China variant uses ITU values.

Timer	Link Type & Variant	Range of Times Granularity = 100ms	Default Time
mtp2-tmr-t1 Alignment ready timer	Highspeed; ITU	160..3500 (16 - 350 seconds)	3000 (300 seconds)
	Lowspeed; ITU	120 - 500 (12 - 50 seconds)	400 (40 seconds)
	Highspeed; ANSI	160 - 3500 (16 to 350 seconds)	1700 (170 seconds)
	Lowspeed; ANSI	120 - 500 (12 - 50 seconds)	130 (13 seconds)
mtp2-tmr-t2 Not aligned timer	Highspeed; ITU	50 - 1500 (5 - 150 seconds)	50 (5 seconds)
	Lowspeed; ITU	50 - 150 (5 - 15 seconds)	50 (5 seconds)
	Highspeed; ANSI	50 - 1500 (5 - 150 seconds)	230 (23 seconds)
	Lowspeed; ANSI	50 - 150 (5 - 15 seconds)	115 (11.5 seconds)
mtp2-tmr-t3 Aligned timer	Highspeed/Lowspeed; ITU	10 - 140 (1 - 14 seconds)	15 (1.5 seconds)
	Highspeed/Lowspeed; ANSI	10 - 140 (1 - 14 seconds)	115 (11.5 seconds)
mtp2-tmr-t4e Emergency proving period timer	Highspeed; ITU	4 - 60 (400 milliseconds - 6 seconds)	5 (500 milliseconds)
	Lowspeed; ITU	4 - 6 (400 - 600 milliseconds)	5 (500 milliseconds)

Timer	Link Type & Variant	Range of Times Granularity = 100ms	Default Time
	Highspeed; ANSI	4 - 60 (400 milliseconds - 6 seconds)	50 (5 seconds)
	Lowspeed; ANSI	4 - 6 (400 - 600 milliseconds)	6 (600 milliseconds)
mtp2-tmr-t4n Normal proving period timer Once set this timer can be reset but it can not be disabled.	Highspeed; ITU	30 - 700 (3 to 70 seconds)	3 (30 seconds)
	Lowspeed; ITU	20 - 95 (2 - 9.5 seconds)	82 (8.2 seconds)
	Highspeed; ANSI	30 - 700 (3 to 70 seconds)	3 (30 seconds)
	Lowspeed; ANSI	20 - 95 (2 - 9.5 seconds)	23 (2.3 seconds)
mtp2-tmr-t5 Sending status indication busy (SIB) timer	Highspeed/Lowspeed ITU/ANSI	1 - 2 (100 - 200 milliseconds)	1 (100 milliseconds)
mtp2-tmr-t6 Remote congestion timer	Highspeed/Lowspeed ITU/ANSI	10 - 60 (1 to 6 seconds)	30 (3 seconds)
mtp2-tmr-t7 Excessive delay of acknowledgement timer	Highspeed/Lowspeed ITU/ANSI	5 - 20 (500 milliseconds - 2 seconds)	10 (1 second)
mtp2-tmr-t8 Interval timer for error interval monitor timer	Highspeed ITU/ANSI	1 - 2 (100 - 200 milliseconds)	1 (100 milliseconds)
mtp3-tmr-t1 Delay to avoid mis-sequencing on changeover timer	Highspeed/Lowspeed ITU/ANSI	5 - 12 (500 - 1200 milliseconds)	5 (500 milliseconds
mtp3-tmr-t12 Waiting for uninhibit acknowledgement timer	Highspeed/Lowspeed ITU/ANSI	8 - 15 (800 - 1500 milliseconds	8 (800 milliseconds
mtp3-tmr-t13 Waiting for force uninhibit timer	Highspeed/Lowspeed ITU/ANSI	8 - 15 (800 - 1500 milliseconds	8 (800 milliseconds
mtp3-tmr-t14 Waiting for inhibition acknowledgement timer	Highspeed/Lowspeed ITU/ANSI	20 - 30 (2000 - 3000 milliseconds	20 (2000 milliseconds

Timer	Link Type & Variant	Range of Times Granularity = 100ms	Default Time
mtp3-tmr-t17 Delay to avoid oscillation of initial alignment failure and link restart	Highspeed/Lowspeed ITU/ANSI	8 - 15 (800 - 1500 milliseconds	8 (800 milliseconds
mtp3-tmr-t2 Waiting for changeover acknowledgement	Highspeed/Lowspeed ITU/ANSI	7 - 20 (700 - 2000 milliseconds	7 (700 milliseconds
mtp3-tmr-t22 Local inhibit test timer	Highspeed/Lowspeed ITU/ANSI	1800 - 3000 (180 - 300 seconds	1800 (180 seconds)
mtp3-tmr-t23 Remote inhibit test timer	Highspeed/Lowspeed ITU/ANSI	1800 - 3000 (180 - 300 seconds	1800 (180 seconds)
mtp3-tmr-t24 Stabilising timer after removal of local processor outage, used in LPO latching to RPO (national option)	Highspeed/Lowspeed ITU/ANSI	5 - 15 (500 - 1500 milliseconds)	5 (500 milliseconds)
mtp3-tmr-t3 Time controlled diversion-delay to avoid mis-sequencing on changeback	Highspeed/Lowspeed ITU/ANSI	5 - 12 (500 - 1200 milliseconds)	5 (500 milliseconds)
mtp3-tmr-t31 BSN requested timer	Highspeed/Lowspeed ITU/ANSI	50 - 100 (5 to 10 seconds)	50 (5 seconds)
mtp3-tmr-t32 SLT timer	Highspeed/Lowspeed ITU/ANSI	40 - 120 (4 - 12 seconds)	100 (10 seconds)
mtp3-tmr-t33 Connecting timer	Highspeed/Lowspeed ITU/ANSI	50 - 100 (5 to 10 seconds)	50 (5 seconds)
mtp3-tmr-t34 Periodic signalling link test timer	Highspeed/Lowspeed ITU/ANSI	300 - 900 (30 to 90 seconds)	600 (60 seconds)
mtp3-tmr-t4 Waiting for changeback acknowledgement (first attempt)	Highspeed/Lowspeed ITU/ANSI	5 - 12 (500 to 1200 milliseconds)	5 (500 milliseconds)
mtp3-tmr-t5 Waiting for changeback acknowledgement (second attempt)	Highspeed/Lowspeed ITU/ANSI	5 - 12 (500 to 1200 milliseconds)	5 (500 milliseconds)

Timer	Link Type & Variant	Range of Times Granularity = 100ms	Default Time
mtp3-tmr-t7 Waiting for signalling data link connection acknowledgement	Highspeed/Lowspeed ITU/ANSI	10 - 20 (1000 - 2000 milliseconds)	10 (1000 milliseconds)

Timer	Link type & Variant	Range of Times	Default Time
sscf-nni-tmr-t1	ATM Broadband ITU/ANSI	1 - 65535 (10 - 655350 milliseconds) Granularity = 10 ms	500 (5 seconds)
sscf-nni-tmr-t2	ATM Broadband ITU/ANSI	1 - 65535 (10 - 655350 milliseconds) Granularity = 10 ms	3000 (30 seconds)
sscf-nni-tmr-t3	ATM Broadband ITU/ANSI	1 - 65535 (10 - 655350 milliseconds) Granularity = 10 ms	1 (10 milliseconds)
sscop-tmr-cc SSCOP CC timer	ATM Broadband ITU/ANSI	1 - 65535 (100 - 6553500 milliseconds) Granularity = 100 ms	2 (200 milliseconds)
sscop-tmr-idle SSCOP idle timer (UNI 3.1 only)	ATM Broadband ITU/ANSI	1 - 65535 (100 - 6553500 milliseconds) Granularity = 100 ms	1 (100 milliseconds)
sscop-tmr-keep-alive SSCOP keep alive timer For stability purposes, tmrKeepAlive >/= tmrPoll and tmrKeepAlive < tmrNoResponse.	ATM Broadband ITU/ANSI	1 - 65535 (100 - 6553500 milliseconds) Granularity = 100 ms	1 (100 milliseconds)
sscop-tmr-no-rsp SSCOP no response timer For stability purposes, tmrNoResponse > tmrKeepAlive.	ATM Broadband ITU/ANSI	1 - 65535 (100 - 6553500 milliseconds) Granularity = 100 ms	15 (1.5 seconds)
sscop-tmr-poll SSCOP poll timer For stability purposes, tmrPoll <= tmrKeepAlive.	ATM Broadband ITU/ANSI	1 - 65535 (100 - 6553500 milliseconds) Granularity = 100 ms	1 (100 milliseconds)

Usage Guidelines

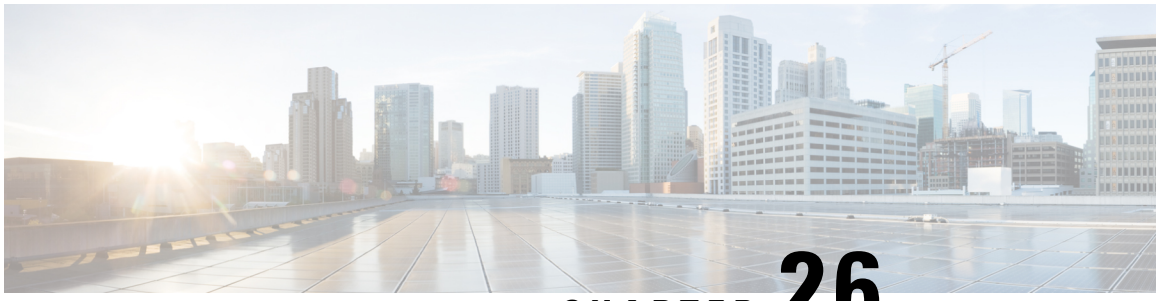
For a single link and specified link-type (highspeed or lowspeed), this command sets the timer values listed above. The SS7 variant is determined when the SS7 routing domain is first defined from the Global Configuration mode.

Repeat the **timeout** command (one timer and value per entry) as needed to configure all required timers.

Important Currently, the China variant uses the same timers, values, and defaults as the ITU variant.

Example

timeout *timer timer_value*



CHAPTER 26

Linkset Configuration Mode Commands

Command Modes

The Linkset configuration mode defines the MTP3 linkset parameters for a specific SS7 routing domain instance.

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-linkset-`*`linkset_id`*`)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

adjacent-point-code

This command defines the point-code for the adjacent (next) network element in the SS7 network.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-linkset-`*`linkset_id`*`)#`

Syntax Description

adjacent-point-code *point-code*
no adjacent-point-code

point-code

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

no

Removes the adjacent-point-code configuration for this linkset in the SS7 routing domain

Important Removing the linkset configuration will result in the termination of all of the links within the linkset.

Usage Guidelines

Use this command to define the point-code for the adjacent element in the SS7 network.

Example

adjacent-point-code *6.202.7*

link

This command creates an MTP3 link configuration for the SS7 linkset and enters the Link configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-linkset-linkset_id)#`

Syntax Description

link id *id* **[link-type [atm-broadband | highspeed-narrowband | lowspeed-narrowband]**
no link id *id*

no

Disables the specified link configuration.

Important Removing the link configuration will result in the termination of traffic on the specified link.

#_octets

Sets the number of octets for the length of the LSSU.

id

This number uniquely identifies the link in the linkset.

id: an integer between 1 and 16.

link-type

Identifies the signalling type for this link; options include:

- ATM broadband -- ATM AAL5 over an optical line card (OLC2)
- high speed-narrowband -- 64 kbps over a channelized optical line card (CLC2)
- low speed-narrowband -- 4.8 kbps over a channelized optical line card (CLC2)

Important Be default link-type is ATM-broadband. To support narrowband SS7, one of the other options must be set.

Usage Guidelines Access the Link configuration mode to configure the parameters for the the link.

Example

Access configuration for link 4:

```
link id 4
```

self-point-code

This command defines the SS7 network point-code to identify this SGSN.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration

configure > ss7-routing-domain *domain_id* **variant** *var_type* **> linkset id** *linkset_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id)#
```

Syntax Description

```
self-point-code point-code
no self-point-code
```

point-code

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

no

Removes the self-point-code configuration for this linkset in the SS7 routing domain.

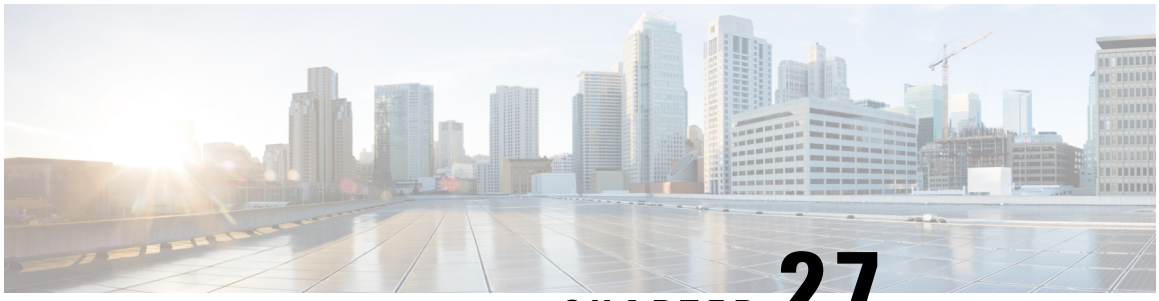
Important Removing the self-point-code will result in the termination of all traffic on this link.

Usage Guidelines

Use this command to define the SS7 point-code to identify this system.

Example

```
self-point-code 6.192.7
```



CHAPTER 27

LMA Service Configuration Mode Commands

The LMA Service Configuration Mode is used to create and manage the Local Mobility Anchor configuration supporting Proxy Mobile IP on a PDN Gateway in an eHRPD and E-UTRAN/EPC network.

Command Modes

Exec > Global Configuration > Context Configuration > LMA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

• timestamp-replay-protection, on page 337

aaa accounting

Enables the LMA to send AAA accounting information for subscriber sessions.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LMA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default | no ] aaa accounting
```

default

Sets the command to the default condition of enabled.

no

Disables the ability of the LMA to send AAA accounting information.

Usage Guidelines

Use this command to enable the LMA service to send all accounting data (start, stop, and interim) to the configured AAA servers.

Important In order for this command to function properly, AAA accounting must be enabled for the context in which the LMA service is configured using the **aaa accounting subscriber radius** command.

Example

The following command disables aaa accounting for the LMA service:

```
no aaa accounting
```

alt-coa-allowed

Allows Alternate Care-of-address support to be added at LMA to separate signaling and control plane traffic.

Product

P-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LMA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[  default | no ] alt-coa-allowed
```

default

Including this keyword with the command disables the feature. The feature is disabled by default.

no

Disables the specified functionality.

Usage Guidelines

This command allows Alternate Care-of-address support to be added at LMA to separate signaling and control plane traffic.

Important The support of the extensions and functionality is defined in RFC 6275 and RFC 6463 for IPv6 and IPv4 transport respectively.

Proxy Mobile IPv6 is a network-based mobility management protocol. The mobility entities involved in the Proxy Mobile IPv6 protocol, the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA), setup tunnels dynamically to manage mobility for a mobile node within the Proxy Mobile IPv6 domain. There is an extension to the Proxy Mobile IPv6 protocol to register an IPv4 or IPv6 data plane address that is different from the Proxy Care-of Address with the LMA. This allows separation of control and data plane. Some of the deployments of Proxy Mobile IPv6 separated the control and data plane end points for Mobile Access Gateway. There will be a separate IP address for the entity that sends and received the Proxy Mobile IPv6 signaling messages. Similarly, there will be a separate IP address for the entity that encapsulates and decapsulates the data traffic to and from the mobile node.

In order to allow the separation of the control and data plane, the address of the data plane traffic endpoint needs to be sent in a separate extension to register two IP addresses with the LMA. The IP address used for the signaling messages will continue to be called the Proxy Care-of-Address. A separate IP address for the data plane is carried in the Proxy Binding Update to indicate the tunnel end point for the data traffic.

The extension Alternate Care-of-Address Mobility Option defined in RFC 6275 should be used. When using IPv6 transport and IPv4 transport, Alternate Ipv4 Care of Address Mobility Option defined in RFC 6463 should be used.

Normally, a binding update specifies the desired care-of-address in the source address field of the IPv6 header. However, in some cases such as when the mobile node wishes to indicate a Care-of Address that it cannot use as a topologically correct source address or when the used security mechanism does not protect the IPv6 header it is not possible.

The Alternate Care-of-Address option is for this type of situation. This option is valid only in binding update. The Alternate Care-of Address field contains an address to use as the care-of-address for binding rather than using the source address of the packet as the care-of-address.

Example

The following command disables Alternate Care-of-address support:

```
no alt-coa-allowed
```

bind address

Binds the LMA service to a logical IP interface serving as the S2a (HSGW) or S5/S8 (S-GW) interface and specifies the maximum number of subscribers that can access this service over the configured interface.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LMA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

bind address *ipv6_address* **[ipv4-address** *ipv4_address* **] [max-subscribers** *num* **]**
no bind address

no

Removes the interface binding from this service.

address *ipv6_address*

Specifies the IPv6 address of the interface configured as the S2a or S5/S8 interface. *ipv6_address* is specified in colon separated notation.

ipv4-address *ipv4_address*

Specifies optional IPv4 HA/P-GW address to support DSMIP6 session using IPv4 transport.*ipv4_address* must be entered as a standard IPv4 address in dotted decimal notation.

max-subscribers *num*

Default: 3000000

Specifies the maximum number of subscribers that can access this service on this interface. *num* must be configured to an integer between 0 and 3,000,000.

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

Usage Guidelines Associate the LMA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an S2a or S5/S8 interface that provides the session connectivity to an HSGW (S2a) or S-GW (S5/S8). Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

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

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

- The total number of S2a or S5/S8 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

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

Example

The following command would bind the logical IP interface with the address of *4551:0db8:85a3:08d3:3319:8a2e:0370:1344* to the LMA service and specifies that a maximum of *300,000* simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 4551:0db8:85a3:08d3:3319:8a2e:0370:1344 max-subscribers
300000
```

heartbeat

Configures the PMIPv6 heartbeat message interval, retransmission timeout, and max retransmission for the LMA Service.

Product P-GW

Privilege Administrator

Syntax Description

```
heartbeat { interval seconds | retransmission { max number [ exceed-action
drop-session ] | timeout seconds } }
default heartbeat { interval | retransmission { max | timeout } }
no heartbeat
```

no

Disables the PMIPv6 heartbeat functionality. The P-GW starts sending heartbeat request to peers when the heartbeat interval is configured.

default

Resets the specified parameter to the system default value.

interval *seconds*

The interval in seconds at which heartbeat messages are sent.

seconds is an integer from 30 through 3600.

Default: 60

retransmission max *number*

The maximum number of heartbeat retransmissions allowed.

number is an integer from 1 through 15.

Default: 3

exceed-action

Specifies the action to be taken after the maximum number of heartbeat retransmission is reached.

Important This keyword is valid only for NEMO-LMA sessions and takes effect if the Heartbeat feature is enabled.

drop-session

Used for dropping the session when path failure is detected.

Important This keyword is valid only for NEMO-LMA sessions and takes effect if the Heartbeat feature is enabled.

retransmission timeout *seconds*

The timeout in seconds for heartbeat retransmissions.

seconds is an integer from 1 through 20.

Default: 3

Usage Guidelines

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol to provide mobility without requiring the participation of the mobile node in any PMIPv6 mobility related signaling. The Local Mobility Anchor (LMA) service sets up tunnels dynamically to manage mobility for a mobile node.

This command provides configuration of heartbeat messages between the LMA and MAG services to know the reachability of the peers, to detect failures, quickly inform peers in the event of a recovery from node failures, and allow a peer to take appropriate action.

Example

The following command enables PMIPv6 heartbeat messaging to known LMA service peers and sets the heartbeat interval to 160 seconds.

```
heartbeat interval 160
```

heartbeat monitor-max-peers

Configures monitoring of a maximum of 128000 PMIP sessions through the heartbeat mechanism.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

```
[ default ] heartbeat monitor-max-peers
```

default

Monitors 256 peers through the heartbeat mechanism.

heartbeat monitor-max-peers

Monitors a maximum of 128000 peers through the heartbeat mechanism.

Usage Guidelines

Use this command to monitor a maximum of 128000 PMIP sessions through the heartbeat mechanism.

This CLI is disabled by default.

Example

The following command enables monitoring of a maximum of 128000 peers through the heartbeat mechanism.

```
heartbeat monitor-max-peers
```

mobility-option-type-value

Changes the mobility option type value used in mobility messages.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

```
mobility-option-type-value { custom1 | custom2 | standard }
default mobility-option-type-value
```

default

Sets the command to the default value of custom1.

custom1

(Default) Non-standard type values used before they were defined by IANA.

custom2

Standard type values, as defined by IANA, and some customer-specific message formats.

standard

Standard type values as defined by IANA. In addition, standard option uses type values defined in RFC 5844 for HoA options for PMIPv6 PBU/PBA/revocation message.

Usage Guidelines

Use this command to change the mobility option type value used in mobility messages.

Example

The following command changes the mobility option type value to standard:

```
mobility-option-type-value standard
```

refresh-advice-option

Configures inclusion of a refresh advice option in the binding acknowledgement message sent by the LMA.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

```
[ default | no ] refresh-advice-option
```

default

Returns the command setting to the default setting of disabled.

no

Disables the inclusion of the refresh advice option in the binding acknowledgement message sent by the LMA

Usage Guidelines

Use this command to enable the LMA to include this option in a binding acknowledgment sent to the requesting MAG. The option provides a "hint" to the MAG of when it should refresh the binding.

As defined in RFC 3775 "Mobility Support in IPv6", the binding refresh advice option can only be present in the binding acknowledgement sent from the mobile node's home agent in reply to a registration request. A refresh interval parameter determines the amount of time until the mobile node must send a new registration to the home agent to avoid de-registration and loss of session.

Important Refer to the refresh-interval-percent and reg-lifetime commands for a complete understanding of registration (binding) lifetimes and refresh intervals.

refresh-interval-percent

Configures percentage of the granted registration lifetime to be used in the refresh interval mobility option in a binding acknowledgement message sent by the LMA service.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

`refresh-interval-percent` *`number`*
`default refresh-interval-percent`

default

Resets the command value to the default setting of 75.

number

Default: 75

Sets the percent value for session lifetimes for this service.

number must be an integer value from 1 to 99.

Usage Guidelines

Use this command to configure the amount of the granted registration lifetime to be used in the refresh interval mobility option in the binding acknowledgement message sent by the LMA service to the requesting MAG.

Refreshing a binding or registration is based on the granted registration lifetime. Since a refresh request must be within the granted range of a registration lifetime, this command provides a method of setting the interval of when a refresh request is sent.

As described in RFC 3775 "Mobility Support in IPv6", if a binding refresh advice option is present in the binding acknowledgement, the refresh interval field in the option must be a value less than the binding lifetime (also returned in the binding acknowledgement). The mobile node then should attempt to refresh its registration at the shorter refresh interval. The home agent will still honor the registration for the lifetime period, even if the mobile node does not refresh its registration within the refresh period.

Important Refer to the refresh-advice-option and reg-lifetime commands for a complete understanding of registration (binding) lifetimes and refresh intervals.

Example

The following command sets the refresh interval percent to *90*:

```
refresh-interval-percent 90
```

reg-lifetime

Configures the Mobile IPv6 session registration lifetime for this service.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

```
reg-lifetime seconds
default reg-lifetime
```

default

Resets the command value to the default setting of 600.

seconds

Default: 600

Sets the time value for session lifetimes for this service.

seconds must be an integer value from1 to 262140.

Usage Guidelines

Use this command to limit PMIPv6 lifetime on this service. If the PBU contains a lifetime shorter than what is specified, it is granted. If the lifetime is longer, then HA service will limit the granted lifetime to the configured value.

Important Refer to the refresh-interval-percent and refresh-advice-option commands for a complete understanding of registration (binding) lifetimes and refresh intervals.

Example

The following command sets the registration lifetime for Mobile IPv6 sessions using this service to *1200* seconds (20 minutes):

```
reg-lifetime 1200
```

revocation

Enables the MIP revocation feature and configures revocation parameters.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

revocation { enable | max-retransmission *number* **| retransmission-timeout** *msecs* **}**
default revocation { enable | max-retransmission | retransmission-timeout }
no revocation enable

default

Resets the keyword to its default value.

no

Disables revocation for this service.

enable

Default: disabled

Enables the MIP registration revocation feature for the LMA service. When enabled, if revocation is negotiated with a MAG and a MIP binding is terminated, the LMA can send a Revocation message to the MAG. This feature is disabled by default.

max-retransmission *number*

Default: 3

The maximum number of retransmissions of a Revocation message before the revocation fails. *number* must be an integer value from 0 through 10.

retransmission-timeout *msecs*

Default: 3000

The number of milliseconds to wait for a Revocation Acknowledgement from the MAG before retransmitting the Revocation message. *msecs* must be an integer value from 500 through 10000.

Usage Guidelines

Use this command to enable or disable the MIP revocation feature on the LMA or to change settings for this feature.

Example

The following command sets the maximum number of retries for a Revocation message to *6*:

revocation max-retransmission 6

The following command sets the timeout between retransmissions to *10*:

revocation retransmission-timeout 10

sequence-number-validate

Configures sequence number validation of the received MIPv6 control packets by the LMA service according to RFC 3775.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

[default | no] sequence-number-validate

default

Resets the command value to the default setting of enabled.

no

Disables the feature.

Usage Guidelines

Use this command to configure the sequence number validation of the received MIPv6 control packets (PBUs) by the LMA service. This feature validates MIPv6 control packets and insures that any incoming packets with a sequence number prior to the last number received is consider invalid.

If this service has no cache entry of the home address included in the PBU, it will accept any sequence value in the initial PBU from the mobile node.

setup-timeout

The maximum amount of time allowed for session setup.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

setup-timeout *seconds*
default setup-timeout

default

Resets the command value to the default setting of 60.

seconds

Default: 60 seconds

The maximum amount of time, in seconds, to allow for setup of a session in this service. *seconds* must be an integer value from 1 through 1000000.

Usage Guidelines

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

Example

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

```
setup-timeout 300
```

signalling-packets

Enables the DSCP marking feature for IP headers carrying outgoing signalling packets.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

```
signalling-packets ip-header-dscp value
{ default | no } signalling-packets ip-header-dscp
```

default

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

no

Disables the specified functionality.

ip-header-dscp *value*

Used to configure the QoS Differentiated Services Code Point (DSCP) marking for IP header encapsulation.

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

Usage Guidelines

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

Example

The following command configures the HSGW service to support DSCP marking for IP headers carrying outgoing signalling packets:

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

simul-bindings

Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

```
simul-bindings number
default simul-bindings
```

default

Resets the command value to the default setting of 1.

number

Default: 1

Configures maximum number of "care of" addresses that can be simultaneously bound for the same user as identified by their NAI and home address. *number* must be an integer value between 1 and 3.

Usage Guidelines

Per RFC 5213 (and 3775), the LMA service creates a binding record known as a binding cache entry (BCE) for each subscriber session it is facilitating. Each BCE is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care of address.

Typically, the LMA service will delete an old binding and create a new one when the information in the registration request changes. However, the mobile node could request that the LMA maintains previously stored BCEs. This command allows you to configure the maximum number of BCEs that can be stored per subscriber if more than one is requested.

Example

The following command configures the service to support up to 2 addresses per subscriber:

```
simul-bindings 2
```

standalone

Configures the LMA service to start in standalone mode.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

`[ default | no ] standalone`

default

Resets the command value to the default setting.

no

Disables the feature.

Usage Guidelines

Use this command to start the LMA service in standalone mode.

timestamp-option-validation

Configures validation of timestamp option in binding update messages. By default, timestamp option is mandatory.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

`[ default | no ] timestamp-option-validation`

default

Resets the command value to the default setting of enabled.

no

Disables the feature.

Usage Guidelines

Use this command to configure timestamp validation in binding update messages.

timestamp-replay-protection

Designates timestamp replay protection scheme as per RFC 4285.

Product

P-GW

SAEGW

Privilege

Administrator

Syntax Description

`timestamp-replay-protection tolerance` *`seconds`*
`{ default | no } timestamp-replay-protection tolerance`

default

Resets the command value to the default setting of 7.

no

Disables the timestamp replay protection feature.

tolerance *seconds*

Default: 7

Defines the acceptable difference in timing (between timestamps) before rejecting packet, in seconds. *seconds* must be an integer value between 0 and 65535.

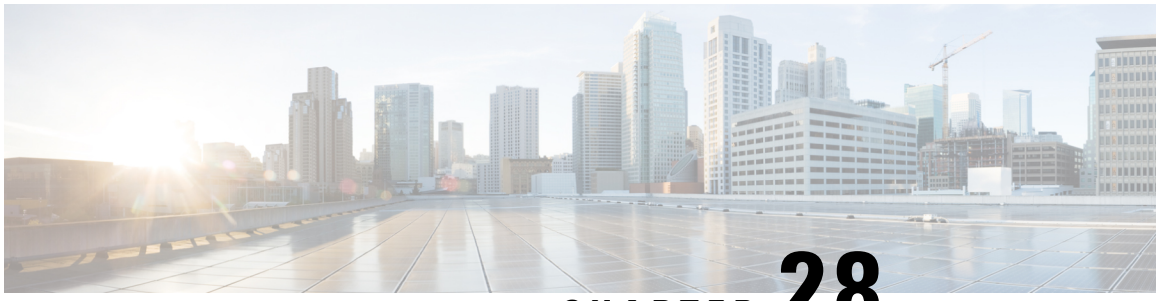
Usage Guidelines

Use this command to define the acceptable difference in timing (between timestamps) before rejecting packet.

Example

The following command sets the acceptable difference for timestamps to 10 seconds:

```
timestamp-replay-protection tolerance 10
```



CHAPTER 28

LNS Service Configuration Mode Commands

The LNS Service Configuration Mode is used to create and manage L2TP services within contexts on the system. L2TP Network Server (LNS) services facilitate tunneling with peer L2TP Access Concentrators (LACs).

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

aaa accounting

Enables the sending of authentication, authorization, and accounting (AAA) accounting information by the LNS.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa accounting [ roaming ]
[ no ] aaa accounting
```

no

Disables this option.

roaming

Enables the sending of AAA accounting information by the LNS only for roaming subscribers.

Usage Guidelines

Use this command to enable the sending of AAA accounting information by the LNS. By default this is enabled.

Example

The following command enables the sending of AAA accounting information by the LNS:

```
aaa accounting
```

authentication

Configures the type of subscriber authentication for PPP sessions terminated at the current LNS.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`authentication { { [ allow-noauth ] [ chap` *`chap_priority`* **`] [ mschap`** *`mschap_priority`* **`] [ pap`** *`pap_priority`* **`] } | msid-auth }`**

allow-noauth

Default: Disabled

Configures the LNS to allow PPP sessions access even though they have not been authenticated. This command issued by itself causes the LNS not to attempt authentication for any PPP sessions.

When the **allow-noauth** option is used in conjunction with commands specifying other authentication protocols and priorities to use, then if attempts to use those protocols fail, the system treats the **allow-noauth** option as the lowest priority.

If no authentication is allowed, the system constructs an Network Access Identifier (NAI) to provide accounting records for the PPP session.

chap *chap_priority*

Default: 1

Configures the LNS to attempt to use Challenge Handshake Authentication Protocol (CHAP) to authenticate the PPP session.

A *chap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

chap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference. CHAP is enabled by default as the highest preference.

mschap *mschap_priority*

Default: Disabled

Configures the LNS to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the PPP session.

A *mschap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

mschap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference.

pap *pap_priority*

Default: 2

This option configures the LNS to attempt to use the Password Authentication Protocol (PAP) to authenticate the PPP session.

A *pap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

pap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference. PAP is enabled by default as the second highest preference.

msid-auth

Default: Disabled

This option configures the LNS to attempt to authenticate the PPP session based on the Mobile Station Identity (MSID).

Usage Guidelines

Use to specify how the LNS service should handle authentication and what protocols to use. The flexibility is given to configure this option to accommodate the fact that not every mobile will implement the same authentication protocols.

By default LNS authentication options are set as follows:

- allow-noauth disabled
- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

Important At least one of the keywords must be used to complete the command.

Example

The following command configures the LNS service to allow no authentication for PPP sessions and would perform accounting using the default NAI-construct of username@domain:

```
authentication allow-noauth
```

The following command configures the system to attempt authentication first using CHAP, then MSCHAP, and finally PAP. If the allow-noauth command was also issued, when all attempts to authenticate the subscriber using these protocols failed, then the subscriber would be allowed access:

```
authentication chap 1 mschap 2 pap 3
```

avp map called-number apn

This command maps an incoming Attribute Value Pair (AVP) to a GGSN Access Point Name (APN) for authentication and authorization of the call.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] avp map called-number apn`

default

Disables mapping.

no

Disables mapping.

Usage Guidelines

For LNS calls received through a LAC, the ICRQ message includes an APN name in the Called Number AVP. This mapping function enables a GGSN system to provide RADIUS authentication/authorization via a defined APN in place of an LNS configuration. If the mapped APN has not been defined within the GGSN configuration then the call will be rejected.

Example

Enter the following command to enable mapping:

`avp map called-number apn`

Enter the following command to disable mapping:

`no avp map called-number apn`

bind

This command assigns the IP address of an interface in the current context to the LNS service.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

bind *ip_address* **[max-subscribers** *max_value* **]**
no bind *ip_address*

no

Unassign, or unbind, the local end point to the LNS service.

ip_address

Specifies the IP address of an interface in the current context. This must be a valid IP address entered using IPV4 dotted-decimal notation.

max-subscribers *max_value*

Default: 10000

Specifies the maximum number of subscribers that can be connected to this service at any time. *max_value* must be an integer from 1 through 2500000.

Usage Guidelines

Use this command to bind the IP address of an interface in the current context to the LNS service.

Example

The following command binds the current context interface IP address *209.165.200.234* to the current LNS service:

```
bind 209.165.200.234
```

The following command removes the binding of the IP address from the LNS service:

```
no bind
```

data sequence-number

Enables data sequence numbering for sessions that use the current LNS service. Data sequence numbering is enabled by default.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] data sequence-number

no

Disables data sequence numbering for sessions.

Usage Guidelines

An L2TP data packet header has an optional data sequence numbers field. The data sequence number may be used to ensure ordered delivery of data packets. This command is used to re-enable or disable the use of the data sequence numbers for data packets.

Example

Use the following command to disable the use of data sequence numbering:

no data sequence-number

Use the following command to re-enable data sequence numbering:

data sequence-number

default

This command sets the specified LAC service parameter to its default value or setting.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

default { authentication | data sequence-number | ip source-violation | keepalive-interval | load-balancing | local-receive-window | max-retransmission | max-session-per-tunnel | max-tunnel-challenge-length | max-tunnels | proxy-lcp-authentication | retransmission-timeout-first | retransmission-timeout-max | setup-timeout| single-port-mode | subscriber| trap all tunnel-authentication}

authentication

Sets the authentication parameters for PPP sessions to the following defaults:

- allow-noauth disabled

- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

data sequence-number

Enables data sequence numbering for sessions.

ip source-violation

Sets the IP source violation parameters to the following defaults:

- drop-limit 10
- period 120 seconds
- reneg-limit 5

keepalive-interval

Sets the interval for send L2TP Hello keepalive if there is no control or data transactions to the default value of 60 seconds.

local-receive-window

Sets the window size to be used for the local side for the reliable control transport to the default of 4.

max-retransmission

Sets the maximum number of retransmissions to the default of 5.

max-session-per-tunnel

Sets the maximum number of sessions per tunnel at any point in time to the default of 65535.

max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge to the default of 16 bytes.

max-tunnels

Sets the maximum number of tunnels for this service to the default of 32000.

proxy-lcp-authentication

Sets sending of proxy LCP authentication parameters to the LNS to the default state of enabled.

retransmission-timeout-first

Sets the first retransmit interval to the default of 1 second.

retransmission-timeout-max

Sets the maximum retransmit interval to the default of 8 seconds.

setup-timeout

Sets the maximum time allowed for session setup to the default of 60 seconds.

single-port-mode

Disables assignment of only port 1107 for incoming tunnels and allows dynamic assignment of ports.

subscriber

Sets the name of the default subscriber configuration to use.

tunnel-authentication

Sets tunnel authentication to the default state of enabled.

trap all

Generates all supported SNMP traps.

tunnel-switching

Sets the ability of the LNS to create subsequent tunnels to the default of enabled.

Usage Guidelines

Use the default command to set LAC service parameters to their default states.

Example

Use the following command to set the keepalive interval to the default value of 60 seconds:

```
default keepalive-interval
```

Use the following command to set the maximum number of sessions per tunnel to the default value of 512:

```
default max-session-per-tunnel
```

ip source-violation

This command configures settings related to IP source-violation detection.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip source-violation { clear-on-valid-packet | drop-limit num | period secs
 | reneg-limit num }
no ip source-violation clear-on-valid-packet
```

clear-on-valid-packet

Default: disabled

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

drop-limit *num*

Default: 10

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

num can be an integer from 1 through 1000000.

period *secs*

Default: 120

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

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

secs can be an integer from 1 through 1000000.

reneg-limit *num*

Default: 5

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

num can be an integer from 1 through 1000000.

Usage Guidelines

This function allows the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDSNs a number of times during a handoff scenario.

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

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

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

If at any time before the call is dropped, the configured source-violation period is exceeded, the counters for drop-limit is decremented by half and reneg-limit is decremented by 1. See period definition above.

Example

To set the maximum number of source violations before dropping a call to 100, enter the following command:

```
ip source-violation drop-limit 100
```

keepalive-interval

This command specifies the amount of time to wait before sending a Hello keepalive message.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
keepalive-interval seconds
no keepalive-interval
```

no

Disables the generation of Hello keepalive messages on the tunnel.

seconds

Default: 60

Specifies the number of seconds to wait before sending a Hello keepalive message as an integer from 30 through 2147483648.

Usage Guidelines

Use this command to set the amount of time to wait before sending a Hello keepalive message or disable the generation of Hello keepalive messages completely. A keepalive mechanism is employed by L2TP in order to differentiate tunnel outages from extended periods of no control or data activity on a tunnel. This is accomplished by injecting Hello control messages after a specified period of time has elapsed since the last data or control message was received on a tunnel. As for any other control message, if the Hello message is not reliably delivered then the tunnel is declared down and is reset. The transport reset mechanism along with

the injection of Hello messages ensures that a connectivity failure between the LNS and the LAC is detected at both ends of a tunnel.

Example

Use the following command to set the Hello keepalive message interval to *120* seconds:

```
keepalive-interval 120
```

Use the following command to disable the generation of Hello keepalive messages:

```
no keepalive-interval
```

local-receive-window

Specifies the number of control messages the remote peer LAC can send before waiting for an acknowledgement.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

local-receive-window *integer*

integer

Default: 4

Specifies the number of control messages to send before waiting for an acknowledgement as an integer from 1 through 256.

Usage Guidelines

Use this command to set the size of the control message receive window being offered to the remote peer LAC. The remote peer LAC may send the specified number of control messages before it must wait for an acknowledgment.

Example

The following command sets the local receive window to *10* control messages:

```
local-receive-window 10
```

max-retransmission

Sets the maximum number of retransmissions of a control message to a peer before the tunnel and all sessions within it are cleared.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-retransmission *integer*

integer

Default: 5

Specifies the maximum number of retransmissions of a control message to a peer as an integer from 1 through 10.

Usage Guidelines

Each tunnel maintains a queue of control messages to be transmitted to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. If no peer response is detected after the number of retransmissions set by this command, the tunnel and all sessions within are cleared.

Use this command to set the maximum number of retransmissions that the LAC service sends before closing the tunnel and all sessions within. it.

Example

The following command sets the maximum number of retransmissions of a control message to a peer to 7:

```
max-retransmissions 7
```

max-session-per-tunnel

Sets the maximum number of sessions that can be facilitated by a single tunnel at any time.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-sessions-per-tunnel *integer*

integer

Default: 512

Specifies the maximum number of sessions as an integer from 1 through 65535.

Usage Guidelines

Use this command to set the maximum number of sessions you want to allow in a tunnel.

Example

The following command sets the maximum number of sessions in a tunnel to *5000*:

max-sessions-per-tunnel 5000

max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge in bytes. The challenge is used for authentication purposes during tunnel creation.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-tunnel-challenge-length *bytes*

bytes

Default: 16

Specifies the number of bytes to set the maximum length of the tunnel challenge as an integer from 4 through 32.

Usage Guidelines Use this command to set the maximum length, in bytes, for the tunnel challenge that is used during tunnel creation.

Example

The following command sets the maximum length of the tunnel challenge to *32* bytes:

```
max-tunnel-challenge-length 32
```

max-tunnels

The maximum number of tunnels that the current LNS service can support.

Product PDSN

GGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **max-tunnels** *integer*

integer

Default: 32000

Specifies the maximum number of tunnels as an integer from 1 through 32000.

Usage Guidelines Use this command to set the maximum number tunnels that this LNS service can support at any one time.

Example

Use the following command to set the maximum number of tunnels for the current LNS service to *20000*:

```
max-tunnels 20000
```

nai-construction domain

Designates the alias domain name to use for Network Access Identifier (NAI) construction.

Product PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`nai-construction domain` *`domain_name`* **`{ @ | % | - | \ | # | / }`**
`no nai-construction domain`

no

Deletes the NAI construction domain alias.

***domain_name* {@|%|-|\|#|/}**

Specifies the desired domain name alias followed immediately by a separator from the valid list. *domain_name* must be an alphanumeric string of from 1 through 79 characters.

Usage Guidelines

Use this command to specify the domain alias and separator to use for NAI construction. The specified domain name must be followed by a valid separator (@ | % | - | \ | # | /).

Example

To specify a domain alias of *mydomain@* with a separator of @, enter the following command:

```
nai-construction domain mydomain@
```

To delete the current setting for the NAI construction domain alias, enter the following command:

```
no nai-construction domain
```

newcall

Configures new call related behavior.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`newcall duplicate-subscriber-requested-address { accept | reject }`
`default newcall duplicate-subscriber-requested-address`

default

Sets or restores default value assigned for specified parameter

duplicate-subscriber-requested-address

Configures how duplicate sessions with same address request are handled.

Example

The following command configures new call with duplicate address request to accept:

```
newcall duplicate-subscriber-requested-address accept
```

peer-lac

Adds a peer LAC address for the current LNS service. Up to eight peer LACs can be configured for each LNS service.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
peer-lac { ip_address | ip_address/mask } [ encrypted ] secret secret [
description text ]
no peer-lac ip_address
```

no peer-lac *ip_address*

Deletes the peer LAC IP address specified by *ip_address*. *ip_address* must be entered using IPv4 dotted-decimal notation.

ip_address

The IP address of a specific peer LAC for the current LNS service. *ip_address* must be entered using IPv4 dotted-decimal notation.

ip_address/mask

A network prefix and mask enabling communication with a group of peer LACs. *ip_address* is the network prefix expressed in IPv4 dotted-decimal notation.

mask is the number of bits that defines the prefix.

encrypted

Specifies the encrypted shared key between the LAC and the LNS service.

This 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.

secret *secret*

Designates the secret which is shared between the current LNS service and the peer LAC. *secret* must ben alphanumeric string of 1 through 127 characters that is case sensitive.

description *text*

Specifies the descriptive text to use to describe the specified peer LAC. *text* must be an alphanumeric string of 0 through 79 characters.

Usage Guidelines

Use this command to add a peer LAC address for the current LNS service.

Specific peer LACs can be configured by specifying their individual IP addresses. In addition, to simplify configuration, communication with a group of peer LACs can be enabled by specifying a network prefix and a mask.

Example

The following command adds a peer LAC to the current LNS service with the IP address of *209.165.200.234*, and specifies the shared secret to be *1b34nnf5d*:

```
peer-lac 209.165.200.234 secret 1b34nnf5d
```

The following command enables communication with up to 16 peer LACs on the 192.168.1.0 network each having a secret of *abc123*:

```
peer-lac 209.165.200.224/27 secret abc123
```

The following command removes the peer LAC with the IP address of *209.165.200.244* for the current LNS service:

```
no peer-lac 209.165.200.244
```

proxy-lcp-authentication

Enables/disables proxy LCP authentication.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] proxy-lcp-authentication`

no

Disables the processing of proxy LCP authentication parameters from the LAC.

proxy-lcp-authentication

Default: Enabled

Enables the processing proxy LCP authentication parameters from the LAC.

Usage Guidelines

When enabled, if proxy LCP authentication parameters are received from the LAC and are acceptable, the LNS resumes the PPP session from the authentication phase and goes to the IPCP phase.

When disabled, PPP is always started from the LCP phase, ignoring and discarding any proxy LCP authentication parameters received from the LAC. Disable this feature in situations where accept proxy LCP Auth AVPs that the peer LAC sends should not be expected.

Example

Use the following command to disable the processing of proxy LCP authentication parameters from the LAC:

`no proxy-lcp-authentication`

Use the following command to re-enable the processing of proxy LCP authentication parameters from the LAC:

`proxy-lcp-authentication`

retransmission-timeout-first

Configures the initial timeout for the retransmission of control messages to the peer LAC.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`retransmission-timeout-first` *`integer`*

integer

Default: 1

Specifies the amount of time (in seconds) to wait before sending the first control message retransmission. This value is an integer from 1 through 100.

Usage Guidelines

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted.

Example

The following command sets the initial retransmission timeout to 3 seconds:

```
retransmission-timeout-first 3
```

retransmission-timeout-max

Configures the maximum amount of time that can elapse before retransmitting control messages to the peer LAC.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

retransmission-timeout-max *integer*

integer

Default: 8

Specifies the maximum time (in seconds) to wait before retransmitting control messages. If this limit is reached, the tunnel, and all sessions within it, is cleared. This value is an integer from 1 through 100.

Usage Guidelines

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. This continues until the limit set by this command is reached. If this limit is reached, the tunnel, and all sessions within it, is cleared.

Example

Use the following command to set the maximum retransmission time-out to *10* seconds:

```
retransmission-timeout-max 10
```

setup-timeout

Configures the maximum amount of time, in seconds, allowed for session setup.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

setup-timeout *seconds*

seconds

Default: 60

Specifies the maximum time (in seconds) to wait for the setup of a session. *seconds* must be an integer from 1 through 1000000.

Usage Guidelines

This command controls the amount of time allowed for tunnel establishment with a peer LAC. If this timer is exceeded the tunnel setup is aborted.

Example

The following command configures a maximum setup time of *120* seconds:

```
setup-timeout 120
```

single-port-mode

When enabled, this command sets the LNS to use only the default local UDP port (port 1701) for the life of a tunnel.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default | no ] single-port-mode
```

no

Disable single port mode

Usage Guidelines

Use this command to control the L2TP LNS tunnel local UDP port assignment mode. If single-port-mode is enabled, the LNS-service uses the standard UDP port (port 1701) for the life of the incoming tunnel. Otherwise, it assigns a new local UDP port number for a tunnel when it responds to a tunnel create request received on the standard port number. This is done for load distributing the tunnel processing between multiple tasks within the system to increase the capacity and performance. Even though all L2TP LACs are required to support such dynamic port assignments during tunnel establishments, there exist some LACs that do not support port assignment other than port 1701. This single-port-mode feature can be enabled to support such LAC peers. This configuration must be applied for the LNS-Service before the **bind** command is executed.

Example

The following command enables single port mode for the current LNS service:

```
single-port-mode
```

trap

This command generates SNMP traps.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] trap all
```

no

Disables SNMP traps.

Usage Guidelines

Use this command to enable/disable all supported SNMP traps.

Example

To enable all supported SNMP traps, enter the following command;

```
trap all
```

tunnel-authentication

Enables/disables L2TP tunnel authentication for the LNS service.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] tunnel-authentication
```

no

Disables tunnel authentication

Tunnel authentication is enabled by default.

Usage Guidelines

When tunnel authentication is enabled, a configured shared secret is used to ensure that the LNS service is communicating with an authorized peer LAC. The shared secret is configured by the **peer-lac** command, the **tunnel l2tp** command in the Subscriber Configuration mode, or the **Tunnel-Password** attribute in the subscribers RADIUS profile.

Example

To disable tunnel authentication, use the following command:

```
no tunnel-authentication
```

To re-enable tunnel authentication, use the following command:

```
tunnel-authentication
```

tunnel-switching

Enables or disables the LNS service from creating tunnels to another LAC for an existing tunnel.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] tunnel-switching

no

Disable tunnel switching.

Tunnel switching is enabled by default.

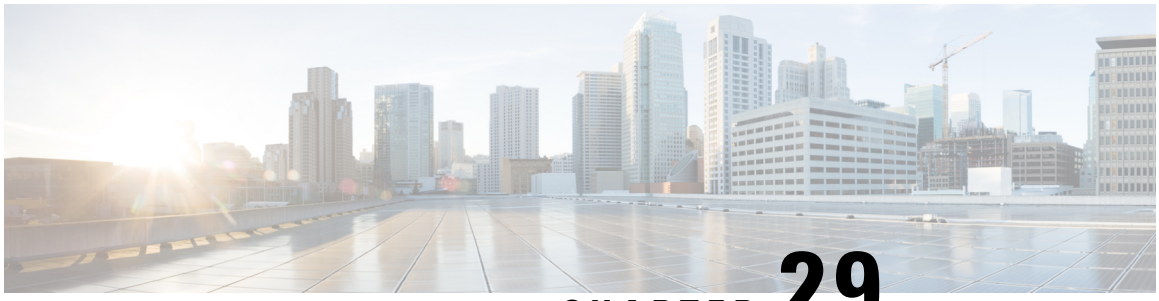
Usage Guidelines

Tunnel switching is when the LNS has a tunnel connected to a LAC and creates a tunnel to a different LAC and routes the data from the original LAC through the new tunnel to the other LAC.

Example

To disable tunnel switching in the LNS, enter the following command;

```
no tunnel-switching
```



CHAPTER 29

Local Policy Actiondef Configuration Mode Commands

Command Modes

The Local Policy Actiondef Configuration Mode is used to define the action definitions to be used for local QoS policies.

Exec > Global Configuration > Local Policy Service Configuration > Local Policy Actiondef Configuration

configure > local-policy-service *service_name* **> actiondef** *actiondef_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-actiondef)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

action

This command configures the action priority for an actiondef.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Local Policy Service Configuration > Local Policy Actiondef Configuration

configure > local-policy-service *service_name* **> actiondef** *actiondef_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-actiondef)#
```

Syntax Description

action priority *priority action_name arguments*
no action priority *priority*

priority *priority*

Specifies a priority for the specified action.

priority must be a unique integer from 1 to 2048.

action_name arguments

The following actions are supported. *arguments* specify a set of parameters to be used when invoking the action.

- **activate-ambr uplink** *bandwidth* **downlink** *bandwidth*

  Sets the aggregated maximum bit rate (AMBR) for the APN.

  Configures uplink and downlink bandwidth. *bandwidth* must be an integer from 1 to 1000000000.

- **activate-flow-detection { initiation | termination } ruledef** *ruledef_name*

  Detects a flow and takes action.

  initiation ruledef: Checks for flow initiation and adds a rule definition.

  termination ruledef: Checks for flow termination and adds a rule definition.

  ruledef_name must be an existing ruledef.

- **activate-lp-rule name** *lprule_name*

  Activates a local-policy rule within service scheme when a subscriber is in the configured RAI or TAI range.

  lprule_name must be an existing local-policy rule within the service scheme expressed as an alphanumeric string of 1 through 63 characters.

Important Local-Policy can support up to 7 lp-rules to be activated for a given session.

When the subscriber moves out of the configured RAI or TAI range, the local-policy rule is deactivated. This option is added as part of Location Based QoS Override feature. For more information on this feature, see the *ECS Administration Guide*.

- **activate-rule name** *rule_name*

  Activates a rule within ECS rulebase for a subscriber.

  rule_name must be an existing rule within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

- **activate-rulebase name** *rulebase_name*

  Associates the session with a specific rulebase.

  rulebase_name must be an existing rulebase within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

- **allow-requested-qos**

  Allow a specific UE initiated QoS request.

- **allow-session**

  Allows the session to continue.

- **deactivate-flow-detection { initiation | termination } ruledef** *ruledef_name*

  Deactivates detection of flow and takes action.

  initiation ruledef: Checks for flow initiation and adds a rule definition.

  termination ruledef: Checks for flow termination and adds a rule definition.

  ruledef_name must be an existing ruledef.

- **deactivate-rule name** *rule_name*

  Deactivates a rule within ECS.

  rule_name must be an existing rule within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

- **deactivate-rulebase name** *rulebase_name*

  Disassociates the rulebase from a session.

  rulebase_name must be an existing rulebase within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

- **default-qos qci** *value* **arp** *value*

  Sets the default QoS parameters for the session

  qci *value* must be an integer from 1 through 254.

  arp *value* must be an integer from 1 through 15 (StarOS v12.1 and earlier) or 1 through 127 (StarOS v12.2 and later).

- **event-triggers { default-bearer-qos-change | ecgi-change | qos-change | tai-change | uli-change }**

  This action specifies to enable the event triggers – Default EPS bearer QoS change event trigger, ECGI-Change event trigger and QoS change event trigger.

  The ECGI-Change event trigger is added as part of Location Based Local-Policy Rule Enforcement feature. For more information on this feature, see the *Gx Interface Support* chapter in the administration guide for the product you are deploying.

  The TAI-Change and ULI-Change event triggers are added as part of Location Based QoS Override feature. For more information on this feature, see the *ECS Administration Guide*.

-

- **reconnect-to-server [send-usage-report] [fetch-usage-from-up]**

  Reconnects to the PCRF server to handle fallback scenario. That is, when the session falls back to local policy, this action specifies to retry connecting to the PCRF server.

  send-usage-report: Triggers CCR-U with volume report immediately. The default behavior is that the CCR-U will not be triggered immediately.

fetch-usage-from-up : This action specifies the fetching of usage report from UP by sending Sx-modify request to UP and uses that usage report values in the CCR-U.

On timer-expiry, if the initial failure is due to CCR-U failure, and if **send-ccru-immediate** is configured, then CCR-U will be sent with the usage report immediately.

- **reject-requested-qos**

  Rejects UE QoS resource request.

- **retry-count** *value*

  Retry action. This applies to start-timer/activate-rule/activate-ruledef.

  value must be an integer from 0 through 65535.

- **start-timer** *name* **duration** *value* **retry-count** *value*

  Starts a named timer. On expiry of this timer, the local policy engine is contacted to initiate the appropriate action, such as termination of a session.

  duration *value*: Enter a timer duration from 0 through 28800 seconds. A value of 0 can be used to leave the local policy until the subscriber disconnects. Default timer value is 14400 (seconds).

  retry-count specifies the maximum number of times the server will be retried before terminating the call.

  retry-count *value* must be an integer from 0 through 65535. Default retry count is 3.

- **stop-timer** *name*

  Stops the designated timer.

- **terminate-session**

  Terminates the session.

Note It is recommended to use a maximum number of 45 action priorities in an actiondef for performance reasons.

no action priority *priority*

Deletes the specified action.

Usage Guidelines

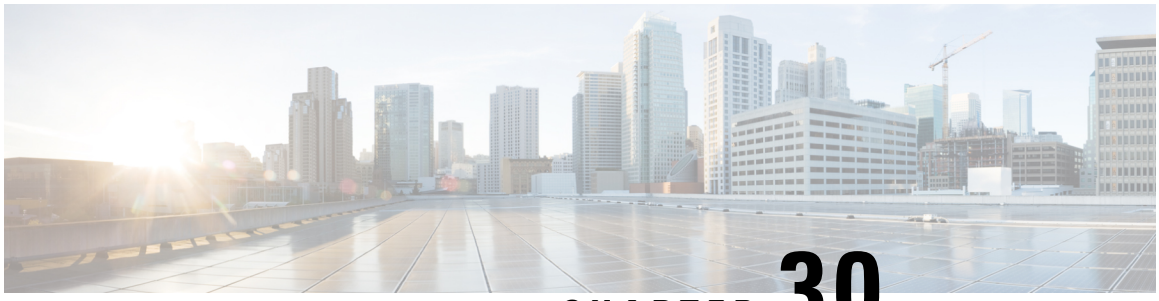
Use this command to enable the setting of parameters to be used when invoking actions. Actions are a series of operations that are triggered by activated rules.

This command can be entered multiple times to configure multiple actions for an actiondef. The actions are examined in priority order until a match is found and the corresponding action is applied.

Example

The following command creates an action to allow a session to continue with priority set to *125*:

```
action priority 125 allow-session
```



CHAPTER 30

Local Policy Eventbase Configuration Mode Commands

Command Modes

The Local Policy Eventbase Configuration Mode is used to configure the events to be used for local QoS policies.

Exec > Global Configuration > Local Policy Service Configuration > Local Policy Eventbase Configuration

configure > local-policy-service *service_name* **> eventbase** *eventbase_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-local-policy-eventbase)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

rule

This command enables the setting of event rules. An event is something that occurs in the system which would trigger a set of actions to take place, such as new-call or rat-change.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Local Policy Service Configuration > Local Policy Eventbase Configuration

configure > local-policy-service *service_name* **> eventbase** *eventbase_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-eventbase)#
```

Syntax Description

rule priority *priority* **[event** *list_of_events* **] ruledef** *ruledef_name* **actiondef** *actiondef_name* **[continue]**
no rule priority *priority*

priority *priority*

Specifies a priority for the specified rule.

priority must be unique and an integer from 1 to 2048.

event *list_of_events*

The event is defined by any of the following events. Upon triggering the event, the rules specified in the eventbase are executed.

- **apn-ambr-mod-failure**: This event is triggered as a result of a APN AMBR Modification failure.
- **def-eps-bearer-qos-mod-failure**: This event is triggered as a result of a Default EPS bearer QoS Modification failure.
- **default-qos-change**: This event is triggered as a result of a default QoS change.
- **ecgi-change**: This event is triggered as a result of any change relating to ECGI. This event trigger is added as part of Location Based Local-Policy Rule Enforcement feature. For more information on this feature, see the *Gx Interface Support* chapter in the administration guide for the product you are deploying.
- **fallback**: This event is triggered as a result of fallback from PCRF.
- **location-change**: This event is triggered as a result of any change relating to location.
- **new-call**: This event is initiated when a new call is established.
- **out-of-credit**: This event is initiated on out of OCS credit.
- **realloc-of-credit**: This event is initiated on OCS reallocation of credit.
- **request-qos**: This event is initiated as the result of UE requested QoS.
- **rule-report-status**: This event is initiated as the result of rule report status provided to PCRF.
- **service-flow**: This event is triggered as a result of a new service flow being detected for the subscriber.
- **tai-change**: This event is triggered as a result of any change relating to TAI. This event trigger is added as part of Location Based QoS Override feature. For more information on this feature, see the *ECS Administration Guide*.
- **timer-expiry**: This event is triggered as a result of the expiry of Local Policy Timer.

ruledef *ruledef_name*

Associates the rule with a specific ruledef.

ruledef_name must be an existing ruledef within this local QoS policy service.

actiondef *actiondef_name*

Associates the rule with a specific actiondef.

actiondef_name must be an existing actiondef within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

continue

Subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

no rule priority *priority*

Deletes the specified rule.

Usage Guidelines

Use this command to create, configure, or delete event rules.

The rules are executed in priority order, and if the rule is matched the action specified in the actiondef is executed. If an event qualifier is associated with a rule, the rule is matched only for that specific event. If a qualifier of **continue** is present at the end of the rule, the subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

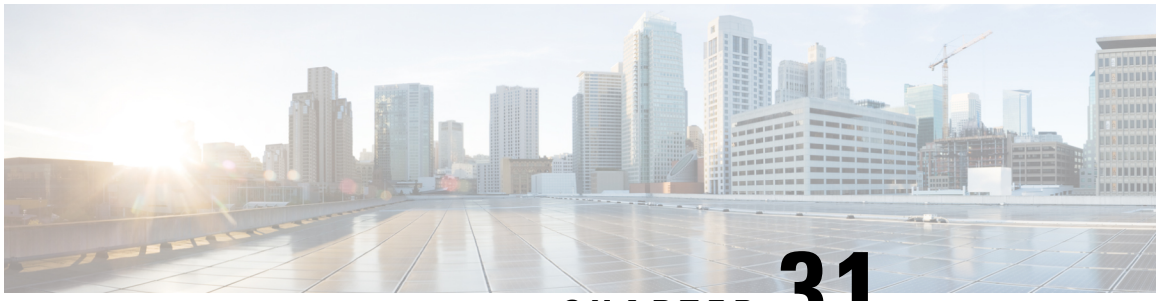
This command can be entered multiple times to configure multiple rules for an eventbase.

Important It is recommended to use a maximum number of 20 rule priorities in an event base for performance reasons.

Example

The following command creates a rule with priority set to *2* and associated with **ruledef** *rule5* and **actiondef** *action7*:

```
rule priority 2 ruledef rule5 actiondef action7
```



CHAPTER 31

Local Policy Ruledef Configuration Mode Commands

Command Modes

The Local Policy Ruledef Configuration Mode is used to configure the rule definitions to be used for local QoS policies.

Exec > Global Configuration > Local Policy Service Configuration > Local Policy Ruledef Configuration

configure > local-policy-service *service_name* **> ruledef** *ruledef_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-ruledef)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

condition

This command is used to configure the conditions which trigger the ruledef event.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Local Policy Service Configuration > Local Policy Ruledef Configuration

configure > local-policy-service *service_name* **> ruledef** *ruledef_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-ruledef)#
```

Syntax Description

condition priority *priority* **{** *variable* **{ eq | ge | gt | le | lt | match | ne | nomatch }** *regex* **|** *string_value* **|** *int_value* **|** *set* **}**
no condition priority *priority*

priority *priority*

Specifies a priority for the specified condition.

priority must be unique and an integer from 1 to 2048.

variable

The following variables are supported:

- **3g-uli mcc** *mcc_num* **mnc** *mnc_num* **tac**

  Configures 3G-ULI parameter with values for MCC, MNC and LAC. Operator takes specific action or applies local-policy rule based on the 3G-ULI value in Change event notification from MME.

  - **mcc** *mcc_num* : MCC is a three digit number from 001 to 999. It is a string of size 3 to 3.
  - **mnc** *mnc_num* : MNC is a two or three digit number from 01 to 999. It is a string of size 2 to 3.
  - **lac**: LAC is a 4 byte field. It is a string of 4 hexadecimal values from 0x1 to 0xffff.

- **apn**

  The APN associated with the current session expressed as an alphanumeric string of 1 through 63 characters.

- **arp**

  The ARP value associated with the current session expressed as an integer from 1 through 15.

- **bandwidth**

  Total bandwidth associated with the QCI and ARP value associated with the request, expressed as an integer from 0 through 1000000000.

- **bsid**

  Base Station Identifier associated with the subscriber expressed as an alphanumeric string of 1 through 63 characters.

- **cause-code**

  Failure Cause Code associated with the subscriber expressed as an alphanumeric string of 1 through 63 characters.

- **date**

  Date value to match. <Clock in format YYYY:MM:DD>

- **day-of-month**

  The day of the month to match the rule to, expressed as an integer from 1 through 31.

- **day-of-week**

Sunday...Saturday, expressed as an integer from 1 to 7.

- **ecgi mcc** *mcc_num* **mnc** *mnc_num* **eci**

  Configures E-UTRAN Cell Global Identifier with values for MCC, MNC and ECI. Operator takes specific action or applies local-policy rule based on the ECGI value in ECGI-Change event notification from MME.

  - **mcc** *mcc_num* : MCC is a three digit number from 001 to 999. It is a string of size 3 to 3.
  - **mnc** *mnc_num* : MNC is a two or three digit number from 01 to 999. It is a string of size 2 to 3.
  - **eci**: ECI is a hexadecimal number from 0x1 to 0xffffffff. It is a string of size 1 to 7.

- **final-unit-action { redirect | restrict-access | terminate } [filter-id] [eq | ge | gt | le | lt | match | ne | nomatch]** *filter-id*

  This variable allows configuring different filter IDs and different Final-Unit-Action (FUA) actions for the events like out-of-credit, etc. Based on the FUA and filter ID values, local policy engine will either install pre-configured redirection rules/pre-configured rule that might drop all packets, or push a different rule/policy.

  When the FUA received from the session manager during out-of-credit scenario matches with the configured FUA, then one of the following actions will be taken. If multiple filter-ids are configured, then at least one filter-id should be matched.

  - **redirect**: Redirects the service
  - **restrict-access** : Restricts the service
  - **terminate**: Terminates the service

  filter-id: This variable denotes the name of the filter list for the user. *filter-id* is a string of 1 through 128 characters. Note that **match**, **nomatch**, **ne**, and **eq** are more appropriate operators though other values can also be used. Wild card values can be specified for string match.

Important This feature of supporting FUA in local policy will be active only when Gx Assume Positive is active.

- **imeisv**

  IMEISV of the user equipment expressed as an alphanumeric string of 1 through 63 characters.

- **imsi**

  IMSI associated with the subscriber expressed as an alphanumeric string of 1 through 63 characters.

- **local-policy-mode [fallback | dual-mode | lp-only]**

  This variable allows selecting different actions for different modes like local-policy only, dual-mode, and fallback mode for the same event.

  - **fallback**: This mode indicates that the action has to be taken only when the call is with local-policy because of failure-handling.
  - **dual-mode**: This mode indicates that action has to be taken if the call is in dual-mode wherein both PCRF and local-policy co-exist.
  - **lp-only**: This mode indicates that action has to be taken when only local-policy exists and PCRF does not.

- **meid**

  MEID associated with the subscriber expressed as an alphanumeric string of 1 through 63 characters.

- **month-of-year**

  Jan, Feb....Dec, expressed as an integer from 1 through 12.

- **msisdn**

  MSISDN associated with the session expressed as an alphanumeric string of 1 through 63 characters.

- **nai**

  NAI associated with the session expressed as an alphanumeric string of 1 through 63 characters.

- **pdn-type**

  Type of PDNs associated with the same APN.

  - **IPV4**: IPv4 PDN Type
  - **IPV4V6**: IPv4v6 PDN Type
  - **IPV6**: IPv6 PDN Type

- **qci**

  QCI associated with the current event expressed as an integer from 1 through 254.

- **radio-access-technology**

  Radio access technology associated with the subscriber:

  - **cdma-1xrtt**: CDMA 1X RTT radio access technology
  - **cdma-evdo**: CDMA-EVDO radio access technology
  - **cdma-evdo-reva**: CDMA EVDO REVA radio access technology
  - **cdma-other**: Other CDMA radio access technologies
  - **ehrpd**: EHRPD radio access technology
  - **eutran**: EUTRAN radio access technology
  - **gan**: GAN radio access technology
  - **gprs-geran**: GPRS GERAN radio access technology
  - **gprs-other**: Other GPRS radio access technology
  - **hspa**: HSPA radio access technology
  - **unknown**: Unknown radio access technology
  - **wcdma-utran**: WCDMA UTRAN radio access technology
  - **wimax**: WiMax radio access technology
  - **wireless-lan**: Wireless LAN radio access technology

- **serving-node-address**

IP address associated with the current node serving the subscriber entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **serving-plmn**

  PLMN associated with the current node serving the subscriber expressed as an alphanumeric string of 1 through 63 characters.

- **tai mcc** *mcc_num* **mnc** *mnc_num* **tac**

  Configures Tracking Area Identification associated with the subscriber. Operator takes specific action or applies local-policy rule based on the TAI value in TAI-Change event notification from MME.

  - **mcc** *mcc_num* : MCC is a three digit number from 001 to 999. It is a string of size 3 to 3.
  - **mnc** *mnc_num* : MNC is a two or three digit number from 01 to 999. It is a string of size 2 to 3.
  - **tac**: TAC is a 4 byte field. It is a string of 4 hexadecimal values from 0x1 to 0xffff.

- **time-of-day**

  Time associated with the change. <Clock in format HH:mm:ss or HH:mm >

eq | ge | gt | le | lt | match | ne | nomatch

eq: Operation equal to

ge: Operation greater than or equal to

gt: Operation greater than

le: Operation less than or equal to

lt: Operation less than

match: Operation match

ne: Operation not equal to

nomatch: Operation nomatch

no condition priority *priority*

Deletes the specified condition.

Usage Guidelines

Use this command to configure the conditions which trigger the ruledef event. A ruledef represents a set of matching conditions.

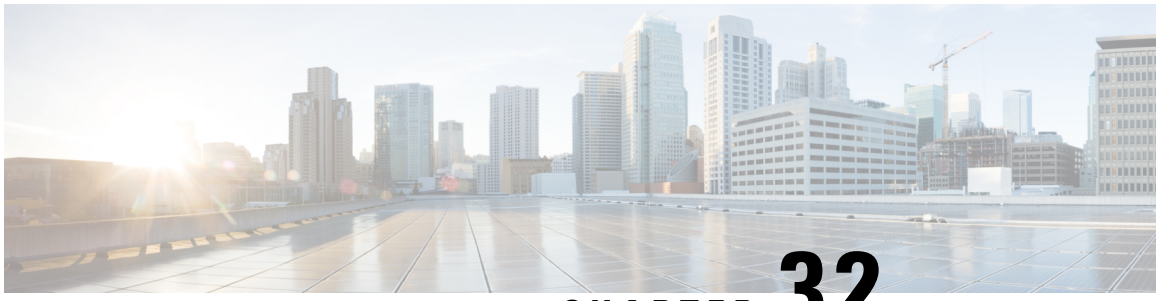
This command can be entered multiple times to configure multiple conditions for a ruledef. The conditions are examined in priority order until a match is found and the corresponding condition is applied.

Note It is recommended to use a maximum number of 20 condition priorities in a ruledef for performance reasons.

Example

The following command creates a condition with priority set to *5* and configured match apn *myapn**:

```
condition priority 5 apn match myapn*
```



CHAPTER 32

Local Policy Service Configuration Mode Commands

Important A maximum of 16 local QoS policy services are supported.

Command Modes

The Local Policy Service Configuration Mode is used to configure the local QoS policy for one or more services.

Exec > Global Configuration > Local Policy Service Configuration

configure > local-policy-service *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-service)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

actiondef

This command enables creating, configuring, or deleting action definitions for an event.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Local Policy Service Configuration

configure > local-policy-service *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-service)#
```

Syntax Description

actiondef *actiondef_name* **[-noconfirm]**
no actiondef *actiondef_name*

no

Deletes the specified actiondef from the local QoS policy service.

actiondef_name

Specifies name of the actiondef.

actiondef_name must be unique within the service expressed as an alphanumeric string of 1 through 63 characters.

If the named actiondef does not exist, it is created, and the CLI mode changes to the Local Policy Actiondef Configuration Mode wherein the actiondef can be configured.

If the named actiondef already exists, the CLI mode changes to the Local Policy Actiondef Configuration Mode for that actiondef.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create, configure, or delete an actiondef. The actiondef configuration is used to configure the action definitions for an event. The event ruledef will have one or more rules and associated action(s).

This command can be entered multiple times to specify multiple actiondefs.

Important It is recommended to use a maximum number of 45 actiondefs in a local QoS policy service for performance reasons. An actiondef can be referenced by multiple eventbases.

Entering this command results in the following prompt:

```
[context_name]hostname(config-local-policy-actiondef)#
```

Local Policy Actiondef Configuration Mode commands are defined in the *Local Policy Actiondef Configuration Mode Commands* chapter.

Example

The following command creates an actiondef named *actiondef1* and enters the Local Policy Actiondef Configuration Mode:

```
actiondef actiondef1
```

eventbase

This command enables creating, configuring, or deleting an eventbase.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Local Policy Service Configuration

configure > local-policy-service *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-service)#
```

Syntax Description

eventbase *eventbase_name* **[-noconfirm]**
no eventbase *eventbase_name*

no

Deletes the specified eventbase from the local QoS policy service.

eventbase_name

Specifies name of the eventbase.

eventbase_name must be unique within the service expressed as an alphanumeric string of 1 through 63 characters.

Important Currently, only one eventbase is supported, and it must be named "default".

If the named eventbase does not exist, it is created, and the CLI mode changes to the Local Policy Eventbase Configuration Mode wherein the eventbase can be configured.

If the named eventbase already exists, the CLI mode changes to the Local Policy Eventbase Configuration Mode for that eventbase.

Note It is recommended to use a maximum number of 20 rule priorities in an event base for performance reasons.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create, configure, or delete an eventbase.

Entering this command results in the following prompt:

```
[context_name]hostname(config-local-policy-eventbase)#
```

Local Policy Eventbase Configuration Mode commands are defined in the *Local Policy Eventbase Configuration Mode Commands* chapter.

Example

The following command creates an eventbase named *default* and enters the Local Policy Eventbase Configuration Mode:

eventbase default

ruledef

This command enables creating, configuring, or deleting a rule definition.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Local Policy Service Configuration

configure > local-policy-service *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-service)#
```

Syntax Description

ruledef *ruledef_name* **[-noconfirm]**
no ruledef *ruledef_name*

no

Deletes the specified ruledef from the local QoS policy service.

ruledef_name

Specifies name of the ruledef.

ruledef_name must be unique within the service expressed as an alphanumeric string of 1 through 63 characters.

If the named ruledef does not exist, it is created, and the CLI mode changes to the Local Policy Ruledef Configuration Mode wherein the ruledef can be configured.

If the named ruledef already exists, the CLI mode changes to the Local Policy Ruledef Configuration Mode for that ruledef.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to create, configure, or delete a ruledef. A ruledef represents a set of matching conditions.

This command can be entered multiple times to specify multiple ruledefs.

Important It is recommended to use a maximum number of 20 ruledefs in a local QoS policy service for performance reasons.

Entering this command results in the following prompt:

```
[context_name]hostname(config-local-policy-ruledef)#
```

Local Policy Ruledef Configuration Mode commands are defined in the *Local Policy Ruledef Configuration Mode Commands* chapter.

Example

The following command creates a ruledef named *rule5* and enters the Local Policy Ruledef Configuration Mode:

ruledef rule5

suppress-cra

This command allows to suppress the Change Reporting Action (CRA) for event triggers enabled in local policy configurations.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Local Policy Service Configuration

configure > local-policy-service *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-service)#
```

Syntax Description

suppress-cra event-triggers { ecgi-change | tai-change | uli-change } +
no suppress-cra

no

This variant is used to configure the default behavior. By default, the CRA notification is sent to MME if one or a combination of these event triggers is installed.

suppress-cra event-triggers { ecgi-change | tai-change | uli-change } +

This keyword restricts sending of CRA towards MME depending on the ECGI-Change, TAI-Change and ULI-Change event triggers configured in local-policy service.

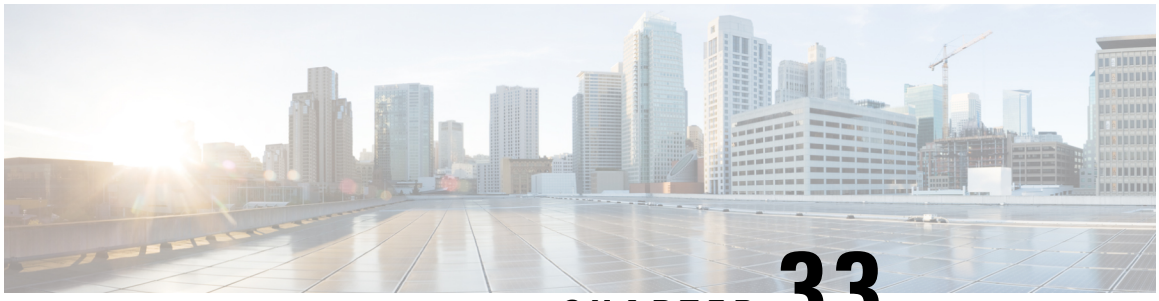
Usage Guidelines

Use this command to control the CRA notification towards MME based on the configured event triggers in the local-policy configuration.

Example

The following command suppresses CRA if ECGI-Change event trigger is installed:

```
suppress-cra event-triggers ecgi-change
```



CHAPTER 33

Location Service Configuration Mode Commands

The Location Service Configuration Mode is used to manage LoCation Services (LCS). Using LCS, the system (MME or SGSN) can collect and use or share location (geographical position) information for connected UEs in support of a variety of location services.

Command Modes

Exec > Global Configuration > Context Configuration > Location Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

associate

Associates or disassociates supportive interfaces or services with this location service instance.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Location Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
associate { diameter { dictionary standard | endpoint endpoint_name } |
map-service map_svc_name | sls-service sls_svc_name  }
default associate diameter dictionary
no associate { diameter endpoint | map-service | sls-service }
```

default

Returns the command to its default value of 'standard'.

no

Disassociates a previously associated interface or service with this location service.

diameter dictionary standard

Associates a Diameter dictionary with this location service. The standard dictionary contains definitions per the 3GPP definition.

diameter endpoint *endpoint_name*

Specifies the Diameter endpoint for this location service, which includes the hostname, peer configuration, and other Diameter base configuration.

map-service *map_svc_name*

Associates a Mobile Application Part (MAP) service with this location service.

This keyword is applicable for SGSN only.

map_sv_svc_name specifies the name for a pre-configured MAP service to associate with this location service.

sls-service *sls_svc_name*

Associates an SLs service with this location service. The SLs service provides an interface between the MME and Evolved Serving Mobile Location Center (E-SMLC).

This keyword is applicable for MME only.

sls_svc_name specifies the name for a pre-configured SLs service to associate with this location service.

Usage Guidelines

Use this command to specify the Diameter dictionary and endpoint to be used for this location service, or associate supportive services with this location service.

The location service provides SLg (MME) interface support or Lg (SGSN) interface support via the Diameter protocol between the MME or SGSN and the GLMC.

Example

The following command associates a pre-configured Diameter endpoint named *test12* to this location service:

```
associate diameter endpoint test12
```

destination-host

Configures the host name of the GLMC to be used for this Location service. When defined, this host name is populated in the destination-host AVP.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Location Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

destination-host *destination_host*
no destination-host

no

Removes the configured destination host.

destination_host

Defines the host name to be used, as an alphanumeric string from 1 to 63 characters.

Usage Guidelines

To comply with 3GPP TS29.172, the Destination-Host AVP is sent to the GMLC for all the Location Report Request (LRR) messages initiated by MME.

Use this command to configure the destination-host AVP for this Location service.

If this command is not configured, the peer host name configured in the diameter endpoint is encoded as Destination-Host AVP. Refer to the **peer** command in the Diameter Endpoint Configuration Mode.

Example

The following command specifies a destination host named *host123* for the location service:

```
destination-host host123
```

pla

Configures the experimental result code for pla.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Location Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

pla ue-state [detached | not-reachable]send experimental-result-code*experimental_result_code*
[no] pla ue-state [detached | not-reachable]send experimental-result-code

no

Disables the experimental result code for pla.

ue-state

Specifies that the pla can be either not-reachable (No paging Response) or detached.

detached

Specifies the UE disconnecting.

not-reachable

Specifies no paging response.

send

Specifies sending of ue-state.

experimental-result-code *experimental_result_code*

Specifies the result code value to be encoded in PLA depending on ue-state when PLR is received with GMLC Location type set to Current or Last Known Location.

experimental_result_code must be an integer between 1000 and 6000.

slr

Controls the Subscriber Location Report (SLR) trigger generated from MME towards GMLC for emergency calls, based on the dedicated bearer states either creation or deletion.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **`[ no ] slr emergency dedicated-bearer-only`**

no

Disables the SLR trigger for dedicated bearer states.

slr

Specifies the SLR message from MME.

emergency

Specifies the trigger for sending the SLR message for emergency calls.

dedicated-bearer-only

Specifies the MME to trigger SLR towards GMLC upon dedicated bearer creation and deletion.

Usage Guidelines Use this command to enable or disable the Subscriber Location Report (SLR) message trigger for emergency calls based on the dedicated bearer states either creation or deletion. In case of multiple dedicated bearers, SLR message with Call-Origination is sent upon the creation of first dedicated bearer and Call-Release is sent upon the deletion of last dedicated bearer irrespective of QCI. This command will override the current/default behavior of MME which initiates the SLR towards GMLC only upon Emergency Attach/PDN creation/PDN deletion and Detach.

By default, MME triggers the SLR message towards GMLC upon successful Emergency Attach/PDN creation/PDN deletion and Detach with appropriate event type (Call-Origination/Call-Release/Call-Handover).

timeout

Configures the timers used to control various location service procedures.

Product SGSN

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

timeout { area-event-invoke-timer *area_event_timer* **| lcsn** *lcsn_seconds* **| periodic-event-invoke-timer** *period_event_timer* **| ue-available-guard-timer** *ue_guard_timer* **}**
default timeout { area-event-invoke-timer | lcsn | periodic-event-invoke-timer | ue-available-guard-timer }

default

Resets the specified timer to the default value.

area-event-invoke-timer *area_event_timer*

This timer, set in seconds, is used to guard the area event invoke procedure.

area_evt_timer is an integer from 10 through 20. Default is 15.

lcsn *lcsn_seconds*

Sets the NAS location service notification timer defining how long the SGSN will wait (in seconds) before aborting the Location Service Request, and release all resources allocated for the transaction.

lcsn_seconds is an integer from 10 through 20. Default is 15.

periodic-event-invoke-timer *period_event_timer*

Thi timer, set in seconds, is used to guard the period location invoke procedure.

period_evt_timer is an integer from 10 to 20. Default is 15.

ue-available-guard-timer *ue_guard_timer*

This timer, set in seconds, is used to guard the packet-switched deferred location request (UE available event) procedures.

ue_guard_timer is an integer from 10 to 600. Default is 600.

Usage Guidelines

Use this command to set the amount of time the SGSN waits to perform various location service procedures.

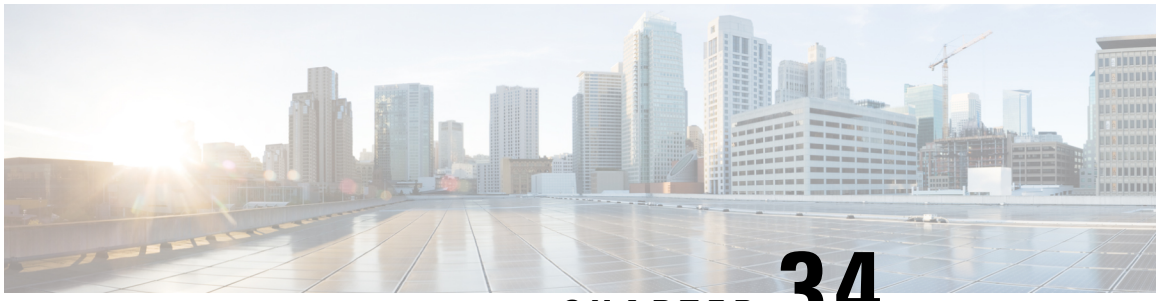
Example

The following command is used to set the time the SGSN will wait, for example *12* seconds, before aborting the Location Service Request:

```
timeout lcns 12
```

The following command is used to set the timeout for the UE available guard timer to *460* seconds:

```
timeout ue-available-guard-timer 460
```



CHAPTER 34

Logical eNode Configuration Mode Commands

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. Commands in this configuration mode must not be used in these releases. For more information, contact your Cisco account representative.

The Logical eNodeB configuration option enables the configuration of one or more logical eNodeBs within the HeNB-GW. The Logical eNodeB configuration can be used to support load balancing within a pool of TAIs.

Command Modes Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration

configure > context *context_name* **> henbgw-network-service** *service_name* **> logical-enb global-enb-id plmn id mcc** *mcc_id* **mnc** *mnc_id* { **home-enb-id** *henb_id* **| macro-enb-id** *menb_id* }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(logical-enb)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

associate mme-pool

Associates a previously configured MME pool to this logical eNodeB. An MME pool must be configured in LTE Policy Configuration mode before using this configuration.

Product

HeNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration

configure > context *context_name* **> henbgw-network-service** *service_name* **> logical-enb global-enb-id plmn id mcc** *mcc_id* **mnc** *mnc_id* { **home-enb-id** *henb_id* **| macro-enb-id** *menb_id* }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(logical-enb)#
```

Syntax Description

```
associate mme-pool pool_name
no associate mme-pool
```

no

Removes the associated MME pool from this logical eNodeB configuration.

pool_name

Identifies the name of the pre-configured MME pool to associate with this logical eNodeB.

pool_name is an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to bind/associate a pre-configured MME pool to this logical eNodeB. The MME pool can be configured in LTE Policy configuration mode. The associate configuration is used to establish associations with other helper services in general.

Each logical eNodeB can connect up to 8 MMEs. Since 8 logical eNodeBs can be configured per HeNB-GW Network service, a total of 64 associations can be established between HeNB-GW and MME.

Example

The following command associates an MME pool named *pool1* with specific logical eNodeB:

```
associate mme-pool pool1
```

associate tai-list-db

Associates a previously configured TAI database name to this logical eNodeB. A TAI database name for TAI configuration must be configured in LTE Policy Configuration mode before using this configuration.

Product

HeNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration

configure > context *context_name* **> henbgw-network-service** *service_name* **> logical-enb global-enb-id plmn id mcc** *mcc_id* **mnc** *mnc_id* { **home-enb-id** *henb_id* **|** **macro-enb-id** *menb_id* }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(logical-enb)#
```

Syntax Description

associate tai-list-db *tai_db_name*
no associate tai-list-db

no

Removes the associated TAI database from this logical eNodeB configuration.

tai_db_name

Identifies the name of the pre-configured TAI database to associate with this logical eNodeB.

tai_db_name is an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to bind/associate a pre-configured TAI database to this logical eNodeB. The MME pool can be configured in LTE Policy configuration mode. The associate configuration is used to establish associations with other helper services in general.

A maximum number of 8 TAI databases are supported. Each TAI database can accommodate up to 256 configurations of Tracking Area Codes (TACs). Therefore a total of 2048 TACs are supported.

Example

The following command associates a TAI database named *henbtai1* with specific logical eNodeB:

```
associate tai-list-db henbtai1
```

bind s1-mme

Binds the pre configured Local SCTP IP Address for S1 association to MME.

Product

HeNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration

configure > context *context_name* **> henbgw-network-service** *service_name* **> logical-enb global-enb-id plmn id mcc** *mcc_id* **mnc** *mnc_id* { **home-enb-id** *henb_id* **|** **macro-enb-id** *menb_id* }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(logical-enb)#
```

Syntax Description

```
bind s1-mme { ipv4-address | ipv6-address } ip_addr
no bind s1-mme
```

no

Removes the binding of S1-MME interface from this logical eNodeB configuration.

ip_addr

Identifies the IP address of the S1-MME interface to associate with this HeNB-GW Network service.

addr_val must be entered in the IPv4 (dotted decimal notation) or IPv6 (: / :: notation).

Usage Guidelines

Use this command to bind the pre-configured IPv4 / IPv6 address of the S1-MME interface to the logical eNodeB.

Example

The following command binds the S1-MME interface having *209.165.200.235* IP address with specific logical eNodeB.

```
bind s1-mme ipv6-address 209.165.200.235
```

s1-mme ip qos-dscp

This command configures the quality of service (Do's) differentiated service code point (DSCP) marking for IP packets sent out on the S1-MME interface, from the HeNB-GW to the MME(s).

Product

HeNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration

configure > **context** *context_name* > **henbgw-network-service** *service_name* > **logical-enb global-enb-id plmn id mcc** *mcc_id* **mnc** *mnc_id* { **home-enb-id** *henb_id* | **macro-enb-id** *menb_id* }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(logical-enb)#
```

Syntax Description

```
s1-mme ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 |
af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5
 | cs6 | cs7 | ef }
default s1-mme ip qos-dscp
```

qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

Default: **af11**

Specifies the DSCP for the specified QoS traffic pattern. **qos-dscp** can be configured to any one of the following:

af11: Assured Forwarding 11 per-hop-behavior (PHB)

af12: Assured Forwarding 12 PHB

af13: Assured Forwarding 13 PHB

af21: Assured Forwarding 21 PHB

af22: Assured Forwarding 22 PHB

af23: Assured Forwarding 23 PHB

af31: Assured Forwarding 31 PHB

af32: Assured Forwarding 32 PHB

af33: Assured Forwarding 33 PHB

af41: Assured Forwarding 41 PHB

af42: Assured Forwarding 42 PHB

af43: Assured Forwarding 43 PHB

be: Best effort forwarding PHB

cs0: Designates use of Class Selector 0 PHB.This is same as DSCP Value BE.

cs1: Designates use of Class Selector 1 PHB

cs2: Designates use of Class Selector 2 PHB

cs3: Designates use of Class Selector 3 PHB

cs4: Designates use of Class Selector 4 PHB

cs5: Designates use of Class Selector 5 PHB

cs6: Designates use of Class Selector 6 PHB

cs7: Designates use of Class Selector 7 PHB

ef: Expedited forwarding PHB

Usage Guidelines

DSCP levels can be assigned to specific traffic patterns to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the S1-MME interface(s).

Example

The following command sets the DSCP-level for data traffic sent over the S1-MME interface to **af12**:

```
s1-mme ip qos-dscp af12
```

s1-mme sctp port

This command configures the local Stream Control Transmission Protocol (SCTP) port used for binding the SCTP socket to communicate with the MMEs over S1-MME interface.

Product

HeNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration

configure > context *context_name* **> henbgw-network-service** *service_name* **> logical-enb global-enb-id plmn id mcc** *mcc_id* **mnc** *mnc_id* { **home-enb-id** *henb_id* **|** **macro-enb-id** *menb_id* }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(logical-enb)#
```

Syntax Description

s1-mme sctp port *port_num*
default s1-mme sctp port

default

Sets the SCTP port to the default value of 36412 to communicate with the MMEs using S1-MME interface.

port_num

Specifies the SCTP port number to communicate with the HeNBs using S1-MME interface as an integer from 1 through 65535. Default: 36412

Usage Guidelines

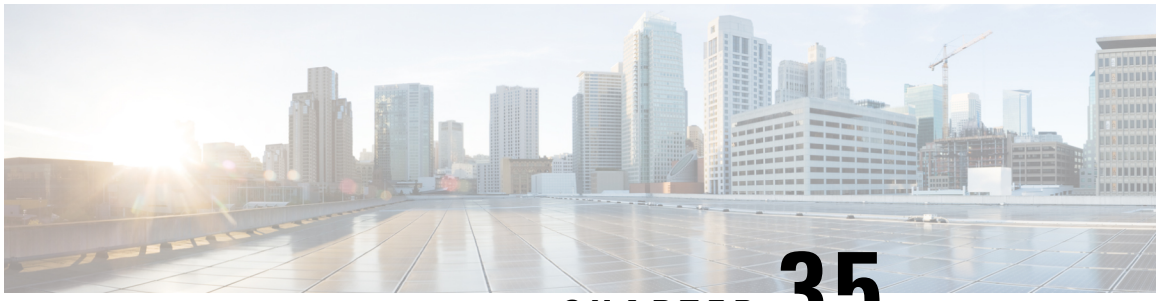
Use this command to assign the SCTP port with SCTP socket to communicate with the HeNB using S1AP.

Only one SCTP port can be associated with one MME service.

Example

The following command sets the SCTP port number **699** to interact with Home eNodeB using S1AP on S1-MME interface:

```
s1-mme sctp port 699
```



CHAPTER 35

Loopback Interface Configuration Mode Commands

Command Modes

The Loopback Interface Configuration Mode is used to create and manage an internal IP network address. The address must be configured with a 32-bit mask.

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **loopback**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

Important Available commands or keywords/variables vary based on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

crypto-map

Applies the specified IPSec crypto-map to this interface.

Product All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **loopback**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

Syntax Description

crypto-map *map_name* **[secondary-address** *sec_ipv4v6_addr* **]**
no crypto-map *map_name*

no

Deletes the application of the crypto map on this interface.

map_name

Specifies the name of the crypto map being applied as an alphanumeric string of 1 through 127 characters that is case sensitive.

secondary-address *sec_ipv4v6_addr*

Applies the crypto map to the secondary address for this interface. *sec_ipv4v6_addr* must be an IPv4 address in dotted-decimal notation or an IPv6 address in colon-separated hexadecimal notation.

Usage Guidelines

In order for ISAKMP and/or manual crypto maps to work, they must be applied to a specific interface using this command. Dynamic crypto maps should **not** be applied to interfaces.

The crypto map must be configured in the same context as the interface.

Example

The following command applies the IPSec crypto map named **cmap1** to this interface:

```
crypto-map cmap1
```

description

Sets the descriptive text for the current interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **loopback**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

Syntax Description

```
description text
no description
```

no

Clears the description for the interface.

text

Specifies the descriptive text as an alphanumeric string of 0 through 79 characters.

Usage Guidelines

Set the description to provide useful information on the interface's primary function, services, end users, etc. Any information useful may be provided.

Example

The following command sets the description **sampleInterfaceDescriptiveText** for the interface:

```
description sampleInterfaceDescriptiveText
```

ip address

Specifies the primary and optional secondary IPv4 addresses and subnets for this interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **loopback**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

Syntax Description

```
ip address ipv4_address { mask | /mask } [ secondary ipv4_address
] [ srp-activate ]
no ip address ipv4_address
```

no

Removes the IPv4 address from this interface.

***ipv4_address*{ mask | /*mask* }**

Configures the IPv4 address and mask for the interface. *ipv4_address* must be entered using IPv4 dotted-decimal notation. IPv4 dotted-decimal or CIDR notation is accepted for the mask.

Important For IPv4 addresses, 31-bit subnet masks are supported per RFC 3021.

secondary *ipv4_address*

Configures a secondary IPv4 address on the interface.

Important You must configure the primary IPv4 address before you will be allowed to configure a secondary address.

srp-activate

Activates the IPv4 address for Interchassis Session Recovery (ICSR). Enable this IPv4 address when the Service Redundancy Protocol (SRP) determines that this chassis is ACTIVE. Requires an ICSR license on the chassis to activate.

Usage Guidelines Use this command to specify the primary and optional secondary IPv4 addresses and subnets for this interface.

Example

The following command configures an IPv4 address **209.165.200.224/27** for this interface:

```
ip address 209.165.200.224/27
```

ip ranged-address

Specifies an IPv4 address and subnet; all addresses in the subnet are local. Configures the range or group of IP address for the loopback interface. This command enables support for multiple Enterprise HAs in one HA service.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **loopback**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

Syntax Description **`[ no ] ip ranged-address`** *`ipv4_address`* **`[ mask | /`***`mask`***` ] [ srp-activate ]`**

no

Removes the IPv4 ranged address from this interface.

***ipv4_address*[mask | /*mask*]**

Configures the IPv4 address and mask for the interface. *ipv4_address* must be entered using IPv4 dotted-decimal notation. IPv4 CIDR notation is accepted for the mask.

Important This interface configuration is allowed only for IPv4 addresses and must be bound to the HA Service.

srp-activate

Enables the IPv6 address when the Service Redundancy Protocol determines this chassis to be ACTIVE.

Usage Guidelines

This command provides Enterprise HA support on HA service for multiple enterprise nodes. Refer *HA Administration Guide* for more information.

This IP address range configuration must meet the following criteria:

- The ranged address must be a primary address.
- The ranged address must be unique across the interface configuration.
- The ranged address must be unique across the context.
- The IP address specified in the ranged address must not be part of any other interface.
- The ranged-address can be an SRP-activated address.

Example

The following command configures a ranged IPv4 address **209.165.201.0/27** for this interface:

```
ip ranged-address 209.165.201.0/27
```

ip vrf

Associates this interface with a specific Virtual Routing and Forwarding (VRF) table.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **loopback**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

Syntax Description

```
ip vrf forwarding vrf_name
no ip vrf forwarding
```

no

Removes the specified VRF table from this interface.

vrf_name

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

Use the **ip vrf forwarding** command in the Context Configuration mode to preconfigure the VRF name.

Usage Guidelines Use this command to associate a preconfigured IP VRF instance for the current interface.

Example

The following command associates this interface with VRF named *vrf012*:

```
ip vrf forwarding vrf012
```

ipv6 address

Specifies an IPv6 address and subnet mask.

Product PDSN

HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **loopback**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

Syntax Description **[no] ipv6 address** *ipv6_address/mask* **[srp-activate]**

no

Removes the IPv6 address from this interface.

ipv6_address/mask

Specifies an individual host IP address to add to this host pool in IPv6 colon-separated hexadecimal CIDR notation.

Important On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

srp-activate

Enables the IPv6 address when the Service Redundancy Protocol determines this chassis to be ACTIVE.

Usage Guidelines Configures the IPv6 address and subnet mask for a specific interface.

Example

The following command configures an IPv6 address *2002:0:0:0:0:0:c014:101/128* for this interface:

```
ipv6 address 2002:0:0:0:0:0:c014:101/128
```

ipv6 ospf

This command configures Open Shortest Path First Version 3 (OSPFv3) parameters on the IPv6 interface.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **loopback**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

Syntax Description

`[ no ] ipv6 ospf [ area { `*`integer | ipv4_address`***` } | cost `***`cost_value`***` | dead-interval `***`dead_interval`***` | hello-interval `***`hello_interval`***` | priority `***`p_value`***` | retransmit-interval `***`retx_interval`***` | transmit-delay `***`td_interval`***` ]`**

no

Removes a previously configured access group association.

area { *integer* | *ipv4_address* }

Enables OSPFv3 routing on this interface.

decimal_value: Specifies the identification number of the area as an integer from 0 to 4294967295.

ipv4_address: Specifies the IP address of the area in IPv4 dotted-decimal notation.

cost *cost_value*

Configures the OSPF interface cost. The link cost is carried in the LSA updates for each link. The cost is an arbitrary number. *cost_value* is an integer from 1 to 65535.

dead-interval *dead_interval*

Configures the OSPF interface dead-interval in seconds, the interval after which a neighbor is declared dead when no hello packets are sent. *dead_interval* is an integer from 1 to 65535.

hello-interval *hello_interval*

Configures the OSPF interface hello-interval in seconds, the interval between hello packets that OSPFv3 sends on an interface. *hello_interval* is an integer from 1 to 65535.

priority *p_value*

Configures the priority of the OSPF interface. *p_value* is an integer from 0 to 255.

retransmit-interval *retx_interval*

Configures the OSPF interface retransmit-interval in seconds, the time between link-state advertisement (LSA) retransmission for adjacencies belonging to the OSPFv3 interface. *retx_interval* is an integer from 1 to 65535.

transmit-delay *td_interval*

Configures the OSPF interface transmit delay in seconds, the estimated time required to send a link-state update packet on the interface. *td_interval* is an integer from 1 to 65535.

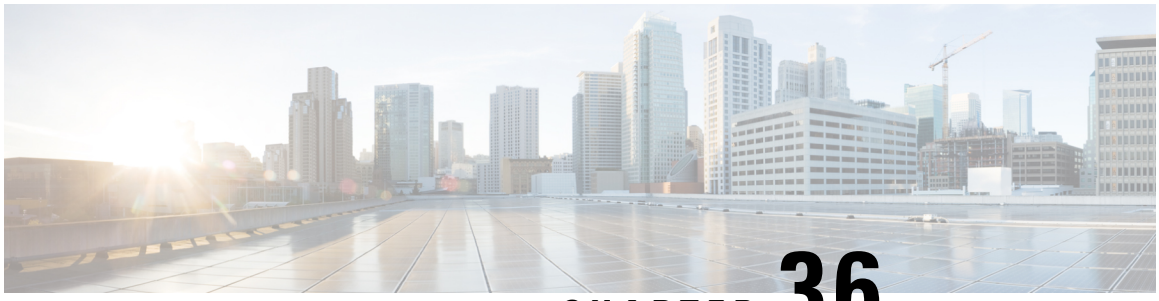
Usage Guidelines

Use this command to configure an OSPFv3 interface in this context.

Example

The following command specifies the link cost as *555*:

```
ipv6 ospf cost 555
```



CHAPTER 36

LTE Custom TAI List Configuration Mode Commands

The LTE Custom TAI List Configuration Mode is used to create and manage custom TAI lists on this system.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > Custom TAI List Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-custom-list tac** *value*

Entering the above command sequence results in the following prompt:

```
[local]hostname(tai-cstm-list)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

tai

Configures a Tracking Area Identifier (TAI) for this custom TAI list.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > Custom TAI List Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-custom-list tac** *value*

Entering the above command sequence results in the following prompt:

```
[local]hostname(tai-cstm-list)#
```

Syntax Description

[no] tai mcc *number* **mnc** *number* **{ tac** *value* **} +**

no

Removes a configured TAI from the TAI management object.

mcc *number*

Specifies the mobile country code (MCC) portion of a PLMN identifier. *number* is an integer from 100 to 999.

mnc *number*

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

tac *value*

Specifies the Tracking Area Code portion of the TAI. *value* is an integer from 1 to 65535. Up to 16 TAC values can be entered on a single line.

+

Indicates that the TAC values can be entered multiple times. Up to 16 TAC values can be entered on a single line.

Usage Guidelines

Use this command to configure one or more TAIs for this custom TAI list. A maximum of 15 TAIs can be configured per Custom TAI List.

A TAC can be added in this custom TAI list only if it has already configured in any of the TAI management objects within this TAI Management Database.

All the TAIs configured within a Custom TAI List are assumed to use same S-GW, time-zone, zone-code, and other configurations within the TAI Management Object. If a Custom TAI List includes TAIs from different objects then those objects should be configured with same S-GW address, time-zone, zone-code, etc.

If the TAU/Attach comes with a TAI that matches a Custom TAI List, the resulting ATTACH_ACCEPT/TAU_ACCEPT will include all the TAIs present in Custom TAI List as well as the received TAI.

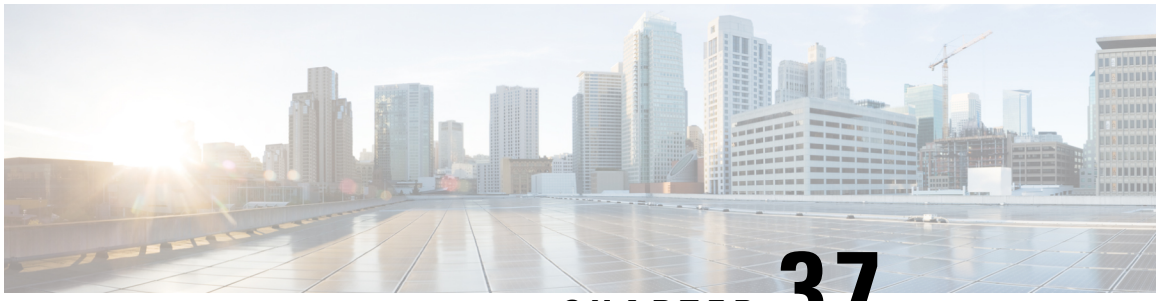
If the Custom TAI List is configured without any TAIs, the ATTACH_ACCEPT/TAU_ACCEPT will include all the TAIs from TAI Management object in which received TAI is present.

Example

The following set of commands show a Custom TAI List with TAC 3024, which includes TACs 3022, 3023, 3025, and 3026:

```
tai-custom-list tac 3024
  tai mcc 311 mnc 480 tac 3022
  tai mcc 311 mnc 480 tac 3023
```

```
tai mcc 311 mnc 480 tac 3025
tai mcc 311 mnc 480 tac 3026
```



CHAPTER 37

LTE Emergency Profile Configuration Mode Commands

This mode configures parameters supporting the IP Multimedia Subsystem (IMS) emergency bearer services. Connectivity to an emergency Packet Data Network (PDN) is statically configured in this mode.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

ambr

Configures the aggregated maximum bitrate (AMBR) for uplink and downlink for this emergency profile.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

Syntax Description

ambr max-ul *bitrate* **max-dl** *bitrate*
no ambr

no

Removes the AMBR configuration for this emergency profile.

max-ul *bitrate*

Configures the maximum aggregated uplink bitrate value. *bitrate* is an integer from 0 to 1410065408.

max-dl *bitrate*

Configures the maximum aggregated downlink bitrate value. *bitrate* is an integer from 0 to 1410065408.

Usage Guidelines Use this command to configure uplink and downlink maximum aggregated bitrate values to be shared across all non-guaranteed bitrate bearers established for the emergency session.

Example

The following command configures the uplink AMBR value to *2000* bps and the downlink AMBR value to *2000* bps:

```
ambr max-ul 2000 max-dl 2000
```

apn

Configures the name and PDN type of the access point name (APN) used for emergency PDN connections.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

Syntax Description

apn *apn_name* **pdn-type { ipv4 | ipv4v6 | ipv6 } [restoration-priority** *priority_value* **]**
no apn

no

Removes the selected APN from the profile.

apn_name

apn_name specifies the APN name of the emergency bearer services which will be used for emergency sessions. *apn_name* must be an alphanumeric string of 1 to 64 characters.

pdn-type { ipv4 | ipv4v6 | ipv6 }

Configures the packet data network type supported by the APN and this profile.

ipv4: Specifies that the PDN supports IPv4 network traffic.

ipv4v6: Specifies that the PDN supports both IPv4 and IPv6 network traffic.

ipv6: Specifies that the PDN supports IPv6 network traffic.

conf

restoration-priority *priority_value*

Configures the APN restoration priority value for emergency sessions for this APN profile. The reactivation of emergency PDNs after a P-GW restart notification is processed in the order of this priority.

priority_value is an integer from 1 to 16 where "1" is the highest priority and "16" is the lowest priority. Default: 16 (lowest priority).

To define the APN restoration priority for non-emergency sessions, refer to the **apn-restoration** command in the APN Profile Configuration Mode.

Usage Guidelines

Use this command to select the APN to be used for emergency bearer services. APNs are configured through the APN Configuration mode. For more information, see the *APN Configuration Mode Commands* chapter.

Example

The following command specifies that the APN named *apn-3.com* is to be used for emergency bearer services and that the PDN supports IPv4 traffic only:

```
apn apn-3.com pdn-type ipv4
```

The following command configures the APN Restoration Priority for APN profile named *eap* with restoration priority value *1*:

```
apn eap pdn-type ipv4 restoration-priority 1
```

associate

Associates a location service with this LTE emergency profile.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

Syntax Description

associate location-service *location_svc_name*
no associate location-service

no

Disassociates a previously associated location service with this LTE emergency profile.

location-service *location_svc_name*

Associates a location service with this LTE emergency profile. Only one location service can be associated with an LTE emergency profile.

location_svc_name specifies the name for a pre-configured location service to associate with the LTE emergency profile as an alphanumeric string of 1 through 63 characters.

Usage Guidelines Use this command to associate a pre-configured location service with an LTE emergency profile. This enables the associated location service to provide location information of emergency calls to the GMLC.

For more information about Location Services (LCS), refer to the **location-service** command in the *Context Configuration Mode Commands I-M* chapter as well as the *Location Services Configuration Mode Commands* chapter.

Further details can be found in the *Location Services* chapter of the *MME Administration Guide*.

lcs-qos

Configures the required Location service (LCS) Quality of Service (QoS) settings for this emergency profile.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

Syntax Description

lcs-qos horizontal-accuracy *variable* **[vertical-accuracy** *variable* **]**
no lcs-qos

no

Removes the configured LCS QoS settings for this emergency profile.

horizontal-accuracy *variable*

Defines the horizontal (longitude and latitude) accuracy of the LCS request.

variable must be entered as an integer from 0 to 127, where 0 is the most accurate.

vertical-accuracy *variable*

Defines the vertical (altitude) accuracy of the LCS request.

variable must be entered as an integer from 0 to 127, where 0 is the most accurate.

Usage Guidelines

Use this command to define the location service QoS settings to be used for this emergency profile. Configuration of these settings is optional.

For Emergency Services, the MME will always set the Response Time to Low Delay. If QoS is configured, the horizontal accuracy is mandatory. If a vertical accuracy is specified in this command, the MME will set the Vertical Requested flag.

Refer to 3GPP TS 29.171 and 3GPP TS 23.032 for more details about these settings.

Example

The following command sets the LCS QoS horizontal accuracy to **20**, which represents an accuracy of 57.3 meters. No vertical accuracy is specified.

```
lcs-qos horizontal-accuracy 20
```

local-emergency-num

This command configures Local Emergency Numbers to be sent in Attach/TAU responses.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

Syntax Description

`[ no ] local-emergency-num` *`emergency_number`* **`{ ambulance | custom`** *`custom_number`* **`| fire | marinegaurd | mountain-rescue | police }`**

no

Removes the specified Local Emergency Number from the list.

emergency_number

The emergency number is a number assigned to a type of emergency number (ambulance, marine, and so on) with a string of size 1 to 10.

custom_number

Is specific to the **custom** local emergency number. *custom_number* is an hexadecimal number from 0x1 to 0xFF.

Usage Guidelines

This command allows the subscriber to download a list of local emergency numbers used by the serving network. This list is downloaded by the network to the User Equipment (UE) at successful registration as well as subsequent registration updates.

Example

The following configuration allows the operator to assign an emergency number for ambulance:

```
local-emergency-num 123 ambulance
```

The following configuration allows the operator to remove the emergency number assigned for ambulance:

```
no local-emergency-num 123 ambulance
```

local-emergency-num-ie

This command is used to configure local emergency numbers to be sent only over TAU messages.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

Syntax Description

```
local-emergency-num-ie { inter-mme-tau | tau }
no local-emergency-num-ie
```

inter-mme-tau

The **local-emergency-num-ie** keyword with **inter-mme-tau** option allows the configured local emergency number list to be sent in a TAU Accept during Inter-MME-TAUs, that is, when the UE switches from a 2G network to 4G network, from a 3G network to 4G network or from a 4G network to 4G network handover (for both idle and connected mode).

tau

The **local-emergency-num-ie** keyword with **tau** option allows the configured local emergency number list to be sent in a TAU Accept message during all TAUs (for example, periodic TAUs and so on).

Usage Guidelines

This command configuration of the local emergency numbers is to be sent only over TAU messages.

Example

The following configuration allows the operator to send the emergency number list over Inter-MME-TAU messages:

```
local-emergency-num-ie inter-mme-tau
```

The following configuration allows the operator to send the emergency number list over all TAU messages:

```
local-emergency-num-ie tau
```

The following command removes the configuration of local emergency numbers sent over TAU messages:

```
no local-emergency-num-ie
```

pgw fqdn

This command configures a fully qualified domain name (FQDN) for P-GW to support emergency bearer services.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

Syntax Description

pgw fqdn *fqdn*
no pgw fqdn

no

Removes the specified P-GW FQDN from this profile.

fqdn

Specifies the domain name of the P-GW as an alphanumeric string of 1 through 256 characters.

Important A maximum of one P-GW FQDN configuration is allowed per profile.

Usage Guidelines Use this command to configure the FQDN for P-GW to support emergency bearer services.

Example

The following command configures the P-GW supporting emergency bearer services for this profile as *pdn-911.gov*:

```
pgw fqdn pdn-911.gov
```

pgw ip-address

This command configures the IPv4 or IPv6 address of the P-GW to support emergency bearer services.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

Syntax Description

```
pgw ip-address address protocol { both | gtp | pmip } weight value
collocated-nodecollocated_node_name ue-usage-type ue_usage_type_value
no pgw ip-address address
```

no

Removes the specified P-GW IP address from this profile.

ip-address *address*

Specifies the IP address for the P-GW in IPv4 dotted-decimal or IPv6 colon-separated hexadecimal notation.

Important A maximum of four P-GW IP address configurations are allowed per profile.

protocol { both | gtp | pmip }

Specifies the protocol that P-GW supports. Options are:

- **both**: Specifies that both GTP and PMIP are supported.
- **gtp**: Specifies that only GTP is supported.

- **pmip**: Specifies that only PMIP is supported.

weight *value*

Assigns a weight to the P-GW IP address to use as a preferred P-GW.

value is an integer from 1 to 100. Lowest value has the least preference.

collocated-node

Configures the collocation name to select the collocated S/PGW node IP addresses for MME.

collocated_node_name must be a string of size 1 to 255.

ue-usage-type

Configures the ue-usage-type for the gateway. *ue_usage_type_value* must be an integer between 1 through 255.

Usage Guidelines

Use this command to configure the IPv4 or IPv6 address for P-GW to support emergency bearer services through this profile.

Example

The following command configures the P-GW with an IPv4 address of *209.165.200.228*, supporting GTP only, and having a weight of *10*:

```
pgw ip-address 209.165.200.228 protocol gtp weight 10
```

qos

Configures the quality of service (QoS) parameters for the emergency bearer service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

Syntax Description

```
qos qci qci arp arp_value preemption-capability { may | shall-not }
vulnerability { not-preemptable | preemtable }
no qos
```

qci *qci*

Specifies the QoS Class Identifier (QCI) for the emergency bearer profile as an integer from 0 through 255.

arp *arp_value*

Defines the address retention priority value as an integer from 1 through 15.

preemption-capability { may | shall-not }

Specifies the preemption capability flag. Options are:

- **may**: Emergency bearer may have Preemption Capability.
- **shall-not**: Emergency bearer shall not have Preemption Capability.

vulnerability { not-preemptable | preemptable }

Specifies the vulnerability flag. Options are:

- **not-preemptable**: Bearer cannot be preempted.
- **preemptable**: Bearer can be preempted.

Usage Guidelines

Use this command to set the QoS ARP and QCI parameters for the emergency bearer configuration.

Example

The following command sets the QCI number to *7*, the ARP value to *2* the preemption capability to *may*, and the vulnerability flag to *preemptable*:

```
qos qci 7 arp 2 preemption-capability may vulnerability preemptable
```

ue-validation-level

Configures the type of user equipment (UE) that can use the emergency bearer service through the profile.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

Syntax Description

```
ue-validation-level { auth-only | full | imsi | none }
default ue-validation-level
```

default

Returns the command to its default setting.

Default: **none**

{ auth-only | full | imsi | none }

Specifies the type of UE allowed to use the emergency bearer service. Options are:

- **auth-only**: Specifies that UEs that have been authenticated are allowed to use the emergency bearer service. These UEs may be in a limited service state, they may be in an area with restricted service or where they are restricted from services. Enabling this option also causes subscription and location validation to be bypassed.
- **full**: Specifies that only UEs that have been authenticated and have successfully passed subscription and location validation are allowed to use the emergency bearer service. Enabling this option indicates that only UEs that are capable of normal attach procedures will be allowed to use the emergency bearer service.
- **imsi**: Specifies that UEs with an International Mobile Subscriber Identity (IMSI) are allowed to use the emergency bearer service regardless of authentication. Even if authentication fails, the UE is granted access.
- **none**: Specifies that all UEs are allowed to use the service. This is the default value for the command.

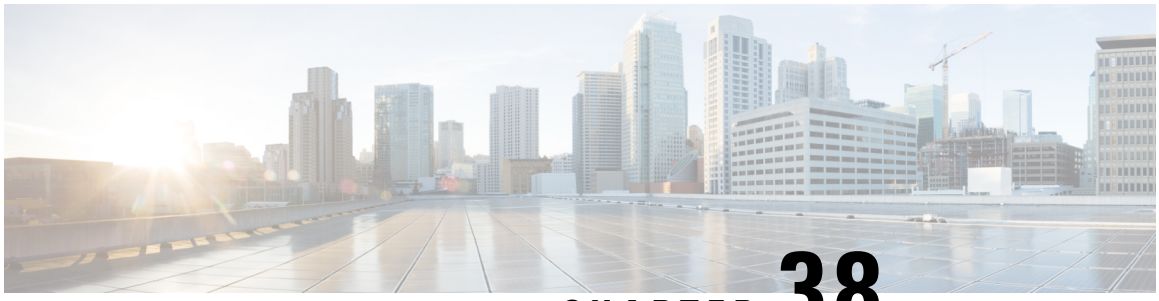
Usage Guidelines

Use this command to indicate which UEs can use the emergency bearer service through this profile.

Example

The following command configures the **imsi** type of UE to use the emergency bearer service to "IMSI required, authentication optional":

```
ue-validation-level imsi
```



CHAPTER 38

LTE Forbidden Location Area Configuration Mode Commands

The LTE Forbidden Location Area Configuration Mode is used to create and manage forbidden 3G location area code (LAC) configurations.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration > LTE Forbidden Location Area Configuration

configure > lte-policy > ho-restrict-list *list_name* **> forbidden location-area plmnid** *plmn_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(forbidden_la)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

lac

Configures a 3G location area code (LAC) or area codes where a UE, associated with this LTE policy, is restricted from participating in a handover scenario.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration > LTE Forbidden Location Area Configuration

configure > **lte-policy** > **ho-restrict-list** *list_name* > **forbidden location-area plmnid** *plmn_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(forbidden_la)#
```

Syntax Description

[no] lac *area_code* **+**

no

Removes a configured forbidden handover area code or area codes from this policy. If no location area code is specified, then all location area codes are removed.

area_code

Specifies an area code or area codes from which UEs are restricted from participating in a handover as an integer from 0 to 65535. Multiple area codes can be entered (up to 128 in a single line, separated by spaces).

+

Indicates that multiple area codes up to 128 in a single line, separated by spaces, can be entered in this command.

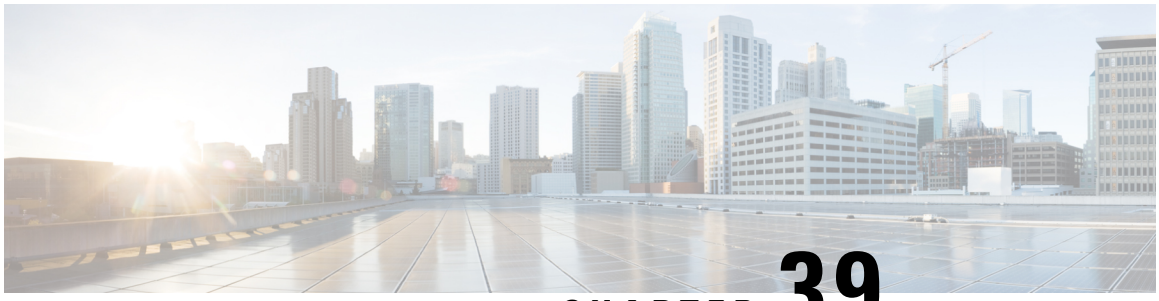
Usage Guidelines

Use this command to configure 3G location-based area codes that will be forbidden to UEs associated with this LTE policy.

Example

The following command configures eight location-based area codes (1, 2, 3, 4, 5, 6, 7, 8) where a UE, associated with this LTE policy, is restricted from participating in a handover scenario:

```
lac 1 2 3 4 5 6 7 8
```



CHAPTER 39

LTE Forbidden Tracking Area Configuration Mode Commands

The LTE Forbidden Tracking Area Configuration Mode is used to create and manage forbidden tracking area code (TAC) configurations.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration > LTE Forbidden Tracking Area Configuration

configure > lte-policy > ho-restrict-list *list_name* **> forbidden tracking-area plmnid** *plmn_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(forbidden_ta)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

tac

Configures a tracking area code (TAC) or area codes where a UE, associated with this LTE policy, is restricted from participating in a handover scenario.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration > LTE Forbidden Tracking Area Configuration

configure > lte-policy > ho-restrict-list *list_name* **> forbidden tracking-area plmnid** *plmn_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(forbidden_ta)#
```

Syntax Description

[no] tac *area_code* **+**

no

Removes a configured forbidden handover area code or area codes from this policy. If no tracking area code is specified, then all tracking area codes are removed.

area_code

Specifies a tracking area code or area codes from which UEs are restricted from participating in a handover as an integer from 0 to 65535. Multiple area codes can be entered (up to 128 in a single line, separated by spaces).

+

Indicates that multiple area codes up to 128 in a single line, separated by spaces, can be entered in this command.

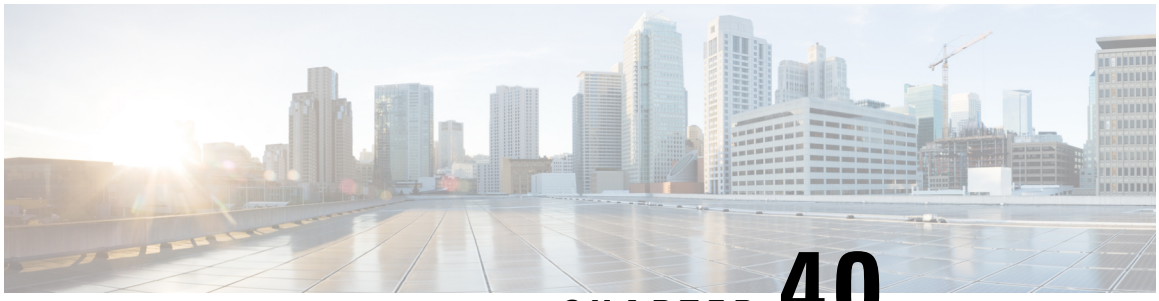
Usage Guidelines

Use this command to configure tracking area codes that will be forbidden to UEs associated with this LTE policy.

Example

The following command configures eight tracking area codes (1, 2, 3, 4, 5, 6, 7, 8) where a UE, associated with this LTE policy, is restricted from participating in a handover scenario:

```
tac 1 2 3 4 5 6 7 8
```



CHAPTER 40

LTE Foreign PLMN GUTI Management Database Configuration Mode Commands

The LTE Foreign PLMN GUTI Management Database Configuration Mode is used to is used to create restrictions on foreign PLMNs, thereby avoiding DNS request attempts to foreign PLMNs.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Foreign PLMN GUTI Management Database

configure > lte-policy > foreign-plmn-guti-mgmt-db

Entering the above command sequence results in the following prompt:

```
[local]host_name(foreign-plmn-guti-mgmt-db)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

plmn

Configures a foreign Public Land Mobile Network (PLMN) entry in the Foreign PLMN GUTI management database. This optional configuration is used to control the acceptance or immediate reject of Attach Requests and TAU Requests containing a GUTI from this PLMN.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Foreign PLMN GUTI Management Database

configure > lte-policy > foreign-plmn-guti-mgmt-db

Entering the above command sequence results in the following prompt:

```
[local]host_name(foreign-plmn-guti-mgmt-db)#
```

Syntax Description

plmn mcc { *mcc_value* | any } mnc { *mnc_value* | any } { allow | reject }
no plmn mcc { *mcc_value* | any } mnc { *mnc_value* | any }

no

Removes the specified PLMN entry from the Foreign PLMN GUTI management database.

mcc { *mcc_value* | any }

Specifies the mobile country code (MCC) portion of the PLMN identifier. *mcc_value* is an integer from 100 to 999. Use the optional **any** keyword to specify a wildcard, representing any MCC.

mnc { *mnc_value* | any }

Specifies the mobile network code (MNC) portion of the PLMN identifier. *mnc_value* is a 2- or 3-digit integer from 00 to 999. Use the optional **any** keyword to specify a wildcard, representing any MNC.

Important The **any** keyword can only be used for the MNC value when a specific MCC value is given. For example, the following command is **not** allowed:

plmn mcc any mnc 456 allow

allow

Configures the MME to allow foreign GUTIs from this PLMN.

reject

Configures the MME to reject foreign GUTIs from this PLMN.

Usage Guidelines

Use this command to create and configure a foreign Public Land Mobile Network (PLMN) entry in the Foreign PLMN GUTI management database. This optional configuration is used to control the acceptance or immediate reject of Attach Requests and TAU Requests containing a GUTI from this PLMN.

If the configured action is Reject, the MME takes the following actions:

- Attach Request: A NAS Identity Request is sent to the UE to determine its IMSI and no DNS lookup is performed to find a peer MME or SGSN.
- TAU Request: A TAU Reject message is sent immediately with cause code 9 (UE Identity cannot be derived by the network) and no DNS lookup is performed to find a peer MME or SGSN.

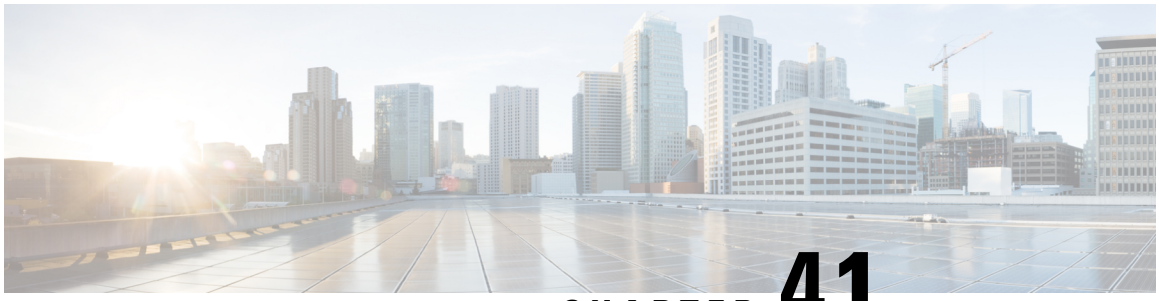
If the configured action is Allow, the MME continues processing the Attach Request or TAU Request and a DNS request may be made.

A maximum of 16 foreign PLMN entries can be added to a Foreign PLMN GUTI management database.

Example

The following command creates a PLMN entry in the foreign PLMN GUTI management database. The entry specifies that GUTIs from PLMNs with the MCC of *123* and any MNC be rejected.

```
plmn mcc 123 mnc any reject
```



CHAPTER 41

LTE HeNBGW MME Pool Configuration Mode Commands

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. Commands in this configuration mode must not be used in these releases. For more information, contact your Cisco account representative.

The MME Pool configuration is used to configure one or more MMEs to which the HeNB-GW is to communicate. This configuration is available under lte-policy configuration mode. Adding or modifying an MME pool instance puts the user into the MME Pool configuration mode.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > HeNBGW MME Pool Configuration

configure > lte-policy > henbgw mme-pool *mme_pool_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(mme-pool)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

mme

Configures a specific MME to HeNBGW.

Product

HeNB-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > HeNBGW MME Pool Configuration

configure > lte-policy > henbgw mme-pool *mme_pool_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(mme-pool)#
```

Syntax Description

[no] mme *mme_name* **{ ipv4-address** *ipv4_address* **[ipv4-address** *ipv4_address* **] | ipv6-address** *ipv6_address* **[ipv6-address** *ipv6_address* **] [sctp port** *port_val* **] }**

no

Removes the configured MME to HeNBGW.

mme_name

Specifies the MME name as an alphanumeric string of size 1 through 63 characters.

ipv4-address *ipv4_address*

Specifies the remote SCTP IPv4 Address for S1 association to MME. *ipv4_address* is specified using a dotted-decimal notation.

ipv6-address *ipv6_address*

Specifies the remote SCTP IPv6 Address for S1 association to MME. *ipv6_address* is specified using a colon-separated hexadecimal notation.

sctp

Configures the S1-MME SCTP parameters.

port *port_val*

Designates the SCTP port.

port_val is an integer ranging from 1 through 65535.

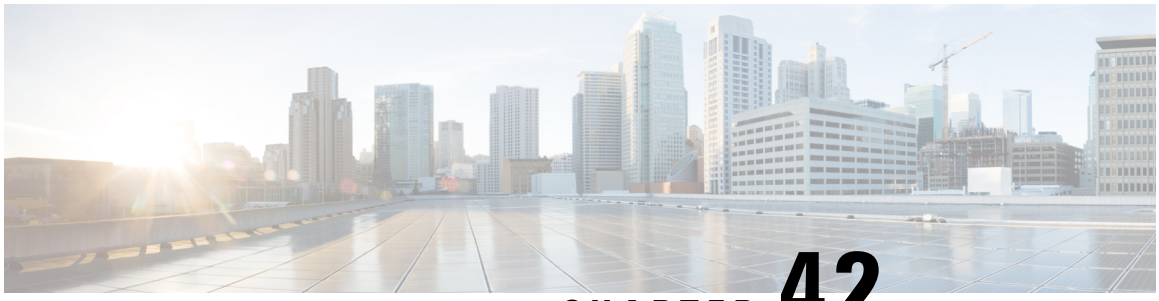
Usage Guidelines

Use this command to configure a specific MME to HeNBGW.

Example

The following command configures the MME with name *mme1*, IPv4 address *209.165.200.225* with SCTP port value *302*:

```
mme mme1 ipv4-address 209.165.200.225 sctp port 302
```



CHAPTER 42

LTE Handover Restriction List Configuration Mode Commands

The LTE Handover Restriction List Configuration Mode is used to create and manage the LTE handover restriction lists for LTE/SAE networks. Handover restriction lists are used to restrict user equipment (UE) from participating in specified handovers. The MME creates the handover restriction lists as part of its local policy and provides them to the eNobeB where the restrictions are enforced.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration

configure > lte-policy > ho-restrict-list *list_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(ho-restrict-list)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

forbidden

Configures the handover restriction lists provided to eNodeBs where handover restrictions are enforced for UEs.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration

configure > **lte-policy** > **ho-restrict-list** *list_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(ho-restrict-list)#
```

Syntax Description

```
[ no ] forbidden { inter-rat { all | cdma2000 | geran | utran } |
location-area plmnid id | tracking-area plmnid id }
default forbidden inter-rat
```

default

Removes the forbidden inter-RAT configuration from the LTE policy.

no

Removes the forbidden configuration from the LTE policy.

inter-rat { all | cdma2000 | geran | utran }

Specifies that one or all Radio Access Technology (RAT) handovers are to be prohibited for UEs associated with the LTE policy.

all: Specifies that all inter-RAT handovers are to be prohibited for UEs associated with the LTE policy.

cdma2000: Specifies that all CDMA2000 handovers are to be prohibited for UEs associated with the LTE policy.

geran: Specifies that all GSM EDGE Radio Access Network (GERAN) handovers are to be prohibited for UEs associated with the LTE policy.

utran: Specifies that all UMTS Terrestrial Radio Access Network (UTRAN) handovers are to be prohibited for UEs associated with the LTE policy.

location-area plmnid *id*

Specifies that handovers to 3G location area codes defined through this keyword and subsequent configuration mode are to be prohibited for UEs associated with the LTE policy. Enters the LTE Forbidden Location Area Configuration Mode. *id* must be a valid PLMN ID expressed as an integer comprised of an MCC (Mobile Country Code) and MNC (Mobile Network Code) [five-digit minimum, six-digit maximum].

Important Up to 16 forbidden location area PLMN IDs can be configured per handover restriction list.

Entering this command results in the following prompt:

```
[context_name]hostname(forbidden_la)#
```

The related commands are defined in the *LTE Forbidden Location Area Configuration Mode Commands* chapter.

tracking-area plmnid *id*

Specifies that handovers to 4G tracking area codes defined through this keyword and subsequent configuration mode are to be prohibited for UEs associated with the LTE policy. Enters the LTE Forbidden Tracking Area

Configuration Mode. *id* must be a valid PLMN ID and be an integer value comprising an MCC and MNC (five-digit minimum, six-digit maximum).

Important Up to 16 forbidden tracking area PLMN IDs can be configured per handover restriction list.

Entering this command results in the following prompt:

```
[context_name]hostname(forbidden_ta)#
```

The related commands are defined in the *LTE Forbidden Tracking Area Configuration Mode Commands* chapter.

Usage Guidelines

Use this command to create the list of restricted handover types that apply to all UEs associated with the LTE policy.

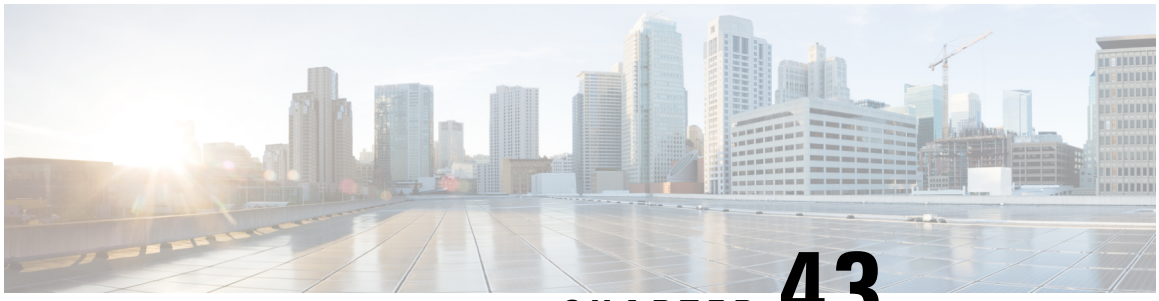
Example

The following command prohibits UEs associated with this LTE policy from participating in a handover to a GERAN network type:

```
forbidden inter-rat geran
```

The following command prohibits UEs, associated with this LTE policy and a mobile network with a PLMN ID of *12345*, from participating in a handover to location area codes defined in the Location Area Configuration Mode:

```
forbidden location-area plmnid 12345
```



CHAPTER 43

LTE MME HeNB-GW Management Database Configuration Mode Commands

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. Commands in this configuration mode must not be used in these releases. For more information, contact your Cisco account representative.

The LTE MME HeNB-GW Management Database Mode is used to create and manage a list of HeNB-GWs. The HeNB-GWs defined in this database are used by the MME during S1-based handovers to Home eNodeBs when the HeNBs are connected to the MME via HeNB-GWs.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > MME HeNB-GW Management Database

configure > lte-policy > mme henbgw mgmt-db *db_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(henbgw-mgmt-db)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

henbgw-global-enbid

This command configures the Global eNodeB Id and TAI of a Home eNodeB within the HeNB-GW management database.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > MME HeNB-GW Management Database

configure > lte-policy > mme henbgw mgmt-db *db_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(henbgw-mgmt-db)#
```

Syntax Description

[no] henbgw-global-enbid mcc *number* **mnc** *number* **enbid** *number*

no

Removes a configured entry in the MME HeNB-GW management database.

mcc *number*

Specifies the mobile country code (MCC) portion of a PLMN identifier as an integer from 100 through 999.

mnc *number*

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

enbid *number*

Specifies the Global eNodeB ID for this HeNB-GW as an integer value from 1 through 1048575.

Usage Guidelines

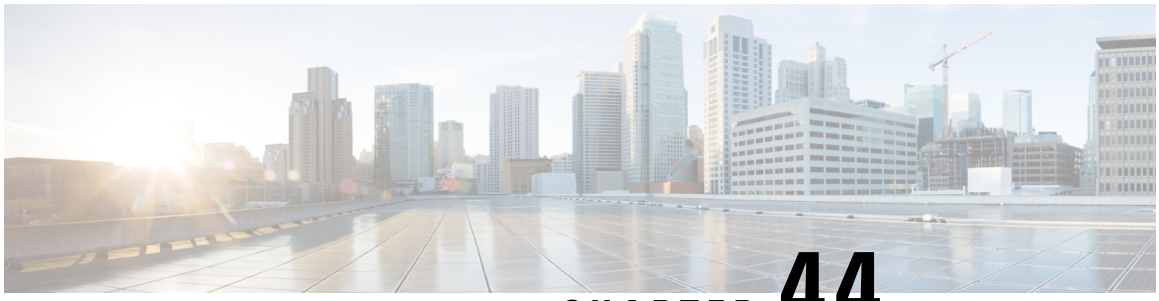
Use this command to configure the global eNodeB ID and TAI of one or more HeNB-GWs within the HeNB-GW management database.

A maximum of 8 HeNB-GWs can be configured within the HeNB-GW management database.

Example

This following command configures the Global eNodeB ID and TAI for an HeNB-GW entry within the HeNB-GW management database:

```
henbgw-global-enbid mcc 123 mnc 456 enbid 789
```



CHAPTER 44

LTE Network Global MME ID Management Database Configuration Mode Commands

The LTE Network Global MME ID Management Database Configuration Mode is used to create associations between PLMN IDs and MME group ID ranges.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Network Global MME ID Management Database Configuration

configure > lte-policy > network-global-mme-id-mgmt-db

Entering the above command sequence results in the following prompt:

```
[local]host_name(network-global-mme-id-mgmt-db)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

plmn

Configures associations between public land mobile network (PLMN) IDs and ranges of MME group IDs. On the S4-SGSN, this command allows the operators to configure a custom list of MME group IDs if networks have been configured with LACs in the 32768-65535 range for UMTS and GPRS coverage.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Network Global MME ID Management Database Configuration

configure > lte-policy > network-global-mme-id-mgmt-db

Entering the above command sequence results in the following prompt:

```
[local]host_name(network-global-mme-id-mgmt-db)#
```

Syntax Description

[no] plmn mcc *mcc_value* **mnc** *mnc_value* **mme-group-id-range first** *id* **last** *id*

no

Removes the selected PLMN ID to MME group ID range from the MME ID management database.

mcc *mcc_value* mnc *mnc_value*

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

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

mme-group-id-range first *id* last *id*

Specifies the range of MME group IDs to apply to the PLMN ID as an integer from 0 to 65535.

Usage Guidelines

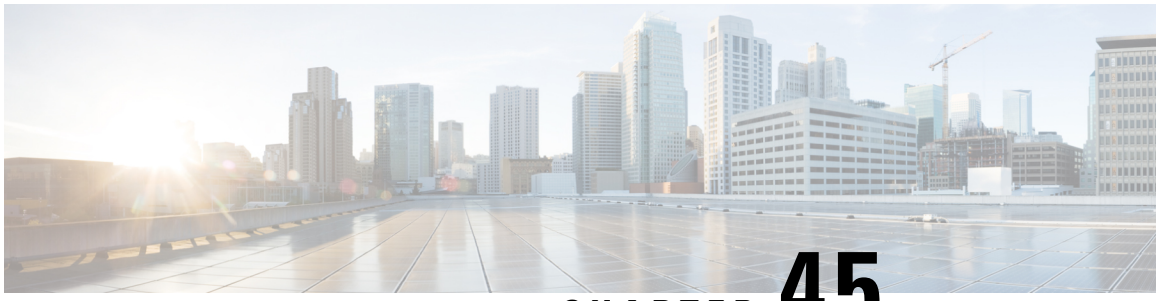
Use this command to create associations between PLMN IDs and a range of MME group IDs.

On the S4-SGSN, use this command to create a custom list of MME group IDs on the S4-SGSN if networks have been configured with LACs in the 32768-65535 range for UMTS and GPRS coverage. The S4-SGSN will use this custom list to identify whether the received LAC is a native LAC or a LAC mapped from a globally unique temporary identifier (i.e., an MME group code part of GUTI). Once the **plmn** configuration is completed, operators must associate the configuration with the GPRS and/or SGSN services configured on the S4-SGSN using the **associate network-global-mme-id-mgmt-db** command. Refer to the *SGSN Service Configuration Mode* and *GPRS Service Configuration Mode* chapters in the *GPRS/UMTS Command Line Reference* for a description of this command.

Example

The following command creates an association between a PLMN ID of *12323* and a set of MME group IDs with a range of *500* through *575*:

```
plmn mcc 12323 mnc 23 mme-group-id-range first 500 last 575
```



CHAPTER 45

LTE Paging Map Configuration Mode Commands

The LTE Paging Map Configuration Mode is used to create and manage the LTE paging maps supporting MME configurations on the system.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Paging Map Configuration

configure > lte-policy > paging-map *map_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(paging-map)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

precedence

Enables the operator to apply a priority for different paging-profiles based on traffic type. When the MME service is associated with a paging map, the system checks the profile map to determine which paging-profile to adopt for a given paging trigger.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Paging Map Configuration

configure > lte-policy > paging-map *map_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(paging-map)#
```

Syntax Description

precedence *priority* **traffic-type { cs [other | sms | voice] | ps [apn-profile** *profile_name* **| arp** *arp_value* **| qci** *qci_value* **| sms paging-profile** *paging_profile_name* **] | signaling [detach | idr | lcs | node-restoration] } paging-profile** *paging_profile_name*
no precedence *priority*

no

Remove the paging map from the system.

precedence *priority*

precedence: For StarOS releases 16.5 and higher, enter an integer from 1 to 19, where 1 is the highest priority and 19 is the lowest priority. For StarOS releases prior to 16.5, enter an integer from 1 to 7, where 1 is the highest priority and 7 is the lowest priority. For releases 20.0 onwards enter an integer from 1 to 35, where 1 is the highest priority and 35 is the lowest priority. The numbers of paging-profiles supported are increased from 8 to 16.

traffic-type { cs [voice | sms | other] | ps [qci *qci_value* | apn-profile *profile_name*] | signaling [detach | idr | lcs | node-restoration] }

Defines the type of traffic of the incoming call.

- **cs** (Circuit Switched) - All data and control activities that involve CSFB. Paging requests from the MSC for mobile-terminated calls alone are treated as CS type. Paging requests for SMS are treated as PS type.

  Optionally, define the CS traffic sub-type:

  - **other**: MM Information Request messages coming from MSC can also trigger paging if UE is in IDLE state. These requests are mapped to 'other' sub-traffic type.
  - **sms**: Paging requests from MSC for mobile terminated SMS requests.
  - **voice**: Paging requests from MSC for mobile terminated voice calls.

  If a sub-traffic-type is not configured then paging-profile configured for CS (with no sub traffic-type qualification) is applied. If no such entry exists, then default heuristics based paging behavior is applied.

- **ps** (Packet Switched) - All data and control activities that involve packet services. SRVCC is also mapped to this traffic-type as the voice is carried using PS service. PS traffic type is further qualified using a set of QCI values or ARP values or APN profile names. These qualified entries are only used for paging triggered by S11 Downlink Data Notifications or Create Bearer Request or Update Bearer Request

  Optionally, define the APN Profile for PS traffic:

  apn-profile *profile_name*

  where *profile_name* is an alphanumeric string of size 1 to 64.

  The MME supports paging profile selection based on APN. A maximum of four APN profiles can be configured per precedence using this command.

  When heuristics paging is enabled, the MME selects the paging profile based on the APN profile, if paging-profile with matching APN profile name is fetched from the APN information corresponding to the EBI received in DDN is configured in the paging-map. If the incoming DDN does not have the EBI information then the APN information is received from the bearers stored in the MME for the UE. If multiple APN information is available, then the mapping with the highest precedence is picked. MME

warns the user of duplicate APN profile names in a given entry. The same APN profile name cannot be configured with more than one precedence level.

Optionally, define the ARP priority based paging for PS traffic type in the paging-map:

arp *arp_value*

The allowed ARP value " *arp_value* " is an integer from 1 through 15.

Optionally, define the QoS Class Identifier (QCI) value for this PS traffic:

qci *qci_value*

The QCI values can be either standard or non-standard. The *qci_value* is an integer from 1 through 9, 65, 66, 69, 70 (standard values) and from 128 up to 255 are non-standard values.

QCI qualified entries can only be used for paging triggered by Downlink Data Notifications received on S11. If the incoming DDN contains EPS Bearer ID (EBI) information, the QCI corresponding to that PDN is used to find the appropriate 'ps qci xx' entry and its configured paging-profile.

If there are multiple EBIs included in the DDN the mapping entry with highest precedence is selected.

If no QCI specific mapping exists, or if the incoming DDN does not have the EBI information then the qci corresponding to the bearers stored in MME for the UE shall be used to find the appropriate 'ps qci xx' entry and its configured paging-profile. The MME warns the user of duplicate QCI values in a given entry, same QCI values cannot be configured with more than one precedence level.

sms

Configures paging profile for SMS via SGd.

- **signaling [detach | idr | lcs | node-restoration]**: UE level signaling requests. This traffic can be optionally qualified according to the following sub-traffic types:

  detach: Paging requests triggered due to UE getting detached.

  idr: Paging triggered in response to an IDR event, such as receiving an IDR Request.

  lcs: (Location Services) – Paging requests triggered due to Positioning Requests coming from SMLC over SLs interface. Mobile Terminated Location Requests arriving on SLg interface can also trigger paging if UE is in IDLE state, and are included in this sub-traffic type.

  node-restoration: Paging requests triggered due to node restoration (for example, due to P-GW Restart Notification (PRN)). By default, no precedence is assigned to node restoration signaling traffic. The MME treats node restoration paging with the least priority.

  If a sub-traffic-type is not configured then paging-profile configured for signaling (with no sub traffic-type qualification) shall be applied. If no such entry exists then default-heuristics based paging behavior is applied.

paging-profile *paging_profile_name*

The paging-profile to apply for paging UE.

Usage Guidelines

Use this command to apply different paging-profiles based on traffic types.

The command defines the order (1 - highest, 35 - lowest) in which the MME checks the entries in this paging-map. If the paging trigger (like Downlink Data Notification or MSC request) matches the traffic-type of that entry, then the corresponding paging-profile is used for paging the UE. If the paging trigger does not

match, then the next entry in the precedence order is picked and checked for a match. If no match is found in the entire paging-map table then default heuristic paging profile is adopted.

If the MME receives another paging trigger (for example from the MSC for CSFB) while paging is already in progress, the MME checks whether a higher precedence paging profile can be applied. If the new trigger has a paging-map entry with a higher precedence, the MME restarts the paging process using the paging-profile associated with the new map entry.

Paging is typically triggered when either the MSC indicates that there is an incoming call to the UE (Call Service, CS), or when the S-GW sends a Downlink Data Notification (Packet Service, PS) to the MME, or when there is a bearer/PDN request coming from the P-GW/S-GW.

The paging profile with the highest precedence is selected when QCI, ARP and APN Profile, all are configured in the paging-map. If no QCI, ARP and APN-Profile specific mapping exists then the default 'PS' traffic type configuration in the paging-map will be picked and the paging-profile corresponding to that mapping is used. If a paging trigger is received while a paging procedure is on-going, and if the new paging trigger has a higher precedence (considering QCI, ARP or APN-profile configuration mapping) then the paging-profile corresponding to that will be used in the next paging retry. One precedence level can be configured with only one of, QCI or ARP or APN-Profile name, at any point of time.

Refer to the *Heuristic and Intelligent Paging* chapter in the *MME Administration Guide* for more information.

Related Commands

Refer to the **paging-profile** command in the *LTE Policy Configuration Commands* chapter to create the paging profiles used in this command.

Example

The following example specifies a special paging-profile for IMS-Voice and a default paging-profile for the rest of PS paging triggers:

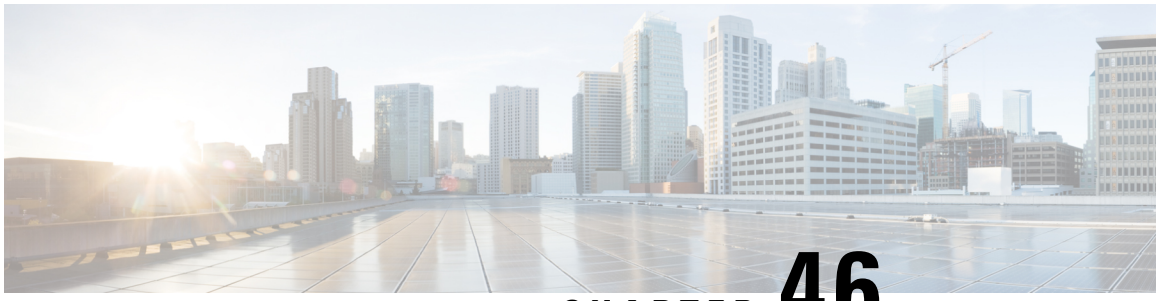
```
precedence 1 traffic-type ps qci 1 paging-profile profile-voice
precedence 2 traffic-type ps paging-profile profile-default
```

In the following example, Mobile Terminated voice triggered paging requests will use *profile-voice*. All other CS traffic types like MM-InformationRequest and MT-SMS use *profile-cs*:

```
precedence 1 traffic-type cs voice paging-profile profile-voice
precedence 2 traffic-type cs paging-profile profile-cs
```

In the following example, signaling paging requests due to a node restoration (P-GW Restart Notification (PRN)) will use the *prn*paging map, and is assigned a lower precedence of 3:

```
precedence 3 traffic-type signaling node-restoration paging-profile prn
```



CHAPTER 46

LTE Paging Profile Configuration Mode Commands

The LTE Paging Map Configuration Mode is used to create and manage the paging profiles that control the different stages of paging for MME configurations on the system.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Paging Profile Configuration

configure > lte-policy > paging-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(paging-profile)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

critical

This command enables paging criticality and continues the paging procedure even when the MMEMgr is busy.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Paging Profile Configuration

configure > lte-policy > paging-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(paging-profile)#
```

Syntax Description

[no] critical *paging_stage*

no

Disables the paging criticality that is configured for all paging stages and applies the default configuration. Stage-1 is considered as critical by default.

critical *paging_stage*

Enables the paging criticality for the specified paging stages. The paging procedure continues even when the MMEMgr is busy. *paging_stage* specifies the paging stage precedence as an integer from 1 to 5 where 1 is the highest and 5 is the lowest.

Usage Guidelines

Use this command to enable paging criticality and continue the paging procedure even when the MMEMgr is busy. By default, stage-1 is considered as critical if the operator does not configure paging criticality for any paging stages.

Example

The following command enables paging criticality for paging-stages 1, 2, and 3:

```
critical 1 2 3
```

paging-stage

Enables the operator to configure different stages of paging in the order of desired execution with parameters that control the pace, volume, and behavior of a given paging stage.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Paging Profile Configuration

configure > lte-policy > paging-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(paging-profile)#
```

Syntax Description

[no] paging-stage *level* **match-criteria { ue-contact-time** *seconds* **| all } action { last-n-enb-last-tai max-n-enb** *value* **| all-enb-last-tai | all-enb-all-tai } t3413-timeout** *seconds* **max-paging-attempts** *attempts* **[t3415-timeout** *t3415_dur* **]**

no

Remove the paging-stage from the system.

level

Defines different levels of paging-stages, each with a different match-criteria and different action. *level* must be an integer from 1 to 5.

match-criteria

Specifies the criteria for selecting a given paging stage.

- **ue-contact-time** *seconds*: Number of seconds elapsed since the MME last heard from UE. This time, if set, acts as an upper time limit to consider a given paging-stage for paging purposes. *seconds* must be an integer from 0 to 86400.
- **all**: No criteria. Operator can use this match-criteria for the final paging stage.

action

Defines how the paging request should be formulated.

- **last-n-enb-last-tai max-n-enb** *value*: Sends paging request to the last known number of eNodeBs (configured using **max-n-enb** *value*) and to the last known TAI. *value* must be an integer from 1 to 5.
- **all-enb-last-tai**: Sends paging request to all eNodeBs and to last known TAI.
- **all-enb-all-tai**: Sends paging request to all eNodeBs and to all TAIs.

t3413-timeout *seconds*

Defines the time-interval in seconds between paging requests. The MME uses this timer for retransmission of an S1 Paging request to UE for PS paging. *timeout* must be an integer from 0 to 20.

CS triggered S1 Paging requests are transmitted only once by the MME (no retransmission). For a CS paging to be sent again, another SGs paging request needs to be sent by MSC/VLR towards MME.

t3415-timeout *t3415_dur*

The keyword **t3415-timeout** *t3415_dur* is used to configure the T3415 paging timeout value. The *t3415_dur* must be an integer in the range 1 up to 20 seconds.

max-paging-attempts *attempts*

Defines the number of paging requests to be sent out during this paging-stage.

attempts must be an integer from 0 to 5.

Usage Guidelines

Use this command to configure paging procedure stages, which in turn control the pace, volume, and behavior of paging for each stage. This command is not enabled by default. There are no re-tries in a paging stage. The MME uses the T3413 timer for non-eDRX UEs to re-transmit paging. For eDRX UEs the MME uses the T3415 timer and on expiry of T3415 timer, the network aborts the paging procedure.

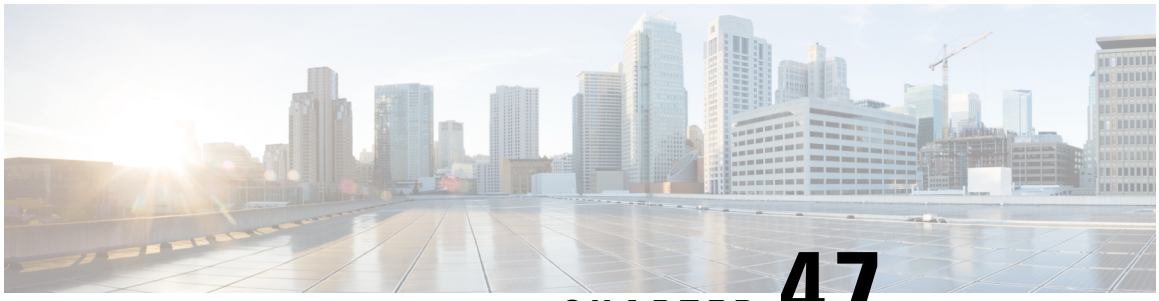
If a session recovery occurs then the eDRX timer re-starts only for the remaining time of the total time configured before session recovery. This is to ensure that the UE and MME are in sync with respect to the paging occasion.

See the **paging-map** command in the *LTE Policy Configuration Commands* chapter to assign a priority for this paging profile based on traffic type.

Example

The following configuration example creates a paging-profile in the lte-policy configuration mode:

```
paging-stage 1 match-criteria all action all-enb-all-tai t3413-timeout 5 max-paging-attempts
 4
```



CHAPTER 47

LTE Peer Map Configuration Mode Commands

The LTE Peer Map Configuration Mode enables the operator to map LTE Policy to a peer profile based on matching criteria and precedence for the criteria.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Peer Map Configuration

configure > lte-policy > peer-map *map_name*

Entering the above command sequence results in the following prompt:

`[local]`*host_name*`(peer-map)#`

Important Available commands or keywords/variables vary based on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

precedence

Configures the matching criteria and precedence for mapping an LTE Policy with a peer profile.

Product

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Peer Map Configuration

configure > lte-policy > peer-map *map_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(peer-map)#
```

Syntax Description

```
precedence priority match-criteria { all peer-profile-name profile_name |
peer-ip-address { ip_address(IPv4/IPv6) | ip_address(IPv4/IPv6)/mask } [
serving-plmnid mcc mcc mnc mnc ] peer-profile-name profile_name |
serving-plmnid mcc mcc mnc mnc [ peer-ip-address { ip_address | ip_address/mask
 } ] peer-profile-name profile_name }
no precedence priority
```

no

Removes the selected precedence priority number from the peer map.

priority must be an integer from 1 to 1024.

priority

priority must be an integer from 1 to 1024. Precedence 1 has highest priority.

match-criteria

Defines the criteria to be used to match peer nodes.

all

Specifies that all peer nodes are to be associated with the peer map.

To map a peer to a profile when there is no specific criteria required, use the **all** keyword.

peer-profile-name *profile_name*

Sets the peer profile with which the matching criteria is associated.

profile_name must be an existing peer profile expressed as an alphanumeric string of 1 through 64 characters.

peer-ip-address *ip_address | ip_address/mask*

Specifies the IP address of the peer node.

ip_address must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6.

ip_address/mask must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6, followed by the mask.

serving-plmnid mcc *mcc* mnc *mnc*

Specifies serving nodes with criteria matching the PLMN ID (MCC and MNC) are to be associated with a specified peer map.

mcc *mcc*: Specifies the mobile country code (MCC) portion of the PLMN ID.

mcc must be a three-digit number between 100 and 999.

mnc *mnc*: Specifies the mobile network code (MNC) portion of the PLMN ID.

mnc must be a two- or three-digit number between 00 and 999.

Usage Guidelines

Use this command to map LTE Policy to a peer profile based on matching criteria and precedence for the criteria.

A maximum of 1024 precedence entries can be configured.

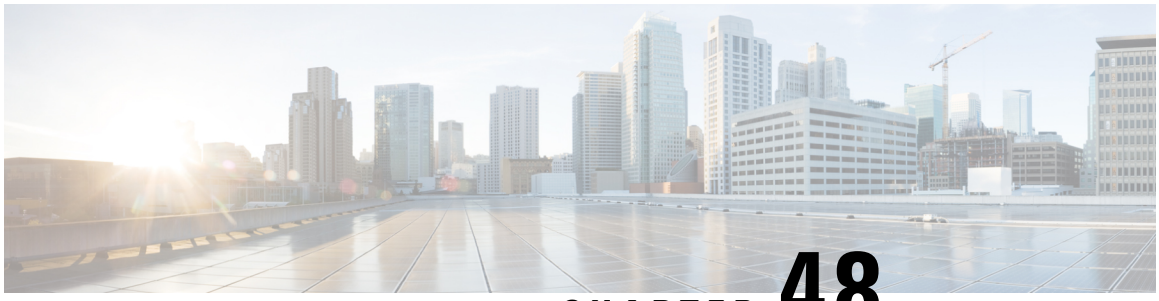
Example

The following command associates the peer profile named pp5 with peers associated with a serving node PLMN ID MCC of 111 and an MNC of 222:

```
precedence 100 match-criteria serving-plmnid mcc 111 mnc 222
peer-profile-name pp5
```

The following command associates the peer profile named pp5 with IP address of the peer node:

```
precedence 1 match-criteria peer-ip-address 209.165.200.225
PEER-profile-name pp5
```



CHAPTER 48

LTE Policy Configuration Mode Commands

The LTE Policy Configuration Mode is used to create and manage the LTE policies supporting ePDG, MME, S-GW, SAEGW, SGSN, and HeNBGW configurations on the system.

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Important Available commands or keywords/variables vary based on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

Syntax Description

monitoring-event-profile *profile_monte profile_name*

events ***<List of Supported Events>***

loss-of-connectivity

Specifies Loss of connectivity.

ue-reachability

Specifies reachability of UE.

location-reporting

Specifies location information.

communication-failure

Specifies Radio connection status.

availability-after-ddn-failure

Specifies whether UE is active after DDN Failure.

idle-status-indication

Indicates that UE moves to idle status. The idle status can be either for ue-reachability or for DDN failure.

pdn-connectivity-status

Indicates PDN status change.

number-of-ue-in-geo-area

Specifies number of UEs present in a geographic area.

external identifier

MME updates HSS to handle the support.

If external identifier is received from HSS as part of Monitoring Event Configuration Grouped AVP it is read and the same is sent in as RIR to SCEF.

If external identifier AVP is NOT received as part of Monitoring Event Configuration AVP but received the same in Subscription Data AVP this will be read and sent in as RIR to SCEF.

- cause-code-group, on page 451
- congestion-action-profile, on page 452
- enb-group, on page 453
- foreign-plmn-guti-mgmt-db, on page 454
- henbgw mme-pool, on page 455
- henbgw overload-control, on page 456
- henbgw qci-dscp-mapping-table, on page 457
- henbgw s1-reset, on page 458
- henbgw session-recovery idle-timeout, on page 458
- ho-restrict-list, on page 459
- imei-tac-group, on page 460
- imsi-group, on page 461
- lte-emergency-profile, on page 462
- mec-tai-grp, on page 463
- mme henbgw mgmt-db, on page 464
- mme paging cache, on page 465
- network-global-mme-id-mgmt-db, on page 466
- paging-map, on page 467
- paging-profile, on page 470
- peer-map, on page 471
- pra-profile dcnr-5g-radio, on page 472
- sgsn-mme, on page 475

- subscriber-map, on page 475
- tai-list-db, on page 476
- tai-mgmt-db, on page 478

cause-code-group

Creates a new cause code group, or specifies an existing cause code group and enters the Cause Code Group Configuration Mode.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

`[ no ] cause-code-group` *`group_name`* **`protocol { bssgp | ranap | s1ap }`**

no

Removes the specified cause code group with all related configuration from the LTE Policy.

group_name

Specify a name of a cause-code-group to create, modify, or remove. This name must be an alphanumeric string of 1 through 16 characters. Each new cause-code-group must have a unique name.

A maximum of 4 cause code groups can be defined across all services (MME+GPRS+SGSN).

protocol

Specifies the protocol for the cause code group being created/accessed. Options include:

- BSSGP for 2G.
- RANAP for 3G
- S1-AP

Usage Guidelines

Use this command to create or modify a group of cause codes.

Entering this command results in a prompt, with the protocol ID included, similar to the following:

```
[context_name]hostname(s1ap-cause-code)#
```

Depending upon the protocol you have selected, the Cause Code Group configuration commands are defined in the

- *BSSGP Cause Code Configuration Mode Commands* chapter of this guide.
- *RANAP Cause Code Configuration Mode Commands* chapter of this guide.
- *S1AP Cause Code Configuration Mode Commands* chapter of this guide.

Example

The following command creates an S1-AP cause code group named *move-ue-to-idle*.

```
cause-code-group move-ue-to-idle protocol s1ap
```

congestion-action-profile

Creates an action profile for MME or ePDG or HeNBGW critical, major and minor congestion thresholds. The profile defines the action to be taken when these thresholds are exceeded.

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

Product

ePDG

HeNBGW

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

[no] congestion-action-profile *profile_name*

no

Removes the specified profile from the system.

profile_name

Specifies the name of the action profile. If the entered name does not refer to an existing profile, a new profile is created. *profile_name* is an alphanumeric string of 1 through 64 characters.

-noconfirm

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

Usage Guidelines

Use this command to establish MME or ePDG action profiles to be associated with critical, major and minor congestion thresholds. This command is also used to remove an existing profile.

Note This command is part of a licensed feature and requires a proper license to function: MME Resiliency Bundle.

For information on setting the action to be taken within this profile, see the *Congestion Action Profile Configuration Mode Commands* chapter in this guide, and the *Congestion Control* chapter in the *System Administration Guide*.

Example

The following command creates a major congestion action profile named *mme_major_profile* and moves to the Congestion Action Profile Configuration mode:

```
congestion-action-profile mme_major_profile
```

Syntax Description `drop | reject  monitoring-event-config-request`

drop|reject

Drops or rejects every new incoming Monitoring Event configuration without any reply.

Usage Guidelines Use this command to drop or reject the Monitoring Event Configuration Request if the system detects congestion.

.

enb-group

Creates eNB Group mode.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description `[ no ] enb-group enb_group_name`

Important Maximum of 20 eNB groups are allowed to be configure at any given point of time.

no

Removes the specific eNB group.

enb-group *enb_group_name*

Creates the eNB Group. *enb_group_name* must be a string of 1 to 64 characters.

bits Must be an Integer from 1 to 28.

By entering this command you enter new mode enb-group

foreign-plmn-guti-mgmt-db

Creates a new, or enters the existing Foreign PLMN GUTI management database.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

foreign-plmn-guti-mgmt-db *db_name* **[-noconfirm]**
no foreign-plmn-guti-mgmt-db *db_name*

no

Remove the specified management database from the system.

-noconfirm

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

db_name

Specifies the name of the management database. If the name does not refer to an existing database, a new database is created.

db_name is an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to create a new, or enter the existing Foreign PLMN GUTI management database. This management database allows for the optional configuration of foreign PLMNs for which Attach Requests or TAU Requests containing a GUTI from such a PLMN can either be allowed or immediately rejected.

A maximum of four separate Foreign PLMN GUTI management databases can be configured.

Entering this command results in the following prompt:

```
[context_name]hostname(foreign-plmn-guti-mgmt-db)#
```

Global MME ID management database commands are defined in the *LTE Foreign PLMN GUTI Management Database Configuration Mode Commands* chapter.

Example

The following command creates a Foreign PLMN GUTI management database named *fguti-db1*.

foreign-plmn-guti-mgmt-db fguti-db1 -noconfirm

henbgw mme-pool

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

Creates or configures a specified MME or MME pool to which the HeNB-GW is to communicate and enters the MME pool configuration mode.

Product

HeNB-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

[no] henbgw mme-pool *pool_name* **[-noconfirm]**

no

Removes an already configured MME or MME pool from the system.

pool_name

Specifies the name of the MME pool being created or accessed. If the pool name does not refer to an existing profile, a new pool is created. *pool_name* is an alphanumeric string of 1 through 63 characters.

-noconfirm

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

Usage Guidelines

Use this command to enter the MME Pool Configuration Mode for an existing pool or for a newly defined MME pool. This command is also used to remove an existing MME pool.

Important A maximum of eight MME pools are allowed per system.

Entering this command results in the following prompt:

```
[context_name]hostname(mme-pool)#
```

MME Pool Configuration Mode commands are defined in the *MME Pool Configuration Mode Commands* chapter.

Example

The following command helps entering the MME Pool Configuration Mode for a new or existing profile named *henb_mme_pool*:

henbgw mme-pool henb_mme_pool

henbgw overload-control

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

Configures HeNBGW overload control parameters.

Product

HeNBGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

henbgw overload-control [load-reduction-indicator *percentage_value* **| ochl-guard-time** *minutes* **]**
default mme henbgw overload-control [load-reduction-indicator | ochl-guard-time]

default

Sets/Restores the default values assigned to HeNBGW overload control parameters. The default value of load Reduction indication is 99 percent.

load-reduction-indicator *percentage_value*

Designates the percentage of HeNBs to relay overload start message if traffic load Reduction indication IE is not present in the overload start message.

percentage_value is the percentage value, which is an integer between 1 and 99.

ochl-guard-time *minutes*

Designates the guard timeout value (in minutes) for sending overload stop messages if overload stop message is not received from MME to all the HeNBs in corresponding MME's overload control HeNBs list. The guard timeout value is an integer between 0 and 2147483647.

Usage Guidelines

Use this command to configure HeNBGW overload control parameters.

Example

The following command configures HeNBGW overload control parameter **ochl-guard-time** as 45 minutes:

```
henbgw overload-control ochl-guard-time 45
```

henbgw qci-dscp-mapping-table

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

Use this command to configure qci-dscp-mapping-table for HENBGW. The maximum limit for the tables that can be configured is 32.

Product

HeNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

```
[ no ] henbgw qci-dscp-mapping-table table_name
```

no

Removes the qci-dscp-mapping-table for HENBGW.

Important This command on execution will open a new mode HeNBGW QCI DSCP Mapping Table mode.

table_name

It is the qci-dscp-mapping-table for HENBGW, a string of size between 1 and 63.

Usage Guidelines

Use this command to configure qci-dscp-mapping-table for HENBGW.

Example

Following command configures qci-dscp-mapping-table by name table1 for HENBGW.

```
henbgw qci-dscp-mapping-table table1
```

henbgw s1-reset

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

Configures option to enable/disable s1-reset/partial-reset messages sent from HeNBGW.

Product HeNBGW

Privilege Administrator

Command Modes Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

```
[ no ] henbgw s1-reset
```

no

This command prefix disables s1-reset/partial-reset messages sent from HeNBGW.

s1-reset

Configures option to enable or disable sending s1-reset/partial-reset messages from HeNBGW.

Example

The following command configures HeNBGW **s1-reset** messages:

```
henbgw  s1-reset
```

henbgw session-recovery idle-timeout

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

Configures HENBGW session recovery. The HENBGW session recovery is valid only when require session recovery is configured. Base session recovery feature will enable recovery of IP-Sec tunnels when integrated IP-Sec is used. Enhanced HENBGW session recovery feature will enable recovery of SCTP/UE sessions in HENBGW. This feature should be enabled if henb(s) have the capability to retain UE S1AP state across SCTP connection restarts.

Product

HeNBGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

henbgw session-recovery [idle-timeout *timeout_value* **]**
no henbgw session-recovery

no

Removes the HENBGW session recovery configuration.

idle-timeout *timeout_value*

Configures the idle timeout.

Designates the maximum duration of the session recovered without any activity, in seconds, before system automatically terminates the session. Zero indicates function is disabled.

The *timeout_value* specifies the idle timeout in seconds (0 is disabled). It is an integer between 0 through 2147483647.

Usage Guidelines

Use this command to configure HENBGW session recovery with idle timeout.

Example

The following command configures HeNBGW session recovery with idle timeout *45* seconds:

henbgw session-recovery idle-timeout *45*

ho-restrict-list

Creates a handover (HO) restriction list or specifies an existing HO restriction list and enters the Handover Restriction List Configuration Mode.

Product

MME

ePDG

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

`[ no ] ho-restrict-list` *`list_name`* `[ -noconfirm ]`

no

Removes the specified restriction list from the system.

-noconfirm

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

list_name

Specifies the name of the HO restriction list. If the entered list name does not refer to an existing list, a new list is created. *list_name* is an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to enter the Handover Restriction List Configuration Mode for an existing list or for a newly defined list. This command is also used to remove an existing list.

Entering this command results in the following prompt:

```
[context_name]hostname(ho-restrict-list)#
```

Handover Restriction List Configuration Mode commands are defined in the *LTE Handover Restriction List Configuration Mode Commands* chapter.

Example

The following command enters the Handover Restriction List Configuration Mode for a new or existing list named *ho_restricit_list1*:

```
ho-restrict-list ho_restrict_list1
```

imei-tac-group

Creates an IMEI-TAC group and provides commands to configure up to 25,000 IMEI-TACs (international mobile equipment identity - type allocation code (IMEI-TAC) that can be used as the filtering criteria for Operator Policy selection.

Important This functionality is available on releases 18.6, 19.4, and 20.0 and higher.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description **`[ no ] imei-tac-group`** *`group_name`*

no

Removes the specified IMEI-TAC group with all related configuration from the LTE Policy.

group_name

Specify a name for the IMEI-TAC group to create, modify, or remove the group. This name must be an alphanumeric string of 1 through 64 characters. Each new IMEI-TAC group must have a unique name.

A maximum of 50 IMEI-TAC groups can be defined on the MME.

Usage Guidelines Use this command to create, modify, or delete an IMEI-TAC group. Create up to 50 IMEI-TAC groups. Each group can contain up to 500 unique IMEI-TAC values and/or up to 20 IMEI-TAC ranges, which can be overlapping.

This command is used as part of the configuration required to enable operator policy selection based on IMEI-TAC. Including the type allocation code (TAC) in the operator policy selection process supports network access restrictions being applied to UEs based on the type of wireless device identified by the IMEI-TAC. For details about this feature and all the other commands required for its configuration, refer to the *Operator Policy Selection Based on IMEI-TAC* chapter in the *MME Administration Guide*.

Example

The following command creates an S1-AP cause code group named *move-ue-to-idle*.

```
cause-code-group move-ue-to-idle protocol s1ap
```

imsi-group

This command configures the International Mobile Subscriber Identity (IMSI) group.

Product MME

SGSN

Privilege Administrator

Command Modes Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

imsi-group *group_name*

imsi-group *group_name*

Specifies the IMSI group name. *group_name* must be an alphanumeric string of 1 through 64 characters. It can have a maximum of 50 groups.

Usage Guidelines

Use this command to create the IMSI group. An IMSI group can contain up to 500 elements of either individual IMSI or range of IMSI numbers. Once an IMSI group is created, each group can be configured with up to 500 unique IMSI values. Multiple lines of IMSI and IMSI-range can be up to 20 lines per group.

This command allows you to enter the IMSI Group Configuration Mode.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-imsi-group)#

IMSI Group Configuration Mode commands are defined in the *IMSI Group Configuration Mode Commands* chapter.

lte-emergency-profile

Creates an LTE emergency profile or specifies an existing emergency profile and enters the LTE Emergency Profile Configuration Mode.

Product

MME

ePDG

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

[no] lte-emergency-profile *profile_name* **[-noconfirm]**

no

Removes an LTE emergency profile from the system.

profile_name

Specifies the name of the LTE emergency profile being created or accessed. If the profile name does not refer to an existing profile, a new profile is created. *profile_name* is an alphanumeric string of 1 through 64 characters.

-noconfirm

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

Usage Guidelines

Use this command to enter the LTE Emergency Profile Configuration Mode for an existing profile or for a newly defined profile. This command is also used to remove an existing profile.

Important A maximum of four LTE emergency profiles are allowed per system.

Entering this command results in the following prompt:

```
[context_name]hostname(lte-emergency-profile)#
```

LTE Emergency Profile Configuration Mode commands are defined in the *LTE Emergency Profile Configuration Mode Commands* chapter.

Example

The following command enters the LTE Emergency Profile Configuration Mode for a new or existing profile named *emergency_profile3*:

`lte-emergency-profile emergency_profile3`

mec-tai-grp

Creates a MEC TAI Group and enters the MEC TAI Group Configuration Mode.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

`[ no ] mec-tai-grp` *`grp_name`*

no

Removes the MEC TAI Group from the system.

mec_tai_grp_name grp_name

Specifies the name of the MEC TAI Group being created. *grp_name* is an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to enter the MEC TAI Group Configuration Mode.

MEC TAI Group Configuration Mode commands are defined in the *MEC TAI Group Configuration Mode Commands* chapter.

Example

The following command enters the MEC TAI Group Configuration Mode:

```
mec-tai-grp mgrp1
```

mme henbgw mgmt-db

Creates an MME HeNB-GW Management Database or specifies an existing database and enters the HeNB-GW Management Database Configuration mode.

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

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

`[ no ] mme henbgw mgmt-db` *db_name* **`[ -noconfirm ]`**

no

Removes the specified management database from the system.

[-noconfirm]

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

db_name

Specifies the name of the management database. If the name does not refer to an existing database, a new database is created. *db_name* is an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to create a new, or enter the existing MME HeNB-GW management database. This command enables configuration for the MME to distinguish between an HeNB-GW and an eNodeB.

In case of S1-based handovers to Home eNodeBs served by a HeNB-GW, the lookup at the MME for the target eNodeB based on global eNodeB id cannot be completed, as the MME is aware of only the HeNB-GW. In those cases, an additional lookup needs to be performed based on the TAI, in order to find the HeNB-GW serving the Home eNodeB. The S1 Handover request message will then be sent to the HeNB-GW and forwarded to the correct Home eNodeB in order to prepare the target RAN node for handover.

One HeNB-GW management database is allowed per LTE Policy.

A maximum of 8 HeNB-GWs can be configured within this management database.

Entering this command results in the following prompt:

`[context_name]hostname(henbgw-mgmt-db)#`

MME HeNB-GW management database commands are defined in the *LTE MME HeNB-GW Management Database Configuration Mode Commands* chapter.

Example

The following command enters the existing LTE MME HeNB-GW Managment Database Configuration Mode (or creates it if it does not already exist) for the database named henbgw_db1:

```
mme henbgw mgmt-db  henbgw_db1
```

mme paging cache

Enable or disables caching of the MME's paging and provides the operator configurable paging cache controls.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

`[local]host_name(lte-policy)#`

Syntax Description

```
mme paging cache { size cache_size | timeout time }
default mme paging cache { size | timeout }
```

default

Resets either the paging cache size or the paging cache timer to default settings.

size *cache_size*

cache_size: Enter an integer from 0 to 10000 to specify the maximum number of Tracking Area Code (TAC) entries to be cached.

Entering the '0' value disables caching and should be followed by use of the **mme paging cache clear** command (in the Exec mode). See the *Example* section.

Default cache size = 5000 TAC entries per SessMgr.

timeout *time*

time: Enter an integer from 1 to 1440 to specify the number of minutes that each Tracking Area Code (TAC) entry remains valid.

A lower cache timeout helps to refresh the cache frequently and enables this functionality to quickly adapt to changes in the network. We recommend the **timeout** value be less than the expected eNodeB flap frequency; for example, if the eNodeBs connected to the MME are expected to disconnect and reconnect every 10 minutes (due to network issues), then the timeout configuration should be less than 10 minutes.

Default timeout = 5 minutes.

Usage Guidelines

Both size and timeout must be configured to enable paging cache optimization. The **mme paging cache** command must be entered twice, once for each parameter.

Example

Use the following configuration to set the paging cache timeout to match the eNodeB flap frequency of 10 minutes:

```
mme paging cache timeout 10
```

Use the following configuration to set the paging cache size to 100:

```
mme paging cache size 100
```

Use the following configuration to set the paging cache size to 0 (to disable caching):

```
mme paging cache size 0
end
mme paging cache clear { all | instance sessmgr_instance }
```

network-global-mme-id-mgmt-db

Creates a new, or enters the existing MME group ID management database.

Product

MME

ePDG

SAEGW

S-GW

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

[no] network-global-mme-id-mgmt-db

no

Remove the global MME ID management database from the system.

Usage Guidelines

Use this command to create a new, or enter the existing MME group ID management database. The MME group ID management database is used to create associations between PLMN IDs and ranges of MME group IDs.

On the S4-SGSN, this command enables operators to create a MME group ID management database that can be associated with an SGSN service.

Important Only one MME group ID management database can be created per system.

Entering this command results in the following prompt:

```
[context_name]hostname(network-global-mme-id-mgmt-db)#
```

plmn mcc [*mcc-value*] **mnc** [*mnc-value*]**mme-group-id-range** [*First id*] [*last id*]

Global MME ID management database commands are defined in the *LTE Network Global MME ID Management Database Configuration Mode Commands* chapter.

paging-map

Creates a paging map or specifies an existing paging map and enters the Paging Map Configuration Mode.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

[no] paging-map *paging_map_name* **[-noconfirm]**

precedence *priority* **traffic-type { cs [other | sms | voice] | ps [apn-profile** *profile_name* **| arp** *arp_value* **| qci** *qci_value* **] | signaling [detach | idr | lcs | node-restoration] } paging-profile** *paging_profile_name*

no

Remove the paging map from the system.

paging_map_name

Specifies the name of the paging map being created or accessed. If the map name does not refer to an existing map, a new map is created. *paging_map_name* must be an alphanumeric string of 1 through 64 characters.

-noconfirm

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

precedence ***priority***

precedence: For StarOS releases 16.5 and higher, enter an integer from 1 to 19, where 1 is the highest priority and 19 is the lowest priority. For StarOS releases prior to 16.5, enter an integer from 1 to 7, where 1 is the highest priority and 7 is the lowest priority. For releases 20.0 onwards enter an integer from 1 to 35, where 1 is the highest priority and 35 is the lowest priority. The numbers of paging-profiles supported are increased from 8 to 16.

traffic-type { cs [voice | sms | other] | ps [qci ***qci_value*** **| apn-profile** ***profile_name*** **] | signaling [detach | idr | lcs | node-restoration] }**

Defines the type of traffic of the incoming call.

- **cs** (Circuit Switched) - All data and control activities that involve CSFB. Paging requests from the MSC for mobile-terminated calls alone are treated as CS type. Paging requests for SMS are treated as PS type.

  Optionally, define the CS traffic sub-type:

  - **other**: MM Information Request messages coming from MSC can also trigger paging if UE is in IDLE state. These requests are mapped to 'other' sub-traffic type.
  - **sms**: Paging requests from MSC for mobile terminated SMS requests.
  - **voice**: Paging requests from MSC for mobile terminated voice calls.

  If a sub-traffic-type is not configured then paging-profile configured for CS (with no sub traffic-type qualification) is applied. If no such entry exists, then default heuristics based paging behavior is applied.

- **ps** (Packet Switched) - All data and control activities that involve packet services. SRVCC is also mapped to this traffic-type as the voice is carried using PS service. PS traffic type is further qualified using a set of QCI values or ARP values or APN profile names. These qualified entries are only used for paging triggered by S11 Downlink Data Notifications or Create Bearer Request or Update Bearer Request

  Optionally, define the APN Profile for PS traffic:

  apn-profile *profile_name*

  where *profile_name* is an alphanumeric string of size 1 to 64.

  The MME supports paging profile selection based on APN. A maximum of four APN profiles can be configured per precedence using this command.

  When heuristics paging is enabled, the MME selects the paging profile based on the APN profile, if paging-profile with matching APN profile name is fetched from the APN information corresponding to the EBI received in DDN is configured in the paging-map. If the incoming DDN does not have the EBI

information then the APN information is received from the bearers stored in the MME for the UE. If multiple APN information is available, then the mapping with the highest precedence is picked. MME warns the user of duplicate APN profile names in a given entry. The same APN profile name cannot be configured with more than one precedence level.

Optionally, define the ARP priority based paging for PS traffic type in the paging-map:

arp *arp_value*

The allowed ARP value " *arp_value* " is an integer from 1 through 15.

Optionally, define the QoS Class Identifier (QCI) value for this PS traffic:

qci *qci_value*

The QCI values can be either standard or non-standard. The *qci_value* is an integer from 1 through 9, 65, 66, 67, 69, 70 (standard values) and from 128 up to 255 are non-standard values.

QCI qualified entries can only be used for paging triggered by Downlink Data Notifications received on S11. If the incoming DDN contains EPS Bearer ID (EBI) information, the QCI corresponding to that PDN is used to find the appropriate 'ps qci xx' entry and its configured paging-profile.

If there are multiple EBIs included in the DDN the mapping entry with highest precedence is selected.

If no QCI specific mapping exists, or if the incoming DDN does not have the EBI information then the qci corresponding to the bearers stored in MME for the UE shall be used to find the appropriate 'ps qci xx' entry and its configured paging-profile. The MME warns the user of duplicate QCI values in a given entry, same QCI values cannot be configured with more than one precedence level.

sms

Configures paging profile for SMS via SGd.

- **signaling [detach | idr | lcs | node-restoration]**: UE level signaling requests. This traffic can be optionally qualified according to the following sub-traffic types:

  detach: Paging requests triggered due to UE getting detached.

  idr: Paging triggered in response to an IDR event, such as receiving an IDR Request.

  lcs: (Location Services) – Paging requests triggered due to Positioning Requests coming from SMLC over SLs interface. Mobile Terminated Location Requests arriving on SLg interface can also trigger paging if UE is in IDLE state, and are included in this sub-traffic type.

  node-restoration: Paging requests triggered due to node restoration (for example, due to P-GW Restart Notification (PRN)). By default, no precedence is assigned to node restoration signaling traffic. The MME treats node restoration paging with the least priority.

  If a sub-traffic-type is not configured then paging-profile configured for signaling (with no sub traffic-type qualification) shall be applied. If no such entry exists then default-heuristics based paging behavior is applied.

paging-profile *paging_profile_name*

The paging-profile to apply for paging UE.

Usage Guidelines

Enter the Paging Map Configuration Mode for an existing or newly defined map. This command is also used to remove an existing map.

Entering this command results in the following prompt:

hostname(paging-map)#

Paging Map Configuration Mode commands are defined in the *LTE Paging Map Configuration Mode Commands* chapter.

Refer to the *Heuristic and Intelligent Paging* chapter in the *MME Administration Guide* for more information about Paging Maps.

Example

The following command enters the existing Paging Map Configuration Mode (or creates it if it does not already exist) for the map named *map1*:

paging-map map1

paging-profile

Creates a paging profile or specifies an existing paging profile and enters the Paging Profile Configuration Mode.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

[local]*host_name*(lte-policy)#

Syntax Description

[no] paging-profile *paging_profile_name* **[-noconfirm]**

no

Remove the paging map from the system.

paging_profile_name

Specifies the name of the paging profile being created or accessed. If the profile name does not refer to an existing profile, a new profile is created. *paging_profile_name* must be an alphanumeric string of 1 through 64 characters.

-noconfirm

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

Usage Guidelines

Enter the Paging Profile Configuration Mode for an existing or newly defined paging profile. This command is also used to remove an existing profile.

Entering this command results in the following prompt:

```
hostname(paging-profile)#
```

Paging Profile Configuration Mode commands are defined in the *LTE Paging Profile Configuration Mode Commands* chapter.

Refer to the *Heuristic and Intelligent Paging* chapter in the *MME Administration Guide* for more information about Paging Profiles.

Example

The following command enters the existing Paging Profile Configuration Mode (or creates it if it does not already exist) for the profile named *profile1*:

paging-profile profile1

peer-map

Creates a peer map and enters the LTE Peer Map Configuration mode.

Product

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

peer-map *map_name* **[-noconfirm]**
no peer-map *map_name*

no

Removes the specified peer map from the LTE policy.

map_name

Specify a name of a peer map to create, modify, or remove. This name must be an alphanumeric string of 1 through 64 characters. Each new peer map must have a unique name.

-noconfirm

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

Usage Guidelines

Use this command to create or modify a peer map.

Entering this command results in the following prompt:

```
[local]host_name(peer-map)#
```

LTE Peer Map Configuration Mode commands are defined in the *LTE Peer Map Configuration Mode Commands* chapter of this guide.

Example

The following command creates a peer map named map5 and enters the LTE Peer Map Configuration mode:

```
peer-map map5
```

pra-profile dcnr-5g-radio

Configures the gNB S1-U IP addresses in ranges. By default, an gNB S1-U IP address is not configured.

For IPv4 addresses or IPv6 addresses, a maximum of 50 entries can be given in a PRA profile. Altogether, a maximum of 100 entries can be given in a PRA profile and only one PRA profile is supported.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

```
[ no ] pra-profile dcnr-5g-radio  profilename1
           [ no ] gnb-s1u ipv4-network <address>/[ mask ]
          [ no ] gnb-s1u ipv4-range from <start-ip/mask> to <end-ip/mask>

           [ no ] gnb-s1u ipv6-prefix <address>/[mask]
           [ no ] gnb-s1u ipv6-prefix-range from <start-ip/mask> to
<end-ip/mask>
           [ no ] gnb-s1u ipv6-prefix-pattern <address/mask> start-bit
<bit position>
             end-bit <bit position> pattern <pattern in hex value>
```

pra-profile

Configures PRA Profile.

profile_name: Specifies the PRA profile name with a string of size 1–63..

- **do**: Spawns an exec mode command which displays information to the administrator.
- **end**: Exits configuration mode and returns to the Exec Mode
- **exit**: Exits current configuration mode, returning to previous mode
- **gnb-s1u**: Configures gNB S1-U Addresses for 5G radio connectivity

- **no**: Disables option.

gnb-s1u

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

- **ipv4-network** : Configures gNB S1-U IPv4 network for 5G radio connectivity.
- **ipv4-range**: Configures gNB S1-U IPv4 address range for 5G radio connectivity.
- **ipv6-prefix**: Configures gNB S1-U IPv6 network for 5G radio connectivity.
- **ipv6-prefix-pattern**: Configures gNB S1-U IPv6 prefix range with hex-pattern for 5G radio connectivity.
- **ipv6-prefix-range**: Configures gNB S1-U IPv6 prefix range for 5G radio connectivity

gnb-s1u ipv4-network *address/mask*

Configures block of addresses. If the mask is not specified, a default mask of 32 bits for the IPv4 address is considered.

When **gnb-s1u ipv4-network** *0.0.0.0* is configured, it indicates that any IPv4 address will be considered as gnb-s1u address, and no lookup is done with the already configured IPv4 addresses in the profile. In this input, default mask is taken irrespective of any configured mask.

gnb-s1u ipv4-range from <start-ip/mask> to <end-ip/mask>

Specifies a range of IP addresses for a given mask. The mask value should be the same in the *start-ip* and in *end-ip*. Following are few conditions:

- In the range, if Network ID is specified, then starting address and ending address is calculated according to the mask.
- In the range, if host address is specified then it will be taken.
- You can specify either Network ID for both the starting address and ending address or Host ID for both the starting address and ending address.
- In the range, if mask is not specified, a default mask of 32 bits is considered for IPv4 and the specified address is considered as host address.

gnb-s1u ipv4-range

- **from**: Enter the first gNB S1-U IPv4 address in the range.
- **to**: Enter the last gNB S1-U IPv4 address in the range.

gnb-s1u ipv6-prefix *address/mask*

Configures block of addresses. If the mask is not specified, default mask of 128 bits for an IPv6 address is considered. For example, if an ipv6 range is specified from 2001:4900:0050:2001::0/64, then all addresses with the network id 2001:4900:0050:2001 is considered.

Note When **gnb-s1u ipv6-prefix :: is** configured, it indicates that any IPv6 address is considered as gnb S1 U address, and there is no lookup with the already configured IPv6 addresses in the profile. In this input, a default mask is taken irrespective of any configured mask.

ipv6-prefix

Configures S1-U IPv6 addresses.

gnb-s1u ipv6-prefix-range from < start-ip / mask > to < end-ip / mask >

Specifies a range of IP addresses for a given mask. Ensure to enter the same mask value in the *start-ip* and in the *end-ip*:

- **from**: Enter the first gNB S1-U IPv6 address in the range.
- **to**: Enter the last gNB S1-U IPv6 address in the range.

  For example, If you specifiy ipv6 range from 2001:4900:0050:2001::0/64 to 2001:4900:0050:20aa::0/64", then all addresses with the network id "2001:4900:0050:2001" to "2001:4900:0050:20aa" is considered.

gnb-s1u ipv6-prefix-pattern <address/mask> start-bit *bit position* end-bit *bit position* pattern *pattern in hex value*

- **start-bit** *bit position* : Starting bit position of the pattern. It should be outside the mask bits
- **end-bit** *bit position* : Ending bit position of the pattern. It should be outside the mask bits.
- **pattern** *pattern in hex value*: Enter the pattern in hexadecimal. A maximum of 64 bit pattern is supported.

Note The start-bit and end-bit position should not be within the mask bits. For example, if you specify gnb-s1u ipv6-prefix-pattern 2001:4900:0050:2000::0/16 start-bit 61 end-bit 64 pattern 0x3", then all addresses with the network id "2001:4900" and with bits 61–64 matching to 0x3 are considered. A maximum of 64-bit pattern is supported for an IPv6 address.

Limitations: Following are the limitations:

- It is recommended to provide non duplicate, or non overlapping IP addresses, or non conflicting inputs across the CLIs.
- It is recommended not to configure multicast or broadcast IP addresses.

Usage Guidelines

Enter the gNB S1-U IP addresses in ranges. By default, an gNB S1-U IP address is not configured.

For IPv4 addresses or IPv6 addresses, a maximum of 50 entries can be given in a PRA profile. Altogether, a maximum of 100 entries can be given in a PRA profile and only one PRA profile is supported.

sgsn-mme

This command is used to enable or disable subscriber data optimization in a SGSN-MME combo node.

Product

SGSN

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

`[local]host_name(lte-policy)#`

Syntax Description

`[ no ] sgsn-mme subscriber-data-optimization`

no

Disables the configured optimization in a SGSN-MME combo node.

subscriber-data-optimization

Enables subscriber data optimization in a SGSN-MME combo node.

Usage Guidelines

This command is used to configure data optimization in a SGSN-MME combo node. When this command is configured in a co-located SGSN and MME node, lower memory or CPU utilization and reduced signaling towards other nodes in network is achieved. This feature is supported by both the S4-SGSN and the Gn-SGSN. For the feature to apply to a Gn-SGSN, the Gn-SGSN must be configured to connect to an HSS. The is a licensed Cisco feature. A separate feature license is required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys section of the Software Management Operations chapter in the System Administration Guide*

Example

The following command is used to enable subscriber data optimization in a SGSN-MME combo node.

`sgsn-mme subscriber-data-optimization`

subscriber-map

Creates a subscriber map or specifies an existing subscriber map and enters the Subscriber Map Configuration Mode.

Product

MME

ePDG

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

[no] subscriber-map *map_name* **[-noconfirm]**

no

Removes the specified subscriber map from the system.

-noconfirm

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

map_name

Specifies the name of the subscriber map. If the map name does not refer to an existing map, a new map is created. *map_name* must be an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Enter the Subscriber Map Configuration Mode for an existing or newly defined map. This command is also used to remove an existing map.

Entering this command results in the following prompt:

```
hostname(subscriber-map)#
```

Subscriber Map Configuration Mode commands are defined in the *LTE Subscriber Map Configuration Mode Commands* chapter.

Example

The following command enters the existing Subscriber Map Configuration Mode (or creates it if it does not already exist) for the map named *map1*:

```
subscriber-map map1
```

tai-list-db

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

Creates or configures a list of Tracking Area Information (TAI). This list is called TAI List Database.

Product

HeNB-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

[no] tai-list-db *db_name* **[-noconfirm]**

no

Removes the specified TAI list database from the system.

-noconfirm

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

db_name

Specifies the name of the TAI list database. If the name does not refer to an existing database, a new database is created. *db_name* is an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Enters the TAI List Database Configuration Mode for an existing or newly defined database. This command is also used to remove an existing database.

Important Maximum of eight TAI List Database instances can be created in a system.

Entering this command results in the following prompt:

```
[context_name]hostname(tai-list-db)#
```

TAI List Database Configuration Mode commands are defined in the *TAI List Database Configuration Mode Commands* chapter.

Example

The following command enters the existing TAI List Database configuration mode (or creates it if it does not already exist) for the database named *tai_db1*:

tai-list-db tai_db1

tai-mgmt-db

Creates a Tracking Area Identifier (TAI) Management Database or specifies an existing database and enters the TAI Management Database Configuration mode. On an S4-SGSN, this command is used as part of configuring S-GWs and their associated RAIs to bypass DNS resolution of RAI FQDN for obtaining the S-GW address.

Product

MME

ePDG

SAEGW

S-GW

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

Syntax Description

[no] tai-mgmt-db *db_name* **[-noconfirm]**

no

Removes the specified management database from the system.

-noconfirm

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

db_name

Specifies the name of the management database. If the name does not refer to an existing database, a new database is created. *db_name* is an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Enter the TAI Management Database Configuration Mode for an existing or newly defined database. This command is also used to remove an existing database.

On the S4-SGSN, once you have created a new, or accessed an existing, TAI Management database, a TAI Management Object must be created or accessed and the S-GWs and their associated RAIs configured using the **rai** and **sgw-address** commands. Refer to the *LTE TAI Object Configuration Mode* chapter for details on these two commands.

A maximum number of 32 TAI-DBs is supported in this release.

Entering this command results in the following prompt:

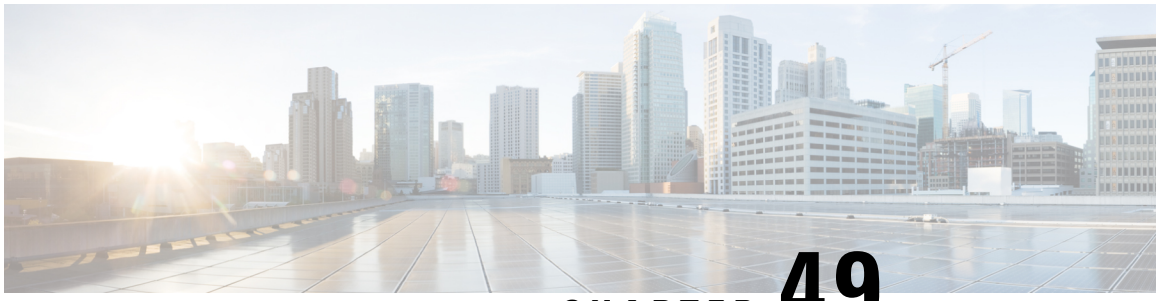
```
[context_name]hostname(tai-mgmt-db)#
```

TAI Management Database Configuration Mode commands are defined in the *TAI Management Database Configuration Mode Commands* chapter.

Example

The following command enters the existing TAI Management Database configuration mode (or creates it if it does not already exist) for the database named *tai_db1*:

```
tai-mgmt-db tai_db1
```



CHAPTER 49

LTE Subscriber Map Configuration Mode Commands

The LTE Subscriber Map Configuration Mode is used to create and manage subscriber maps for applying operator policy templates to individual subscribers and/or groups of subscribers.

Subscriber mappings are ordered lists containing explicit UE matching criteria. The maps are examined for specific UE identity information such as the UE's IMSI. The system uses the first map that matches the criteria to associate an operator policy with the UE.

Subscriber maps can be modified but will only affect future subscribers and not subscribers already attached to UEs.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Subscriber Map Configuration

configure > lte-policy > subscriber-map *subscriber_map_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(subscriber-map)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

precedence

Sets the order of precedence, the matching criteria and the association to an operator policy for subscribers meeting the match criteria.

Product

MME

SAEGW

SaMOG

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Subscriber Map Configuration

configure > lte-policy > subscriber-map *subscriber_map_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(subscriber-map)#
```

Syntax Description

For MME:

precedence *number* **match-criteria { all | imei-tac group** *group_name* **| imsi mcc** *mcc_num* **mnc** *mnc_num* **[msin first** *start_range* **last** *end_range* **] | imsi-group** *group_name* **| msisdn-group** *group_name* **| service-plmnid** *plmnid* **} operator-policy-name** *policy_name*

For SaMOG:

precedence *number* **match-criteria { all | domain** *domain_name* **| imei-tac group** *group_name* **| service-plmnid** *plmid* **[ssid** *ssid* **] | ssid** *ssid* **| imsi mcc** *mcc_num* **mnc** *mnc_num* **[msin first** *start_range* **last** *end_range* **] [service-plmnid** *plmn_id* **] [ssid** *ssid* **] } operator-policy-name** *policy_name*

For SAEGW and S-GW:

precedence *number* **match-criteria { all | imsi mcc** *mcc_num* **mnc** *mnc_num* **[msin first** *start_range* **last** *end_range* **] } operator-policy-name** *policy_name*

For all:

no precedence *number*

no

Removes the selected precedence number definition from the subscriber map.

number

Specifies the order of precedence for the subscriber map. 1 (the lowest number) takes the highest precedence.

In releases prior to 21.8: *number* must be an integer value from 1 to 1024.

In 21.8 and later releases: *number* must be an integer value from 1 to 10000.

match-criteria

Specifies that the keyword following this keyword is the criteria to be used to match a UE.

all

Specifies that all UEs are to be associated with the operator policy.

imei-tac group *group_name*

MME only; releases 18.6 and higher.

Identifies a previously configured IMEI-TAC group (with **imei-tac-group** command LTE-Policy configuration mode) to associate with this precedence definition. IMEI-TAC groups comprise up to 500 individual IMEI-TACs and/or up to 20 ranges of IMEI-TAC values. The IMEI-TAC group contents are used as the selection criteria for the MME to select/re-select an operator policy based on the UE's unique international mobile equipment identity - type allocation code (IMEI-TAC). *group_name* must be a string of up to 64 alphanumeric characters.

Beginning with releases 19.4 and higher, it is possible to configure greater level of granularity for the IMEI-TAC matching criteria by optionally including, either singly or in pairs, as part of the command:

- mcc + mnc
- imsi
- service-plmnid

So with release 19.4 the behavior of the syntax has modified slightly so that if **imei-tac-group** is the selected matching criteria, then the command syntax would be similar to:

precedence *precedence_value* **match-criteria imei-tac group** *group_name* **[imsi mcc** *mcc* **mnc** *mnc* **| msin { first** *start_msin_value* **last** *end_msin_value* **}] [service-plmnid** *plmn_id***] operator-policy** *policy_name*

Warning The use of the range value starting with '0' is inoperable during IMEI retrieval based on operator policy (IMEI-TAC). All attach requests with missing IMEI, selects the "000000" operator policy when configured.

imsi mcc *mcc_num* mnc *mnc_num* [msin first *start_range* last *end_range* | service-plmnid *id*]

Specifies that UEs with criteria matching the International Mobile Subscriber Identifier (IMSI) information (MCC and MNC) are to be associated with a specified operator policy.

mcc *mcc_num*: Specifies the mobile country code (MCC) portion of the IMSI identifier as an integer value between 100 and 999.

mnc *mnc_num*: Specifies the mobile network code (MNC) portion of the IMSI identifier as a 2- or 3-digit integer value between 00 and 999.

msin first *start_range* **last** *end_range*: Optionally specifies a range of Mobile Subscriber Identification Numbers that further narrows the match criteria for the IMSI match configuration. *start_range* and *end_range* must each be an integer value of 10 digits.

service-plmnid *plmn_id*: Optionally specifies a local service PLMN ID number used further narrow the IMSI-based operator policy selection. *plmn_id* must be an integer value of five digits minimum and six digits maximum (the combination of the MCC and MNC).

imsi-group*group_name*

Specifies the IMSI group. *group_name* must be an alphanumeric string of 1 through 64 characters.

msisdn-group*group_name*

Specifies the MSISDN group. *group_name* must be an alphanumeric string of 1 through 64 characters

service-plmnid*plmn_id*

Specifies a local service PLMN ID number used for PLMN ID-based operator policy selection. *id* must be an integer value of five digits minimum and six digits maximum (the combination of the MCC and MNC).

ssid *id*

Specifies a local SSID used for SSID-based operator policy selection to support the SaMOG Local Break Out (LBO) feature. The operator policy and associated call control profile are selected based on the SSID received in the Called-Station-Id attribute in Access-Request.

id must be an alphanumeric string of 1 through 32 characters.

The SaMOG LBO feature is license dependant. Contact your Cisco account representative for more information.

operator-policy-name *policy_name*

Sets the operator policy with which the matching criteria is associated. *policy_name* must be an existing operator policy expressed as an alphanumeric string of 1 through 64 characters. Operator policies are configured in the Operator Policy Configuration Mode. For more information about operator policies, refer to the *Operator Policy Configuration Mode Commands* chapter.

Usage Guidelines

The operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It is also used to control the behavior or visiting subscribers in roaming scenarios, enforce roaming agreements, and provide a measure of local protection against foreign subscribers.

Example

The following command associates the operator policy named *op_pol1* with UEs associated with an IMSI MCC of *111*, an MNC of *222*, and a service PLMN ID of *123456*:

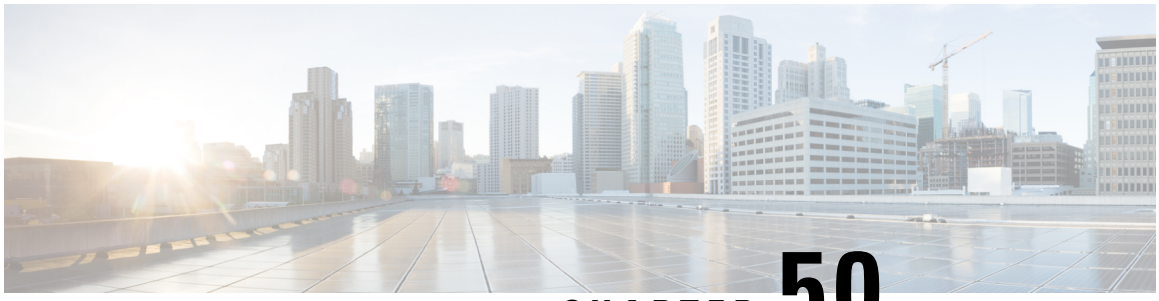
```
precedence 100 match-criteria imsi mcc 111 mnc 222 service-plmnid 123456
 operator-policy-name op_pol1
```

The following command gives the match-criteria configuration a precedence of *155* and instructs the MME to select and apply the *nokia1* operator policy for UEs with IMEI-TAC that matches one of the following IMEI-TAC: *35850000* or *01124500*

```
precedence 155 match-criteria imei-tac value 35850000 01124500
operator-policy-name nokia1
```

The following command identifies this as having the highest precedence and sets the matching criteria for the operator policy selection to based on IMEI-TAC + MCC-MNC of UE + Serving PLMNID:

```
precedence 1 match-criteria imei-tac-group myGroup imsi mcc 123 mnc 234
service-plmnid 56789 operator-policy-name BESTpol
```



CHAPTER 50

LTE TAI Management Database Configuration Mode Commands

The LTE TAI Management Database Configuration Mode is used to create and manage the LTE Tracking Area Identifier (TAI) management database on this system.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration

configure > lte-policy > tai-mgmt-db *db_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(tai-mgmt-db)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

access-type

This command is used to configure the NB-IoT RAT per TAI database.

Product MME

Privilege Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration

configure > lte-policy > tai-mgmt-db *db_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(tai-mgmt-db)#`

Syntax Description

`[ no ] access-type nb-iot`

no

Removes the configured access type for the TAI database.

nb-iot

Configures the access type as NB-IoT for a TAI database.

Usage Guidelines

The LTE TAI Management Database Configuration Mode is used to create and manage the LTE Tracking Area Identifier (TAI) management database on the system. Enter the TAI Management Database Configuration Mode for an existing or newly defined database. This command is also used to remove an existing database. Use this command to configure the access type of a TAC or group of TACs as NB-IoT RAT. As per 3GPP standards, the same TAC cannot belong to both EUTRAN and NB-IoT RATs. This command is not enabled by default. The default RAT is WB-EUTRAN.

Example

The following command is used to configure the access type as NB-IoT:

`access-type nb-iot`

network-name

This command configures the long (full) and short network name used in the Long and Short network name IE in the EMM Information message that is sent to the UE from the MME.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration

configure > lte-policy > tai-mgmt-db *db_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(tai-mgmt-db)#`

Syntax Description

`[ no ] network-name [ full` *`full_name`* **`| short`** *`short_name`* **`]`**

no

Removes a configured network-name.

full *full_name*

Defines the full (long) network name. *full_name* is an alphanumeric string of 1 through 251 characters.

short *short_name*

Defines the short network name. *short_name* is an alphanumeric string of 1 through 251 characters.

Usage Guidelines

Use this command to configure the full and short network name on the tai-db object.

This configuration affects the actions of the MME when the MME is configured to set the UE time. If this configuration exists, and there is no interaction with an MSC that sends a EMM INFORMATION message, the MME uses the above configuration while sending an EMM INFORMATION message.

There is no default for this configuration. If this configuration does not exist at the tai-db level and tai-mgmt-object level, no network name will be signaled in a EMM Information message.

tai-custom-list

Creates a new custom TAI list, and/or enters the tai-cstm-list configuration mode.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration

configure > lte-policy > tai-mgmt-db *db_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-db)#
```

Syntax Description

tai-custom-list tac *value* **[-noconfirm]**

tac *value*

Specifies the Tracking Area Code portion of the TAI as an integer from 1 through 65535.

A maximum of 1000 Custom TAI Lists can be configured per TAI Management Database.

Usage Guidelines

Use this command to enter the Custom TAI List Configuration Mode for an existing object or for a newly defined object.

Prior to 17.0, the MME could have a tracking area in only one tracking area list (TAI List). Consequently, the tracking area list assigned to subscribers attaching from different TAIs will be same, even if the adjacency of these tracking areas is not same. This resulted in the MME getting TAUs even as subscribers moved to the adjacent area.

With this functionality, you can configure adjacency lists as TAI Lists, thus reducing the Tracking Area Updates (TAU) received by MME. This feature enables the MME to send configured customized TAI List in ATTACH_ACCEPT/TAU_ACCEPT when a request is received from the custom or border TAIs.

Entering this command results in the following prompt:

```
[local]hostname{tai-cstm-list}#
```

Custom TAI List Configuration Mode commands are defined in the *LTE Custom TAI List Configuration Mode Commands* chapter.

Example

The following command creates a Custom TAI List for TAC 2325 and enters the Custom TAI List Configuration Mode:

```
custom-tai-list tac 2325
```

tai-mgmt-obj

Creates new, or removes/enters existing, LTE Tracking Area Identifier (TAI) object configurations. On the S4-SGSN, this command is required as part of configuring S-GWs and their associated RAIs to bypass DNS resolution of RAI FQDN for obtaining the S-GW address.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration

configure > lte-policy > tai-mgmt-db *db_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-db)#
```

Syntax Description

[no] tai-mgmt-obj *object_name* **[-noconfirm]**

no

Removes a configured TAI management object from the TAI management database.

-noconfirm

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

object_name

Specifies the name of the TAI management object and enters the LTE TAI Management Object Configuration Mode as an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to enter the LTE TAI Management Object Configuration Mode for an existing object or for a newly defined object. This command is also used to remove an existing object.

On the S4-SGSN, after creating the TAI Management Object and entering TAI Management Object Configuration Mode, the **rai** and **sgw-address** commands are used to complete the S-GW for RAI configuration. Refer to the *LTE TAI Management Object Configuration* mode chapter for details on these commands.

The maximum number of TAI-Objects that can be configured per TAI-DB is 4000. The total number of TAI-Objects across all 32 TAI-DBs is limited to 16000.

Entering this command results in the following prompt:

```
[context_name]hostname(tai-mgmt-obj)#
```

LTE TAI Management Object Configuration Mode commands are defined in the *LTE TAI Management Object Configuration Mode Commands* chapter.

Example

The following command creates a TAI management object called *tai-obj3* and enters the LTE TAI Management Object Configuration Mode:

```
tai-mgmt-obj tai-obj3
```

timezone

Configures the timezone to be used for the UE timezone in S11 and Non Access Stratum (NAS) messages.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration

configure > lte-policy > tai-mgmt-db *db_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-db)#
```

Syntax Description

```
timezone { + | - } hours value [ minutes { 0 | 15 | 30 | 45 } |
daylight-savings-time-increment { 0 | 1 | 2 } ]
no timezone
```

no

Removes the timezone configuration from the management database.

+|-

Specifies the offset direction from the Coordinated Universal Time (UTC).

hours *value*

Specifies the offset from UTC in hours. *value* must be an integer from 0 through 14.

minutes { 0 | 15 | 30 | 45 }

Optionally specifies the offset minutes added to the hours value.

daylight-savings-time-increment { 0 | 1 | 2 }

Specifies the number of hours the timezone should be offset due to daylight savings time. This allows the MME to serve areas that have daylight savings time different than that of the MME. This keyword is available in release 14.0 and higher.

If the TAI management database/object is configured for daylight savings using this keyword, the daylight savings time adjustment is applied in these messages only if the system time is within a daylight savings period.

Usage Guidelines

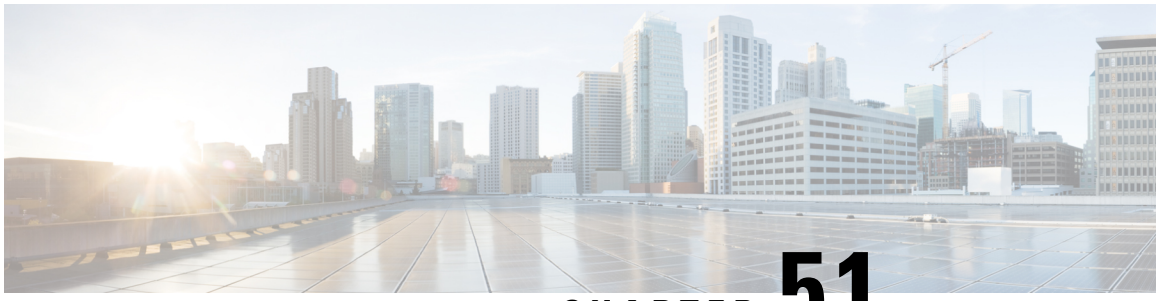
Use this command to configure the timezone to be used for the UE timezone in S11 and NAS messages.

Important Time zone configurations at the TAI Management Object level take precedence over time zone configurations at the TAI Management Database level. If neither is configured, the system defaults to the MME (system) time zone.

Example

The following command sets the timezone mapping for this management database to plus-3 hours and 15 minutes from UTC:

```
timezone + hours 3 minutes 15
```



CHAPTER 51

LTE TAI Management Object Configuration Mode Commands

The LTE TAI Management Object Configuration Mode is used to create and manage the LTE Tracking Area Identifiers for the TAI database.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

access-type

This command is used to configure the NB-IoT RAT per TAI object.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

`[ no ] access-type nb-iot`

no

Removes the configured access type for the TAI object.

nb-iot

Configures the access type as NB-IoT for a TAI object.

Usage Guidelines

The LTE TAI Management Object Configuration Mode is used to create and manage the LTE Tracking Area Identifiers for the TAI database. This mode is used to create, remove or modify the existing LTE Tracking Area Identifier (TAI) object configurations. Use this command to configure the access type of a TAC or group of TACs as NB-IoT RAT. As per 3GPP standards, the same TAC cannot belong to both EUTRAN and NB-IoT RATs. This command is not enabled by default. The default RAT is WB-EUTRAN.

Example

The following command is used to configure the access type as NB-IoT:

`access-type nb-iot`

emergency-services-not-supported

This command disables emergency services at a TAI object management level per TAC basis.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

[no] emergency-services-not-supported

no

For the **emergency-services-not-supported** command, the **no** command prefix enables emergency services at TAI management object level.

Usage Guidelines

In a shared RAN network, there are several TACs contolled by several operators connected to the same MME, and disabling emergency services for a particular TAC becomes a challenge. To over come this, MME provides the **emergency-services-not-supported** command, which disables emergency services at a TAI management object level per TAC basis.

Example

The following command disables emergency services per TAC:

emergency-services-not-supported

ims-voice-over-ps

Configures support for IMS Voice over Packet-Switched information element for this TAI List.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

[no] ims-voice-over-ps

no

Disables support for IMS Voice over PS for this TAI List.

Usage Guidelines

Use this command to enable support for IMS Voice over PS for this TAI List.

When enabled, the IMS Voice Over PS Indicator is sent in the S6a Insert-Subscriber-Data Answer message. This indicates whether the TAI supports 'IMS Voice over PS session'.

If IMS Voice over PS support is configured globally within the Call Control Profile (using the **network-feature-support-ie ims-voice-over-ps** command) as well as on a per TAI basis, the global configuration (from call control profile) is honored.

Example

The following command enables the MME to send the IMS Voice over PS indicator in the S6a Insert-Subscriber-Data Answer message for this TAI list.

```
ims-voice-over-ps
```

lai

Configures a Location Area Identifier (LAI) for this TAI management object.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

```
lai mcc number  mnc number lac area_code
no lai
```

no

Removes a configured LAI from the TAI management object.

mcc *number*

Specifies the mobile country code (MCC) portion of a PLMN identifier as an integer from 100 through 999.

mnc *number*

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

lac *area_code*

Specifies the Location Area Code portion of the TAI as an integer from 1 through 65535.

Usage Guidelines

Use this command to configure an LAI for this management object.

Example

The following command adds an LAI to this management object with an MCC of *111*, an MNC of *22*, and a LAC of *101*:

```
lai mcc 122 mnc 22 lac 101
```

network-name

This command configures the long (full) and short network name used in the Long and Short network name IE in the EMM Information message that is sent to the UE from the MME.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

`[ no ] network-name [ full` *`full_name`* **`| short`** *`short_name`* **`]`**

no

Removes a configured network-name.

full *full_name*

Defines the full (long) network name. *full_name* is an alphanumeric string of 1 through 251 characters.

short *short_name*

Defines the short network name. *short_name* is an alphanumeric string of 1 through 251 characters.

Usage Guidelines

Use this command to configure the full and short network name on the tai-mgmt-obj.

This configuration affects the actions of the MME when the MME is configured to set the UE time. If this configuration exists, and there is no interaction with an MSC that sends an EMM INFORMATION message, the MME uses the above configuration while sending a EMM INFORMATION message.

There is no default for this configuration. If this configuration does not exist at the tai-db level and tai-mgmt-object level, no network name will be signaled in a EMM Information message.

rai

Configures a Routing Area Identifier (RAI) for an associated S-GW for this TAI management object.

Product

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > **lte-policy** > **tai-mgmt-db** *db_name* > **tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

rai mcc *number* **mnc** *number* **lac** *area_code* **rac** *rac_value*
no rai

no

Removes a configured LAI from the TAI management object.

mcc *number*

Specifies the mobile country code (MCC) portion of a PLMN identifier as an integer from 100 through 999.

mnc *number*

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

lac *area_code*

Specifies the Location Area Code portion of the TAI as an integer from 1 through 65535.

rac

Specifies the Routing Area Code portion of the TAI as an integer from 1 to 255.

Usage Guidelines

On the S4-SGSN, use this command as part of the configuration of the selection of an SGW for RAI on the S4-SGSN for operators wishing to bypass the DNS resolution of RAI FQDN for obtaining the SGW address.

Once the RAI is configured, the SGW address that serves this RAI must be configured with the **sgw-address** command. For details on this command, refer to the description of **sgw-address** in this chapter.

Example

The following command adds a RAI to this management object with an MCC of *111*, an MNC of *22*, and a LAC of *110*:

```
rai mcc 111 mnc 22 lac 101 rac 110
```

sgw-address

Configures an IP address for a Serving Gateway (S-GW), a supported S5/S8 protocol type, and selection weight used in a pool for S-GW selection. On an S4-SGSN, this command is used as part of the configuration to bypass DNS resolution of RAI FQDN for an S-GW.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

sgw-address *ipv4_or_ipv6_address* **s5-s8-protocol { both | gtp | pmip } weight** *number* **attach-only | collocated-node** *collocated_node_name* **ue-usage-type** *ue_usage_type_value*
no sgw-address *ipv4_or_ipv6_address* **s5-s8-protocol { both | gtp | pmip } [collocated-node** *collocated_node_name* **]ue-usage-type** *ue_usage_type_value*

no sgw-address *ipv4_or_ipv6_address* s5-s8-protocol { both | gtp | pmip }

Removes the configured S-GW address from this TAI management object.

ipv4_or_ipv6_address

Specifies the IP address of the S-GW in the selection pool in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Up to 32 S-GW addresses can be configured per TAI management object.

s5-s8-protocol { both | gtp | pmip }

Specifies the S5/S8 interface type found between the configured S-GW and the P-GW.

both: Specifies that both the GTP and PMIP protocols are supported over the S5/S8 interface. The **both** option is not supported on the SGSN.

gtp: Specifies that the GTP protocol is supported over the S5/S8 interface. This is the only option supported by the SGSN.

pmip: Specifies that the PMIP protocol is supported over the S5/S8 interface. The **pmip** option is not supported on the SGSN.

weight *number*

Specifies the priority or weight of the S-GW address used during weighted round-robin selection within this TAI management object. *number* must be an integer from 1 through 100.

attach-only

Specifies the SGW preference for SGW-relocation.

collocated-node

Configures the collocation name to select the collocated S/PGW node IP addresses for MME.

collocated_node_name must be a string of size 1 to 255.

ue-usage-type

Configures the ue-usage-type for the gateway. *ue_usage_type_value* must be an integer between 1 through 255.

Usage Guidelines

Use this command to configure a pool of S-GW addresses used for S-GW selection.

On the S4-SGSN, use this command to complete the configuration of bypassing DNS resolution of RAI FQDN to obtain the S-GW address. This command is not valid on the S4-SGSN until the following commands have been executed:

- **tai-mgmt-db** in *LTE Policy Configuration Mode*
- **tai-mgmt-obj** in *LTE Management Database Configuration Mode*
- **rai** in *LTE TAI Management Object Configuration Mode*

Example

The following command configures an S-GW with an IPv4 address of *209.165.200.228*, a supported S5/S8 protocol type of GTP, and a selection weight of *3*:

```
sgw-address 209.165.200.228 s5-s8-protocol gtp weight 3
```

sgw-address-resolution-mode

This command specifies the address resolution mode of the SGW address(s) configured in this object. This command is applicable only for S4-SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

```
sgw-address-resolution-mode { fallback-for-dns | local }
```

default

Resets the configuration to the default value, that is **fallback-for-dns**.

fallback-for-dns

Instructs the system to try DNS resolution. If the DNS query fails, the SGSN will use locally configured addresses. The S4-SGSN will use locally configured SGW address on DNS failure

Default: enabled

local

Instructs the system to only use locally configured S-GW addresses and not to use DNS query.

Default: disabled

Usage Guidelines

Use this command to specify the DNS query or local address resolution for this LTE TAI Management Object. The addresses will be valid only for lac and rac defined under tai-mgmt-object.

Example

The following command sets the address resolution mode to use local addresses *only if* the DNS query fails:

```
sgw-address-resolution-mode fallback-for-dns
```

tai

Configures a Tracking Area Identifier (TAI) for this TAI management object.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

`[ no ] tai mcc` *`number`* **`mnc`** *`number`* **`{ tac`** *`value`* **`} +`**

no

Removes a configured TAI from the TAI management object.

mcc *number*

Specifies the mobile country code (MCC) portion of a PLMN identifier as an integer from 100 through 999.

mnc *number*

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

tac *value* +

Specifies the Tracking Area Code portion of the TAI as an integer from 1 through 65535. Up to 16 TAC values can be entered on a single line.

Usage Guidelines Use this command to configure one or more TAIs for this management object. Up to 16 TAIs can be configured per management object.

Example

The following command adds a TAI to this management object with an MCC of *111*, an MNC of *22*, and a TAC value of *1001*:

```
tai mcc 122 mnc 22 tac 1001
```

timezone

Configures the timezone to be used for the UE timezone in S11 and Non-Access Stratum (NAS) messages.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > **lte-policy** > **tai-mgmt-db** *db_name* > **tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

```
timezone { + | - } hours value [ minutes { 0 | 15 | 30 | 45 } |
daylight-savings-time-increment { 0 | 1 | 2 } ]
no timezone
```

Removes the timezone configuration from the management object.

+ | -

Specifies the offset direction from Coordinated Universal Time (UTC).

hours *value*

Specifies the offset from UTC in hours as an integer from 0 through 14.

minutes { 0 | 15 | 30 | 45 }

Optionally specifies the offset minutes added to the hours value.

daylight-savings-time-increment { 0 | 1 | 2 }

Specifies the number of hours the timezone should be offset due to daylight savings time. This allows the MME to serve areas that have daylight savings time different than that of the MME. This keyword is available in release 14.0 and higher.

If the TAI management database/object is configured for daylight savings using this keyword, the daylight savings time adjustment is applied in these messages only if the system time is within a daylight savings period.

Usage Guidelines

Use this command to configure the timezone to be used for the UE timezone in S11 and NAS messages.

Important Time zone configurations at the TAI Management Object level take precedence over time zone configurations at the TAI Management Database level. If neither is configured, the system defaults to the MME (system) time zone.

Example

The following command sets the timezone mapping for this management object to plus-3 hours and 15 minutes from UTC:

```
timezone + hours 3 minutes 15
```

up-address

Displays the addresses of User Plane Nodes Serving all TAI's in this Object.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

`[ no ] up-address { IP-ADDRESS | IP-ADDRESS/MASK } mef-address`*`ip_address`*

no

Removes the addresses of User Plane Nodes Serving all TAI's in this Object.

up-address { IP-ADDRESS | IP-ADDRESS/MASK }

Specifies the addresses of User Plane Nodes Serving all TAI's in this Object.

{ IP-ADDRESS | IP-ADDRESS/MASK } must be an IPV4 in ##.##.##.## notation or IPV6 in ####:####:####:####:####:####:####:#### notation. IPV6 also supports :: notation.

must be an IPV4 in ##.##.##.##/x notation or IPV6 in ####:####:####:####:####:####:####:####/x notation. IPV6 also supports :: notation.

mef-address*ip_address*: Configures the peer MEF server address for MEF signalling. *ip_address* must be any IPV4 address of notation ##.##.##.## or IPV6 address of notation ####:####:####:####:####:####:####:#### . IPV6 also supports :: notation.

Example

The following command displays the addresses of User Plane Nodes Serving all TAI's in this Object :

up-address *209.165.201.4*

zone-code

Configures a zone code for the management object.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax Description

In releases prior to 21.1:

zone-code *zc_id*
no zone-code

In 21.1 and later releases:

[no] zone-code *zonecode_value* **[***zonecode_value2***[...[** *zonecode_value10* **]]]**

no

Removes the configured zone-code from the management object. The operator needs to enter the zone code value(s) to be removed from the configuration (See Example).

zc_id

Identifies the zone code configuration instance as an integer from 1 through 65535.

zonecode_value

Identifies te zone code configuration instance as an integer from 1 through 65535. Under a TAI-Object, up to 10 zone code values can be configured.

Usage Guidelines

Important While there is no limit to the number of zone codes that can be created, only 10 LACs per zone code can be defined.

Use this command to define zone code restrictions. Regional subscription data at the home subscriber service (HSS) is used to determine the regional subscription area in which the subscriber is allowed to roam. The regional subscription data consists of a list of zone codes which are comprised of one or more location areas (identified by a LAC) into which the subscriber is allowed to roam. Regional subscription data, if present in the Insert-Subscriber-Data-Request (IDR) and the Update-Location-Answer (ULA) from the HSS, defines the subscriber's subscription area for the addressed MME. It contains the complete list (up to 10 zone codes) that apply to a subscriber in the currently visited PLMN. During the Location Update procedure, the zone code list is received in the ULA from the HSS. The zone code list is validated against the configured values in this command. If matched, the Location Update procedure is allowed to proceed. If not matched, the response is that the Network Node Area is restricted and the Location Update procedure fails.

In release 21.1, this command is modified to configure up to 10 zone code values under the same TAI-Object. It allows specific zone codes to be managed based on call-control-profile / HSS (per roaming partner). Also, it supports overlapping of zones by allowing multiple zone code values to which a TAI-Object belongs. For more information, refer to *Access Restriction based on Regional Zone Code* chapter in the *MME Administration Guide*.

Example

The following command sets the zone code for this management object to *1*:

```
zone-code 1
```

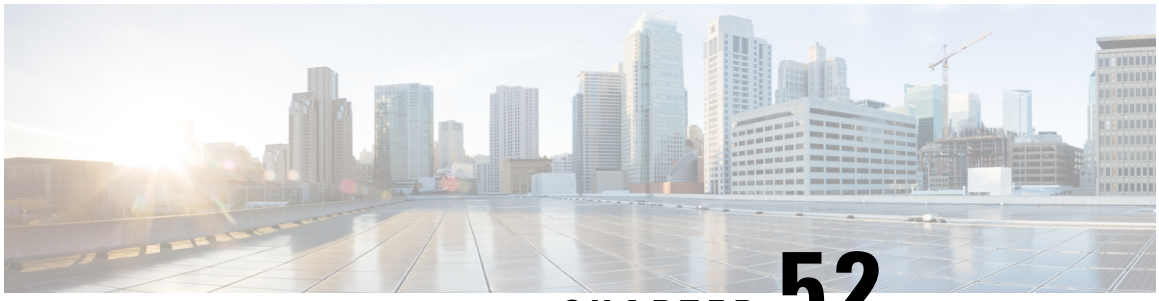
The following CLI shows the configuration of 5 zone code values:

```
zone-code 11 12 13 14 15
```

The following CLI shows the configuration to remove 3 zone code values from the above configuration:

```
no zone-code 11 12 13
```

In the above configuration example, zone code value **11 12 13** are removed from the configuration, and the zone code values **14** and **15** still remain configured under the TAI-Object.



CHAPTER 52

MAG Service Configuration Mode Commands

The MAG Service Configuration Mode is used to create and manage a Mobility Access Gateway service in an HSGW (eHRPD network) or a P-MIP S-GW (LTE-SAE network). The MAG is the PMIP client and communicates with the Local Mobility Anchor (LMA) configured on a PDN Gateway (P-GW).

Command Modes

Exec > Global Configuration > Context Configuration > MAG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

bind

Binds the service to a logical IP interface serving as the S2a (HSGW, SaMOG) or S5/S8 (S-GW) interface and specifies the maximum number of subscribers that can access this service over the configured interface.

Product

HSGW

S-GW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

bind { address *ipv6_address* **| ipv4-address** *ipv4_address* **} [max-subscribers** *num* **]**
no bind address

no

Removes the interface binding from this service.

address *ipv6_address*

Specifies the IPv6 address of the interface configured as the S5/S8 interface.

ipv6_address is specified in IPv6 colon-separated-hexadecimal notation.

ipv4-address *ipv4_address*

Specifies the IPv4 address of the interface configured as the S2a or S5/S8 interface.

Important The SaMOG PMIPv6-based S2a interface currently supports IPv4 bind address only.

ipv4_address is specified in IPv4 colon-separated-hexadecimal notation.

max-subscribers *num*

Default: 1500000

Specifies the maximum number of subscribers that can access this service on this interface.

num must be an integer from 0 through 3000000.

Important The maximum number of subscribers supported depends on the installed license key and the number of active packet processing cards in the system. A fully loaded system can support 3,000,000 total subscribers. Refer to the **license key** command and the *Usage* section (below) for additional information.

Usage Guidelines Associate the MAG service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an S2a or S5/S8 interface that provides the session connectivity to/from a P-GW. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

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

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

- The total number of S2a or S5/S8 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port to which these interfaces will be bound

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

Example

The following command would bind the logical IP interface with the address of *4551:0db8:85a3:08d3:3319:8a2e:0370:1344* to the MAG service and specifies that a maximum of *300,000* simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 4551:0db8:85a3:08d3:3319:8a2e:0370:1344 max-subscribers
300000
```

encapsulation

Configures data encapsulation type to be used for specific MAG service.

Product HSGW

S-GW

SaMOG

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
encapsulation { gre | ipip }
default encapsulation
```

default

Resets the encapsulation type to be used by this service to the default option of GRE.

gre

gre: Specifies that GRE encapsulation is to be used for PMIPv6 tunnel data between the MAG and the Local Mobility Anchor (LMA). This is the default for this command.

Important The SaMOG PMIPv6-based S2a interface currently supports GRE encapsulation only.

ipip

ipip: Specifies that IP-in-IP encapsulation is to be used for PMIPv6 tunnel data between the MAG and the LMA.

Usage Guidelines

Use this command to select the encapsulation type to be used for PMIPv6 tunnel data between the MAG and the LMA.

Example

The following command sets the encapsulation data to IP-in-IP:

```
encapsulation ipip
```

heartbeat

Configures the PMIPv6 heartbeat message interval, retransmission timeout, and max retransmission for the MAG Service.

Product

HSGW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
heartbeat { interval seconds | retransmission { max number | timeout seconds
 } }
default heartbeat { interval | retransmission { max | timeout } }
no heartbeat
```

no

Disables the PMIPv6 heartbeat functionality. The HSGW starts sending heartbeat request to peers when the heartbeat interval is configured.

default

Resets the specified parameter to the system default value.

interval *seconds*

The interval in seconds at which heartbeat messages are sent.

seconds is an integer from 30 through 3600.

Default: 60

retransmission max *number*

The maximum number of heartbeat retransmissions allowed.

number is an integer from 1 through 15.

Default: 3

retransmission timeout *seconds*

The timeout in seconds for heartbeat retransmissions.

seconds is an integer from 1 through 20.

Default: 3

Usage Guidelines

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol to provide mobility without requiring the participation of the mobile node in any PMIPv6 mobility related signaling. The Mobile Access Gateway (MAG) service sets up tunnels dynamically to manage mobility for a mobile node.

This command provides configuration of heartbeat messages between the MAG and LMA services to know the reachability of the peers, to detect failures, quickly inform peers in the event of a recovery from node failures, and allow a peer to take appropriate action.

Example

The following command enables PMIPv6 heartbeat messaging to known MAG service peers and sets the heartbeat interval to 160 seconds.

```
heartbeat interval 160
```

information-element-set

Identifies the information element set of mobility options to be used in Proxy Binding Update (PBU) messages sent by the MAG to the LMA.

Product

HSGW

S-GW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
information-element-set { custom1 | custom2 [ disable-ie hardware-ie ] |
 custom3 | standard }
default information-element-set
```

default

Resets the command to the default value of "standard".

{ custom1 | custom2 [disable-ie hardware-ie] | custom3 | standard }

custom1: Specifies that a custom set of mobility options will be used in proxy binding update messages that are sent in Vendor Specific Mobility Options. These options are:

- User Location Info
- Hardware Identifier
- Access Network Charging Identifier

custom2 [disable-ie hardware-ie]: Specifies that a custom set of mobility options will be used in proxy binding update messages that are sent in Vendor Specific Mobility Options. When enabled, BSID will be sent in S2a PMIPv6 message.

If the **disable-ie hardware-ie** keyword is included with this command, then the information elements in PBU and the hardware ID in PBU are disabled. When information element custom2 is enabled, all the supported mobility options are enabled including hardware ID for a specific customer. The **disable-ie**keyword only disables the hardware ID mobility option in PBU. The **hardware-id** mobility option format is supported like **custom1**.

custom3: Specifies that a custom set of mobility options will be used in proxy binding update messages that are sent in Vendor Specific Mobility Options.

standard: Specifies that a standard set of mobility options are to be used in proxy binding update messages. 3GPP specification 29.275 defines these as Protocol Configuration Options.

Important The information element set of mobility options for SaMOG PMIPv6-based S2a interface must be set to **standard**. Any other configuration may result in a call setup failure.

Usage Guidelines Use this command to identify the type of information element set of mobility options to be used in PBU messages sent form the MAG to the LMA. The mobility options can be either standards-based (3GPP 29.275) or custom (vendor-specific as defined by 3GPP 29.275).

Example

The following command identifies the information element set of mobility options to use in PBU messages as custom:

```
information-element-set custom1
```

max-retransmissions

Configures maximum number of retransmissions of Proxy MIP control messages to the Local Mobility Anchor (LMA).

Product HSGW

S-GW

SaMOG

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
max-retransmissions num
default max-retransmissions
```

default

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

num

Default: 5

Specifies the maximum number of times the MAG service will attempt to communicate with the LMA before it marks it as unreachable.

count must be an integer from 0 through 4294967295.

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

Example

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

```
max-retransmissions 3
```

mobility-header-checksum

Switches between RFC3775 and RFC6275 for the "next header" value in the mobility header.

Product HSGW

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
mobility-option-type-value { rfc3775 | rfc6275 }
default mobility-option-type-value
```

default

Sets the command to the default value of rfc3775.

rfc3775

Configures the "next header" value to 2, as defined in RFC3775.

rfc6275

Configures the "next header" value to 135, as defined in RFC6275.

Usage Guidelines Use this command to switch between RFC3775 and RFC6275 for the "next header" value in the mobility header. This value is used for appending and calculating the checksum for outbound mobility messages from MAG to LMA. For inbound messages from LMA to MAG, either of the two values are acceptable for verifying the checksum.

Example

The following command configures the "next header" value to 2, as defined in RFC3775:

```
mobility-option-type-value rfc3775
```

mobility-option-type-value

Changes the mobility option type value used in mobility messages.

Product

HSGW

S-GW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

mobility-option-type-value { custom1 | standard }
default mobility-option-type-value

default

Sets the command to the default value of custom1.

custom1

(Default) Non-standard type values used before they were defined by IANA.

standard

Standard type values as defined by IANA. In addition, standard option uses type values defined in RFC 5844 for home address (HoA) options for the PMIPv6 PBU/PBA/revocation message.

Usage Guidelines

Use this command to change the mobility option type value used in mobility messages.

Example

The following command changes the mobility option type value to standard:

mobility-option-type-value standard

policy

Configures policies applied to MAG service.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
policy include-bsid-binding-update { all | none { dereg
 | handoff | init |  renew } }
 [ default ] policy include-bsid-binding-update
```

default

Restores the command to the default values of **init** and **handoff**.

include-bsid-binding-update { all | none { dereg | handoff | init | renew } }

Configures the MAG Service to include BSID (Base Station Identification) in the PBU (Proxy Binding Update) sent by MAG to the P-GW. By default, BSID information is included in the update (**handoff**) and initialization (**init**) packets.

all: Include BSID in all the types of PBU that are sent.

none: Include BSID in none of the PBUs.

dereg: Include BSID in the PBU sent during deregistration.

handoff: Include BSID in the PBU sent during a handoff.

init: Include BSID in the PBU sent during initialization.

renew: Include BSID in the PBU sent during 'registration lifetime' renewal.

Usage Guidelines

Configures policies applied to MAG service.

Example

The following command configures the MAG Service to include BSID in the PBU during initalization, 'registration renewal', and deregistration.

```
policy include-bsid-binding-update init renew dereg
```

reg-lifetime

Configures the Mobile IPv6 session registration lifetime for this service.

Product

HSGW

S-GW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

reg-lifetime *seconds*
default reg-lifetime

default

Resets the command value to the default setting of 600.

seconds

Default: 600

Sets the time value (in seconds) for session lifetimes for this service.

seconds must be an integer from1 through 262140.

Usage Guidelines

Use this command to limit PMIPv6 lifetime on this service. If the Proxy Binding Acknowledge (PBA) from the LMA contains a lifetime shorter or longer than what is specified, it is used instead.

Example

The following command sets the registration lifetime for Mobile IPv6 sessions using this service to *1200* seconds (20 minutes):

reg-lifetime 1200

renew-percent-time

Configures percentage of lifetime at which a registration renewal is sent to the Local Mobility Anchor (LMA).

Product

HSGW

S-GW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

renew-percent-time *percent*
default renew-percent-time

default

Resets the command to the default value of 75.

percent

Default: 75

Specifies the time percentage when the registration renewal is sent to the LMA. *percent* is a percentage value of the registration lifetime expressed as an integer from 1 through 100.

Usage Guidelines

Use this command to specify when a registration renewal is sent to the LMA for subscribers using this service.

If the registration lifetime is 600 seconds (10 minutes) and this command is set to 75 (percent), then the registration renewal message is sent after 450 seconds of the registration lifetime has expired.

Example

The following command sets the registration renewal time for subscribers using this service to *90* percent of the registration lifetime:

```
renew-percent-time 90
```

retransmission-policy

Configures the retransmission policy for Proxy MIP control message retransmissions.

Product

HSGW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
retransmission-policy { exponential-backoff | normal }
default retransmission-policy
```

default

Returns the command to its default setting of exponential-backoff.

{ exponential-backoff | normal }

Sets the retransmission timeout behavior for this service.

exponential-backoff: Specifies that the Proxy Binding Update (PBU) retransmission uses an exponential backoff to increase the retransmission timeout for each retry.

normal: Specifies that the PBU retransmission uses the configured retransmission timeout value for all PBU retransmission retries.

Usage Guidelines

Use this command to specify the retransmission policy for PMIP control messages.

Example

The following command sets the retransmission timeout policy for PMIP control packets to "normal":

```
retransmission-policy normal
```

retransmission-timeout

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

Product

HSGW

S-GW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

retransmission-timeout *time*
{ default | no } retransmission-timeout

default

Resets the timeout setting to the default value of 3,000 milliseconds.

no

Deletes a previously configured timeout value.

time

Default: 3000

Specifies the maximum allowable time (in milliseconds) for the MAG service to wait for a response from the LMA before it: (a) attempts to communicate with the LMA again (if the system is configured to retry the LMA) or (b) marks the LMA as unreachable.

time must be an integer from 100 through 100000.

Usage Guidelines Use the retransmission timeout command in conjunction with the **max-retransmissions** command in order to configure the MAG services behavior when it does not receive a response from a particular LMA.

Example

The following command configures a retransmission timeout value of 5000 milliseconds:

```
retransmission-timeout 5000
```

signalling-packets

Enables the QoS Differentiated Services Code Point (DSCP) marking feature for IP headers carrying outgoing signalling packets.

Product HSGW

S-GW

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

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

no

Disables the specified functionality.

ip-header-dscp *value*

Used to configure the QoS Differentiated Services Code Point (DSCP) marking for IP header encapsulation.

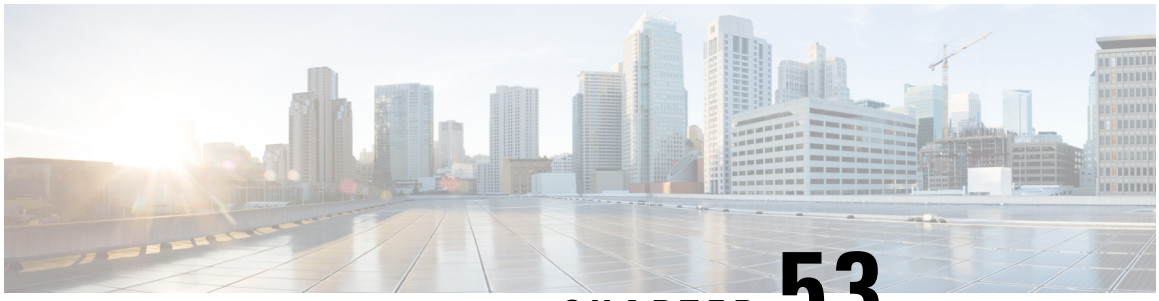
value: Represents the DSCP setting as the first six most-significant bits of the ToS field. It can be configured to any hexadecimal value from 0x0 through 0x3F. Default is 0x0.

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

Example

The following command configures the HSGW service to support DSCP marking for IP headers carrying outgoing signalling packets:

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



CHAPTER 53

MEC TAI Group Configuration Mode Commands

The MEC TAI Group Configuration Mode is used to create and manage the MEC Tracking Area Identity supporting MME configurations on the system.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > MEC TAI Group Configuration

configure > lte-policy > mec-tai-grp group_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(mec-tai-grp)#
```

Important Available commands or keywords/variables vary based on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

tai

Configures the Tracking Area Identity for MEC TAI Group .

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > mec-tai-grp *grp_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(mec-tai-grp)#
```

Syntax Description

[no] tai mcc *mcc_value* **mnc** *mnc_value* **{ tac** *value1... value20* **| tac-range from** *tac_value_from* **to** *tac_value_to* **}**

no

Removes the configuration of tai.

tai

Specifies the Tracking Area Identity.

mcc ***mcc_value***

Specifies the Mobile Country Code.*mcc_value* must be a three digit integer between 0 to 999.

mnc ***mnc_value***

Specifies the Mobile National Code.*mnc_value* must be a two / three digit integer between 00 to 999.

tac ***value1... value20***

Specifies the Tracking Area Code. Upto 20 Tracking Area Codes can be entered on one line. It can be configured by entering TAC directly or using range. *value1... value20* must be an integer between 0 to 65535.

tac-range from ***tac_value_from*** **to** ***tac_value_to***

Specifies the Range of Tracking Area Code. Maximum of 5 ranges in a MEC TAI group can be configured. *tac_value_from* and *tac_value_to* must be an integer between 0 to 65535.

Usage Guidelines

Use this command to configure the Tracking Area Identity for MEC TAI Group.

Example

The following command configures tai with mcc *50*, mnc *45* with tac range from *10* to *20*:

```
tai mcc 50 mnc 45 tac-range from 10 to 20
```

up-address

Configures the up-address of User Plane Nodes Serving all TAIs in this object .

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > mec-tai-grp *grp_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(mec-tai-grp)#
```

Syntax Description

`[ no ] up-address ( IP-ADDRESS | IP-ADDRESS/MASK } mef-address` *`iPV4/iPV6_address`*

no

Removes the addresses of User Plane Nodes Serving all TAIs in this object.

up-address (IP-ADDRESS | IP-ADDRESS/MASK }

Specifies the Tracking Area Identity.Configures the addresses of User Plane Nodes Serving all TAIs in this Object. **IP-ADDRESS** must be an IPV4 ##.##.##.## or IPV6 ####:####:####:####:####:####:####:####. Also supports :: notation **IP-ADDRESS/MASK** must be an IPV4 ##.##.##.##/x or IPV6 ####:####:####:####:####:####:####:####/x.

mef-address *iPV4/iPV6_address*

Configures the peer MEF server address for MEF signalling.*iPV4/iPV6_address* must be IPV4 ##.##.##.## or IPV6 ####:####:####:####:####:####:####:#### (IPV6 also supports :: notation).

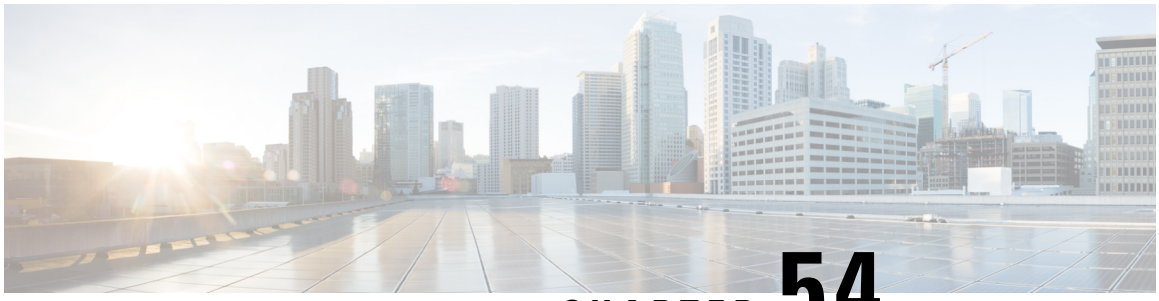
Usage Guidelines

Use this command to configure the up-address of User Plane Nodes Serving all TAIs in this object.

Example

The following command configures the up-address of User Plane Nodes Serving all TAIs in this object with Ipv4 address *209.165.200.235* and mef-address *209.165.200.254* :

`up-address 209.165.200.235 mef-address  209.165.200.254`



CHAPTER 54

MAP Service Configuration Mode Commands

Mobile Application Part (MAP) is a protocol which provides an application layer for the various nodes in the core mobile network and GPRS and UMTS core network to communicate with each other in order to provide services to mobile phone users. The MAP service provides the application-layer protocol support used to access the Home Location Register (HLR).

Command Modes

The MAP Service Configuration Mode is used to configure properties for Mobile Application Part (MAP) service.

Exec > Global Configuration > Context Configuration > MAP Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

access-protocol

Configures access protocol parameters for the MAP service as defined for a specific SCCP network instance.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAP Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-map-service-service_name)#`

Syntax Description

`[ no ] access-protocol { sccp-network` *`sccp_id`* **`[ ssn`** *`subsys_num`* **`] }`**

sccp-network *sccp_id*

Specifies the ID number of the SCCP network to use for the SGSN connection.

sccp_id : Must be an integer from 1 to 16.

ssn *subsys_num*

Identifies the subsystem number for the destination.

subsys_num: Enter an integer from 1 through 255.

no

Removes the access protocol SCCP network instance ID from the configuration.

Usage Guidelines

Use this command to associate access protocol parameters to a specific instance of the MAP service for an SCCP network.

Example

The following command associates the access protocols with the SCCP network ID #10:

`access-protocol sccp-network` *`10`*

application-context-name

Configure the operation timer(s) for one or more MAP application contexts.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAP Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-map-service-service_name)#`

Syntax Description

application-context-name *application* **operation-timer** *value*
default application-context-name *application* **operation-timer**

default

Resets the operation timers for all applications to system defaults.

application

Select one of the following applications to enable the application:

- **authentication-failure-report** : Sets the reporting operation timer for authentication failure. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **cancel-location** : Sets the cancel location operation timer. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **check-imei** : Sets the check-IMEI operation timer. The setting range for this timer is 15 to 30 seconds for releases 8.0 and 8.1 and 1 to 30 seconds for releases 9.0 and higher. The default setting is 15 seconds.
- **delete-subscriber-data** : Sets the delete subscriber data operation timer. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **mo-fwd-sm** : Sets the operation timer for forwarding mobile-originated SMS. The setting range for this timer is 1 to 10 minutes and the default setting is 1 minute (60 seconds).
- **ms-purge** : Sets the operation timer for MS-purge function. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **mt-fwd-sm** : Sets the operation timer for forwarding mobile-terminated SMS. The setting range for this timer is 1 to 10 minutes and the default setting is 1 minute (60 seconds).
- **ready-for-sm** : Sets the operation timer for the ready for SMS operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **send-authentication-info** : Sets the operation timer for the sending authentication information operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **stand-alone-insert-subscriber-data** : Sets the operation timer for the standalone insert subscriber data operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **ugl-insert-subscriber-data** : Sets the operation timer for the insert subscriber data portion of the update GPRS location operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **update-gprs-location** : Sets the operation timer for the update GPRS location operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.

operation-timer*value*

Configures the operation timer for the selected application. Timer values are indicated above.

Usage Guidelines Repeat this command entering a different application each time to enable multiple applications.

Example

```
application-context-name stand-alone-insert-subscriber-data operation-timer
 20
```

auth-vectors

Configures the number of authorization vectors to be requested from the home location register (HLR) during call setup to provide subscriber authentication.

Product SGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name)#
```

Syntax Description

```
auth-vectors number-to-request number
default auth-vectors number-to-request
```

default

Resets the number of vectors requested from the HLR to the system default.

number-to-request *number*

number: Must be an integer from 1 to 5 to define the number of authorization vectors be requested from the HLR.

Default is 5.

Usage Guidelines Set the number of requests to be received from the HLR.

Example

```
auth-vectors number-to-request 4
```

equipment-identity-register

Defines the information relevant to the equipment-identity-register (EIR) used by the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAP Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-map-service-service_name)#`

Syntax Description

equipment-identity-register { isdn *E.164_num* **| point code** *pt_code* **} [check-imei-every-n-events** *times***| check-imei-sub-every-n-events** *times***| source-ssn** *ssn***] [include-imsi | map-include-imsi]**
no equipment-identity-register { isdn *E.164_num* **| point code***pt_code* **}] [include-imsi | map-include-imsi]**

no

Deletes the EIR configuration.

isdn *number*

Enter the E.164 number of the EIR.

number: must be a string of 1 to 15 digits.

point code *pt_code*

Enter SS7 point code address of the EIR in dotted-decimal format according to variant settings:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- or a string of 1 to 11 characters

source-ssn *ssn*

Identifies the subsystem number (SSN) to be used.

ssn must be an integer from 1 to 255.

check-imei-every-n-events *times*

Configures the frequency with which a 'check IMEI' message is sent to the EIR. When set, the SGSN skips sending the 'check IMEI' message for the first N-1 where IMDI/IMEISV is received.

times :

- For releases 8.0 and 8.1, the value must be an integer from 1 to 15.
- For releases 15.0 and higher, the value must be an integer from 1 to 15.

Important This feature requires the enabling of **verify-equipment-identity** for IMEI or IMEISV as specified with the the **gmm retrieve-equipment-identity imei** command of the call-control-profile configuration mode.

check-imei-sub-every-n-events *times*

check-imei-sub-every-n-events times: Performs IMEI check every N events for each subscriber . times must be an integer ranging from 1 to 15.

include-imsi

Enables inclusion of IMSI checking during the IMEI check procedure. By default this function is not included.

map-include-imsi

Enables the inclusion of IMSI parameter in the CHECK_IMEI Request. By default, IMSI is not included in the CHECK_IMEI Request.

Usage Guidelines

Configure the identity of the EIR that the SGSN uses and the interaction parameters.

Increasing the **check-imei-every-n-events** frequency enables the EIR to avoid overload as the number of data-only devices attaching to the network increases.

Example

Configure EIR with point code 1.255.1 to perform IMEI check after every 61st received Attach Request message:

```
equipment-identity-register point code 1.255.1 check-imei-every-n-events
62
```

Configure IMSI to be included in the MAP-CHECK-IMEI operation:

```
equipment-identity-register point code 1.255.1 check-imei-every-n-events
62  include-imsi
```

gmlc

This command identifies the gateway mobile location center (GMLC) associated with the Location Service functionality.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAP Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name)#
```

Syntax Description

```
gmlc { isdn E.164_number | point-code point-code } [ gsn-address ipv4 address ]
 [ source-ssn SSN_value ]
no gmlc { isdn | point-code }
```

no

Deletes the GMLC configuration. When the **no** form of the command is used the SGSN aborts all active Location Requests towards that GMLC and stops the Location Service functions.

isdn *number*

Enter the E.164 number of the GMLC.

number: must be a string of 1 to 15 digits.

Important **isdn** can not be used if **point-code** is used.

point-code *pt_code*

Enter SS7 point code address of the GMLC in dotted-decimal format according to variant settings:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- or a string of 1 to 11 characters

Important **point-code** can not be used if **isdn** is used.

gsn-address *ipv4 address*

Identifies the IP address of the GMLC of the local PLMN. The address will be published to the HLR in the MAP Update_GPRS_Location Request.

ipv4 address must be a standard dotted-decimal notation.

Important Even though **gsn-address** is optional per the CLI grammar, this keyword is a mandatory parameter when configuring the GMLC for the location service feature in the SGSN.

source-ssn *ssn*

Identifies the subsystem number (SSN) to be used.

ssn must be an integer from 1 to 255.

Usage Guidelines

This command identifies the GMLC associated with the MAP Service configuration in support of the Location Services functionality enabled on the SGSN.

Only one GMLC can be defined per MAP Service configuration.

Related Commands:

- **associate map-service** in the Location Service configuration mode associates this MAP service when configuration Location Services functionality.

Example

Use a command similar to the following to define a gateway mobility location center (GMLC) with an ISDN ID of *491720499*, a GSN address of *209.165.201.1*, and an SSN of *131*:

```
gmlc isdn 491720499 gsn-address 209.165.201.1 ssn 131
```

hlr

This command enters the configuration mode for the home location register (HLR). The HLR is a database containing the subscriber profile information for all mobile stations (MS) / user equipment (UE) connecting to a specific GPRS or UMTS core network.

Important The commands and options for this mode are documented in the HLR Configuration Mode chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MAP Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name)#
```

Syntax Description

hlr

policy

This command configures the Transaction Capabilities Application Part (TCAP) -specific MAP policy for either ANSI or ITU SS7 variants.

Product SGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-map-service-service_name)#`

Syntax Description **`[ default ] policy tcap { use-received-destination-address | use-received-source-address }`**

use-received-destination-address

Selecting this keyword overwrites stored CG and CD addresses with a new address received in first TC CNT msg

use-received-source-address

Selecting this keyword instructs the MAP service to use the received source address for the dialog.

Usage Guidelines Use this command to determine how TCAP will handle MAP messages.

Example

`policy tcap use-received-destination-address`

short-message-service

This command enables and disables the short message service (SMS service) and provides access to the SMS Service configuration mode.

Product SGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-map-service-service_name)#`

Syntax Description **`short-message-service`**
`no short-message-service`

no

Disables the SMS service.

Usage Guidelines Enter the command to access the SMS service configuration mode to fine tune the SMS functionality.

Example

```
short-message-service
```

timeout

Use this command to configure the m1 timeout value for the LCS procedure..

Product SGSN

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name)#
```

Syntax Description **timeout m1** *seconds*

m1 *seconds*

This keyword sets the expiry value for the SGSN's m1 timer, which sets the time the SGSN waits to send a negative PSL Response and clear the location request.

seconds is an integer from 60 to 600. Default is 120.

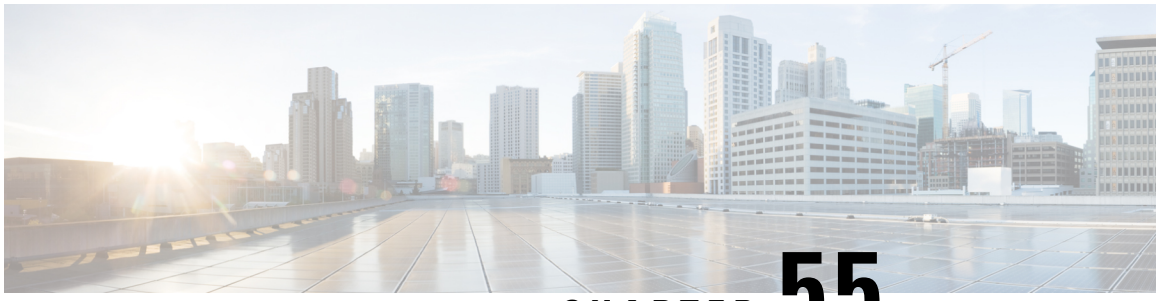
Usage Guidelines The m1 timer is used for location service (LCS) specific map message PSL (provide subscriber location). The gateway mobile location center (GMLC), associated with the LCS functionality, also maintains an m1 timer when it sends a PSL Request to the SGSN. If the GMLC's timer expires before receiving a response from the SGSN, then the GMLC aborts the location procedure.

This command enables the operator to determine the amount of time the SGSN should wait before sending a negative PSL Response and cleaing the location request to complete the LCS procedure.

Example

Set the expiry value of the m1 timer to *240* seconds.

```
timeout m1 240
```



CHAPTER 55

MIP HA Assignment Table Configuration Mode Commands

Command Modes

The Mobile IP HA Assignment Table Configuration Mode is used to assign specific Home Agent (HA) IP addresses to ranges of Mobile Node (MN) IP addresses.

Exec > Global Configuration > Context Configuration > MIP HA Assignment Table

configure > context *context_name* **> mobile-ip ha assignment-table** *table_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mobile-ip-ha-assignment)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

hoa-range

This command assigns ranges of Mobile Node (MN) IP addresses to specific Home agent IP addresses.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MIP HA Assignment Table

configure > context *context_name* **> mobile-ip ha assignment-table** *table_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mobile-ip-ha-assignment)#`

Syntax Description

[no] hoa-range *ip_addressip_address2* **ha** *ip_address3*

no

Removes the specified Home Agent assignment from the assignment table.

ip_address ip_address2

Specifies a range of MN IP addresses. *ip_address* and *ip_address2* must be specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

ha *ip_address3*

Specifies the IP address of the Home Agent to assign to MNs that are within the specified range. *ip_address3* must be specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage Guidelines

Use this command to assign ranges of MN IP addresses to specific HAs.

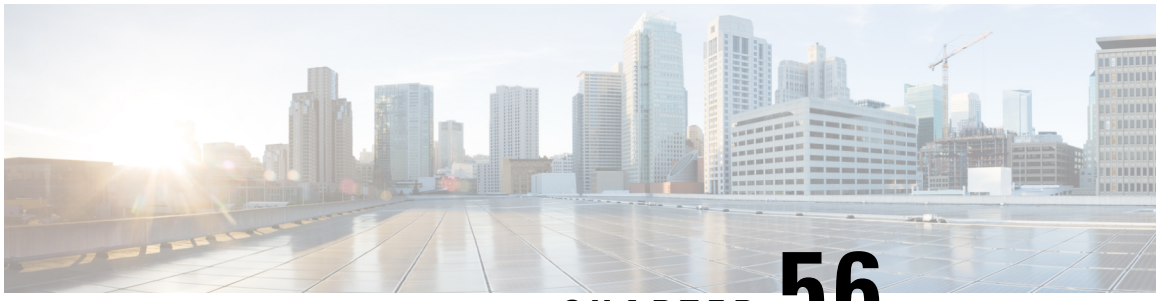
Important A maximum of eight MIP HA assignment tables can be configured per context with a maximum of eight MIP HA assignment tables across all contexts.

Important A maximum of 256 non-overlapping hoa-ranges can be configured per MIP HA Assignment table with a maximum of 256 non-overlapping hoa-ranges across all MIP HA Assignment tables.

Example

The following command assigns any MN IP address that falls in the range of *209.165.200.224* through *209.165.201.0* to the HA with the IP address of *209.165.200.234*:

```
hoa-range 209.165.200.224 209.165.201.0 ha 209.165.200.234
```



CHAPTER 56

MPLS-LDP Configuration Mode Commands

Command Modes

The MPLS-LDP Configuration Mode is used to configure Label Distribution Protocol (LDP) specific parameters for MPLS-IP forwarding.

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration

configure > context *context_name* **> mpls-ip > protocol ldp**

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

advertise-labels

Configures the Label Advertisement parameters.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration

configure > context *context_name* **> mpls-ip > protocol ldp**

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] advertise-labels { explicit-null | implicit-null }`
`default advertise-labels`

no

Disables the label advertisement parameters.

default

Advertises the labels from the label space allocated for LDP protocol.

explicit-null

Advertises the Explicit NULL label for all the prefixes.

implicit-null

Advertises the Implicit NULL label for all the prefixes.

Usage Guidelines

Use this to configure advertisement of the Implicit NULL or Explicit NULL label for all the prefixes advertised by the system in this context.

Example

The following command configures the MPLS-IP forwarding to advertise the Explicit NULL label for all the prefixes:

`advertise-labels explicit-null`

The following command configures the MPLS-IP forwarding to advertise the Implicit NULL label for all the prefixes:

`advertise-labels implicit-null`

discovery

Configures the Label Distribution Protocol (LDP) neighbor discovery parameters.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration

configure > context *context_name* **> mpls-ip > protocol ldp**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
discovery { hello { hello-interval integer_value | hold-interval integer_value
 } | transport-address ipv4_addr }
default discovery hello
no discovery transport-address
```

default

Sets the LDP discovery hello interval at 5 seconds and hold interval at 15 seconds.

no

Disables the LDP neighbor discovery.

hello { hello-interval *integer_value* | hold-interval *integer_value* }

Configures the LDP Hello parameters.

hello-interval configures the frequency of sending the Discovery Hello packets in seconds.

integer_value is an integer from 5 through 21845.

Default: 5

hold-interval configures the Discovery Hold time interval in seconds.

integer_value is an integer from 15 through 65535.

Default: 15

transport-address *ipv4_addr*

Configures the LDP transport address as an IPv4 address entered in dotted-decimal notation. Transport address is the same as the LDP router ID.

Usage Guidelines

This is an optional command that is used to configure LDP peer discovery parameters. The LDP discovery hold-interval is always set to three times the LDP discovery hello-interval. Transport address is the address used for the TCP session over which LDP is running. If the transport address is not configured, the LDP router-id is used as transport address. Any update to transport address will take effect only if LDP is disabled and re-enabled. The "default" option sets the hello intervals to the default values.

Example

The following command sequence configures the LDP peer discovery parameters:

```
discovery hello hello-interval 10
discovery hello hold-interval 30
discovery transport-address 209.165.200.228
```

enable

Enables the Label Distribution Protocol (LDP).

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration

configure > context *context_name* **> mpls-ip > protocol ldp**

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] enable`

no

Disables the LDP protocol.

Usage Guidelines

This command is used to enable or disable the LDP protocol. By default the LDP protocol is disabled.

Example

Use the following command to enable the LDP protocol:

`enable`

router-id

Configures the Label Distribution Protocol Router ID.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration

configure > context *context_name* **> mpls-ip > protocol ldp**

Entering the above command sequence results in the following prompt:

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

Syntax Description

router-id *ipv4_addr*
no router-id

no

Disables the router ID.

ipv4_addr

Must be an IPv4 address entered in dotted-decimal notation.

Usage Guidelines

This command is used to configure the LDP router-id. This is an optional parameter. If the ID is not configured, the largest operational loopback address is selected as the LDP router ID. If LDP has started, any change will take effect only after disabling and enabling LDP.

Example

The following command sequence configures an LDP router ID:

router-id 209.165.200.228

session

Configures the LDP session parameters.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration

configure > context *context_name* **> mpls-ip > protocol ldp**

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ldp)#

Syntax Description

session timers { hold-interval *integer_value* **| keepalive-interval** *integer_value* **}**
default session timers

default

Configures the default values for hold-interval parameter at 45 and keepalive-interval parameter at 15.

timers

Configures the LDP session keepalive parameters.

hold-interval *integer_value*

Configures the session hold time interval in seconds.

integer_value is an integer from 45 through 65535.

Default: 45

keepalive-interval *integer_value*

Configures the frequency of sending keepalive packets in seconds.

integer_value is an integer from 15 through 21845.

Default: 15

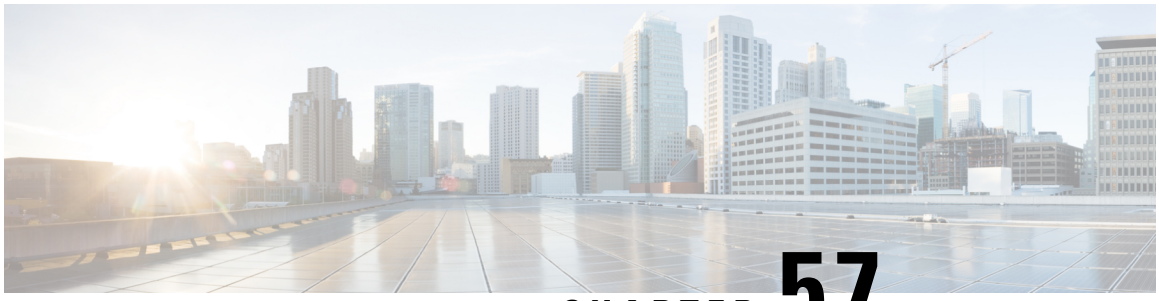
Usage Guidelines

This optional command is used to configure LDP session timers. LDP session hold-interval is always set to three times the LDP session keepalive-interval. The "default" option sets the session keepalive and hold intervals to the default values.

Example

The following command sequence configures the LDP session parameters:

```
session timers keepalive-interval 30
session timers hold-interval 45
default session timers
```



CHAPTER 57

MIPv6 HA Service Configuration Mode Commands

The MIPv6 HA Service Configuration Mode is used to create and manage Mobile IPv6 (MIPv6) access privileges.

Command Modes

Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context *context_name* **> mipv6ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

aaa accounting

Configures the sending of subscriber session AAA accounting by the Home Agent (HA) service.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context *context_name* **> mipv6ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

Syntax Description

[no] aaa accounting

no

Disables AAA accounting for the HA service.

Usage Guidelines

Enabling the HA service will send all accounting data (start, stop, and interim) to the configured AAA servers. The default is AAA accounting enabled.

Important In order for this command to function properly, AAA accounting must be enabled for the context in which the HA service is configured using the **aaa accounting subscriber radius** command.

AAA accounting for the HA service can be disabled using the **no** version of the command.

Example

The following command disables AAA accounting for the HA service:

```
no aaa accounting
```

bind

Designates the address of the MIPv6HA service and specifies the maximum number of subscribers that can access this service over the interface.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context *context_name* **> mipv6ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

Syntax Description

```
bind address IPv6_address [ max-subscribers count ]
no bind address
```

no

Removes the bound address from the HA service.

address

Specifies the IPv6 address of the MIPv6HA service using IPv6 colon-separated-hexadecimal notation.

max-subscribers *count*

Default: 3000000

Specifies the maximum number of subscribers that can access this service on this interface.

count is an integer from 0 through 4000000.

Important The maximum number of subscribers supported depends on the installed license key and the number of active packet processing cards installed in the system. Refer to the **license key** command for additional information.

Usage Guidelines

Use this command to associate the HA service with a specific logical IP address. The logical IP address or interface takes on the characteristics of a Pi interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

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

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

- The total number of interfaces that you will configuring for use as Pi interfaces
- The maximum number of subscriber sessions that all of these interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port to which these interfaces will be bound

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

Example

The following command binds the logical IP interface with the address of *2001:4A2B::1f3F* to the HA service and specifies that a maximum of *600* simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 2001:4A2B::1f3F max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```

default

Restore default values assigned for specified parameter.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context *context_name* **> mipv6ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

Syntax Description

```
default { aaa | refresh-advice-option | refresh-interval-percent |
reg-lifetime | sequence-number-validate | setup-timeout | simul-bindings
 | subscriber | timestamp-replay-protection }
```

aaa

Restores the AAA setting configured by the **aaa** command to its default of enabled.

refresh-advice-option

Restores the refresh-advice-option setting to its default of disabled.

refresh-interval-percent

Restores the refresh-interval-percent setting to its default of 75.

reg-lifetime

Restores the Mobile IP session registration lifetime setting configured by the **reg-lifetime** command to its default: 600 seconds.

sequence-number-validate

Restores the sequence-number-validate setting to its default of enabled.

setup-timeout

Restore the maximum amount of time allowed for setting up a session to the default: 60 seconds.

simul-bindings

Restores the simultaneous bindings setting to its default: 1.

subscriber

Configures settings for the default subscriber.

timestamp-replay-protection

Restores the timestamp-replay-protection scheme according to RFC 4285.

Usage Guidelines After the system has been modified from its default values, this command is used to set or restore specific parameters to their default values.

Example

The following command is used to return the simultaneous bindings setting parameter to it's default value:

```
default simul-bindings
```

refresh-advice-option

Configures inclusion of refresh advice option in the Binding Acknowledgement sent by the Home Agent (HA).

Product PDSN

HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context *context_name* **> mipv6ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

Syntax Description **refresh-advice-option**

Usage Guidelines Includes the refresh advice option in the binding acknowledgements sent by the home agent. Default is disabled.

refresh-interval-percent

Configures the percentage of the granted lifetime to be used in the refresh interval mobility option in the Binding Acknowledgement sent by the Home Agent (HA).

Product PDSN

HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context *context_name* **> mipv6ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

Syntax Description

refresh-interval-percent *value*

value

value represents a percentage expressed as an integer from 1 through 99. Default is 75.

Usage Guidelines

Use this command to configure the amount of the granted lifetime to be used in the refresh interval mobility option in the Binding Acknowledgement sent by the Home Agent (HA).

Example

The following command sets the refresh-interval-percent value to 50%:

refresh-interval-percent 50

reg-lifetime

Specifies the longest registration lifetime that the HA service will be allowed in any Registration Request message from the mobile node.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context *context_name* **> mipv6ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

Syntax Description

reg-lifetime *time*
no reg-lifetime

no

Sets the registration lifetime to infinite.

time

Specifies the registration lifetime in seconds. *time* is an integer from 1 through 262140. Default is 600.

Usage Guidelines

Use to limit a mobile nodes' lifetime. If the mobile node requests a shorter lifetime than what is specified, it is granted. However, Per RFC 2002, should a mobile node request a lifetime that is longer than the maximum allowed by this parameter, the HA service will respond with the value configured by this command as part of the Registration Reply.

Example

The following command configures the registration lifetime for the HA service to be 2400 seconds:

reg-lifetime 2400

The following command configures an infinite registration lifetime for MIPv6 calls:

no reg-lifetime

sequence-number-validate

Configures sequence number validation of the received MIPV6 control packet by the Home Agent (HA) according to RFC 3775.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context *context_name* **> mipv6ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mipv6ha-service)#`

Syntax Description

sequence-number-validate

Usage Guidelines

Use this command to enable sequence number validation of the received MIPV6 control packet by the Home Agent (HA) as per RFC 3775. Default is enabled.

setup-timeout

The maximum amount of time allowed for session setup.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context *context_name* **> mipv6ha-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mipv6ha-service)#`

Syntax Description

setup-timeout *seconds*

seconds

Default: 60 seconds

The maximum amount of time (in seconds) to allow for setup of a session expressed as an integer from 1 through 1000000. Default is 60 seconds.

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

Example

To set the maximum time allowed for setting up a session to 5 minutes (300 seconds), enter the following command:

```
setup-timeout 300
```

simul-bindings

Specifies the maximum number of "care-of" addresses that can be simultaneously bound for the same user as identified by NAI and Home address.

Product PDSN

HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context *context_name* **> mipv6ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

Syntax Description **simul-bindings** *number*

number

Configures maximum number of "care of" addresses that can be simultaneously bound for the same user as identified by their NAI and home address. *number* is an integer from 1 through 3. Default is 1.

Usage Guidelines Per RFC 2002, the HA service creates a mobile binding record (MBR) for each subscriber session it is facilitating. Each MBR is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care-of address.

Typically, the HA service will delete an old binding and create a new one when the information in the Registration Request changes. However, the mobile could request that the HA maintains previously stored MBRs. This command allows you to configure the maximum number of MBRs that can be stored per subscriber if the requested.

Example

The following command configures the service to support up to *2* addresses per subscriber:

```
simul-bindings 2
```

timestamp-replay-protection tolerance

Designates timestamp replay protection scheme as per RFC 4285.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context *context_name* **> mipv6ha-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

Syntax Description

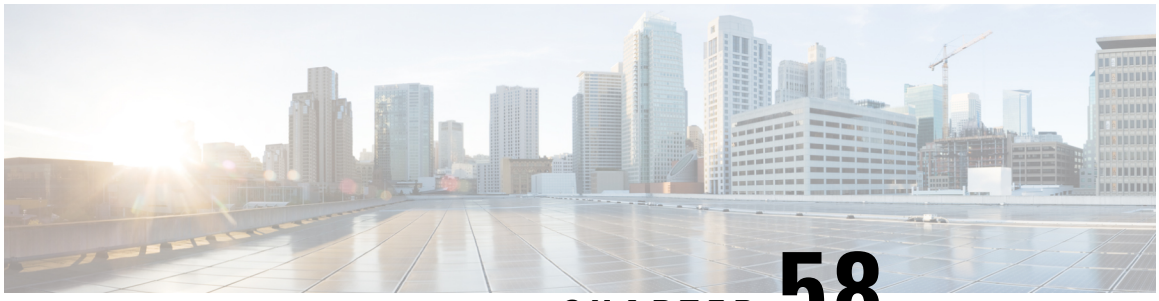
timestamp-replay-protection tolerance*seconds*

tolerance *seconds*

Defines the acceptable difference in timing (between timestamps) before rejecting packet, in seconds. *seconds* must be an integer from 0 through 65535. The default is 7.

Usage Guidelines

Use this command to define the acceptable difference in timing (between timestamps) before rejecting packet.



CHAPTER 58

MME-eMBMS Service Configuration Mode Commands

The MME-eMBMS Service Configuration Mode is used to create and manage the MME's LTE Evolved Multimedia Broadcast Multicast Service configuration for the LTE/SAE network.

Command Modes

Exec > Global Configuration > Context Configuration > MME-eMBMS Service

configure > context *context_name* **> mme-embms-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mme-embms-service)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

associate

Associates or disassociates supportive services and templates with the MME-eMBMS service.

Product MME

Privilege Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME-eMBMS Service

configure > context *context_name* **> mme-embms-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-embms-service)#
```

Syntax Description

[no] associate { egtp-service *service_name* **[context** *ctxt_name* **] | sctp-param-template** *template_name*

no

Disassociates a previously associated service or template from this MME-eMBMS service configuration.

egtp-service *service_name*

Specifies the name for a pre-configured eGTP service to associate with the MME-eMBMS service. The eGTP service provides eGTP-C protocol interface support between EPS nodes. Only one eGTP service can be associated with an MME-eMBMS service.

The eGTP service should be configured prior to issuing this command. For more information about the eGTP service, refer to the egtp-service command in the Context Configuration Mode Commands chapter and the eGTP Service Configuration Mode Commands chapter.

service_name is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

context *ctxt_name*

Identifies a specific context name where the named eGTP service is configured. If this keyword is omitted, the eGTP service must exist in the same context as the MME-eMBMS service.

ctxt_name is an alphanumeric, case-sensitive string of 1 through 63 characters.

sctp-param-template *template_name*

Associates a Stream Control Transmission Protocol (SCTP) parameter template with this MME-eMBMS service. For more information on the SCTP parameter template, refer to the *sctp-param-template* command in the *Global Configuration Mode Commands* chapter and the *SCTP Parameter Template Configuration Mode Commands* chapter.

template_name specifies the name for a pre-configured SCTP parameter template to associate with this MME-eMBMS service. The name entered must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to associate a pre-configured eGTP service or SCTP parameter template with the MME-eMBMS service.

Example

The following command disassociates a previously configured association between the MME-eMBMS service and the already configured *egtp1* eGTP service :

```
no associate egtp-service egtp1
```

bind

Binds the MME-eMBMS service to a logical IP interface serving as the M3 interface.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME-eMBMS Service

configure > context *context_name* **> mme-embms-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-embms-service)#
```

Syntax Description

bind { ipv4-address *address* **[ipv4-address** *secondary_address* **] | ipv6-address** *address* **[ipv6-address** *secondary_address* **] }**
no bind

no

Removes a previously configured IP address used for binding the SCTP (local bind address) to communicate with the eNodeBs using an S1-MME interface.

{ ipv4-address *address* [ipv4-address *secondary_address*] | ipv6-address *address* [ipv6-address *secondary_address*] }

Specifies the IP address for the interface configured as an M3 interface in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. Optionally configure a secondary IP address for either address type.

Usage Guidelines

Use this command to associate the MME-eMBMS service with a specific logical IP address that will be used for binding the SCTP socket that communicates with the eNodeB using M3. Only one IP address can be configured with this command for one MME service.

Example

The following command would bind the logical IP interface with the address of *209.165.200.225* to the MME-eMBMS service to interact with eNodeB:

```
bind ipv4-address 209.165.200.225
```

The following command disables a binding that was previously configured:

```
no bind
```

mmemgr-recovery

Sets the action the MME takes regarding the peers (MCEs) upon recovery after an MME Manager crash/failure.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME-eMBMS Service

configure > context *context_name* **> mme-embms-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-embms-service)#
```

Syntax Description **mmemgr (no-reset | reset-peers }**

no-reset

Configures the MME-eMBMS service not to have the MME perform a reset of peer associations upon recovery of the MMEMgr after a manager crash/failure.

This is the default setting.

reset-peers

Configures the MME-eMBMS service to have the MME perform a reset of peer associations upon recovery of the MMEMgr after a manager crash/failure.

Important Currently, this option is not supported.

Usage Guidelines If the MMEMgr crashes or fails, the configuration (defined with this command) instructs the MME what actions to take at the time of recovery in reference to the peer association.

Example

The following command instructs the MME not to reset associations :

mmemgr-recovery no-reset

plmn-id

Configures the carrier's Public Land Mobile Network (PLMN) identifier to associate with this eMBMS service area.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME-eMBMS Service

configure > context *context_name* **> mme-embms-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-embms-service)#
```

Syntax Description **plmn-id mcc** *mcc* **mnc** *mnc*

mcc *mcc*

Specifies the mobile country code (MCC) portion of the PLMN identifier. The *mcc* must be an integer from 100 through 999.

mnc *mnc*

Specifies the mobile network code (MCC) portion of the PLMN identifier. The *mnc* must be a 2- or 3-digit integer from 00 through 999.

Usage Guidelines Use this command to specify the PLMN identifier to associate with the eMBMS area for this MME's eMBMS service.

Example

The following command configures the PLMN identifier with an MCC of 462 and MNC of 02:

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

sctp port

Configures the SCTP port number to be associated with the M3AP interface of the eMBMS service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME-eMBMS Service

configure > context *context_name* **> mme-embms-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-embms-service)#
```

Syntax Description **sctp port** *port_number*

port_number

Enter an integer from 1 to 65535. The default is 36412.

Usage Guidelines Use this command to identify the SCTP port for the M3AP interface.

Example

The following command configures sctp port *34414* as the sctp port number associated with the M3AP interface :

```
sctp port 34414
```

setup-timeout

Specifies the maximum amount of time allowed for session setup.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME-eMBMS Service

configure > context *context_name* **> mme-embms-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-embms-service)#
```

Syntax Description

setup-timeout *seconds*

no setup-timeout

seconds

The maximum amount of time, in seconds, to allow for setup of a session. Where *seconds* must be an integer from 1 through 10000. The default is 60.

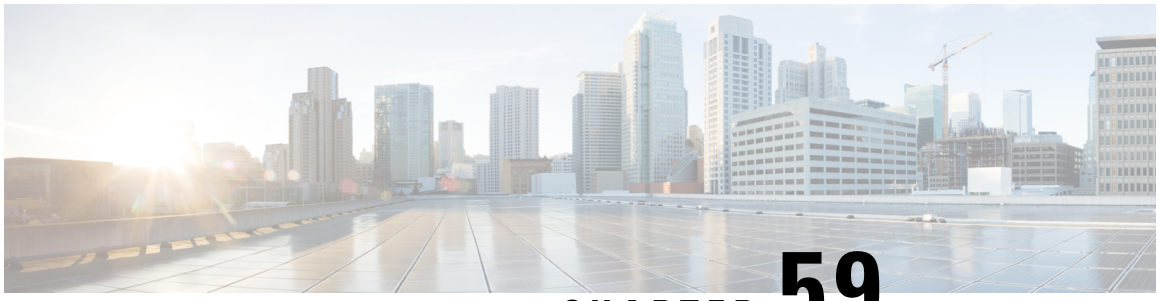
Usage Guidelines

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

Example

The following command sets the maximum setup time as *120* seconds:

```
setup-timeout 120
```



CHAPTER 59

MME LAC Pool Area Configuration Mode Commands

The MME LAC Pool Area Configuration Mode is used to create and manage the Location Area Code (LAC) pool areas.

Command Modes

Exec > Global Configuration > Context Configuration > SGs Service Configuration > MME LAC Pool Area Configuration

configure > context *context_name* **> sgs-service** *service_name* **> pool-area** *pool_area_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgs-pool-area)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

hash-value

Configures the Visitor Location Register (VLR) hash value mapping for this pool area.

Product MME

Privilege Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGs Service Configuration > MME LAC Pool Area Configuration

configure > context *context_name* **> sgs-service** *service_name* **> pool-area** *pool_area_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgs-pool-area)#
```

Syntax Description

hash-value { *value* | non-configured-values | range *value* to *value* } use-vlr *vlr_name*
no hash-value { *value* | non-configured-values | range *value* to *value* }

no

Removes the configured hash-value from the pool-area configuration.

value

Specifies the VLR hash value to be used with the configured VLR. *value* must be an integer from 0 through 999.

non-configured-values

Specifies that the VLR configured in this command is to be used with non-configured hash values.

range *value* to *value*

Specifies a range of hash values to use with the configured VLR as an integer from 0 through 999.

use-vlr *vlr_name*

Specifies the VLR to be used with the hash value configuration when selected. The *vlr_name* must be an alphanumeric string of size 1 through 63 characters.

Usage Guidelines

Use this command to configure hash values to be used with VLRs.

In Release 12.2 and later, a maximum of 48 hash lists can be created per pool area. In older releases, a total of 32 hash lists can be created per pool area.

In a pool configuration, the MME selects the VLR that corresponds to the hash of the UE's IMSI. If that VLR is inactive, the MME will use the default VLR (as defined by the **non-configured-value** option). If no default VLR has been configured, or if the default VLR is inactive, the MME selects the next available VLR from the pool.

If the chosen VLR is active at the time of selection and then subsequently becomes inactive when the request is sent to it, the current request fails. On the next request from the UE, the VLR selection mechanism is applied again. A VLR that failed previously will only be selected again if it became active since the earlier failure.

Example

The following command configures all hash values within a range of *0* to *500* to use a VLR named *vlr1*:

```
hash-value range 0 to 500 use-vlr vlr1
```

The following command configures hash values of *501* to use a VLR named *vlr2*:

hash-value 501 use-vlr vlr2

The following command configures all non-configured hash values to use a VLR named *vlr3*:

hash-value non-configured-values use-vlr vlr3

lac

Configures a 3G location area code or area codes that define this pool area.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGs Service Configuration > MME LAC Pool Area Configuration

configure > **context** *context_name* > **sgs-service** *service_name* > **pool-area** *pool_area_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgs-pool-area)#`

Syntax Description

[no] lac *area_code* **+**

no

Removes a configured forbidden handover area code or area codes from this policy. If no location area code is specified, then all location area codes are removed.

area_code

Specifies an area code or area codes used to select a VLR for the pool area as an integer from 0 through 65535. Multiple area codes can be entered (up to 16 in a single line, separated by spaces).

Usage Guidelines

Use this command to configure 3G location-based area codes that define this pool area.

In Release 12.2 and later, a maximum of 96 areas can be added per pool area (in a single line, or separately). In older releases, a total of 16 area codes can be added (in a single line, or separately).

Example

The following command configures eight location-based area codes (1, 2, 3, 4, 5, 6, 7, 8) that define this pool area:

lac 1 2 3 4 5 6 7 8

plmnid

Configures the Public Land Mobile Network (PLMN) identifier for the LAC pool area.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGs Service Configuration > MME LAC Pool Area Configuration

configure > **context** *context_name* > **sgs-service** *service_name* > **pool-area** *pool_area_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgs-pool-area)#
```

Syntax Description

plmnid { any | mcc *mcc_value* **mnc** *mnc_value* **}**
no plmnid

no

Removes the configured PLMN identifier for the LAC pool area.

any

This keyword specifies any PLMN identifier can be configured for the LAC pool area.

mcc ***mcc_value***

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc ***mnc_value***

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

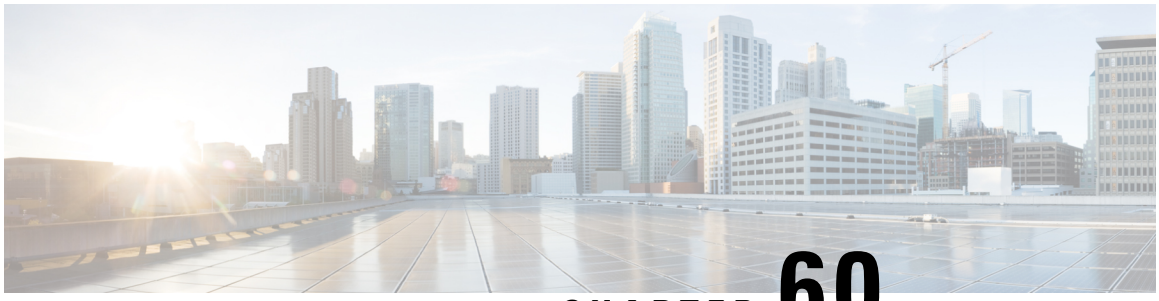
Usage Guidelines

Use this command to set the PLMN identifier for the LAC pool area. Any PLMN identifier can be configured for the LAC pool area or a specific PLMN identifier can be configured by providing the MCC and MNC of the PLMN identifier.

Example

The following command configures the PLMN identifier with MCC value as *102* and MNC value as *20* for this MME service:

```
plmnid mmc 102 mnc 20
```



CHAPTER 60

MME Manager Configuration Mode Commands

The MME Manager Configuration Mode is used to configure the MME Manager(s).

Command Modes

Exec > Global Configuration > MME Manager Configuration

configure > mme-manager

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(mme-manager)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

congestion-control

This command enables or disables CPU Usage based congestion control for MME Manager(s), and configures congestion parameters (CPU Threshold and Tolerance values).

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > MME Manager Configuration

configure > mme-manager

Entering the above command sequence results in the following prompt:

```
[local]host_name(mme-manager)#
```

Syntax Description

congestion-control cpu-utilization [threshold *threshold_value* **tolerance** *tolerance_value* **]**
no congestion-control [cpu-utilization]

no

Enables or disables congestion control.

cpu-utilization

Specifies the average CPU utilization in %.

threshold *threshold_value*

Specifies the thresholds for various resources. *threshold_value* must be an integer from 1 to 100.

Default: 90%

tolerance *tolerance_value*

Specifies the tolerance limit. *tolerance_value* must be an integer from 1 to 100.

Default: 10

Usage Guidelines

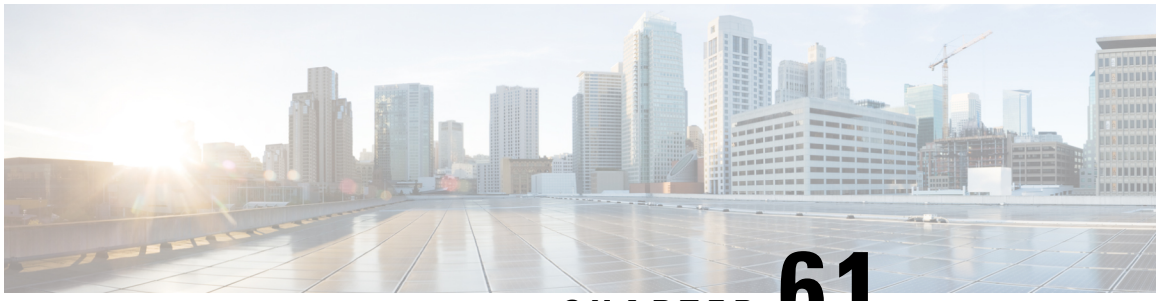
Use this command to enable or disable CPU Usage based congestion control for MME Manager(s), and configure congestion parameters (CPU Threshold and Tolerance values). This command is enabled by default.

See the *Auto Disabling of eNodeB Paging* chapter in the *MME Administration Guide* for more information.

Example

The following command enables congestion control with threshold value in % set to *90* and tolerance value set to *10*:

```
congestion-control cpu-utilization threshold 90 tolerance 10
```



CHAPTER 61

MME MSC Pool Area Configuration Mode

The MME MSC Pool Area Configuration Mode is used to create and manage the MSC Pool Areas used by the MME for communicating with the Mobile Switching Center (MSC) for Single Radio Voice Call Continuity (SRVCC).

Command Modes

Exec > Global Configuration > Context Configuration > MME Service Configuration > Pool Area Configuration

configure > context *context_name* **> mme-service** *service_name* **> pool-area** *pool_area_name* **type hash-value**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-pool-area-hash-value)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

hash-value

Configures the selection of MSC in a MSC pool area based on the hash value derived from the IMSI.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service Configuration > Pool Area Configuration

configure > context *context_name* **> mme-service** *service_name* **> pool-area** *pool_area_name* **type hash-value**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-pool-area-hash-value)#
```

Syntax Description

hash-value { *hash_value* | range *start_value* to *end_value* } use-msc *msc_name*
no hash-value { *hash_value* | range *start_value* to *end_value* }

no

Removes the configured hash value for this pool area.

hash-value

Specifies the specific hash value for this pool area.

hash_value must be an integer from 0 through 999.

range *start_value* to *end_value*

Specifies the range of hash values for this pool area.

start_value specifies the start value for range of hash and is an integer value from 0 through 999.

end_value specifies the end value for range of hash and is an integer value from 0 through 999.

The *start_value* must be lower than the *end_value*.

use-msc *msc_name*

Specifies the MSC to use when this pool area is selected.

msc_name is the name of the MSC as configured in the MME Service using the **msc** command; *msc_name* must be an alphanumeric string of 1 to 39 characters.

Usage Guidelines

This command associates an MSC with this pool. It also assigns the MSC to use based on the hash value as computed from the IMSI digits [(IMSI div 10) modulo 1000].

A maximum of 24 hash values can be configured within each pool area.

If no matching MSC is found, the SRVCC handover fails.

Example

The following command configures hash values from *111* to *222* to use the MSC named *mscwest1* in this pool.

```
hash-value range 111 to 222 use-msc mscwest1
```

plmn-id

Associates a Public Land Mobile Network (PLMN) identifier with a Mobile Switching Center (MSC) pool area.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service Configuration > Pool Area Configuration

configure > context *context_name* **> mme-service** *service_name* **> pool-area** *pool_area_name* **type hash-value**

or

configure > context *context_name* **> mme-service** *service_name* **> pool-area** *pool_area_name* **type round-robin**

Entering the above command sequences result in the following prompts, respectively:

```
[context_name]host_name(config-mme-pool-area-hash-value)#
[context_name]host_name(config-mme-pool-area-round-robin)#
```

Syntax Description

plmn-id mcc *code* **mnc** *code*
no plmn-id

no

Removes the configured plmn-id assigned to this MSC pool area.

mcc *code*

Specifies the Mobile Country Code for this mobile access network. *code* must be a three-digit integer from 200 to 999.

mnc *code*

Specifies the Mobile Network Code for this mobile access network. *code* must be a two- or three-digit integer from 00 to 999.

Usage Guidelines

Use this command to associate a PLMN with an MSC pool area. This PLMN is used to select an MSC pool area based on the target PLMN as specified in the SRVCC handover request.

When configured, the MME attempts to select an MSC using the following selection order:

1. Pool area that matches the PLMN and of type hash.
2. Pool area that matches the PLMN and of type round-robin.
3. Pool area that does not have PLMN associated and of type hash.
4. Pool area that does not have PLMN associated and of type round-robin.

When this command is used, only one PLMN can be assigned per pool area of the same type (either hash-value or round-robin). A hash value pool area and a separate round robin pool area can be configured with the same PLMN. In this case, the hash value pool has the higher priority.

If no matching MSC is found, the SRVCC handover fails.

Example

The following command identifies the mobile network with MCC of **123** and MNC of **12**.

```
plmn-id mcc 123 mnc 12
```

use-msc

Associates a Mobile Switching Center (MSC) with the pool area.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service Configuration > Pool Area Configuration

configure > context *conext_name* **> mme-service** *service_name* **> pool-area** *pool_area_name* **type round-robin**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-pool-area-round-robin)#
```

Syntax Description

[no] use-msc *msc_name*

no

Removes the associated MSC name from this pool area.

use-msc *msc_name*

Associates an MSC name with this pool area.

msc_name is the name of the MSC as configured in the MME Service using the **msc** command. *msc_name* must be an alphanumeric string of 1 to 39 characters.

Usage Guidelines

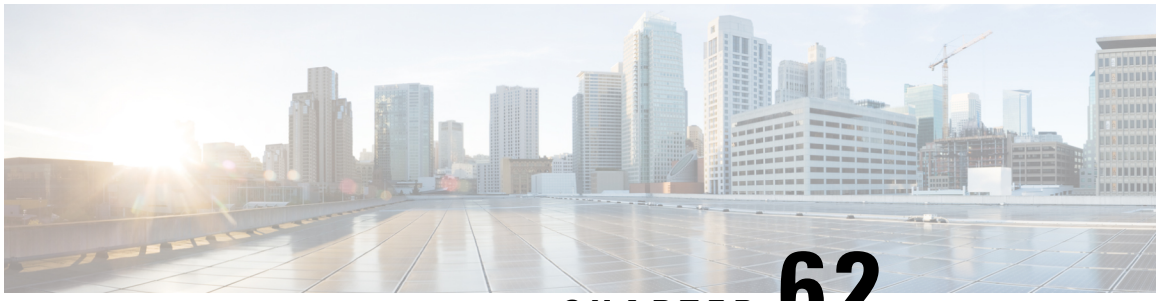
This command associates an MSC with this pool area. With a round-robin pool area selection, the MME selects the next MSC within the pool based on a round-robin scheme.

A maximum of 24 MSC associations can be defined within each round-robin pool area.

Example

The following command associates the MSC named *mscsouth1* to this pool.

```
use-msc mscsouth1
```



CHAPTER 62

MME Service Configuration Mode Commands

The MME Service Configuration Mode is used to create and manage the LTE Mobility Management Entity (MME) services for the LTE/SAE network. This service works in conjunction with MME-HSS Service and eGTP Service.

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

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

Caution Restarting the MME service leads to termination of UE sessions at the MME, purge of subscriber data and closure of all connections towards peer nodes such as eNodeB, HSS, S-GW, etc. It may also lead to termination of other services associated with the MME. It is strongly advised to make any configuration changes that restarts the service only while in maintenance mode or at startup.

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

• trace cell-traffic, on page 699
• ue-db, on page 700

associate

Associates or disassociates supportive services and policies, such as an Evolved GPRS Tunnelling Protocol (eGTP) service, an HSS peer service, or an MME policy subscriber map with an MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

associate { { access-policy *policy_name* **| decor-profile** *profile_name* **access-type { eutran | nb-iot | all } | egtp-mef-service** *egtp_mef_service_name* **context** *context_name* **| egtp-s10-s3-service** *service_name* **| egtp-service** *egtp_svc_name* **| egtp-sv-service** *egtp_sv_svc_name* **| foreign-plmn-guti-mgmt-db** *db_name* **| gtpc-load-control-profile** *profile_name* **| gtpc-overload-control-profile** *profile_name* **| henbgw-mgmt-db** *db_name* **| hss-peer-service** *hss_svc_name* **| ipne-service** *ipne_svc_name* **| location-service** *location_svc_name* **| lte-emergency-profile** *profile_name* **| network-global-mme-id-mgmt-db | s102-service** *s102_svc_name* **[context** *context_name* **] | sbc-service** *sbc_svc_name* **| scef-service** *service_name* **| sctp-param-template** *template_name* **| sgs-service** *sgs_svc_name* **| sgtpc-service** *sgtpc_svc_name* **smsc-service** *smsc_svc_name* **} [context** *ctx_name* **] | subscriber-map** *map_name* **| tai-mgmt-db** *database_name* **}**
no associate { access-policy | decor-profile *profile_name* **access-type { eutran | nb-iot | all } | egtp-mef-service | egtp-service | egtp-sv-service | foreign-plmn-guti-mgmt-db | gtpc-load-control-profile | gtpc-overload-control-profile| henbgw-mgmt-db | hss-peer-service | ipne-service | location-service | lte-emergency-profile | network-global-mme-id-mgmt-db | s102-service | sctp-param-template | sgs-service | sgtpc-service | smsc-service | subscriber-map | tai-mgmt-db }**

no

Disassociates a previously associated service with this MME service.

access-policy *policy_name*

Specifies the access-policy to be associated with the MME Service. *policy_name* must be an alphanumeric string of 1 through 64 characters.

associate monitoring-event-profile*profile_monte*

Specifies the monitoring event profile to be associated with the MME Service.

decor-profile *profile_name*

Specifies the DECOR profile to be associated with the MME Service.

access-type { eutran | nb-iot | all }

Configures the type of network access in a DCN — E-UTRAN, NB-IoT, or both.

egtp-mef-service *egtp_mef_service_name*

Associates the given egtp-service for MEF interface at the MME.

egtp_mef_service_name must be a string from 1 to 63.

context *context_name*: Specifies the context to which the service belongs.

egtp-s10-s3-service *service_name*

Associates EGTP service for S10/S3 interface to support Inter-Operator S10 Handover.

service_name must be an alphanumeric string of size 1 to 63 characters.

egtp-service *egtp_svc_name*

Associates an eGTP service with MME service.

egtp_svc_name specifies the name for a pre-configured eGTP service to associate with the MME service. The eGTP service provides eGTP-C protocol interface support between EPS nodes. For more information on the eGTP service, refer to the **egtp-service** command in the *Context Configuration Mode Commands* chapter and the *eGTP Service Configuration Mode Commands* chapter.

Only one eGTP service can be associated with a service. The eGTP service should be configured prior to issuing this command.

egtp-sv-service *egtp_sv_svc_name*

Associates an eGTP Sv service with this MME service.

egtp_sv_svc_name specifies the name for a pre-configured eGTP Sv service to associate with the MME service. For more information on the eGTP Sv service, refer to the **egtp-service** command in the *Context Configuration Mode Commands* chapter.

foreign-plmn-guti-mgmt-db *db_name*

Associates a Foreign PLMN GUTI management database with this MME service.

db_name specifies the name for a pre-configured foreign PLMN GUTI management database to associate with the MME service. For more information on the Foreign PLMN GUTI management database, refer to the **foreign-plmn-guti-mgmt-db** command in the *LTE Policy Configuration Mode Commands* chapter.

Only one Foreign PLMN GUTI management database can be associated to an MME service. The Foreign PLMN GUTI management database should be configured prior to issuing this command.

Multiple MME services can be associated to the same Foreign PLMN GUTI management database.

gtpc-load-control-profile *profile_name*

Associates a GTP-C Load Control Profile with this MME service

The *profile_name* specifies the name of a GTP-C load control profile to associate with the MME service.

For more information on the GTPC Load Control Profile, refer to the feature chapter "*GTP-C Load and Overload Control on MME*" in the *MME Administration Guide*.

gtpc-overload-control-profile *profile_name*

Associates a GTP-C Overload Control Profile with this MME service

The *profile_name* specifies the name of a GTP-C overload control profile to associate with the MME service.

For more information on the GTPC Overload Control Profile, refer to the feature chapter "*GTP-C Load and Overload Control on MME*" in the *MME Administration Guide*.

henbgw-mgmt-db *db_name*

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

Associates the specified HeNB-GW management database with the MME service.

db_name specifies the name for an LTE MME HeNB-GW Management Database to associate with the MME service as an alphanumeric string of 1 through 64 characters. This is required to support S1 HANDOVERs to Home eNodeBs connected via a HeNB-GW.

hss-peer-service *hss_svc_name*

Associates an HSS peer service with this MME service.

hss_svc_name specifies the name for a pre-configured HSS peer service to associate with the MME service as an alphanumeric string of 1 through 64 characters. The HSS peer service provides S6a and S13 interface support via the Diameter protocol between the MME and an HSS (S6a) or EIR (S13). For more information about the HSS peer service, refer to the **hss-peer-service** command in the *Context Configuration Mode Commands* chapter and the *HSS Peer Service Configuration Mode Commands* chapter.

Only one HSS peer service can be associated to a service. The HSS peer service should be configured prior to issuing this command.

ipne-service *ipne_svc_name*

Associates an IPNE service with this MME service.

ipne_svc_name must be an alphanumeric string of 1 to 63 characters to identify a pre-configured, uniquely-named IPNE service. For more information about the IPNE service, refer to the sections for the *IPNE Service Configuration Mode Commands* and the *IPNE Endpoint Configuration Mode Commands*.

location-service *location_svc_name*

Associates a location service with this MME service. Only one location service should be associated with an MME Service.

location_svc_name specifies the name for a pre-configured location service to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information about Location Services (LCS),

refer to the **location-service** command in the *Context Configuration Mode Commands* chapter and the *Location Services Configuration Mode Commands* chapter.

lte-emergency-profile *profile_name*

Associates an LTE emergency profile with this MME service.

profile_name specifies the name for a pre-configured LTE emergency profile to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information about the LTE emergency profile, refer to the **lte-emergency-profile** command in the *LTE Policy Configuration Mode Commands* chapter and the *LTE Emergency Profile Configuration Mode Commands* chapter.

network-global-mme-id-mgmt-db

Associates the configured global MME ID management database with this MME service. The global MME ID management database is configured through the LTE Policy Configuration Mode using the **network-global-mme-id-mgmt-db** command.

s102-service *s102_svc_name* [context *context_name*]

Associates the specified S102 service that manages the S102 interface with this MME service.

s102_svc_name specifies the name for a pre-configured S102 service to associate with this MME service. Enter a string of 1 through 63 alphanumeric characters.

context *context_name* identifes the context in which the S102 service has been created and configured.

Each MME service can be associated with one unique S102 service.

The S102 service is **not** a critical parameter for the MME service. Removing this configuration will **not** restart the MME service.

For more information about the S102 service, refer to the **s102-service** command in the *Global Configuration Mode Commands* chapter and the *S102 Service Configuration Mode Commands* chapter.

sbc-service *sbc_svc_name*

Important Beginning with Release 18.4, this keyword is only accessible or configurable if a valid SBc license key is installed. For information about obtaining such a license, contact your Cisco Representative.

Associates the specified SBc service with this MME service.

sbc_svc_name specifies the name for a pre-configured SBc service to associate with this MME service as an alphanumeric string of 1 through 63 characters.

Each MME service can be associated with one unique SBc service.

The SBc service is **not** a critical parameter for the MME service. Removing this configuration will **not** restart the MME service.

For more information about the SBc service, refer to the **sbc-service** command in the *Global Configuration Mode Commands* chapter, the *SBc Service Configuration Mode Commands* chapter, and the *Cell Broadcast Center - SBc Interface* feature chapter in the *MME Administration Guide*.

sctp-param-template *template_name*

Associates a Stream Control Transmission Protocol (SCTP) parameter template with this MME service.

template_name specifies the name for a pre-configured SCTP parameter template to associate with this MME service as an alphanumeric string of 1 through 63 characters. For more information on the SCTP parameter template, refer to the **sctp-param-template** command in the *Global Configuration Mode Commands* chapter and the *SCTP Parameter Template Configuration Mode Commands* chapter.

sgs-service *sgs_svc_name*

Associates an SGs service with this MME service.

sgs_svc_name specifies the name for a pre-configured SGs service to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information on the SGs service, refer to the **sgs-service** command in the *Context Configuration Mode Commands* chapter and the *MME SGs Service Configuration Mode Commands* chapter.

sgtpc-service *sgtpc_svc_name*

Associates an SGTPC service with this MME service.

sgtpc_svc_name specifies the name for a pre-configured SGTPC service to associate with the MME service as an alphanumeric string of 1 through 64 characters.

Important When co-locating an SGSN and MME, the MME Service cannot be associated with the same SGTP service that is used by the SGSN.

For more information on the SGTPC service, refer to the **sgtp-service** command in the *Context Configuration Mode Commands* chapter and the *SGTP Service Configuration Mode Commands* chapter.

smsc-service *smsc_svc_name*

Associates an SMSC service with this MME service.

smsc_svc_name specifies the name for a pre-configured SMSC service to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information on the SMSC service, refer to the **smsc-service** command in the *Context Configuration Mode Commands* chapter and the *MME SMSC Service Configuration Mode Commands* chapter.

context *ctx_name*

Identifies a specific context name where the named service is configured. If this keyword is omitted, the named service must exist in the same context as the MME service.

ctx_name is name of the configured context of the named service expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

subscriber-map *map_name*

Associates this MME service with a pre-configured subscriber map.

map_name specifies the name of a pre-configured subscriber map to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information on subscriber maps, refer to the

subscriber-map command in the *LTE Policy Configuration Mode Commands* chapter and the *LTE Subscriber Map Configuration Mode Commands* chapter.

tai-mgmt-db *database_name*

Associates this MME service with a pre-configured TAI Management Database.

database_name specifies the name of a pre-configured TAI Management Database to associate with the MME service as alphanumeric string of 1 through 64 characters. For more information on subscriber maps, refer to the **tai-mgmt-db** command in the *LTE Policy Configuration Mode Commands* chapter and the *LTE TAI Management Database Configuration Mode Commands* chapter.

Usage Guidelines

Use this command to associate a pre-configured service or policy with an MME service.

To configure a DECOR profile, refer to the *Configuring DCN Profile* section in the *Dedicated Core Networks on MME* chapter in the *MME Administration Guide*.

Caution This is a critical configuration. The MME service cannot be started without this configuration. Any change to this configuration will cause the MME service to be restarted. Removing or disabling this configuration will stop the MME service.

Example

The following command associates a pre-configured eGTP service called *egtp1* in the *dst_ctx* context to an MME service:

```
associate egtp-service egtp1 context dst_ctx
```

The following command associates a pre-configured HSS peer service called *hss1* in the same context as MME service to an MME service:

```
associate hss-peer-service hss1
```

bind s1-mme

Binds the MME service to a logical IP interface serving as the S1-MME interface.

Product

Important Before modifying this bind configuration using the **no bind s1-mme** command, we recommend that the MME Administrator use the **clear mme-service db record** command, under the Exec mode, to empty the MME records database.

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
bind s1-mme { ( ipv4-address address [ { ipv4-address secondary_address } | {
 ipv6-addresssecondary_address } ] ) | ( ipv6-address address [ {
ipv6-addresssecondary_address } | { ipv4-address secondary_address } ] ) [
crypto-template name ] [ max-subscribers number ]
no bind s1-mme
```

no

Removes a previously configured IP address used for binding the SCTP (local bind address) to communicate with the eNodeBs using an S1-MME interface.

{ (ipv4-address *address* [{ ipv4-address *secondary_address* } | { ipv6-address *secondary_address* }]) | (ipv6-address *address* [{ ipv6-address *secondary_address* } | { ipv4-address *secondary_address* }]

Specifies the IP address for the interface configured as an S1-MME interface in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. Optionally configure a secondary IP address for either address type.

crypto-template *name*

Specifies an existing crypto template name used when implementing IP Security (IPSec) on the S1-MME interface. *name* is an alphanumeric string of 1 through 104 characters.

max-subscribers *number*

Specifies the maximum number of subscribers that can access this service on this interface as an integer from 0 through 8000000.

For Release 15.0, the ASR 5500 platform supports up to 10,000,000 MME UE sessions.

Usage Guidelines

Use this command to associate the MME service with a specific logical IP address that will be used for binding the SCTP socket that communicates with the eNodeB using S1AP. Only one IP address can be configured with this command for one MME service.

The MME passes the IP address during setting up the SCTP association with the eNodeB.

Caution This is a critical configuration. The MME service can not be started without this configuration. Any change to this configuration will cause the MME service to be restarted. Removing or disabling this configuration will stop the MME service.

Important Up to two IPv4 or IPv6 addresses can be configured to support SCTP multi-homing. SCTP multi-homing is supported only when the two configured IP addresses are of the same type. If the configured IP addresses are different types, then the MME service is reachable either through the IPv4 or the IPv6 address, but SCTP multi-homing is not supported.

Example

The following command would bind the logical IP interface with the address of *209.165.200.225* to the MME service to interact with eNodeB:

bind s1-mme ipv4-address 209.165.200.225

The following command disables a binding that was previously configured:

no bind s1-mme

The following command would bind the logical IP interface with the address of 209.165.200.226 as primary IPv4 address and aaaa:aaaa:10::1 as secondary IPv6 address to the MME service to interact with eNodeB configured with IPv4 address and IPv6 address respectively:

bind s1-mme ipv4-address 209.165.200.226 ipv6-address aaaa:aaaa:10::1

The following command would bind the logical IP interface with the address of aaaa:aaaa:10::1 as primary IPv6 address and 209.165.200.227 as secondary IPv4 address to the MME service to interact with eNodeB configured with IPv6 address and IPv4 address respectively:

bind s1-mme ipv6-address aaaa:aaaa:10::1 ipv4-address 209.165.200.227

buffer-ubreq-from-3g-to-4g

Enables the buffering of UBReq by sending UBResp with Cause Code 16 during 3G to 4G HO/TAU.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

buffer-ubreq-from-3g-to-4g

no

Removes the buffer-ubreq-from-3g-to-4g entry from the mme-service object.

Usage Guidelines

Use this command to to enable/disable buffering of Update Bearer Request with Cause Code 16 during 3G to 4G Handover/TAU and improves the KPI success rate of GTPv2 Update Bearer Request failures during 3G to 4G handover/TAU procedures.

Example

The following command would enable update bearer request being received during a 3G to 4G handover or TAU procedure:

buffer-ubreq-from-3g-to-4g

The following command disables the update bearer request being received during a 3G to 4G handover or TAU procedure:

no buffer-ubreq-from-3g-to-4g

clear-route-multipath-zero

Enables clearing dynamic route table for multipath zero condition.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] clear-route-multipath-zero

clear-route-multipath-zero

Enables clearing dynamic route table if diameter lookup finds dynamic route entry with multipath zero. This will take effect only for the subsequent mme diameter session.

no

Disables clearing dynamic route table for multipath zero condition.

Usage Guidelines

Use this command to enable or disable clearing dynamic route table if diameter lookup finds dynamic route entry with multipath zero. This will take effect only for the subsequent mme diameter session. This command clears dynamic route table of the particular session manager for which multipath 0 is detected.

Example

The following command enables clearing dynamic route table for multipath zero condition:

clear-route-multipath-zero

cp-data-max-retransmissions

This command configures the maximum number of retransmissions of CP data for MO or MT SMS scenario in MME.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default ] cp-data-max-retransmissions` *`num_retrans`*

default

Sets the default value to 2.

num_retrans

Specifies the number of times CP Data for SMS is retransmitted. *num_retrans* must be an integer from 1 to 10.

Usage Guidelines

Use the following configuration to configure the maximum number of retransmissions of CP data for MO or MT SMS scenario in MME.

Example

The following command configures *2* retransmissions of CP data for SMS.

`cp-data-max-retransmissions 2`

csg-change-notification

This command enables or disables the Closed Subscriber Group (CSG) Information reporting (notification) mechanism on the MME. When enabled, the MME includes the CSG Information Reporting Action IE with the appropriate Action field for subscribers.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] csg-change-notification`

default

By default, this feature is disabled. Using the **default** command prefix causes the MME to reset the configuration for this parameter to the default so that the feature is disabled.

no

Disables the feature.

Usage Guidelines Use this command to enable or disable CSG change notification to the SGW/PGW.

By default **csg-change-notification** is disabled; the MME does not send CSG notification to the SGW/PGW.

dcnr

Enables Dual Connectivity with New Radio (DCNR) to support 5G Non Standalone (NSA).

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] dcnr**

no

Disables the DCNR configuration.

Usage Guidelines Use this command to enable DCNR for 5G NSA support.

ddn-delay

Configures Delay Value IE Support in MME.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **ddn-delay***ddn_delay_value*

[no] ddn-delay

no

Removes the configured downlink-data-notification delay value

ddn-delay *ddn_delay_value*

Configures the downlink-data-notification delay value in multiples of 50 milliseconds. *ddn_delay_value* is an integer and it must be between 0 and 255

Usage Guidelines Use this command to enable configure ddn-delay value.

decor

This command specifies the Dedicated Core Network (DCN) configuration and enables MME to advertise or request UE Usage Type over the S6a interface.

Product MME

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] decor custom-actions [ air explicit-air-flags | ula gw-selection | nas-reroute [ reject ] ] s6a ue-usage-type`

`[ default ] decor custom-actions [ air explicit-air-flags | ula gw-selection | nas-reroute [ reject ] ]`

no

Disables the specified DECOR configuration.

default

Configures default air-flags in AIR

decor

Specifies a dedicated core network configuration.

custom-actions

Configures the specific decor actions.

air

Configures UUT actions in AIR message.

explicit-air-flags

Fills air-flags in AIR, irrespective of UUT stored in DB.

ula

Configures UUT actions in ULA message.

gw-selection

Enables GW selection based on UUT received in ULA.

nas-reroute

Enables NAS re-route based on Ue-Usage-Type received in ULA.

reject

Rejects the rerouted call based on Ue-Usage-Type received in ULA.

s6a

Configures the S6a interface.

ue-usage-type

Specifies the UE Usage Type that needs to be sent in the Authentication-Information-Request message over the S6a interface.

Usage Guidelines

Use this command to specify a Dedicated Core Network configuration and enable the MME to advertise or request the UE Usage Type over the S6a interface.

dns

Specifes the context where the Domain Name System (DNS) client service is configured for DNS query to select an MSC, P-GW, S-GW, peer SGSN, peer MME or peer AMF for this MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

dns { msc | peer-amf | peer-mme | peer-sgsn | pgw | sgw } [context *ctx_name* **]**
no dns { msc | peer-amf | peer-mme | peer-sgsn | pgw | sgw }

no

Removes a previously specified context having a DNS client service configured for DNS query to select a MSC, peer MME, peer SGSN, peer AMF, P-GW or S-GW with this MME service.

msc

Specifies the context where a DNS client service is configured for DNS queries for selecting a Mobile Switching Center (MSC) for SRVCC.

peer-amf

Specifies the context where a DNS client service is configured for DNS queries for selecting a peer AMF.

peer-mme

Specifies the context where a DNS client service is configured for DNS queries for selecting a peer MME.

peer-sgsn

Specifies the context where a DNS client service is configured for DNS queries for selecting a peer SGSN for inter-RAT handovers.

pgw

Specifies the context where a DNS client service is configured for DNS queries for selecting a P-GW.

sgw

Specifies the context where a DNS client service is configured for DNS queries for selecting an S-GW.

context *ctx_name*

Optionally associates the specific context name where the DNS client service is configured for this MME service. If this keyword is omitted, the DNS client service is configured to use the same context as this MME service.

ctx_name is name of the configured context of the DNS client service expressed as an alphanumeric string of 1 through 79 characters that is case sensitive.

Usage Guidelines

Use this command to specify a pre-configured context where a DNS client service is configured.

The DNS Client service configured in the specified context provides the DNS query support to locate MSCs, peer MMEs, peer-SGSNs, peer-AMFs, P-GWs, or S-GWs for this MME service. For more information on DNS Client service and support, refer to the *DNS Client Service Configuration Mode Commands* chapter.

A maximum of one context can be specified for each keyword.

Example

The following command associates a pre-configured context *dns_ctx1* where a DNS client service is configured for DNS query to MSC for this MME service:

```
dns msc context dns_ctx1
```

The following command associates a pre-configured context *dns_ctx1* where a DNS client service is configured for DNS query to P-GW for this MME service:

```
dns pgw context dns_ctx1
```

The following command associates a pre-configured context *dns_ctx2* where a DNS client service is configured for DNS query to S-GW:

```
dns sgw context dns_ctx2
```

edrx hsfn-reference

This command configures the Hyper SFN synchronization reference time for eDRX.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax

```
edrx hsfn-reference ref_time adjust leap_seconds
no edrx hsfn-reference
```

no

Disables the H-SFN synchronization reference time configuration.

hsfn-reference *ref_time*

Specifies the UTC Time at which H-SFN=0 starts. *ref_time* must be entered in the UTC Time format as follows: **YYYY:MM:DD:hh:mm:ss**. For example: 2016:03:01:12:34:56.

adjust *leap_seconds*

Specifies the number of leap seconds that need to be adjusted. *leap_seconds* must be an integer from 0 to 100.

Usage Guidelines

Use this command to configure the Hyper SFN synchronization reference time for eDRX. This command is disabled by default.

A maximum of 2 H-SFN reference time configuration is allowed. The first configuration will be the latest leap-second adjustment UTC time and the second configuration will be the next or declared leap-second adjustment UTC time.

For example:

Consider the following H-SFN reference time configuration:

```
asr5000(config-mme-service)# edrx hsfn-reference 2017:01:01:00:00:00 adjust 5
```

When the next leap second adjustment is announced with new time **2018:01:01:00:00:00**, MME can be configured any time before 2018:01:01 with the following configuration.

```
asr5000(config-mme-service)# edrx hsfn-reference 2018:01:01:00:00:00 adjust 6
```

When another leap second adjustment is announced with another new time 2018:06:30:00:00:00, MME can be configured any time before 2018:06:30 with the following configuration, and deletes the oldest time reference (2017:01:01) configuration.

```
asr5000(config-mme-service)# no edrx hsfn-reference 2017:01:01:00:00:00
asr5000(config-mme-service)# edrx hsfn-reference 2018:06:30:00:00:00 adjust 7
```

For HSFN-Start in GPS format, the number of leap seconds must be provided from 1980:1:06. For example: at 2017:01:01:00:00:00, the number of leap seconds from 1980:1:06 are 18.

For HSFN-Start in UTC format, the number of leap seconds must be provided from the HSFN-Start time. For example: at 2000:03:01:12:34:5, the number of leap seconds from 2000:03:01:12 are 5.

Example

edrx hsfn-start 2016:03:01:12:34:56

edrx hsfn-start

This command configures the Hyper SFN synchronization start time for eDRX.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax

edrx hsfn-start *start_time* **[gps | utc]**
no edrx hsfn-start

no

Disables the H-SFN synchronization time configuration.

hsfn-start *start_time*

Specifies the time at which H-SFN=0 starts in GPS or UTC format. The UTC time format is **YYYY:MM:DD:hh:mm:ss**. For example: 2016:03:01:12:34:56.

gps | utc

The **gps** and **utc** keywords are optional. If not explicitly provided, then H-SFN=0 starts in UTC format.

- **gps**: Specifies the time at which H-SFN=0 starts in GPS format. GPS time starts from 1980:01:06:00:00:00.

  For example: **edrx hsfn-start 2000:03:01:12:34:56 gps**

- **utc**: Specifies the time at which H-SFN=0 starts in UTC format. UTC time starts from 1972:06:30:00:00:00.

  For example: **edrx hsfn-start 2000:03:01:12:34:56 utc**

- After the HSFN-start configuration, the HSFN-reference can be configured to adjust the leap seconds.

Usage Guidelines Use this command to configure the Hyper SFN synchronization start time for eDRX in GPS or UTC format.

Example

The following command configures the HSFN start time **2016:03:01:12:34:56** in UTC format:

```
edrx hsfn-start 2016:03:01:12:34:56
```

The following command configures the HSFN start time **2016:03:01:12:34:56** in GPS format:

```
edrx hsfn-start 2016:03:01:12:34:56 gps
```

emm

Defines the Evolved Mobility Management timer parameters, such as timeout durations for timers and retransmission counts, for Non-Access Stratum (NAS) message retransmission in MME service.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
emm { implicit-detach-timeout detach_dur | mobile-reachable-timeout
mob_reach_durmt-queue-timeout mtq_timer |  | t3346-timeout t3346_dur |
t3412-extended-timeout t3412_ext_dur | t3412-timeout t3412_dur | t3413-timeout
 t3413_dur | t3415-timeout t3415_dur | t3422-timeout t3422_dur | t3423-timeout
 t3423_dur | t3450-timeout t3450_dur | t3460-timeout t3460_dur | t3470-timeout
 t3470_dur | tc1n-timeout tc1n_timer | tr1n-timeout tr1n_timer | tr2n-timeout
tr1n_timer }
default emm { implicit-detach-timeout | mobile-reachable-timeout |
mt-queue-timeout | t3346-timeout | t3412-extended-timeout | t3412-timeout
 | t3413-timeout | t3415-timeout| t3422-timeout | t3423-timeout |
t3450-timeout | t3460-timeout | t3470-timeout | tc1n-timeout | tr1n-timeout
 | tr2n-timeout }
```

default

Resets the specified timer timeout to the system default value.

implicit-detach-timeout *detach_dur*

Sets the timer timeout duration (in seconds) after which subscriber will implicitly detached from the network if there is no activity. Generally this timer value is 240 seconds (4 minutes) more than the timeout value of the T3423 timer.

This timer starts when mobile reachable timer expires while the network is in EMM-IDLE mode and stops when a NAS signalling connection established.

detach_dur is an integer from 1 through 12000. Default: 3480

mobile-reachable-timeout *mob_reach_dur*

Sets the timeout timer duration (in seconds) after which reachability procedure will be discarded and reattempt starts.

mob_reach_dur is an integer from 1 through 12000. Default: 3480

mt-queue-timeout *mtq_timer*

Configures the timer to hold MT SMS in MT queue. MT SMS will be present in the queue while the previous SMS is being processed. The timer expiry will return error to SMSC for an absent subscriber.

mtq_timer specifies the timeout in seconds, as an integer from 1 to 300. Default: 30 seconds

t3346-timeout *t3346_dur*

Sets the EMM backoff timer duration (in seconds). If an EMM request is rejected by MME because of congestion, it shall have EMM cause as congestion (#22) and shall include back-off timer (T3346) IE. The back-off timer shall be chosen randomly and shall be 10% below or above the configured T3346 timer value.

t3346_dur is an integer from 0 through 11160 (0-186 minutes). Default: 1500 seconds (25 minutes).

While storing this back-off timer expiry time, the MME shall adjust the mobile reachability timer and/or implicit detach timer. This is to make sure that the sum of the mobile reachability timer + implicit detach timer is greater than the back-off timer duration.

The MME will store the DB for at least the EMM back-off timer duration even if the attach is rejected because of congestion. The MME will not start any timer for EMM back-off. Instead, back-off timer expiry time will be stored in the DB as the DB is stored for at least back-off timer duration.

If an EMM call is rejected due to congestion control for EMM, the DB created during ULA will not be cleared and the purge timer will be started for a time period 10% greater than the back-off timer duration. This is done to make sure that DB is available during back-off timer duration to reject any requests during this period and also to avoid the HSS signaling again if the UE comes back immediately after the back-off timer duration.

The MME will not reject any requests related to handovers as part of this feature even if EMM back-off timer is running.

The MME will drop attach requests received during congestion while EMM back-off timer is running based on configuration in congestion-action-profile. For example, if configuration is enabled to reject new call only when low priority indication is set and the UE comes without low priority indication while back off timer is running, the MME will accept the new call attempt from the UE.

The MME will not reject/drop attach requests received even if EMM back-off timer is running if the congestion gets cleared.

The MME will forward SGS paging requests received from MSC for a UE attached in MME even if back-off timer is running.

t3412-extended-timeout *t3412_ext_dur*

Sets the extended periodic TAU timer duration (in seconds), enabling the Operator to configure longer values for the periodic TAU timer and Mobile Reachable timer. This helps the MME to reduce network load from periodic TAU signaling and to increase the time until the UE detects a potential need for changing the RAT or PLMN.

t3412_ext_dur is an integer from 0 through 1116000 (0-186 minutes). Default: 3600 seconds (60 minutes).

The UE must include the "MS network feature support" IE in the Attach Request/TAU Request. This IE indicates to the MME that the UE supports the extended periodic timer T3412, in which case the MME sends the extended-3412 IE in the Attach/TAU response. The MME will not forward the extended-T3412 timer value to any UE which has not indicated that it supports this extended-t3412 timer.

The MME supports storing the Subscribed-Periodic-RAU-TAU-Timer value if received as part of subscription data, and deleting this stored value if the corresponding withdrawal flag is received in the DSR command.

For homers, the MME will send the extended-3412 IE value as received in Subscribed-Periodic-RAU-TAU-Timer IE in subscription data.

For roamers, the MME takes the presence of Subscribed-Periodic-RAU-TAU-Timer IE in subscription data as an indication and shall send the extended-3412 IE with the value from the local configuration.

The MME adjusts the configured mobile reachability timer value if the subscribed extended-3412 timer value received from HSS is greater than the sum of the mobile reachability timer + implicit detach timer such that the extended-3412 timer value becomes 10% less than the mobile reachability timer + implicit detach timer.

Refer to 3GPP TS 23.401 Section 4.3.17.3 (Version 10.4.0) and 29.272 for more details.

t3412-timeout *t3412_dur*

Sets the timeout duration (in seconds) for the T3412 timer. This timer is used for periodic tracking area update (P-TAU). When this timer expires, the periodic tracking area updating procedure starts and the timer is set to its initial value for the next start.

This timer starts when the UE goes from EMM-CONNECTED to EMM-IDLE mode and stops when the UE enters EMM-CONNECTED mode.

t3412_dur is an integer from 1 through 11160. Default: 3240

t3413-timeout *t3413_dur*

Sets the timeout duration (in seconds) for the T3413 timer. The timer starts when MME initiates the EPS paging procedure to the EMM entity in the network and requests the lower layer to start paging. This timer stops for the paging procedure when a response received from the UE.

t3413_dur is an integer from 1 through 20. Default: 6

t3415-timeout *t3415_dur*

The keyword **t3415-timeout** *t3415_dur* is used to configure the T3415 paging timeout value. The *t3415_dur* is an integer value in the range 1 up to 20 seconds. The default value is 6 seconds.

t3422-timeout *t3422_dur*

Sets the timeout duration (in seconds) for the T3422 timer. This timer starts when MME initiates the detach procedure by sending a DETACH REQUEST message to the UE and stops upon receipt of the DETACH ACCEPT message.

t3422_dur is tan integer from 1 through 20. Default: 6

t3423-timeout *t3423_dur*

Sets the timeout duration (in seconds) for the T3423 timer. This timer starts when UE enters the EMM-DEREGISTERED state or when entering EMM-CONNECTED mode. It stops while the UE is in EMM-REGISTERED.NO-CELL-AVAILABLE state and Idle mode Signalling Reduction (ISR) is activated.

t3423_dur is an integer from 1 through 11160. Default: 3240

t3450-timeout *t3450_dur*

Sets the timeout duration (in seconds) for the T3450 timer. This timer starts when MME initiates the Globally Unique Temporary Identifier (GUTI) reallocation procedure by sending a GUTI REALLOCATION COMMAND message to the UE and stops upon receipt of the GUTI REALLOCATION COMPLETE message.

This timer is also used for the Tracking Area update procedure.

t3450_dur is an integer from 1 through 20. Default: 6

t3460-timeout *t3460_dur*

Sets the timeout duration (in seconds) for the T3460 timer. This timer starts when the network initiates the authentication procedure by sending an AUTHENTICATION REQUEST message to the UE and stops upon receipt of the AUTHENTICATION RESPONSE message.

t3460_dur is an integer from 1 through 20. Default: 6

t3470-timeout *t3470_dur*

Sets the timeout duration (in seconds) for the T3470 timer. The MME starts this timer when the network initiates the identification procedure by sending an IDENTITY REQUEST message to the UE and stops upon receipt of the IDENTITY RESPONSE message.

t3470_dur is an integer from 1 through 20. Default: 6

tc1n-timeout *tc1n_timer*

Configures the retransmission timer to send CP SMS data to UE for MO/MT scenario.

tc1n_timer specifies the timeout in seconds, as an integer from 1 to 20. Default: 30 seconds

tr1n-timeout *tr1n_timer*

Configures the wait time to receive RP-Ack from UE for MT SMS, before sending error to SMSC.

tr1n_timer specifies the timeout in seconds, as an integer from 1 to 300. Default: 30 seconds

tr2n-timeout *tr2n_timer*

Configures the wait time to send RP-Ack to UE for MO SMS, before sending protocol error to UE.

tr2n_timer specifies the timeout in seconds, as an integer from 1 to 300. Default: 30 seconds

Usage Guidelines

Use this command to set EMM timers.

The following tables describe the triggers and states for timers:

Table 1: EPS Mobility Management Timers – UE Side

Timer	State	Cause of Start	Normal Stop	On Expiry
T3402	• EMM-DEREGISTERED • EMM-REGISTERED	• At attach failure and the attempt counter is equal to 5. • At tracking area updating failure and the attempt counter is equal to 5.	• ATTACH REQUEST sent • TRACKING AREA UPDATE REQUEST sent	Initiation of the at procedure or TAU procedure
T3410	EMM-REGISTERED-INITIATED	ATTACH REQUEST sent	• ATTACH ACCEPT received • ATTACH REJECT received	Start T3411 or T3 as described in subclause 5.5.1.2.
T3411	• EMM-DEREGISTERED. ATTEMPTING-TO-ATTACH • EMM-REGISTERED. ATTEMPTING-TO-UPDATE	• At attach failure due to lower layer failure, T3410 timeout or attach rejected with other EMM cause values than those treated in subclause 5.5.1.2.5. • At tracking area updating failure due to lower layer failure, T3430 timeout or TAU rejected with other EMM cause values than those treated in subclause 5.5.3.2.5.	• ATTACH REQUEST sent • TRACKING AREA UPDATE REQUEST sent	Retransmission o ATTACH REQUI or TRACKING A UPDATE REQUI
T3412	EMM-REGISTERED	In EMM-REGISTERED, when EMM-CONNECTED mode is left.	• When entering state EMM-DE-REGISTERED or • When entering EMM-CONNECTED mode.	Initiation of the periodic TAU procedure

Timer	State	Cause of Start	Normal Stop	On Expiry
T3416	• EMM-REGISTERED-INITIATED • EMM-REGISTERED • EMM-DEREGISTERED-INITIATED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-SERVICE-REQUEST-INITIATED	RAND and RES stored as a result of a UMTS authentication challenge	• SECURITY MODE COMMAND received • SERVICE REJECT received • TRACKING AREA UPDATE ACCEPT received • AUTHENTI-CATION REJECT received • AUTHENTI-CATION FAILURE sent • EMM-DE-REGISTERED or EMM-NULL entered	Delete the sto RAND and R
T3417	EMM-SERVICE-REQUEST-INITIATED	• SERVICE REQUEST sent • EXTENDED SERVICE REQUEST sent in case f and g in subclause 5.6.1.1	• Bearers have been set up • SERVICE REJECT received	Abort the proc

Timer	State	Cause of Start	Normal Stop	On Expiry
T3417ext	EMM-SERVICE-REQUEST-INITIATED	• EXTENDED SERVICE REQUEST sent in case d in subclause 5.6.1.1 • EXTENDED SERVICE REQUEST sent in case e in subclause 5.6.1.1 and the CSFB response was set to "CS fallback accepted by the UE".	• Inter-system change from S1 mode to A/Gb mode or Iu mode is completed • Inter-system change from S1 mode to A/Gb mode or Iu mode is failed • SERVICE REJECT received	Abort the procedu
T3418	• EMM-REGISTERED-INITIATED • EMM-REGISTERED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-DEREGISTERED-INITIATED • EMM-SERVICE-REQUEST-INITIATED	AUTHENTICATION FAILURE (EMM cause = #20 "MAC failure" or #26 "Non-EPS authentication unacceptable") sent	AUTHENTICATION REQUEST received	On first expiry, th should consider t network as false

Timer	State	Cause of Start	Normal Stop	On Expiry
T3420	• EMM-REGISTERED-INITIATED • EMM-REGISTERED • EMM-DEREGISTERED-INITIATED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-SERVICE-REQUEST-INITIATED	AUTHENTICATION FAILURE (cause = #21 "synch failure") sent	AUTHENTICATION REQUEST received	On first expiry should consid network as fal
T3421	EMM-DEREGISTERED-INITIATED	DETACH REQUEST sent	DETACH ACCEPT received	Retransmissio DETACH RE
T3423	EMM-REGISTERED	T3412 expires while the UE is in EMM-REGISTERED. NO-CELL-AVAILABLE and ISR is activated.	• When entering state EMM-DE-REGISTERED or • When entering EMM-CONNECTED mode.	Set TIN to "P-

Timer	State	Cause of Start	Normal Stop	On Expiry
T3430	EMM-TRACKING-AREA-UPDATING-INITIATED	TRACKING AREA UPDATE REQUEST sent	• TRACKING AREA UPDATE ACCEPT received • TRACKING AREA UPDATE REJECT received	Start T3411 or T3 as described in subclause 5.5.3.2.
T3440	• EMM-REGISTERED-INITIATED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-DEREGISTERED-INITIATED • EMM-SERVICE-REQUEST-INITIATED • EMM-REGISTERED	• ATTACH REJECT, DETACH REQUEST, TRACKING AREA UPDATE REJECT with any of the EMM cause values #11, #12, #13, #14 or #15 • SERVICE REJECT received with any of the EMM cause values #11, #12, #13 or #15 • TRACKING AREA UPDATE ACCEPT received after the UE sent TRACKING AREA UPDATE REQUEST in EMM-IDLE mode with no "active" flag	• Signalling connection released • Bearers have been set up	Release the signa connection and proceed as descril in subclause 5.3.1
T3442	EMM-REGISTERED	SERVICE REJECT received with EMM cause #39	TRACKING AREA UPDATE REQUEST sent	None
NOTE 1: The default value of this timer is used if the network does not indicate another value in an EMM signalling proce				
NOTE 2: The value of this timer is provided by the network operator during the attach and tracking area updating proced				
NOTE 3: The value of this timer may be provided by the network in the ATTACH ACCEPT message and TRACKING A UPDATE ACCEPT message. The default value of this timer is identical to the value of T3412.				
NOTE 4: The value of this timer is provided by the network operator when a service request for CS fallback is rejected b network with EMM cause #39 "CS domain temporarily not available".				

Table 2: EPS Mobility Management Timers – Network Side

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2 4th EXPIRY (N
T3413	EMM-REGISTERED	Paging procedure initiated	Paging procedure completed	Network depe
T3422	EMM-DEREGISTERED-INITIATED	DETACH REQUEST sent	DETACH ACCEPT received	Retransmissio DETACH RE
T3450	EMM-COMMON-PROC-INIT	• ATTACH ACCEPT sent • TRACKING AREA UPDATE ACCEPT sent with GUTI • GUTI REALLOCATION COMMAND sent	• ATTACH COMPLETE received • TRACKING AREA UPDATE COMPLETE received • GUTI RE-ALLOCATION COMPLETE received	Retransmissio same message ATTACH AC TRACKING UPDATE AC GUTI REALLOCAT COMMAND
T3460	EMM-COMMON-PROC-INIT	• AUTHENTICATION REQUEST sent • SECURITY MODE COMMAND sent	• AUTHENTI-CATION RESPONSE received • AUTHENTI-CATION FAILURE received • SECURITY MODE COMPLETE received • SECURITY MODE REJECT received	Retransmissio same message AUTHENTIC REQUEST or SECURITY MODE COMMAND

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 4th EXPIRY (NOTE
T3470	EMM-COMMON-PROC-INIT	IDENTITY REQUEST sent	IDENTITY RESPONSE received	Retransmission of IDENTITY REQU
Mobile reachable timer	All except EMM-DEREGISTERED	Entering EMM-IDLE mode	NAS signalling connection established	Network depende but typically pagi halted on 1st expi
Implicit detach timer	All except EMM-DEREGISTERED	The mobile reachable timer expires while the network is in EMM-IDLE mode and ISR is activated	NAS signalling connection established	Implicitly detach UE on 1st expiry
T3415	EMM- REGISTERED	In EMM-REGISTERED state, when paging is triggered for eDRX enabled UE in EMM-IDLE mode.	When the UE enters the EMM-CONNECTED mode by SERVICE REQUEST or a PERIODIC TAU procedure.	Abort the paging procedure
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.				
NOTE 2: The value of this timer is network dependent.				

Table 3: EPS Session Management Timers – UE Side

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 4th EXPIRY (NOTE
T3480	PROCEDURE TRANSACTION PENDING	BEARER RESOURCE ALLOCATION REQUEST sent	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE ALLOCATION REJECT received	Retransmission of BEARER RESOU ALLOCATION REQUEST
T3481	PROCEDURE TRANSACTION PENDING	BEARER RESOURCE MODIFICATION REQUEST sent	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or DEACTIVATE EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE MODIFICATION REJECT received	Retransmission of BEARER RESOU MODIFICATION REQUEST

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2 4th EXPIRY (N
T3482	PROCEDURE TRANSACTION PENDING	An additional PDN connection is requested by the UE which is not combined in attach procedure	ACTIVE DEFAULT EPS BEARER CONTEXT REQUEST received or PDN CONNECTIVITY REJECT received	Retransmissio PDN CONNECTIV REQUEST
T3492	PROCEDURE TRANSACTION PENDING	PDN DISCONNECT REQUEST sent	DEACTIVATE EPS BEARER CONTEXT REQUEST received or PDN DISCONNECT REJECT received	Retransmissio PDN DISCON REQUEST
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in t corresponding procedure description.				

This command can be repeated to set each timer as needed.

The retransmission of all type of NAS messages can be configured through **nas-max-retransmissions** command.

Example

The following command sets the timeout value for EPS paging procedure timer T3413 for *10* seconds.

```
emm t3413-timeout 10
```

enb-cache-timeout

Configures the amount of time that eNodeB information is stored in cache after the eNodeB terminates the connection.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

enb-cache-timeout *min*
default enb-cache-timeout

default

Returns the command to its default value of 10.

min

Specifies the amount of time (in minutes) that the MME stores eNodeB information after the eNodeB terminates the connection. *min* is an integer value from 1 through 1440. Default: 10

Usage Guidelines

Use this command to set the amount of time the MME stores eNodeB information in cache after the eNodeB terminates the connection.

Example

The following command sets the amount of time the MME stores eNodeB information to *15* minutes:

```
enb-cache-timeout 15
```

encryption-algorithm-lte

Configures the precedence for LTE encryption algorithms to use for security procedures through this MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
encryption-algorithm-lte priority1 { 128-eea0 | 128-eea1 | 128-eea2 |
128-eea3 } [ priority2 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ] [
 priority3 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ] [ priority4 {
 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ]
default encryption-algorithm-lte
```

default

Removes the preconfigured encryption algorithm and sets the default LTE encryption algorithm for security procedures with configured priority. The lowest value has the highest preference.

The default configuration of LTE encryption algorithm is:

- priority1 with 128-eea0 encryption algorithm
- priority2 with 128-eea1 encryption algorithm
- priority3 with 128-eea2 encryption algorithm

priority1

Specifies the preference of encryption algorithm for security procedures on this MME service as priority 1.

priority2

Specifies the preference of encryption algorithm for security procedures on this MME service as priority 2.

priority3

Specifies the preference of encryption algorithm for security procedures on this MME service as priority 3.

priority4

Specifies the preference of encryption algorithm for security procedures on this MME service as priority 4.

128-eea0

Sets the Null ciphering algorithm (128-EEA0) for LTE encryption as the encryption algorithm for security procedures.

Default: priority1

128-eea1

Sets the SNOW 3G synchronous stream ciphering algorithm (128-EEA1) for LTE encryption as the encryption algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2.

Default: priority2

128-eea2

Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures.

Default: priority3

128-eea3

Sets the ZUC algorithm (128-EEA3) for LTE encryption as the encryption algorithm for security procedures.

Default: priority4

Usage Guidelines

Use this command to set the LTE encryption algorithms for security procedures to use with this MME service.

Caution When this command is executed, all the existing priority-to-algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

Caution Configuration of the same algorithm to multiple priorities is prohibited.

Example

The following command sets the 128-EEA1 as the LTE encryption algorithm with priority 2 for security procedures with an MME service:

```
encryption-algorithm-lte priority2 128-eea1
```

esm

Defines the Evolved Session Management timer parameters like timeout durations for timers and retransmission counts for the retransmission of Non-Access Stratum (NAS) messages in MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

esm { t3396-timeout *t3396_dur* **| t3485-timeout** *t3485_dur* **| t3486-timeout** *t3486_dur* **| t3489-timeout** *t3489_dur* **| t3495-timeout** *t3495_dur* **}**
default esm { t3396-timeout | t3485-timeout | t3486-timeout | t3489-timeout | t3495-timeout }

default

Resets the specified Evolved Session Management timer timeout to the system default value.

t3396-timeout *t3396_dur*

Sets the ESM backoff timer duration (in seconds). If an ESM request is rejected because of congestion, the reject will have ESM cause "Insufficient resources" and will include a back-off timer IE (T3396). This back-off timer is chosen randomly and will be 10% below or above the configured T3396 timer value.

t3396_dur is an integer from 0 through 11160 (0-186 minutes). Default: 1500 seconds (25 minutes).

The MME will not start any timer for SM back-off, nor store the SM back-off timer expiry time. If an SM request is received and if congestion exists, the request would be rejected based and a new random value will be sent as the ESM back-off timer value.

The MME will reject any subsequent requests from the UE targeting to the same APN based on the presence of congestion at that time and not based on the SM back-off time previously sent to the UE.

If the ESM cause value is #26 "insufficient resources" or #27 "missing or unknown APN", the MME will include a value for timer T3396 in the reject message. If the ESM cause value is #26 "insufficient resources" and the request message was sent by a UE accessing the network with access class 11 - 15 or if the request type in the PDN CONNECTIVITY REQUEST message was set to "emergency", the MME will not include a value for timer T3396.

t3485-timeout *t3485_dur*

Sets the timeout duration (in seconds) for the T3485 timer. This timer is used by the default EPS bearer context activation procedure.

This timer starts when the MME sends an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message to UE and stops when receives ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT or ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message from UE.

t3485_dur is an integer from 1 through 60. Default: 8

t3486-timeout *t3486_dur*

Sets the timeout duration (in seconds) for theT3486 timer. This timer is used by the default EPS bearer context modification procedure.

This timer starts when the MME sends a MODIFY EPS BEARER CONTEXT REQUEST message to the UE and stops when it receives a MODIFY EPS BEARER CONTEXT ACCEPT received or a MODIFY EPS BEARER CONTEXT REJECT message from UE.

t3485_dur is an integer from 1 through 60. Default: 8

t3489-timeout *t3489_dur*

Sets the timeout duration (in seconds) for the T3489 timer. This timer is used for the default EPS bearer context deactivation procedure.

This timer starts when the MME sends an ESM INFORMATION REQUEST message to the UE and stops when receives a ESM INFORMATION RESPONSE message from the UE.

t3495_dur is an integer from 1 through 60. Default: 4

t3495-timeout *t3495_dur*

Sets the timeout duration (in seconds) for the T3495 timer. This timer is used for default EPS bearer context deactivation procedure.

This timer starts when the MME sends a DEACTIVATE EPS BEARER CONTEXT REQUEST message to UE and stops when receives DEACTIVATE EPS BEARER CONTEXT ACCEPT or DEACTIVATE EPS BEARER CONTEXT REJECT message from UE.

t3495_dur is tan integer from 1 through 60. Default: 8

Usage Guidelines

Use this command to set Evolved Session Management timers.

The following tables describe the triggers and states for timers:

Table 4: EPS Session Management Timers – Network Side

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 4th EXPIRY (NOTE
T3485	BEARER CONTEXT ACTIVE PENDING	• ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST sent • ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST sent	• ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT received or • ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT received or • ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT received or • ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT received	Retransmission of same message
T3486	BEARER CONTEXT MODIFY PENDING	MODIFY EPS BEARER CONTEXT REQUEST sent	• MODIFY EPS BEARER CONTEXT ACCEPT received or • MODIFY EPS BEARER CONTEXT REJECT received	Retransmission of MODIFY EPS BEARER CONTI REQUEST
T3489	PROCEDURE TRANSACTION PENDING	ESM INFORMATION REQUEST sent	ESM INFORMATION RESPONSE received	Retransmission of ESM INFORMAT REQUEST on 1st 2nd expiry only
T3495	BEARER CONTEXT INACTIVE PENDING	DEACTIVATE EPS BEARER CONTEXT REQUEST sent	DEACTIVATE EPS BEARER CONTEXT ACCEPT received	Retransmission of DEACTIVATE EI BEARER CONTI REQUEST
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.				

This command can be repeated to set each timer as needed.

The retransmission of all type of NAS messages can be configured through **nas-max-retransmissions** command.

Example

The following command sets the timeout value for the default EPS bearer context activation procedure timer (T3485) for 10 seconds.

```
esm t3485-timeout 10
```

gtpv2

Configures GTPv2 piggybacking support from the MME to the P-GW. A piggybacking flag is sent by the MME to a P-GW in the S11 "Create Session Request" message and determines whether dedicated bearer creation (Create Bearer Request) is piggybacked onto the "Create Session Response" message or not.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] gtpv2 piggybacking`

default

Returns the command to its default setting of enabled.

no

Disables the feature.

piggybacking

Specifies that piggybacking is to be performed by the P-GW.

Usage Guidelines

Use this command to enable the sending of a piggybacking flag to the P-GW over the S11 interface requesting that the Create Bearer Request message is piggybacked on the Create Session Response message (sent from the P-GW to the MME.

Example

The following command disables this feature:

`no gtpv2 piggybacking`

henbgw henb-type

Configures the target HeNB type (home or macro or both) behind HeNBGW. Based on this configuration, MME allows TAI-based lookup of target eNB, if target eNB ID is not found by MME during handover.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
henbgw henb-type { all | home-enb | macro-enb }
no henbgw henb-type
```

no

Removes the existing configuration, if previously configured. By default, when the **henbgw henb-type** command is not executed explicitly, target eNB type is set as home-enb.

henb-type { all | home-enb | macro-enb }

Configures HeNB type. TAI-based lookup depends on HeNB type.

- **all**: Configures HeNB type both macro-enb (20-bits) and home-enb (28-bits).
- **home-enb**: Configures HeNB type home-enb (28-bits). This is the default keyword.
- **macro-enb**: Configures HeNB type macro-enb (20-bits).

Usage Guidelines

Use this command to configure the target eNB type or target henb-type. Based on this configuration, MME allows TAI-based lookup of target eNB, if target eNB ID is not found by MME during handover. By default, TAI-based lookup is performed only for home-eNB ID with 28-bits.

Important The target eNB type configuration is effective only when the **henbgw henb-type** CLI command is configured within mme-service and the HeNBGW-mgmt-db is associated with HeNBGWs inside mme-service.

For detailed information on TAI-based routing feature, refer to the *MME Administration Guide*.

Example

The following command sets the target HeNB type as home-enb with 28-bits.

```
henbgw henb-type home-enb
```

henbgw selection

Configures HeNBGW selection using HeNB MSB 10 bits for the same TAI.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

henbgw selection msb-10-bits
no henbgw selection

no

Removes the configured HeNBGW selection for same TAI.

henbgw selection msb-10-bits

Configures HeNBGW selection using HeNB MSB 10 bits for the same TAI.

- **henbgw**: Configures HeNBGW options.
- **selection**: Configures HeNBGW selection for same TAI.
- **msb-10-bits** Configures HeNBGW selection using HeNB MSB 10 bits for same TAI. By default this is disabled.

Important HeNBGW selection using HeNB MSB 10 bits is performed only when TAIs are shared across multiple HeNBGWs.

Example

Following command configures HeNBGW selection using HeNB MSB 10 bits for the same TAI.

henbgw selection msb-10-bits

heuristic-paging

Enables or disables the heuristic or optimized paging feature for the service.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] heuristic-paging [paging-map *paging_map_name* **]**

default

Returns the command to its default setting of disabled.

no

Disables the feature.

paging-map *paging_map_name*

Specifies the paging-map to be associated with this MME service. This keyword is only supported in Release 14.0 and higher.

Usage Guidelines

Caution The paging profiles need to be configured prior to configuring TAI management objects (tai-mgmt-db and tai-mgmt-obj). Otherwise, the configuration would lead to high paging load in the MME node, at peak traffic time, causing service outage

Use this command to enable or disable the heuristic paging feature for the service. Also known as idle-mode paging, enabling this feature prompts the MME service to keep track of the eNodeBs to which the access terminal (AT) most commonly attaches, thus reducing the signalling otherwise associated with continuous paging.

If no paging-map is associated when this command is issued, the default heuristic paging behavior is used (as opposed to intelligent paging behavior).

Refer to the *Heuristic and Intelligent Paging* chapter in the *MME Administration Guide* for more information about this command.

Important Heuristic (optimized) Paging is a licensed feature and will not appear as a command option unless the proper licensed is installed.

ho-resource-release-timeout

Configures the timer that is started when the source MME initiates a handover.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

ho-resource-release-timeout *timeout*
default ho-resource-release-timeout

default

Returns the command to the default setting of 5000 milliseconds.

timeout

Specifies the time in milliseconds that the MME will hold on to bearers and E-RABs after an S1-based handover has been initiated.

timeout must be an integer from 500 through 15000.

Default: 5000.

Usage Guidelines

Use this command to configure the amount of time in milliseconds that the MME will hold on to bearers and E-RABs after an S1-based handover has been initiated. When this timer expires, the source MME will send a UE Context Release to the source eNodeB. Refer to 3GPP TS 23.401 Section 5.5.1.2.2 for additional information about the use of this timer.

Example

The following command configures the timer for 10000 milliseconds (10 seconds).

ho-resource-release-timeout 10000

integrity-algorithm-lte

Configures the precedence of LTE integrity algorithms to use for security procedures through this MME service. By default the integrity algorithm is enabled on MME service and cannot be disabled.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-mme-service)#

Syntax Description

integrity-algorithm-lte priority1 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } [priority2 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 }] [priority3 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 }] [priority4 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 }]
default integrity-algorithm-lte

default

Removes the preconfigured integrity algorithm and sets the default LTE integrity algorithm for security procedures.

The default configuration of LTE integrity algorithm is:

- priority1 with 128-eia0 integrity algorithm
- priority2 with 128-eia1 integrity algorithm
- priority3 with 128-eia2 integrity algorithm

priority1

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 1.

This is the mandatory and default priority keyword.

priority2

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 2.

priority3

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 3.

priority4

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 4.

128-eia0

Sets the Null ciphering algorithm (128-EIA0) for LTE integrity as the integrity algorithm for security procedures.

Default: priority1

128-eia1

Sets the SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2.

Default: priority2

128-eia2

Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE integrity as the integrity algorithm for security procedures.

Default: priority3

128-eia3

Sets the ZUC algorithm (128-EIA3) for LTE integrity as the integrity algorithm for security procedures.

Default: priority4

Usage Guidelines Use this command to set the LTE integrity algorithms for security procedures to use with this MME service.

Caution Integrity algorithm is a mandatory aspect and cannot be disabled in MME service.

Caution When this command is executed, all the existing priority-to-algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

Caution Configuration of the same algorithm to multiple priorities is prohibited.

Example

The following command sets the AES ciphering algorithms (128-EIA2) as the LTE integrity algorithm with priority as *1* for security procedures with an MME service:

```
integrity-algorithm-lte priority1 128-eia2
```

inter-rat-nnsf

Configures an NNSF (NAS Node Selection Functionality) entry to define a list of Served MMECs (MME codes) that is indicated to the eNodeB in the S1 Setup Response. This optional configuration is used to aid the eNodeB when selecting the MME for inter-rat handovers when the MME is co-located with an SGSN.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

inter-rat-nnsf collocated-mme plmn-id mcc *mcc_value* **mnc** *mnc_value* **group-id** *mme_group_id* **{ mme-codes** *mmec* **| mme-code-range** *first_mme_code* **to** *last_mme_code* **}**
no inter-rat-nnsf collocated-mme plmn-id mcc *mcc_value* **mnc** *mnc_value* **group-id** *mme_group_id*

no

Removes the specified NNSF entry.

collocated-mme

Specifies that the MME is co-located with an SGSN.

plmn-id mcc *mcc_value* mnc *mnc_value*

Specifies the PLMN-ID for this MME service.

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

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

group-id *mme_group_id*

Configures the group id for this MME service.

mme_group_id must be an integer value from 0 through 65536.

mme-codes *mmec*

Configures a list of MMEC (MME codes) to be used.

mmec: must be entered as a series of codes, each separated by a space, such as: 10 25 102 103 105. Each code must be an integer from 0 through 255.

A maximum of 16 MME Codes are allowed to be configured per inter-rat-nnsf entry.

mme-code-range *first_mme_code* to *last_mme_code*

Configures a range of MMEC (MME codes) to be used. Identify an unlimited number of MME codes, for a particular PLMN-ID and Group-ID combination, as part of a range of MME codes.

first_mme_code: must be the first MME code in the range and it must be an integer from 0 through 255.

last_mme_code: must be the last MME code in the range and it must be an integer from 0 through 255 and it must be an integer greater than the value entered for the *first_mme_code*.

Usage Guidelines

Use this command to indicate a list of served MMECs, in addition to the one assigned to the MME service. The complete list shall be notified to the eNodeB as Served MMECs in the S1 Setup Response. This would aid the eNodeB in selecting a co-located MME during 2G/3G to 4G handovers.

When a UE moves from 2G/3G to 4G, selecting a co-located MME is not possible without some explicit configuration. In this scenario, the entire second Most-Significant-Byte of P-TMSI is copied into the MME-Code (MMEC) field. Depending on the NRI length, this could result in 'n' different MMEC values for the same NRI value. For example:

- NRI length = 6 bits
- NRI value = 5 (Binary 00 0101)
- Possible MMECs: Binary 00 0101 xx -> {20, 21, 22, 23}

Selecting a co-located MME is only possible if the eNodeB knows that any UE meant for the above set of MMECs should be directed to a given MME. This command enables the operator to specify MMECs that can possibly be mapped from a given NRI value.

A maximum of 16 MME Codes are allowed to be configured per inter-rat-nnsf entry. This allows 4 SGSNs with NRI length of 6, or 2 SGSNs with NRI length of 5. If more than 16 MMECs are required, an alternative is to pick a dummy MME-Group-ID value and create a new nnsf-entry. The Serving MME-Group-ID could also be used for this purpose as MME-Group-Id has no significance during MME node selection.

A Maximum of 32 inter-rat-nnsf entries are allowed. Regardless of the maximum entries configured, the maximum limits placed by S1AP stack take precedence. For example, if the number of plmns configured under 'network-sharing' and 'inter-rat-nnsf' exceeds the maxnoofPLMNsPerMME(32) limit set by S1AP-S1-Setup-Response, then inter-rat-nnsf entries that exceed the limit(32) do not get included in the S1 Setup Response message.

Example

For NRI length = 6; NRI Value = 10 (Binary: 00 1010), when a UE moves from 2G/3G to 4G and maps MME Code (8 bits) from P-TMSI, the MME Code value could be:

- Binary: 00 1010 xx, where xx can be binary 10 or 01 or 00 or 11
- Decimal: 40 or 41 or 42 or 43

So, all of the above values should be configured as MMECs as part of **inter-rat-nnsf**, as follows:

```
inter-rat-nnsf collocated-mme plmn-id mcc 121 mnc 102 mme-id group-id
32000 mme-codes 40 41 42 43
```

When updating an existing NNSF entry, any new MMECs must be included with the existing MMECs. For example, to add additional MMECs (48 49 50 51) to the above command, enter the entire command again as follows:

```
inter-rat-nnsf collocated-mme plmn-id mcc 121 mnc 102 mme-id group-id
32000 mme-codes 40 41 42 43 48 49 50 51
```

isda

This command specifies/selects the Insert Subscriber Data Answer sent to the HSS.

Product

MME

Privilege

Administrator.

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax

```
isda loc-validity-timeout timer_value
[ no ] isda loc-validity
```

no

Disables the ISDA location validity configuration.

loc-validity-timeout *timer_value*

Specifies the expiry time for the age of the UE's location information. During this time, if the EPS Location Information with current location is requested in the ISDR, the MME does not process a location procedure with the eNodeB, but sends the location information from the cache.

The *timer_value* specifies the amount of time in seconds. The timer is an integer value that ranges from 1 to 1000 seconds.

Usage Guidelines Use this command to allow MME to immediately send the cached location information through the IDA within a configured time.

Example

isda loc-validity-timeout 200

isda-guard-timeout

Sets the number of seconds for the Insert Subscription Data Answer (ISDA) guard timer. The time the MME waits for current location information for the UE. If the current location is not learned before expiry, because there is no paging response or location reporting control from the eNB, then the MME sends the ISDA with the last-known location upon expiry of this timer.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **`[ no ] isda-guard-timeout`** *`seconds`*

no

Disables any configuration for this timer and resets the wait time to the default of 25 seconds.

seconds

Enter an integer from 1 to 100.

Usage Guidelines With this command, the operator can configure the ISDA guard timer to any value from 1 to 100 seconds. Upon expiry of this wait timer, the MME sends the ISDA with the last-known location of the UE if the MME receives the Insert Subscriber Data Response (ISDR) with both the location flags set (current and last-known locations). Only when the ISDR is received, with both flags set, is the ISDA guard timer started. In situations where the MME receives the ISDR with only the last-known location flag set, then the MME immediately sends the ISDA with location information - no delay and this timer is not started even if configured.

When the ISDA guard timer expires, the paging procedure does not stop until the page timer expires but the MME ignores the paging timer and sends the ISDA with the last-known location if the ISDR was received with both location flags set and the UE is in EMM-idle mode.

While the MME is serving the ISDR (where both location flags are set) from the HSS, if the HSS tries to send another similar request then the MME responds to the HSS with DIAMETER_UNABLE_TO_COMPLY.

This timer is separate from the paging timer and configuration of the ISDA guard timer can reduce the overall delay before sending the ISDA.

Example

Instruct the MME to wait *10* seconds before sending the ISDA with the last-known location of the UE:

```
isda-guard-timeout 10
```

isr-capability

Enables or disables the Idle-mode Signaling Reduction (ISR) feature on the MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no | default] isr-capability

default

Sets the ISR feature to the default setting (disabled) on MME service.

no

Disables the ISR feature on MME service.

Usage Guidelines

Use this command to enable or disable the ISR feature on the MME service. When enabled, the MME can perform ISR functions with a peer SGSN which also supports ISR.

Refer to the *Idle-mode Signaling Reduction* chapter in the *MME Administration Guide* for more information about this command

Important This functionality is a license-controlled feature. A valid feature license must be installed to enable Idle-mode Signaling Reduction.

legacy-tai-list-encoding

Using this command instructs the MME to override the default behavior (described in *Usage* section below) and enables the MME to use "010" encoding value for the Tracking Area Identity (TAI) list IE for TAIs belonging to different PLMNs.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] legacy-tai-list-encoding

no

Disables the use of "010" encoding value for the TAI list IE for TAIs belonging to different PLMNs and returns the MME to using the TAI list value encoding based on PLMN and TAC values of TAI entries, the default behavior.

Usage Guidelines

The operator can use this command to configure the encoding of TAI list values to "010" irrespective of PLMN and TAI values, which overrides the default behavior (for releases 17.4 and forward). This commnd ensures backward compatibility with previous releases.

If this command is not used, or the **no** command prefix is used, then the MME uses the default function and encodes the TAI list IE value per the 3GPP TS 24.301. The default behavior has the MME automatically encode "000", "001", or "010" depending upon the TAC values and PLMN configuration so that the TAI list value for the IE is based on the list of Tics belonging to one PLMN, with consecutive or non-consecutive TAC values configured in the TAI entries.

Example

Use the following command to override the MME's default behavior and to encode TAI list values to "010":

legacy-tai-list-encoding

local-cause-code-mapping apn-mismatch

Configures the reject cause code to send to a UE when an APN mismatch occurs.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping apn-mismatch emm-cause-code {
eps-service-not-allowed-in-this-plmn | esm-failure esm-cause-code
unknown-apn | no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
default local-cause-code-mapping apn-mismatch
```

default local-cause-code-mapping apn-mismatch

Returns the cause code mapping to its default value: **esm-failure esm-cause-code unknown-apn**.

apn-mismatch emm-cause-code { eps-service-not-allowed-in-this-plmn | esm-failure esm-cause-code unknown-apn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when an APN mismatch occurs.

- **eps-service-not-allowed-in-this-plmn**
- **esm-failure esm-cause-code unknown-apn** - Default.

  For the **esm-failure** cause code only, the **unknown-apn** ESM code is also reported to the UE.

- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when an APN mismatch occurs, such as when an APN is present in the HSS subscription but the HSS subscription for this IMSI has other APNs present in the subscription. By default, the MME sends the UE the **#23 - ESM Failure** cause code for this condition.

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "PLMN not allowed" cause code to the APN mismatch condition:

```
local-cause-code-mapping apn-mismatch emm-cause-code plmn-not-allowed
```

local-cause-code-mapping apn-not-subscribed

Gives the operator the option to specify the local cause-code mapping when the UE-requested APN is not subscribed.

Product MME

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **local-cause-code-mapping apn-not-subscribed esm-cause-code requested-service-option-not-subscribed**
default local-cause-code-mapping apn-not-subscribed

default

Returns the local cause code mapping to the default of #27 (Unknown or Missing APN).

Usage Guidelines The operator can specify "Requested-Option-Not-Subscribed" cause code value #33 will be sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found. If the command option is not configured, then by default the MME uses the cause code value #27 (Unknown or Missing APN) in standalone PDN Connectivity Reject message when the UE-requested APN is not subscribed.

Example

The following instructs the MME to use cause code #33 ("Requested-Option-Not-Subscribed") in place of the default #27 (Unknown or Missing APN):.

local-cause-code-mapping apn-not-subscribed esm-cause-code requested-service-option-not-subscribed

local-cause-code-mapping apn-not-supported-in-plmn-rat

This command maps the operator-preferred ESM/EMM cause code to be sent in Activation Reject messages in place of the standard 3GPP Release 11 rejection cause #66 when activation of the requested APN is not supported in current RAT and PLMN combination.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **local-cause-code-mapping apn-not-supported-in-plmn-rat { { emm-cause-code** *emm_cause_number* **esm-cause-code** *esm_cause_number* **[attach] [tau] } |**

```
esm-cause esm_cause_code esm-proc }
default local-cause-code-mapping apn-not-supported-in-plmn-rat [ attach
| esm-proc | tau ]
```

default

Returns the cause code mapping to its default values. The default cause code values for Attach procedures are emm-cause-code 19 and esm-cause-code 66. The default cause code values for TAU procedures are emm-cause-code 15 and esm-cause-code 66 respectively. The default cause code for ESM procedure is 66.

apn-not-supported-in-plmn-rat

The keyword **apn-not-supported-in-plmn-rat** specifies that the cause codes to be used for a rejection due to the requested APN not being supported in the current RAT and PLMN combination are those that are mapped in the configuration.

emm-cause-code *emm_cause_number* esm-cause-code *esm_cause_number* [attach] [tau]

MME only.

The keyword **emm-cause-code** configures the operator-preferred EMM cause code to be used if a NAS Request is rejected due to this configuration.

- *emm_cause_number* specifies the EMM code replacement integer. The system accepts a value in the range 0 through 255, however, the standards-compliant valid values are in the range 2 through 111.
- **esm-cause-code** configures the operator-preferred ESM cause code to be used if a NAS Request is rejected due to this configuration.
- *esm_cause_number* specifies the ESM code replacement integer. The system accepts a value in the range 0 through 255, however, the standards-compliant valid values are in the range 8 through 112.
- The **attach** keyword filter instructs the MME to use the mapped replacement cause code if an Attach procedure is rejected due to the noted APN not supported error condition.
- The **tau** keyword filter instructs the MME to use the mapped replacement cause code if an TAU procedure is rejected due to the noted APN not supported error condition.

esm-cause-code *esm_cause_number* esm-proc

MME only.

esm-cause-code configures the operator-preferred ESM cause code to be used if a bearer management Request is rejected due to this configuration.

- *esm_cause_number* specifies the ESM cause code replacement integer in the range 0 through 255.
- The **esm-proc** keyword filter instructs the MME to use the mapped replacement cause code if an ESM procedure is rejected due to the noted APN not supported error condition.

Usage Guidelines

This command is used to remap the ESM and EMM cause codes sent in activate rejections (due to APN not supported) to operator desired ESM or EMM cause codes. The default cause code values for Attach procedures are emm-cause-code 19 and esm-cause-code 66. The default cause code values for TAU procedures are emm-cause-code 15 and esm-cause-code 66. The default cause code for esm-proc is 66.

Example

The following command is used to remap cause code #66 to cause code #20, this cause code will be sent if a bearer management request is rejected.

```
local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code 20
 esm-proc
```

local-cause-code-mapping auth-failure

Configures the reject cause code to send to a UE when an authentication failure occurs.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping auth-failure emm-cause-code {
eps-service-not-allowed-in-this-plmn | illegal-ms | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
default local-cause-code-mapping auth-failure
```

default local-cause-code-mapping auth-failure

Returns the cause code mapping to its default value: **illegal-ms**.

auth-failure emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when an authentication failure occurs.

- **eps-service-not-allowed-in-this-plmn**
- **illegal-ms**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when an authentication failure occurs. By default, the MME sends the UE the **#3 - Illegal MS** cause code when encountering a context transfer failure from an MME.

This condition occurs for TAU and ATTACH procedures in the following cases:

- The Authentication response from the UE does not match the expected value in the MME.
- Security Mode Reject is send by the UE.
- The UE responds to any identity request with a different type of identity (ie, the MME could query for IMSI and the UE responds with IMEI).

The following are not considered for the authentication failure condition:

- HSS returning a result code other than SUCCESS.
- HSS not available.
- EIR failures.
- UE not responding to requests.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "network-failure" cause code to the authentication failure condition:

```
local-cause-code-mapping auth-failure emm-cause-code network-failure
```

local-cause-code-mapping congestion

Configures the reject cause code to send to a UE when a procedure fails due to a congestion condition.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping congestion emm-cause-code { congestion [
esm-cause-code { congestion | insufficient-resources |
service-option-temporarily-out-of-order } ] |
eps-service-not-allowed-in-this-plmn | network failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
default local-cause-code-mapping congestion
```

default local-cause-code-mapping congestion

Returns the cause code mapping to its default value: **emm-cause congestion esm-cause congestion**.

congestion emm-cause { congestion [esm-cause-code { congestion | insufficient-resources | service-option-temporarily-out-of-order }] | eps-service-not-allowed-in-this-plmn | network failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access when the system is exceeding any of its congestion control thresholds.

- **congestion** - Default
- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

esm-cause-code { congestion | insufficient-resources | service-option-temporarily-out-of-order }

Specifies the EPS Session Management (ESM) cause code to return when a UE requests access when the system is exceeding any of its congestion control thresholds.

- **congestion** - Default
- **insufficient-resources**
- **service-option-temporarily-out-of-order**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a UE procedure fails due to a congestion condition on the MME. By default, the MME sends the UE the **#22 - Congestion**EMM cause code and ESM cause code when encountering congestion.

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "network failure" cause code to the congestion event:

```
local-cause-code-mapping congestion emm-cause-code network-failure
```

local-cause-code-mapping ctxt-xfer-fail-mme

Configures the reject cause code to send to a UE when a UE context transfer failure from a peer MME occurs.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping ctxt-xfer-fail-mme emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed |
unknown-ue-context }
default local-cause-code-mapping ctxt-xfer-fail-mme
```

default local-cause-code-mapping ctxt-xfer-fail-mme

Returns the cause code mapping to its default value:**unknown-ue-context**.

ctxt-xfer-fail-mme emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed | unknown-ue-context }

Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from an old MME occurs.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**
- **unknown-ue-context** - Default

Usage Guidelines

Use this command to configure the cause code returned to a UE when a UE context transfer failure from a peer MME occurs. By default, the MME sends the UE the **#9 - MS identity cannot be derived by the network** cause code for this condition.

After the peer node has been identified, the MME sends a Context Request to the peer node. If the peer node is an MME, and if the context transfer procedure fails, this condition is detected.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "network-failure" cause code to the context transfer failure from MME condition:

```
local-cause-code-mapping ctxt-xfer-fail-mme emm-cause-code network-failure
```

local-cause-code-mapping ctxt-xfer-fail-sgsn

Configures the reject cause code to send to a UE when a UE context transfer failure from a peer SGSN occurs.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping ctxt-xfer-fail-sgsn emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed |
unknown-ue-context }
default local-cause-code-mapping ctxt-xfer-fail-sgsn
```

default local-cause-code-mapping ctxt-xfer-fail-sgsn

Returns the cause code mapping to its default value:**unknown-ue-context**.

ctxt-xfer-fail-sgsn emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed | unknown-ue-context }

Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from an old SGSN occurs.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**
- **unknown-ue-context** - Default

Usage Guidelines

Use this command to configure the cause code returned to a UE when a UE context transfer failure from a peer SGSN occurs. By default, the MME sends the UE the **#9 - MS identity cannot be derived by the network** cause code when encountering this condition.

After the peer node has been identified, the MME sends a Context Request to the peer node. If the peer node is an SGSN, and if the context transfer procedure fails, this condition is detected.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "network-failure" cause code to the context transfer failure from SGSN condition:

```
local-cause-code-mapping ctxt-xfer-fail-sgsn emm-cause-code network-failure
```

local-cause-code-mapping gw-unreachable

Configures the reject cause code to send to a UE when a gateway (S-GW or P-GW) does not respond during an EMM procedure.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping gw-unreachable emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
[ attach [ tau ] | tau [ attach ] ] | { no-bearers-active tau }
default local-cause-code-mapping gw-unreachable [ attach | tau ]
```

default local-cause-code-mapping gw-unreachable [attach | tau]

Returns the cause code mapping to its default value: **#19 - ESM Failure** cause code for Attach procedures, and **no-bearers-active**- #40 - NO-EPS-BEARER-CONTEXT-ACTIVATED for TAU procedures.

gw-unreachable emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a gateway does not respond.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-bearers-active**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

[attach [tau] | tau [attach]] | { no-bearers-active tau }

Optionally, the MME can return separate cause codes for Attach procedures and TAU procedures. This capability is available for any of the above EMM cause codes except **no-bearers-active**, which can only be defined for TAU procedures.

Usage Guidelines

Use this command to configure the cause code returned to a UE when a gateway does not respond. By default, the MME sends the UE the **#19 - ESM Failure** cause code when encountering this condition.

Defaults:

Prior to StarOS 15.0 MR5, the MME sends the UE the **#19 - ESM Failure** cause code when encountering this condition.

In StarOS 15.0 MR5 and higher releases, the MME sends the UE the **#19 - ESM Failure** cause code for Attach procedures, and **#40 - NO-EPS-BEARER-CONTEXT-ACTIVATED** for TAU procedures.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "network-failure" cause code to the gateway unreachable condition:

```
local-cause-code-mapping gw-unreachable emm-cause-code network-failure
```

local-cause-code-mapping hss-unavailable

Configures the reject cause code to send to a UE when the HSS does not respond.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping hss-unavailable emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
default local-cause-code-mapping hss-unavailable
```

default local-cause-code-mapping hss-unavailable

Returns the cause code mapping to its default value:

hss-unavailable emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when the HSS does not respond.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure** - Default
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when the HSS does not respond. By default, the MME sends the UE the **#17 - Network failure** cause code when encountering this condition.

This condition is detected in the following cases:

- HSS resolution fails in the MME.
- HSS does not respond in time.

The cause code configured for this condition will be signaled in TAU and ATTACH REJECT messages.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "tracking-area-not-allowed" cause code to the HSS unavailable condition:

```
local-cause-code-mapping hss-unavailable emm-cause-code
tracking-area-not-allowed
```

local-cause-code-mapping newcall-policy-restrict

Configures the EPS Mobility Management (EMM) reject cause code to send to a UE when a UE requests access but the call control profile has set the call disposition to reject.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping newcall-policy-restrict emm-cause-code {
congestion | eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
default local-cause-code-mapping newcall-policy-restrict
```

default local-cause-code-mapping newcall-policy-restrict

Returns the cause code mapping to its default value: **congestion**.

newcall-policy-restrict emm-cause-code *emm_cause_code*

Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access but the call control profile has set the call disposition to reject.

emm_cause_code must be one of the following options:

- **congestion** - Default.
- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a UE procedure fails, such as when the UE requests access to a restricted zone. By default, the MME sends the UE the **#22 - Congestion** cause code when encountering this condtion.

Example

The following command sets the "network-failure" cause code for newcall-policy-restrict calls:

```
local-cause-code-mapping newcall-policy-restrict emm-cause-code
network-failure
```

local-cause-code-mapping no-active-bearers

Configures the reject cause code to send to a UE when the context received from a peer SGSN (during a TAU procedure) does not contain any active PDP contexts.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping no-active-bearers emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure | no-bearers-active
 | no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
default local-cause-code-mapping no-active-bearers
```

default local-cause-code-mapping no-active-bearers

Returns the cause code mapping to its default value: **no-bearers-active**.

no-active-bearers emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-bearers-active | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when no active PDP context exists.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-bearers-active** - Default
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when the context received from a peer SGSN (during a TAU procedure) does not contain any active PDP contexts. By default, the MME sends the UE the **#40 - No PDP context activated** cause code when encountering this condition.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "plmn-not-allowed" cause code to the no active bearer condition:

```
local-cause-code-mapping no-active-bearers emm-cause-code plmn-not-allowed
```

local-cause-code-mapping odb packet-services

Configures the ESM and EMM cause codes to send to a UE depending on the Operator Determined Barring (ODB) condition.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

local-cause-code-mapping odb packet-services emm-cause-code *cc_value* **[esm-cause-code** *cc_value* **]**
default local-cause-code-mapping odb packet-services

default local-cause-code-mapping odb packet-services

Returns the EMM cause code mapping to its default value: **#15 - NO_SUITABLE_CELL_IN_TRACKING_AREA**.

packet-services emm-cause-code *cc_value* [esm-cause-code *cc_value*]

Specifies the EPS Mobility Management (EMM) cause code to return when ODB condition is hit.

emm-cause-code *cc_value* : Specifies the EMM cause code for ODB all packet services. The EMM cause code value is an integer from 0 to 255.

esm-cause-code *cc_value* : This is an optional keyword used to specify the ESM cause code as an integer from 0 to 255.

Usage Guidelines

Use this command to configure the cause code returned to a UE when ODB condition is hit, such as when the subscriber does not have an LTE/EPS subscription. By default, the MME sends the UE the **#15 - NO_SUITABLE_CELL_IN_TRACKING_AREA** cause code for this condition.

Related Commands:

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signaled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the EMM cause code #15 (NO_SUITABLE_CELL_IN_TRACKING_AREA) to the ODB condition:

```
local-cause-code-mapping odb packet-services emm-cause-code 15
```

local-cause-code-mapping odb roamer-to-vplmn

Configures the ESM and EMM cause codes to send to a UE depending on the Operator Determined Barring (ODB) condition.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

local-cause-code-mapping odb roamer-to-vplmn emm-cause-code *cc_value* **[esm-cause-code** *cc_value* **]**
default local-cause-code-mapping odb roamer-to-vplmn emm-cause-code

default local-cause-code-mapping odb roamer-to-vplmn emm-cause-code

Returns the EMM cause code mapping to its default value: **#15 - NO_SUITABLE_CELL_IN_TRACKING_AREA**.

roamer-to-vplmn emm-cause-code *cc_value* [esm-cause-code *cc_value*]

Specifies the EPS Mobility Management (EMM) cause code to return when ODB condition is hit.

emm-cause-code *cc_value* : Specifies the EMM cause code for ODB roamer to visited PLMN. The EMM cause code value is an integer from 0 to 255.

esm-cause-code *cc_value* : This is an optional keyword used to specify the ESM cause code as an integer from 0 to 255.

Usage Guidelines

Use this command to configure the cause code returned to a UE when ODB condition is hit, such as when the subscriber does not have an LTE/EPS subscription. By default, the MME sends the UE the **#15 - NO_SUITABLE_CELL_IN_TRACKING_AREA** cause code for this condition.

Related Commands:

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signaled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the EMM cause code #15 (NO_SUITABLE_CELL_IN_TRACKING_AREA) to the ODB condition:

```
local-cause-code-mapping odb packet-services emm-cause-code 15
```

local-cause-code-mapping peer-node-unknown

Configures the reject cause code to send to a UE when peer node resolution is not successful.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping peer-node-unknown emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
default local-cause-code-mapping peer-node-unknown
```

default local-cause-code-mapping peer-node-unknown

Returns the cause code mapping to its default value: **unknown-ue-context**

peer-node-unknown emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when the peer node is not known.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**
- **unknown-ue-context** - Default

Usage Guidelines

Use this command to configure the cause code returned to a UE when peer node resolution is not successful. By default, the MME sends the UE the **#9 - MS identity cannot be derived by the network** cause code when encountering this condition.

During processing of a TAU Request, the resolution of a peer MME that had allocated the temporary identity that is signaled to the UE takes several steps in the MME. This resolution can be done based on DNS or based on local configuration. This condition occurs when all mechanisms for peer node resolution are done with no success.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "plmn-not-allowed" cause code to the peer node unknown condition:

```
local-cause-code-mapping peer-node-unknown emm-cause-code plmn-not-allowed
```

local-cause-code-mapping pgw-selection-failure

Configures the reject cause code to send to a UE when a failure occurs during P-GW selection.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping pgw-selection-failure emm-cause-code { {
esm-failure esm-cause-code unknown-apn }|
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
default local-cause-code-mapping pgw-selection-failure
```

default local-cause-code-mapping pgw-selection-failure

Returns the cause code mapping to its default value: **network-failure**.

pgw-selection-failure emm-cause-code { { esm-failure esm-cause-code unknown-apn } | eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a failure occurs during P-GW selection.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure** - Default
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**
- **esm-failure**
- **esm-cause-code**
- **unknown-apn**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a failure occurs during P-GW selection. By default, the MME sends the UE the **#17 - Network failure** cause code when encountering this condition. To overcome the impact in MME 4G attach SR calculations, the MME sends the UE the **#19 - ESM failure #27 - Unknown APN**cause code when encountering this condition.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "plmn-not-allowed" cause code to the P-GW selection failure condition:

```
local-cause-code-mapping pgw-selection-failure emm-cause-code
plmn-not-allowed
```

Example

The following command maps the "esm-failure" "esm-cause-code" and "unknown-apn" cause code to the P-GW selection failure condition:

```
local-cause-code-mapping pgw-selection-failure emm-cause-code { esm-failure
 esm-cause-code unknown-apn }
```

local-cause-code-mapping restricted-zone-code

Configures the reject cause code to send to a UE when a procedure fails.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping restricted-zone-code emm-cause-code {
eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area
 | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area |
tracking-area-not-allowed }
default local-cause-code-mapping restricted-zone-code
```

default local-cause-code-mapping restricted-zone-code

Returns the cause code mapping to its default value: **no-suitable-cell-in-tracking-area**.

restricted-zone-code emm-cause-code *emm_cause_code*

Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access to a restricted zone.

emm_cause_code must be one of the following options:

- **eps-service-not-allowed-in-this-plmn**
- **no-suitable-cell-in-tracking-area** - Default.
- **plmn-not-allowed**

- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a UE procedure fails, such as when the UE requests access to a restricted zone. By default, the MME sends the UE the **#15 - No Suitable Cells in Tracking Area** cause code when encountering this condition.

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "PLMN not allowed" cause code to the restricted zone code event:

```
local-cause-code-mapping restricted-zone-code emm-cause-code
plmn-not-allowed
```

local-cause-code-mapping sgw-selection-failure

Configures the reject cause code to send to a UE when a failure occurs during S-GW selection.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping sgw-selection-failure emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
default local-cause-code-mapping sgw-selection-failure
```

default local-cause-code-mapping sgw-selection-failure

Returns the cause code mapping to its default value: **network-failure**.

sgw-selection-failure emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a failure occurs during S-GW selection.

- **eps-service-not-allowed-in-this-plmn**

- **network-failure** - Default
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a failure occurs during S-GW selection. By default, the MME sends the UE the **#17 - Network failure** cause code when encountering this condition.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "plmn-not-allowed" cause code to the S-GW selection failure condition:

```
local-cause-code-mapping sgw-selection-failure emm-cause-code
plmn-not-allowed
```

local-cause-code-mapping vlr-down

Configures the cause code to send in a ATTACH ACCEPT or TAU ACCEPT to a UE that attachment to the VLR has failed because a VLR down condition is present.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping vlr-down emm-cause-code { congestion |
cs-domain-unavailable | imsi-unknown-in-hlr | msc-temp-unreachable |
network-failure }
default local-cause-code-mapping vlr-down
```

default local-cause-code-mapping vlr-down

Returns the cause code mapping to its default value: **msc-temp-unreachable**.

vlr-down emm-cause-code *emm_cause_code*

Specifies the EPS Mobility Management (EMM) cause code to return when a VLR down condition is present.

emm_cause_code must be one of the following options:

- **congestion**
- **cs-domain-unavailable**
- **imsi-unknown-in-hlr**
- **msc-temp-unreachable**- Default.
- **network-failure**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a VLR down condition is present. By default, the MME sends the UE the **#16: "MSC temporarily not reachable** cause code when encountering this condition.

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "network failure" EMM cause code to the VLR down condition:

```
local-cause-code-mapping vlr-down emm-cause-code network-failure
```

local-cause-code-mapping vlr-unreachable

Configures the cause code to send in a ATTACH ACCEPT or TAU ACCEPT to a UE that attachment to the VLR has failed because a VLR unreachable condition is present.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
local-cause-code-mapping vlr-unreachable emm-cause-code { congestion |
cs-domain-unavailable | imsi-unknown-in-hlr | msc-temp-unreachable |
network-failure }
default local-cause-code-mapping vlr-unreachable
```

default local-cause-code-mapping vlr-unreachable

Returns the cause code mapping to its default value: **msc-temp-unreachable**.

vlr-down emm-cause-code *emm_cause_code*

Specifies the EPS Mobility Management (EMM) cause code to return when a VLR unreachable condition is present.

emm_cause_code must be one of the following options:

- **congestion**
- **cs-domain-unavailable**
- **imsi-unknown-in-hlr**
- **msc-temp-unreachable** - Default.
- **network-failure**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a VLR unreachable condition is present. By default, the MME sends the UE the **#16: "MSC temporarily not reachable** cause code when encountering this condition.

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the "network failure" EMM cause code to the VLR unreachable condition:

```
local-cause-code-mapping vlr-unreachable emm-cause-code network-failure
```

location-reporting

Enables or disables the UE location reporting function on the MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no | default ] location-reporting
```

default

Disables the location reporting feature on MME service.

no

Disables the location reporting feature on MME service.

Usage Guidelines

Use this command to enable or disable the UE location reporting feature on the MME service. When enabled the MME forwards a location report request for a specific UE from the P-GW to the eNodeB.

Important Location reporting, also known as User Location Information (ULI) Reporting, is a licensed feature and requires the purchase of the ULI Reporting feature license.

Example

The following command sets the MME service to allow for location reporting for UEs:

```
location-reporting
```

lte-m-rat

Enables configuration for LTE-M-RAT Access type.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name )lte-m-ratflag-LTEMPI#
```

Syntax Description

```
[ no | default | remove ]lte-m-rat flag-LTEMPI
```

no

Diables the configuration from call-control profile and fallback to the mme-service configuration.

default

Resets the configuration from call-control profile and fallback to the mme-service configuration.

remove

Removes the configuration from call-control profile and fallback to the mme-service configuration.

lte-m-rat

Enables configuration for LTE-M Access Type.

flag-LTEMPI

Configures the LTE-M RAT Indication to S-GW to pass the LTE-M RAT type to the P-GW.

Usage Guidelines Use this command to enable or disable LTE-M-RAT Access type.

Example

The following command enables the LTE-M-RAT Access type.

```
lte-m-rat flag-LTEMPI { 1 | 0 }
```

mapping

Configures how the MME maps the Target RNC-ID fields to the Target eNodeB-ID and TAC fields for Inter-RAT Gn/Gp handovers.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
mapping rncid-to-enbid { maptype-default-includes-only-enb |
maptype1-includes-enb-tai }
no mapping rncid-to-enbid
```

no

Sets the command to use the default value of **maptype-default-includes-only-enb**.

maptype-default-includes-only-enb

Default mapping logic

Maps the Target RNC-ID fields to Target eNodeB-ID fields as follows:

- PLMN of LAI => PLMN of MME
- LAC of LAI => MME Group ID
- RAC => Not used.
- RNC-ID (12 or 16bits) => Lowest 12 or 16 bits of eNB ID.
- TAC is picked from the list of TAIs supported by the target eNB.

maptype1-includes-enb-tai

Maps the Target RNC-ID fields to Target eNodeB-ID fields as follows:

- PLMN of LAI => PLMN of TAI and eNB
- LAC of LAI => TAC of TAI
- RAC => Lowest 8 bits of eNB ID
- RNC-ID (12bits) => Highest 12 bits of eNB ID

Usage Guidelines Use this command to configure how the MME maps the Target RNC-ID fields to the Target eNodeB-ID and TAC fields for Inter-RAT Gn/Gp handovers.

max-bearers per-subscriber

Specifies the maximum number of EPS bearers that a subscriber may simultaneously use to access this MME service.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-bearers per-subscriber *max_bearer*
default max-bearers per-subscriber

default

Configures the maximum EPS bearers for a subscriber to use simultaneously to the default value of 11.

max_bearer

Specifies the maximum number of EPS bearers for a subscriber may simultaneously use to access this MME service.

max_bearer is an integer from 1 through 11. Default: 11

Usage Guidelines Use this command to set the maximum number of EPS bearers that a subscriber may simultaneously use to access this MME service.

Example

The following command specifies that a maximum of *6* simultaneous EPS bearers can be facilitated for a subscriber at any given time:

```
max-bearers per-subscriber 6
```

max-paging-attempts

This command configures the maximum number of paging attempts allowed for network requested service creation to a subscriber.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-paging-attempts *max_paging_attempts*
default max-paging-attempts

default

Configures the maximum number of paging attempts to the default value of 3.

max_paging_attempts

Specifies the maximum number of paging attempts allowed for network requested service creation to a subscriber.

max_paging_attempts is an integer from 1 through 10. Default: 3

Usage Guidelines

Use this command to set the maximum number of paging attempts allowed for network requested service creation to a subscriber.

When Heuristic Paging is enabled, this setting applies only to messages sent to all eNodeBs in all TAIs present in the TAI list. Paging to the last known eNodeB and paging the TAI from which the UE was last heard is attempted only once. As a result, when max-paging-attempts is set to 3, a maximum of 5 paging retries are attempted with Heuristic Paging enabled.

Refer to the *Heuristic and Intelligent Paging* chapter in the *MME Administration Guide* for more information about Heuristic Paging.

Example

The following command specifies that a maximum of *6* paging attempt retransmissions allowed for network requested service creation to a subscriber:

max-paging-attempts 6

max-pdns per-subscriber

Specifies the maximum number of Packet Data Networks (PDNs) that a subscriber may simultaneously access through this MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-pdns per-subscriber *max_pdn*
default max-pdns per-subscriber

default

Configures the maximum PDNs that a subscriber can simultaneously access through this MME service to the default value of 3.

max_pdn

Specifies the maximum number of PDNs that a subscriber may simultaneously access through this MME service.

max_pdn is an integer from 1 through 11. Default: 3

Usage Guidelines

Use this command to set the maximum number of PDNs that a subscriber may simultaneously access through this MME service.

Example

The following command specifies that a maximum of *2* simultaneous PDNs can be accessed by a subscriber at any given time through this MME service:

max-pdns per-subscriber 2

minimization-drive-test

Enables Minimization Drive Test(MDT) handling on MME.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] minimization-drive-test

no

Disables the Minimization Drive Test(MDT) handling on MME.

minimization-drive-test

This command enables Minimization Drive Test(MDT) handling on MME.

Example

The following command enables Minimization Drive Test(MDT) handling on MME:

minimization-drive-test

mme-id

Configures the MME identifier within an MME service. The MME identifier is constructed form the MME group ID and MME Code.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

mme-id group-id *grp_id* **mme-code** *mme_code*
no mme-id

no

Removes the configured MME identifier for this MME service.

Caution Removing the MME identifier is a disruptive operation; the MME service is removed from the system.

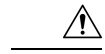
group-id *grp_id*

Specifies the group identifier for the group of which this MME belongs as an integer from 0 through 65535.

mme-code *mme_code*

Specifies the unique code for this MME service as an integer from 0 through 255.

Usage Guidelines Use this command to set the MME identifier for this MME service. This MME identifier will be the identity of this MME in network.



Caution Changing or removing the MME identifier is a disruptive operation; the MME service will be re-started or removed from service.

Example

The following command configures the MME identifier with group id as *41025* and MME code as *101* for this MME service:

```
mme-id group-id 41025 mme-code 101
```

mmemgr-recovery

Configures the recovery action for the MME manager.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
mmemgr-recovery { no-reset | reset-s1-peers }
default mmemgr-recovery
```

default

Resets the function configuration to the MME's default value of reset S1 peers.

no-reset

Specifies that the recovery action is **not** to reset S1 peers.

reset-s1-peers

Specifies that the recovery action is to reset S1 peers. This is the default action.

Usage Guidelines Use this command to set a recovery action for the MME Manager.

Example

The following command configures the MME Manager recovery action to reset all S1 peers:

mmemgr-recovery reset-s1-peers

monitoring-events

Enables Monitoring Events for UE on MME.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description `[ no ] monitoring-events`

default

Disables monitoring-events at the time of MME service configuration.

Usage Guidelines Use this command to enable monitoring-events for each MME service.

Example

The following command configures the monitoring-events:

monitoring-events

msc

Creates and manages an Mobile Switching Center (MSC) server configuration, for the MME service, for an MSC enhanced with Single Radio Voice Call Continuity (SRVCC). The MSC server acts as an endpoint for the Sv interface.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

msc { *msc_name* | [*ipv4_address* | *ipv6_address*] } [**ip-address** [*ipv4_address* | *ipv6_address*] [**offline | online**]
no msc { *msc_name* | [*ipv4_address* | *ipv6_address*] }

no *msc_name*

Removes the MSC configuration from the MME service.

msc_name

Specifies a name for this peer MSC server.

msc_name must be an alphanumeric string from 1 to 63 characters.

ip-address *ipv4_address* | *ipv6_address*

Specifies the IP address of the peer MSC server in either IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

In Release 16.0 and higher, the MME supports DNS-based MSC selection. If DNS-based selection is configured, the DNS lookup is done first, then it will fall back to local ip address.

offline

Mark this MSC server offline for maintenance. Once this command is issued, the MME will no longer send future handover requests to this MSC server. No GTPv2 messages are generated when offline/online mode is changed.

Once the MSC server is set for offline, the **online** keyword must be used to return the server to online mode.

online

Mark this MSC server for online mode. Once this command is issued, the MSC server is added back into the MSC selection algorithm and normal operation is returned. By default, an MSC server is online unless the **offline** keyword is specified.

Usage Guidelines

Use this command to configure a peer MSC server used during SRVCC handovers. For details on the configuration of the MSC and the MME's usage of SRVCC, refer to the *Single Radio Voice Call Continuity* feature chapter in the *MME Administration Guide*.

Also, this command can set an MSC server offline for maintenance.

Example

For Release 16.0 and higher, the following command defines an MSC server *msc1* that will be selected by DNS. Any MSCs configured for DNS-based selection must be defined without an IP address:

```
msc msc1
```

The following command defines a *default* MSC server with an IPv4 address of *209.165.200.244*. The MME will select the default when no other MSC selection logic (DNS selection or MSC pool areas) are configured, or when these fail to return an MSC address.

```
msc default ip-address 209.165.200.244
```

For Release 15.0 and higher:

The following command defines an MSC server *mscwest* with an IPv4 address of *209.165.200.228*:

```
msc mscwest ip-address 209.165.200.228
```

The following command marks the above MSC server offline:

```
msc mscwest ip-address 209.165.200.244 offline
```

The following command defines a *default* MSC server with an IPv4 address of *209.165.200.244*. The MME will select the default when MSC pool areas are not configured, or when an MSC address fails to be returned.

```
msc default ip-address 209.165.200.244
```

For Release 14.0 and earlier:

The following command specifies an IPv4 address for the peer MSC server as *209.165.200.228*:

```
msc 209.165.200.228
```

msc-mapping

This command creates a mapping between the MSC ISDN number and the MSC's IP-address (either IPv4 or IPv6) to ensure location continuity for SRVCC handover. This mapping is required to include the MSV ID in the target service node IE for the Emergency_Call_Handover event.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

msc-mapping ip-address { *ipv4_address* | *ipv6_address* } isdn *isdn_number*
msc-mapping ip-address { *ipv4_address* | *ipv6_address*

no

Removes a specific MSC IP address mapping definition from the MME Service configuration.

ip-address

ipv4_address | *ipv6_address* Specifies the IP address for the MSC as an IPv4 dotted-decimal or as an IPv6 colon-separated-hexadecimal notation.

isdn

isdn_number: Enter a numeric string upto 15 digits long.

Usage Guidelines

The MME Service supports a maximum of 24 MSC IP address to ISDN mapping definitions.

Use the **show mme-service** command to see the MSC IP address to ISDN mappings created with this command.

Example

Map the IPv4 *192.168.61.2* address of the MSC to ISDN *123456789012345*

```
msc-mapping ip-address 209.165.200.226 isdn 123456789012345
```

nas gmm-qos-ie-mapping

Configures which QOS the MME uses in NAS GMM QoS IE and GTPv1 Context response message when the subscriber comes to MME via a handover from a GN/GP SGSN.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
nas gmm-qos-ie-mapping { gngp-imported-qos | native-eps-qos }
```

gngp-imported-qos

Configures the MME to send the QoS received from GN/GP SGSN (whenever applicable).

native-eps-qos

Configures the MME to send the EPS (4G) QoS received from HSS.

This is the default setting.

Usage Guidelines

When a subscriber comes to MME via a handover from Gn/Gp SGSN, this command controls whether the MME is to use the QoS received from the SGSN, or whether to use the updated EPS QoS received from the HSS. This value is then mapped to gmm-qos-ie in subsequent NAS messages and in GTPv1 Context response messages.

Example

The following command configures the MME to use the QoS values from the Gn/Gp SGSN in gmm-qos-ie NAS messages and GTPv1 Context response messages.

```
nas gmm-qos-ie-mapping gngp-imported-qos
```

nas-max-retransmission

Sets the retransmission counter for all type of Non-Access Stratum (NAS) messages in an MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

nas-max-retransmissions *nas_retrans_count*
default nas-max-retransmissions

default

Resets the retransmission counter to the default value of 4.

nas_retrans_count

Sets the maximum number of retransmission of NAS messages permitted during any procedure after which the activation procedure will be discarded.

nas_retrans_count is an integer from 1 through 10. Default: 4

Usage Guidelines

Use this command to set maximum number of retries allowed for any type of NAS messages.

NAS Messages sent by the MME which require a response from the UE for procedure completion are retransmitted. Retransmission happens based on timer expiry. The timers are configured through the **emm** and **esm** commands. NAS messages are retransmitted per configuration, and if no response is received from the UE, the pending transaction is abandoned. If the transaction is a DETACH or PDN DISCONNECT REQUEST, the transaction is completed without further UE signaling.

The timeout duration configured through the **emm** and **esm** commands will be applicable between two retries.

Example

The following command sets the maximum number of retries allowed as *4* for all type of NAS messages in an MME service.

```
default nas-max-retransmissions
```

network-sharing

Configures additional PLMN IDs for this MME service. Refer to the **plmn-id** command to create the base PLMN identifier for an MME service. Each PLMN ID consists of the Mobile Country Code (MCC) and Mobile Network Code (MNC). A maximum of four network sharing entries can be configured per MME service. These PLMN IDs will be communicated to the eNodeBs in the S1 SETUP response and MME CFG Update messages.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

network-sharing plmn-id mcc *number* **mnc** *number* **mme-id group-id** *id* **mme-code** *code*
no network-sharing plmn-id mcc *number* **mnc** *number*

no

Disables the network sharing mode on this MME service.

Caution Removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

plmnid mcc *number* mnc *number*

Sets the mobile country code (MCC) and mobile network code (MNC) of the PLMN ID for this service.

mcc *number*: Specifies the MCC portion of the PLMN identifier as an integer from 100 through 999.

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

mme-id group-id *id*

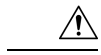
Specifies the group identifier for the group to which this MME belongs as an integer from 0 through 65535.

mme-code *code*

Specifies the unique code for an MME service as an integer from 0 through 255.

Usage Guidelines

Use this command to configure additional PLMN IDs for an MME service. In a given MME service, each PLMN ID (MCC and MNC) must be unique.



Caution Changing or removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

Example

The following command configures the network sharing parameters to an MCC of *123*, an MNC of *12*, a MME-ID/Group ID of *100*, and a MME code of *50*:

```
network-sharing plmnid mcc 123 mnc 12 mme-id group-id 100 mme-code 50
```

nri

Configures the network resource identifier (NRI) length used for source SGSN discovery via NRI-FQDN (Fully Qualified Domain Name) based DNS resolution.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **`[ no ] nri length`** *`length`* **`plmn-id mcc`** *`mcc_value`* **`mnc`** *`mnc_value`*

no

Removes a configured NRI length.

length *length*

Specifies the number of bits to be used in the P-TMSI (bits 23 to 18) to define the NRI as an integer from 1 through 8.

plmn-id mcc *mcc_value* mnc *mnc_value*

Specifies the PLMN-ID of the SGSN pool.

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

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

Usage Guidelines Use this command to retrieve the NRI (identity of an SGSN) stored in bits 23 to 18 of the packet-temporary mobile subscriber identity (P-TMSI). Up to eight NRI length values can be configured.

Important In the absence of this configuration, the MME treats the NRI as invalid. The MME will use a plain RAI-based FQDN (and not an NRI-based FQDN) for DNS queries made to resolve the source SGSN.

Example

The following command creates an NRI length of *5* and associates it with an SGSN pool with the PLMN-ID of *123*:

```
nri length 5 plmnid mcc 123 mnc 23
```

NR UE Capability IE

Enables or Disables NR UE Security Capability IE in messages over S1AP and S10 Interfaces to the peer.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context > Context name

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

nr-ue-security-capability-ie

By Default the CLI is enabled. MME includes **NR UE Security Capability IE** as part of below messages over S1AP interfaces :

- INITIAL-CONTEXT-SETUP-REQUEST
- PATH-SWITCH-REQ-ACK
- UE-CONTEXT-MODIFICATION-REQUEST
- HANDOVER-REQUEST
- DOWNLINK-NAS-TRANSPORT

Messages over S10 interfaces are:

- FORWARD RELOCATION REQUEST
- CONTEXT RESPONSE

Syntax Description

[no] nr-ue-security-capability-ie

no

Disables a configuration

MME ignores "UE Additional Security Capability" received over Attach/TAU request. It does not replay (Replayed UE Additional Security Capability") in the Security Mode Command,

MME does not include NR UE Security Capability IE and UE Additional Security Capability over S1AP and S10 respectively.

Usage Guidelines

Use this command to enable or disable the nr-ue-security-capability-ie in messages over S1AP and S10 interfaces.

Example 1

The following show output command enables the configuration:

```
context ingress
mme-service mme1
nr-ue-security-capability-ie
```

Example 2

The following show output command disables the configuration:

```
context ingress
  mme-service mme1
  no nr-ue-security-capability-ie
```

peer-mme

Configures parameters that, when matched by another MME, specifies that MME as a peer for inter-MME relocations.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

peer-mme { echo-params interval *interval* **retransmission-timeout** *retransmission-timeout* **max-retransmissions** *max-retransmissions* **reconnect-interval** *reconnect-interval* **| gummei mcc** *number* **mnc** *number* **group-id** *id* **mme-code** *code* **address** *ipv4_address* **| tai-match priority** *value* **mcc** *number* **mnc** *number* **tac {** *area_code* **| any |** *start_area_code* **to** *end_area_code* **} address** *ipv4_address* **}**
no peer-mme { echo-params | gummei mcc *number* **mnc** *number* **group-id** *id* **mme-code** *code* **| tai-match priority** *value* **}**

no

Removes the configured path management for Peer MME or peer Globally Unique MME Identifier (GUMMEI) or TAI match priority from this service.

echo-params interval *interval* retransmission-timeout *retransmission-timeout* max-retransmissions *max-retransmissions* reconnect-interval *reconnect-interval*

Configures the path management for Peer MME.

interval *interval*: Configures echo interval in seconds. *interval* must be an ineteger between 60 and 300.

retransmission-timeout *retransmission_timeout*: Configures echo retransmission timeout in seconds. *retransmission_timeout* must be an ineteger between 1 and 20.

max-retransmissions *max-retransmissions*: Configures maximum retries for echo request. *max-retransmissions* must be an ineteger between 0 and 15.

reconnect-interval *reconnect_interval*: Configures echo interval to be used once a peer node is detected to be unreachable. Retransmission is not applicable in this time. *reconnect_interval* must be an ineteger between 60 and 86400.

gummei mcc *number* mnc *number* group-id *id* mme-code *code* address *ipv4_address*

Specifies that an MME with values matching those configured in this GUMMEI is to be considered a peer MME. This variable supports the lookup of an IP address for a peer MME based on the exact match of the supporting keyword below (which make up the GUMMEI).

mcc *number*: Sets the mobile country code (MCC) for peer match as an integer from 100 through 999.

mnc *number*: Sets the mobile network code (MNC) for this peer match as a 2- or 3-digit integer from 00 through 999.

group-id *id*: Specifies the group identifier for the group to which this MME belongs as an integer from 0 through 65535.

mme-code *code*: Specifies the unique code for an MME service as an integer from 0 through 255.

address *ipv4_address*: Specifies the IP address of the peer MME in IPv4 dotted-decimal notation.

tai-match priority *value* mcc *number* mnc *number* tac { *area_code* | any | *start_area_code* to *end_area_code* } address *ipv4_address*

Specifies that an MME with values matching those configured in this Tracking Area Identifier (TAI) match, is to be considered a peer MME. This keyword provides a priority-ordered list of TAI descriptions where the Tracking Area Code (TAC) field may be either an exact value, a range of values, or a "wildcard" value. It also provides an IP address of the peer MME corresponding to the TAI description.

priority *value*:

mcc *number*: Sets the mobile country code (MCC) for peer match as an integer from 100 through 999.

mnc *number*: Sets the mobile network code (MNC) for this peer match as an integer from 00 through 999.

tac *area_code*: Sets a specific Tracking Area Code (TAC) for the peer MME match as an integer from 1 through 65535.

tac any: Specifies that any TAC value can be considered for a peer MME.

tac *start_area_code* **to** *end_area_code*: Specifies a range of TACs. MMEs within this range and matching the rest of the criteria in this command are to be considered peer MMEs. *start_area_code* and *end_area_code* are integers from 1 through 268435455.

address *ipv4_address*: Sets a specific IP address for this TAI peer MME match in IPv4 dotted-decimal notation.

Usage Guidelines

Use this command to configure parameters that, when matched by another MME, specifies that MME as a peer for inter-MME relocations.

This command allows configuration for two relocation scenarios:

- **gummei**: an MME receives either an Attach or a TAU request with a Globally Unique Temporary Identity (GUTI) that originated from another MME.
- **tai-match**: an MME receives an S1 Handover Required message and must select a new MME based on the TAI.

Up to 32 peer-mme gummei or tai-match entries may be configured per MME service.

Example

The following command identifies a peer MME with GUMMEI parameters:

```
peer-mme gummei mcc 123 mnc 12 group-id 40000 mme-code 100 address
209.165.200.228
```

peer-sgsn rai

Statically configures Routing Area Identity (RAI) parameters of the peer SGSN environment to facilitate MME-SGSN relocations over S3 or Gn/Gp interfaces.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
peer-sgsn rai mcc mcc_value mnc mnc_value [ nri value ] rac value lac value address
 ip_address capability [ gn ] [ gp ] [ s16 ] [ s3 ]
no peer-sgsn rai mcc mcc_value mnc mnc_value [ nri value ] rac value lac value
```

no

Deletes the specified peer-SGSN RAI parameter configuration from the MME Service configuration.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc *mnc_value*

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

nri *value*

Specifies the Network Resource Identifier (NRI) value, used as an additional identity, as an integer from 0 through 65535.

rac *value*

Specifies the Routing Area Code (RAC) used to facilitate a lookup for a specific peer SGSN as an integer from 0 through 255.

lac *value*

Specifies the Location Area Code (LAC) value, used to facilitate a lookup for a specific peer SGSN, as an integer from 0 through 65535.

address *ip_address*

Specifies an existing IP address of the peer SGSN in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

capability [gn] [gp] [s16] [s3]

Configures the GTP interface capability of the peer SGSN.

gn: Specifies that the peer SGSN is capable of communication over the Gn interface.

gp: Specifies that the peer SGSN is capable of communication over the Gp interface.

s16: Specifies that the peer SGSN is capable of communication over the S16 interface.

s3: Specifies that the peer SGSN is capable of communication over the S3 interface.

Usage Guidelines

Use this command to configure parameters to facilitate a lookup for a specific peer SGSN. These parameters, when matched by an SGSN, specifies that SGSN as a peer for inter-RAT relocations.

The **peer-sgsn** command allows configuration for two relocation scenarios:

- Routing Area Identity (RAI) configuration is used for the lookup of an IP address for a peer MME based on the exact match of the RAI (and optionally NRI).
- Radio Network Controller Identification (RNC-ID) configuration is used for the lookup of an IP address for a peer MME based on the exact match of the RNC-ID.

Up to 32 (combined total) peer-SGSN RAI and RNC-ID entries may be configured per MME service.

Example

The following command configures an SGSN lookup using RAI parameters with Gp interface capability:

```
peer-sgsn rnc-id mcc 123 mnc 12 nri 1557 rac 33 lac 3542 address
209.165.200.226 capability gp
```

peer-sgsn-echo-params

Configures echo parameters for peer SGSN with GN/GP Capability.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
configure
  context context_name
    mme-service mme_service_name
      peer-sgsn echo-params interval interval retransmission-timeout
retransmission_timeout max-retransmissions max-retransmissions reconnect-interval
 reconnect_interval
           no peer-sgsn echo-params
           end
```

no

Removes the path management configuration for peer SGSN with Gn/Gp capability.

interval *interval*: Configures echo interval in seconds. *interval* must be an ineteger between 60 and 300.

retransmission-timeout *retransmission_timeout*: Configures echo retransmission timeout in seconds. *retransmission_timeout* must be an ineteger between 1 and 20.

max-retransmissions *max-retransmissions*: Configures maximum retries for echo request. *max-retransmissions* must be an ineteger between 0 and 15.

reconnect-interval *reconnect_interval*: Configures echo interval to be used once a peer node is detected to be unreachable. Retransmission is not applicable in this time. *reconnect_interval* must be an ineteger between 60 and 86400.

Example

Configures echo parameters for peer SGSN with GN/GP Capability with interval 75, retransmission-timeout 8, max-retransmissios 10 and reconnect-interval 75:

```
peer-sgsn echo-params interval 75 retransmission-timeout 8
max-retransmissions 10 reconnect-interval 75
```

peer-sgsn rnc-id

Statically configures Radio Network Controller Identification (RNC-ID) parameters of the peer SGSN environment to facilitate MME-SGSN relocations over S3 or Gn/Gp interfaces.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

peer-sgsn rnc-id mcc *mcc_value* **mnc** *mnc_value* **rnc** *value* **address** *ip_address* **capability [gn] [gp] [s16] [s3]**
no peer-sgsn rnc-id mcc *mcc_value* **mnc** *mnc_value* **rnc** *value*

no

Deletes the specified peer-SGSN RAI parameter configuration from the MME Service configuration.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc *mnc_value*

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

rnc *value*

Specifies the Radio Network Controller (RNC) identification number used to facilitate a lookup for a specific peer SGSN as an integer from 0 through 65535.

address *ip_address*

Specifies an existing IP address of the peer SGSN in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

capability [gn] [gp] [s16] [s3]

Configures the GTP interface capability of the peer SGSN.

gn: Specifies that the peer SGSN is capable of communication over the Gn interface.

gp: Specifies that the peer SGSN is capable of communication over the Gp interface.

s16: Specifies that the peer SGSN is capable of communication over the S16 interface.

s3: Specifies that the peer SGSN is capable of communication over the S3 interface.

Usage Guidelines

Use this command to configure parameters to facilitate a lookup for a specific peer SGSN. These parameters, when matched by an SGSN, specifies that SGSN as a peer for inter-RAT relocations.

The **peer-sgsn** command allows configuration for two relocation scenarios:

- Radio Network Controller Identification (RNC-ID) configuration is used for the lookup of an IP address for a peer MME based on the exact match of the RNC-ID.
- Routing Area Identity (RAI) configuration is used for the lookup of an IP address for a peer MME based on the exact match of the RAI (and optionally NRI).

Multiple peer-sgsn RNC-ID records can be configured for the same MCC/MNC/RNC, each with different IP addresses. During a handover, if the initial peer SGSN rejects the forward relocation request, the MME will step through any alternate peer SGSNs to attempt the handover.

Up to 32 (combined total) peer-SGSN RAI and RNC-ID entries may be configured per MME service.

Example

The following command configures an SGSN lookup using RNC-ID parameters with Gn interface capability:

```
peer-sgsn rnc-id mcc 123 mnc 12 rnc 2000 address 209.165.200.228 capability
 gn
```

pgw-address

Configures the IPv4 or IPv6 address of the PDN Gateway (P-GW), specifies the protocol for S5 and S8 interfaces, and sets other parameters within the MME service. By default S5 and S8 use GTP protocol for this.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
pgw-address { ipv4_address | ipv6_address } [ collocated-node collocated_node_name
 s5-s8-protocol pmip ]  ue-usage-type ue_usage_type_value [ weight weight ]
no pgw-address { ipv4_address | ipv6_address } [ s5-s8-protocol pmip ]
```

no

Removes a previously configured IP address for a P-GW along with the S5 and S8 interface of P-MIP protocol type, and other parameters from this MME service.

ipv4_address* | *ipv6_address

Specifies the IP address of the P-GW in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

collocated-node

Configures the collocation name to select the collocated S/PGW node IP addresses for MME.

collocated_node_name must be a string of size 1 to 255.

s5-s8-protocol pmip

Specifies that Proxy-MIP is to be used for S5 and S8 interfaces with the P-GW. By default S5 and S8 interface uses GTP protocol.

pmip Sets the protocol to Proxy-MIP for S5 and S8 interface.

ue-usage-type

Configures the ue-usage-type for the gateway. *ue_usage_type_value* must be an integer between 1 through 255.

weight *weight*

Specifies the weight (preference) assigned to the address P-GW for load balancing. *weight* is an integer from 1 through 100 where 1 is the least preferred and 100 is the most preferred. If no weight is specified, the P-GW address is assigned a default weight of 1.

If a weight is assigned to an address, the weights of the P-GW(s) (that are operational) are totaled, and then a weighted round-robin selection is used to distribute new primary PDP contexts among the P-GW(s) according to their weights. As with all weighted round-robin algorithms, the distribution does not look at the current distribution, but simply uses the weights to distribute new requests. For example, two P-GWs assigned weights of 70 and 30 would distribute 70% of calls to one, and 30% to the other. The sum of all weights do not need to total 100.

Usage Guidelines

Use this command to configure the PDN Gateway (P-GW) addresses to use with MME service. This command also changes the default protocol from GTP to P-MIP for the S5 and S8 interface, and assigns a weight to use when sharing the load between associated P-GWs. A maximum of 16 P-GW addresses can be configured with this command.

This command only changes the use of protocol for the S5 and S8 interface. By default a P-GW uses GTP protocol for S5 and S8 interfaces. This command allows an operator to change the protocol to P-MIP for S5 and S8 interface.

When weight is used, the weights of the operational P-GW(s) are totaled and then weighted round-robin selection is used to distribute new default bearer contexts among P-GW(s).

Example

The following command associates the P-GW IP address of *209.165.200.225* to the MME service with S5 and S8 protocol as P-MIP and weight as *90*:

```
pgw-address 209.165.200.225 s5-s8-protocol pmip weight 90
```

The following command removes the above configured P-GW IP address and other parameters:

```
no pgw-address 209.165.200.225 s5-s8-protocol pmip
```

plmn-id

Configures the Public Land Mobile Network (PLMN) identifier for this MME service. The PLMN identifier consists of the Mobile Country Code (MCC) and Mobile Network Code (MNC). A single PLMN ID can be configured per MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] plmn-id mcc *mcc_value* **mnc** *mnc_value*

no

Removes the configured PLMN identifier for this MME service.

⚠

Caution Removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc *mnc_value*

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

Usage Guidelines

Use this command to set the PLMN identifier for this MME service.

Caution Changing or removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

One PLMN identifier is supported per MME service.

Important To configure additional PLMN IDs for this MME service, refer to the **network-sharing** command described in this chapter.

Example

The following command configures the PLMN identifier with MCC value as *102* and MNC value as *20* for this MME service:

```
plmn-id mmc 102 mnc 20
```

policy attach

Configures parameters for the UE Attach procedure.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
policy attach { imei-query-type { imei | imei-sv | none } [
verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted |
deny-unknown | verify-emergency ] ] | reject-non3gpp-char-apn | set-ue-time
 { disable | enable [ prefer-mme after-attach | prefer-msc ] }
default policy attach { imei-query-type | reject-non3gpp-char-apn |
set-ue-time }
```

default

Returns the command to its default setting. Default values are:

imei-query-type: none

reject-non3gpp-char-apn: Reject Attach request with non-3GPP character APN

set-ue-time: disabled

imei-query-type { imei | imei-sv | none }

Configures the IMEI query type for UE attach.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.

reject-non3gpp-char-apn

Enables MME to immediately reject the attach procedure without any APN remapping, if the UE requested APN contains non 3GPP characters. The attach procedure is rejected with ESM cause-code #27 "missing or unknown APN" and T3396 value IE is included in the Attach reject message.

set-ue-time { disable | enable [prefer-mme after-attach | prefer-msc] }

Configures the MME to set the time in the UE during the Attach procedure. Default: **disabled**.

[prefer-mme | prefer-msc]: Specifies which UE-time to use when delivering EMM messages to the UE for cases when a UE performs combined registration.

prefer-mme: The MME shall always send its UE-time information (based on the MME's own settings), and ignore any EMM Information messages sent by the MSC.

after-attach: The MME sends the EMM Information request message after the attach accept procedure.

prefer-msc: In cases where a successful Location Update is performed to a MSC, the MME shall NOT send MME configured information to the UE, and shall transmit only MSC-sent information. In cases where a Location Update procedure is not required (for example, for UEs that are performing EPS only ATTACH), or in cases where the Location Update Procedure is unsuccessful, the MME shall send the MME configured information.

Usage Guidelines

Use this command to configure various MME settings used during the UE Attach procedure.

Example

The following command configures the MME to query the UE for its IMEI and to verify the UEs equipment identity over the S13 interface with an EIR:

```
policy attach imei-query-type imei verify-equipment-identity
```

policy erab-setup-rsp-fail

Sets the handling for ERAB-SETUP-RESPONSE failure message.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

policy erab-setup-rsp-fail retry-timer *retry_timer* **max-retries** *max_retries*

{ default | no } policy erab-setup-rsp-fail retry-timer

policy erab-setup-rsp-fail retry-timer *retry_timer* max-retries *max_retries* { default | no } policy erab-setup-rsp-fail retry-timer

Configures the IMEI query type for UE attach.

- **no** Disables the retry timer mechanism.
- **default** Restores the default value to existing behavior by disabling the retry timer mechanism.
- **policy** Specifies the user-defined policies like idle mode detach behavior etc.
- **erab-setup-rsp-fail** Sets the handling for ERAB-SETUP-RESPONSE failure message.
- **retry-timer** *retry_timer* Configures the retry timer for ERAB Setup Procedure. *retry_timer* must be an integer between 1 and 15.
- **max-retries** *max_retries* Configures the maximum retry limit for ERAB Setup Procedure. *max_retries* must be an integer between 1 and 10.

Usage Guidelines

Use this command to sets the handling for ERAB-SETUP-RESPONSE failure message.

Example

The following command configures the handling for ERAB-SETUP-RESPONSE failure message:

```
policy erab-setup-rsp-fail retry-timer retry_timer max-retries max_retries
```

policy idle-mode

Configures the user-defined behavioral policies of session management for an LTE subscriber in an MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
policy idle-mode detach { explicit | implicit }
default policy idle-mode detach
```

default

Sets the policy configuration to the default behavior for subscriber IDLE mode Detach. The default behavior is Detach Explicit.

idle-mode detach

Configures the IDLE mode Detach behavior of a UE.

detach

Defines the Detach procedure while the UE is in IDLE mode.

explicit

Enables the Explicit Detach while a UE is in IDLE mode. The system will page the UE before Detach procedure is started, and then perform the Explicit Detach procedure. This is the default behavior.

implicit

Enables the Implicit Detach while a UE is in IDLE mode. The system never sends any message to the UE before Detach, and executes the Implicit Detach procedure immediately.

Usage Guidelines

Use this command to set the user-defined policies for session management in this MME service.

Example

The following command sets the Idle Mode Detach policy to Implicit for a user in this MME service:

```
policy idle-mode detach implicit
```

policy inter-rat

Configures inter-RAT policy settings.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
policy inter-rat { ignore-sgsn-context-id | indirect-forwarding-tunnels
always | select-topologic-sgw }
no policy inter-rat { ignore-sgsn-context-id | indirect-forwarding-tunnels
 | select-topologic-sgw }
```

no

Disables the function.

ignore-sgsn-context-id

Configures the MME to ignore any Context-ID mismatch between HSS and HLR and to use the Context-ID from the HSS to override the Context-ID from the source SGSN. If this option is disabled (default), the MME will drop the PDN when there is a Context-ID mismatch.

indirect-forwarding-tunnels always

Enables establishment of Indirect Data Forwarding Tunnels (IDFT) for Gn/Gp-based Serving Radio Network Subsystem (SRNS) relocations. By default, the MME is configured to never establish IDFT.

select-topologic-sgw interface gn

Configures the MME to select the S-GW based on topological closeness to the P-GW for Gn/Gp handoff scenarios. Weighted distribution will occur across node pairs in the same degree and same order. By default this functionality is disabled.

During inter-RAT Gn/Gp based handoffs, the MME does not learn the P-GW host name from the old Gn/Gp SGSN as part of UE context. Without the P-GW host name, selection of the topologically closest S-GW is not possible per 3GPP standards. This functionality enables the MME to use a proprietary mechanism for learning the P-GW host name. For S3 & S10 cases, there is no need to enable this command, as GTPv2 allows the P-GW host name to be communicated to/from S4-SGSN/MME.

This functionality requires the **gw-selection co-location** or **gw-selection topology** commands to be enabled in the call-control-profile mode.

Note: The P-GW is anchored in the inter-RAT handoff scenarios, so regardless of the preferred weight specified in **gw-selection**, the MME always considers the S-GW's weight for weighted distribution purposes.

Usage Guidelines Use this command to enable or disable establishment of indirect data forwarding tunnels for Gn/Gp-based SRNS relocations, and to enable or disable Context-Identifier overriding, and to enable or disable learning the P-GW host name during Gn/Gp handoffs for purposes of topologically-close S-GW distribution.

Example

The following command enables establishment of indirect data forwarding tunnels for Gn/Gp-based SRNS relocations:

```
policy inter-rat indirect-forwarding-tunnels always
```

policy network

Configures the MME to indicate to the P-GW that all peer SGSNs support dual-addressing for bearers and, subsequently, dual-addressing must be supported for all IPv4 and IPv6 PDNs. Dual-addressing on SGSNs is based on the UE's capability to support inter-RAT roaming.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default | no ] policy network dual-addressing-supported
```

default

Returns the command to its default setting of disabled.

no

Removes the ability to send dual-addressing support messaging from the MME to the P-GW.

dual-addressing-supported

Specifies that the MME shall indicate to the P-GW that dual-addressing is supported.

Usage Guidelines Use this command to configure the MME to send messaging to the P-GW that indicate that all peer SGSNs support dual-addressing for bearers and, subsequently, dual-addressing must be supported for all IPv4 and IPv6 PDNs.

Important This command can be used for Pre-release 8 and Release 8 SGSNs.

policy overcharge-protection

Enables overcharge protection where the MME can detect and signal a Loss of Signal Contact to the S-GW which in turn informs the P-GW to stop charging.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

policy overcharge-protection s1ap-cause-code-group *group_name*
{ default | no } policy overcharge-protection

default

Returns the command to its default setting of disabled. This provides the same behavior as the **no** keyword option.

no

Disables overcharge protection. This provides the same behavior as the **default** keyword option.

s1ap-cause-code-group *group_name*

group_name: Specify the name of a preconfigured S1-AP Cause Code Group.

When the received cause code from the eNodeB matches any the cause codes defined in this Cause Code Group, the MME sets the ARRL (Abnormal Release of Radio Link) bit in the Indication IE of the Release Access Bearer Request to the S-GW.

For more information about creating an S1-AP Cause Code Group, refer to the **cause-code-group** command in the *LTE Policy Configuration Mode Commands* chapter, and the **class** command in the *S1AP Cause Code Configuration Mode Commands* chapter.

Usage Guidelines

Important Overcharge protection is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Use this command to enable or disable overcharging protection for this MME service. When enabled, the MME can detect and signal a Loss of Signal Contact to the S-GW which in turn informs the P-GW to stop charging for the UE.

Refer to the *Overcharging Protection* chapter of the *MME Administration Guide* for more information about this feature.

Example

The following command enables overcharging protection for the S1-AP cause code defined in the S1AP Cause Code Group *group1*:

```
policy overcharge-protection s1ap-cause-code-group group1
```

policy overload

Configures the traffic overload policy to control congestion in this service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
policy overload { drop | reject }
default policy overload
```

default

Sets the traffic overload policy action to the fault behavior of Reject.

drop

Specifies that the system is to drop the incoming packets with new session requests to avoid overload on MME node. Default: Disabled

reject

Configures the system to reject the new session/call request and responds with a reject message when the threshold for allowed call sessions is crossed on the MME node. Default: Enabled

Usage Guidelines

Use this command to set the user-defined policies for new call connection attempts when an MME service is overloaded.

Congestion policies at the service-level can be configured for an individual service. When congestion control functionality is enabled, these policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

Example

The following command sets the nw call connect policy to reject the new session/call request in an MME service:

policy overload reject

policy pdn-connect

Configures parameters for the PDN Connect procedure.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

policy pdn-connect reject-non3gpp-char-apn
default policy pdn-connect reject-non3gpp-char-apn

default

Returns the command to its default setting of accepting the PDN Connect request with non-3GPP character APN.

reject-non3gpp-char-apn

Enables MME to immediately reject the PDN connect procedure without any APN remapping, if the UE requested APN contains non 3GPP characters. The PDN connect procedure is rejected with ESM cause-code #27 "missing or unknown APN" and T3396 value IE is included in the PDN connect reject message.

Usage Guidelines

Use this command to configure various MME settings used during the PDN connect procedure.

Example

The following command configures the MME to reject PDN connect request with non-3GPP character APN:

policy pdn-connect reject-non3gpp-char-apn

policy pdn-deactivate

Configures the MME to deactivate a PDN connection if the charging characteristics (CC) AVP changes in the standalone Insert Subscriber Data Request (ISDR) or the Update Location Answer (ULA).

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] policy pdn-deactivate cc-change

no

This command filter instructs the MME to disable the PDN deactivation configuration defined with this **policy** command.

pdn-deactivate

This keyword configures the MME to deactivate the PDN connection based on the AVP included to filter the keyword.

cc-change

This filter represents the charging characteristics AVP. If it is included in the command, then the MME deactivates the PDN connection when the charging characteristics (CC) AVP changes in the standalone Insert Subscriber Data Request (ISDR) or the Update Location Answer (ULA).

Usage Guidelines

With **policy pdn-deactivate cc-change** configured, the MME updates the subscriber DB with the CC information so that the MME would be able to create a PDN connection with the new CC values.

If the deactivated PDN is the last PDN, then the UE is detached from the network and during the UE's next Attach procedure the updated CC information is taken from the subscriber DB and included in a Create Session Request.

If the information is absent from the DB, and if CC IE is not present in transferred PDNs of Context Response message during 3G to 4G TAU, then the MME does not send local default CC IE in CSReq and the PDN is activated

'Disabled' is the default behavior. If deactivation for CC changes is not enabled, then the MME updates the APN's CC information in the subscriber DB and keeps the PDN active if the CC information changes in or is absent from the ISDR.

To confirm the MME's current configuration regarding PDN deactivation, use the following command. The illustration below is a partial display to indicate the current configuration, which will be either 'enabled' or 'disabled':

show mme-service name *service_name*

```
…
…
Policy S1-Reset                      : Idle-Mode-Entry
Policy PDN-Deact CC-Change           : Enabled
Policy Nas-Non-Del                   : Disabled
…
```

Example

The following command configures the MME to deactivate the PDN connection when the CC information changes in or is absent from received ISDR:

```
policy pdn-deactivate cc-change
```

policy pdn-modify

Configures policy for PDN modification procedures.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] policy pdn-modify retry-qos-modify

no

Removes the existing configuration on the re-try of the Modify Bearer Command.

pdn-modify

This keyword specifies that the policy applies to the PDN modification procedure.

retry-qos-modify

Use this keyword to configure the retry of failed HSS initiated QoS modification procedure in next IDLE to ACTIVE transition.

Default: Disabled

Usage Guidelines

Use this command to either enable or disable the retry for QoS modification procedure in the next IDLE to ACTIVE transitions if the previous HSS initiated modification failed due to the following triggers:

- If S1-UE-CONTEXT-RELEASE is received when the Update Bearer procedure in progress.
- If there is an E-RAB modify failure.

If this configuration is enabled, the MME sends the Update-Bearer-Response with cause "EGTP_CAUSE_TEMP_REJECTED_DUE_TO_HANDOVER_IN_PROGRESS" for the first time when the HSS initiated modification fails due to either no response for ERAB-MODIFY from eNodeB or ERAB modify failure and moves the UE to IDLE state.

The basic assumption is that the PGW will retry the Update-Bearer-Request due to the cause sent by the MME in Update-Bearer-Response, this results in PAGING towards the UE and the UE triggers an IM-EXIT procedure. As part of IM-EXIT procedure, the updated QoS values are sent in the INITIAL-CONTEXT-SETUP message towards eNodeB and "MODIFY-EPS-BEARER-CONTEXT-REQUEST" in Downlink NAS message towards UE. This planned retry procedure is performed once after the HSS initiated QoS modification procedure fails due to any of the triggers mentioned above. The MME does not perform the re-try when the UBR gets rejected either partially or a negative response is received from the UE (for example, EGTP Cause - UE REFUSES), validation failures (for example, EGTP Cause - MANDATORY IE INCORRECT, MANDATORY IE MISSING, CONTEXT NOT FOUND) and other successful scenarios.

Example

The following command is used to configure the PDN policy modification procedure and to configure the retry of failed HSS initiated QoS modification procedure in next IDLE to ACTIVE transition:

```
policy pdn-modify retry-qos-modify
```

policy pdn-reconnection

Configures the action by the MME when a PDN connection request to an already connected APN is being processed by the MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
policy pdn-reconnection { multiple | reject | restart }
default policy pdn-reconnection
```

default

Sets the policy for PDN reconnection to its default behavior of Reject.

multiple

Allows multiple connections to a PDN with the same APN and PDN Type. In this case, the existing connection is left unchanged, and the MME attempts to establish an additional connection to the PDN. Default: Disabled

reject

Configures the MME to deny or reject the request, by sending a PDN Connection Reject command. This is the default behavior. Default: Enabled

restart

Deletes the existing connection and initiates an attempt to establish a new connection. Default: Disabled

Usage Guidelines

Use this command to set the user-defined policies for PDN reconnection attempt procedures initiated by a UE in an MME service.

While attached the UE can request connections to PDNs. The PDNs are identified by APN (Access Point Name) and PDN Type (ipv4, ipv6 or ipv4v6).

If the UE requests connection to a PDN for which a connection with the same APN name and PDN type already exists, the MME can: 1) deny or reject the request, by sending a PDN connection reject command; 2) allow multiple connections to a PDN with same APN and PDN Type; or 3) delete the existing connection, and attempt to establish a new connection.

Example

The following command sets the PDN reconnect policy to delete the existing PDN and start the attempt to establish a new connection in an MME service:

```
policy pdn-reconnection restart
```

policy s1-reset

Configures how the MME responds to an S1 interface reset.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
policy s1-reset { detach-ue | idle-mode-entry }
default policy s1-reset
```

default

Returns the command to its default setting of **idle-mode-entry**.

detach-ue

detach-ue: Specifies that UEs are to be implicitly detached from the service upon S1 interface reset.

idle-mode-entry

idle-mode-entry: Specifies that UEs are to be placed into an idle mode condition during S1 interface reset.

Usage Guidelines Use this command to configure how the MME reacts to an S1 interface reset condition.

Example

The following command configures the MME to place UEs into an idle state while the S1 interface is being reset:

```
policy s1-reset idle-mode-entry
```

policy sctp-down

Configures how the MME responds to a failure of the Stream Control Transmission Protocol (SCTP) connection from the eNodeB.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
policy sctp-down { detach-ue | idle-mode-entry }
default policy sctp-down
```

default

Returns the command to its default setting of **idle-mode-entry**.

detach-ue

detach-ue: Specifies that UEs are to be detached from the service when the SCTP connection from the eNodeB fails.

idle-mode-entry

idle-mode-entry: Specifies that UEs are to be placed into an idle mode condition when the SCTP connection from the eNodeB fails.

Usage Guidelines Use this command to configure how the MME reacts to an SCTP connection failure condition.

Example

The following command configures the MME to place UEs into an idle state while the SCTP connection from the eNodeB fails:

```
policy sctp-down idle-mode-entry
```

policy service-request

Configure the behavior of the MME when an initial context setup failure is received during a service request or extended service request procedure.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

policy service-request initial-context-setup-failure s1ap-cause-code-group *group_name* **action idle-mode-entry**
default policy service-request initial-context-setup-failure

default

Returns the command to its default behavior, where it detaches the UE when an initial context setup failure is received during a service request or extended service request procdure.

initial-context-setup-failure s1ap-cause-code-group *group_name* action idle-mode-entry

Configures the behavior of the MME when an initial context failure is received from the eNodeB during a service request or extended service request. By default, the MME detaches the UE. This command configures the MME to move the UE to IDLE MODE instead.

group_name: Specify the name of a preconfigured Cause Code Group. The MME takes the configured action to move the UE to IDLE MODE when the cause code returned from the eNodeB matches any of the cause codes defined in this Cause Code Group.

Refer to the **cause-code-group** command in the *LTE Policy Configuration Mode Commands* chapter, and the **class** command in the *S1AP Cause Code Configuration Mode Commands* chapter for more information.

action idle-mode-entry : Configures the MME to move the UE to IDLE MODE when the cause code returned from the eNodeB matches any of the cause codes in the specified S1-AP cause code group.

Usage Guidelines

Use this command to configure the behavior of the MME when an initial context setup failure is received during a service request or extended service request procedure.

Example

The following command configures the MME to detach the UE when an initial context failure occurs and the eNodeB returns a cause code which matches any of the cause codes configured in the *idle* S1-AP cause code group:

```
policy service-request initial-context-setup-failure s1ap-cause-code-group
 idle action idle-mode-entry
```

policy srvcc

Configures the MME to initiate an HSS Purge after the SRVCC HO where the UE supports DTM. It also allows configuration of a purge timeout value in seconds.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
policy  srvcc  purge-timer seconds
default policy  srvcc
no policy  srvcc  purge-timer
```

default

Returns the command to its default behavior, where the MME does **not** initiate a HSS Purge after the SRVCC HO.

no

Returns the command to its default behavior, where the MME does **not** initiate a HSS Purge after the SRVCC HO. This provides the same function as the **default** keyword.

purge-timer *seconds*

Defines how long in seconds the Purge Timer will run. This is applicable only for SRVCC Handoff without PS Handoff support scenarios.

For example, if **purge-timer** is set to 20 seconds :

If the Context Transfer happens 10 seconds after SRVCC HO, the MME intiates an HSS Purge.

If the Context Transfer happens 30 seconds after SRVCC HO, the MME will NOT initiate an HSS Purge because the Purge Timer has expired.

seconds must be entered as an integer from 1 through 24000.

Usage Guidelines

Use this command to configure the MME to perform the Purge UE procedure to the HSS for UEs which support Dual Transfer Mode (DTM). When configured, the MME initiates an HSS Purge after the following two SRVCC HO scenarios:

For SRVCC Handoff with PS Handoff support, the Purge S6a message is sent immediately after successful completion of the Handoff. For this scenario, the configurable purge timer is not used.

For SRVCC Handoff without PS Handoff support, the configurable timer is initiated and the Purge S6a message is sent if a SGSN Context Request is received prior to timer expiry. If a Context Failure occurs, no HSS Purge S6a message is sent.

Example

The following command configures the MME to perform the Purge UE procedure and sets the purge timer to 20 seconds.

```
policy  srvcc  purge-timer 20
```

policy tau

Configures parameters for the tracking area update (TAU) procedure.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
policy tau { imei-query-type { imei | imei-sv | none } [
verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted |
deny-unknown | verify-emergency ] ] | initial-context-setup-failure
s1ap-cause-code-group group_name action detach-ue | set-ue-time { disable
| enable [ prefer-mme | prefer-msc ] }
default policy tau { imei-query-type  | initial-context-setup-failure |
set-ue-time }
```

default

Returns the command to its default settings:

imei-query-type: **none**

initial-context-setup-failure: Returns the MME to the default behavior, where it moves the UE to IDLE MODE when an initial context setup failure is received during a TAU procedure.

set-ue-time: **disabled**

imei-query-type { imei | imei-sv | none }

Configures the IMEI query type for TAUs.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.

initial-context-setup-failure s1ap-cause-code-group *group_name* action detach-ue

Configures the behavior of the MME when an initial context failure is received from the eNodeB during the processing of a TAU request. By default, the MME moves the UE to IDLE MODE. This keyword configures the MME to detach the UE.

group_name: Specify a preconfigured Cause Code Group. The MME takes the configured action to detach the UE when the cause code returned from the eNodeB matches any of the cause codes defined in this Cause Code Group.

Refer to the **cause-code-map** command in the LTE Policy Configuration mode, and the **class** command in the S1AP Cause Code Configuration mode for more information.

action detach-ue : Configures the MME to detach the UE when the cause code returned from the eNodeB matches any of the cause codes in the specified S1-AP cause code group.

set-ue-time { disable | enable [prefer-mme | prefer-msc] }

Configures the MME to set the time in the UE during the TAU procedure. Default: **disabled**.

[prefer-mme | prefer-msc]: Specifies which UE-time to use when delivering EMM messages to the UE for cases when a UE performs combined registration.

prefer-mme: The MME shall always send its UE-time information (based on the MME's own settings), and ignore any EMM Information messages sent by the MSC.

prefer-msc: In cases where a successful Location Update is performed to a MSC, the MME shall NOT send MME configured information to the UE, and shall transmit only MSC-sent information. In cases where a Location Update procedure is not required (for example, for UEs that are performing EPS only ATTACH), or in cases where the Location Update Procedure is unsuccessful, the MME shall send the MME configured information.

Usage Guidelines

Use this command to configure various MME settings used during the tracking area update (TAU) procedure.

Example

The following command configures the MME to query the UE for its IMEI and to verify the UEs equipment identity over the S13 interface with an EIR:

```
policy tau imei-query-type imei verify-equipment-identity
```

The following command configures the MME to detach the UE when an initial context failure occurs and the eNodeB returns a cause code which matches any of the cause codes configured in the "detach" S1-AP cause code group:

```
policy tau initial-context-setup-failure s1ap-cause-code-group detach
action detach-ue
```

pool-area

Creates an MSC server pool area for the Sv interface or specifies an existing pool area, and enters MME MSC Server Pool Area Configuration Mode.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

pool-area *pool_area_name* **type { hash-value | round-robin }**
no pool-area *pool_area_name*

no

Removes the configured pool-area for this MME service.

pool_area_name

Specifies the name of the pool-area as an alphanumeric string of 1 through 63 characters.

type { hash-value | round-robin }

Defines the MSC server selection scheme, either:

hash-value: The MME selects the MSC server based on the result of the IMSI [(IMSI div 10) modulo 1000].

round-robin: The MME selects the MSC server based on the round-robin scheme.

Usage Guidelines

Use this command to create an MSC server pool area for the Sv interface or specify an existing pool area configuration and enter the MME Pool Area Configuration Mode.

The command also defines the MSC server selection method for the pool area, using either the IMSI hash value, or round-robin.

This command is also used to remove an existing pool area.

A maximum of 24 pool areas can be configured per MME service.

When configured, the MME attempts to select an MSC using the following selection order:

1. Pool area that matches the PLMN and of type hash.
2. Pool area that matches the PLMN and of type round-robin.
3. Pool area that does not have PLMN associated and of type hash.

4. Pool area that does not have PLMN associated and of type round-robin .

Entering this command results in one of the following prompts, based on the pool selection method specified:

```
[context_name]host_name(config-mme-pool-area-hash-value)#
```

```
[context_name]host_name(config-mme-pool-area-round-robin)#
```

Additional commands are defined in the *MME MSC Server Pool Area Configuration Mode Commands* chapter.

Example

The following command defines a pool area named *msc_pool_east* and configures it for the round robin selection mode.

```
pool-area msc_pool_east type round-robin
```

ps-lte

Configures the Public Safety LTE (PS-LTE) mode of operation for this MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ps-lte sgw { ipv4_address | ipv6_address }
no ps-lte
```

no

Disables PS-LTE mode of operation.

sgw { *ipv4_address* | *ipv6_address* }

Configures the IP address of the S11 interface of the S-GW to use for PS-LTE mode of operation.

ip_address specifies the IP address for the S-GW in IPv4 dotted-decimal or IPv6 colon-separated notation.

Usage Guidelines

This feature requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Use this command to enable the MME service for use in a Public Safety LTE (PS-LTE) network. In this mode, the MME is co-located with an S-GW and at least one P-GW, and the MME must always use the co-located S-GW and a co-located P-GW for all calls that it handles. This requires configuring the IP addresses of the S11 interface of the S-GW as part of the MME service configuration.

Configuration of the S5/S8 interface to the P-GW must be configured separately as part of an APN profile configuration (refer to the **pgw-address** command within the *APN Profile Configuration Mode* chapter in the *Command Line Interface Reference*).

When enabled, all other S-GW selection mechanisms are overridden. The MME will only use the S-GW configured for PS-LTE operation and the P-GW configured in the matching APN profile, regardless of any other configuration present.

Example

The following command enables PS-LTE mode for this MME service and configures the IP address of the S11 interface for the S-GW as 209.165.200.231.

```
ps-lte sgw 209.165.200.231
```

relative-capacity

Configures a relative capacity variable that is sent to the eNodeB for use in selecting an MME in order to load balance the pool.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

relative-capacity *number*
default relative-capacity

default

Returns the command to its default setting of 255.

number

Specifies the relative capacity or weight of an MME compared to others in an MME pool as an integer from 0 through 255.

Default: 255

Usage Guidelines

Use this command to configure the relative capacity or weight of this MME in comparison to other MMEs in a pool. This value is sent to the eNodeB in the S1AP S1 SETUP RESPONSE message.

If this value is changed after the S1 interface is initialized, the MME CONFIGURATION UPDATE message is used to update the eNodeB with the change.

Example

The following command sets this MME with a relative capacity or weight of *100*:

```
relative-capacity 100
```

s13

Enables the MME to send additional Mobile Identity check Requests (MICR) towards the EIR over the S13 interface.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] s13 additional-id-check { attach | handover | tau }

no

This command filter instructs the MME to remove and disable the specified feature configuration from the MME Service configuration.

additional-id-check { attach | handover | tau }

attach - This keyword instructs the MME to send additional MICR in response to an Attach procedure.

handover - This keyword instructs the MME to send additional MICR in response to a Handover procedure.

tau - This keyword instructs the MME to send additional MICR in response to a Tracking Area Update procedure.

Usage Guidelines

By default, this additional imei checking functionality is disabled. Use this command to configure the MME to send additional Mobile Identity check Requests (MICR) towards the EIR over the S13 interface. You must choose at least one triggering UE procedure. You may repeat the command as needed to configure multiple triggering UE procedures.

Example

The following commands must be issued separately. They instruct the MME to send additional IMEI check Requests to the EIR during UE Attach procedures and UE Handovers :

```
s13 additional-id-check attach
s13 additional-id-check handover
```

s1-mme ip

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending packets of a particular 3GPP QoS class over the S1-MME interface.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
s1-mme ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 |
af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5
 | cs6 | cs7 | ef }
default s1-mme ip qos-dscp
```

qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

Default: **af11**

Specifies the DSCP for the specified QoS traffic pattern. **qos-dscp** can be configured to any one of the following:

af11: Assured Forwarding 11 per-hop-behavior (PHB)

af12: Assured Forwarding 12 PHB

af13: Assured Forwarding 13 PHB

af21: Assured Forwarding 21 PHB

af22: Assured Forwarding 22 PHB

af23: Assured Forwarding 23 PHB

af31: Assured Forwarding 31 PHB

af32: Assured Forwarding 32 PHB

af33: Assured Forwarding 33 PHB

af41: Assured Forwarding 41 PHB

af42: Assured Forwarding 42 PHB

af43: Assured Forwarding 43 PHB

be: Best effort forwarding PHB

cs0: Class Selector 0 PHB

cs1: Class Selector 1 PHB

cs2: Class Selector 2 PHB

cs3: Class Selector 3 PHB

cs4: Class Selector 4 PHB

cs5: Class Selector 5 PHB

cs6: Class Selector 6 PHB

cs7: Class Selector 7 PHB

ef: Expedited forwarding PHB

Usage Guidelines DSCP levels can be assigned to specific traffic patterns to ensure that packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the IP header of every subscriber packet transmitted over the S1-MME interface(s).

Example

The following command sets the DSCP-level for traffic sent over the S1-MME interface to **af12**:

```
s1-mme ip qos-dscp af12
```

s1-mme sctp port

Configures the source Stream Control Transmission Protocol (SCTP) port that will be used for binding the SCTP socket to communicate with the eNodeB using S1AP with this MME service.

Product MME

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
s1-mme sctp port port_num
default s1-mme sctp port
```

default

Sets the SCTP port to the default value of 36412 to communicate with the eNodeBs using S1-MME interface.

port_num

Specifies the SCTP port number to communicate with the eNodeBs using S1-MME interface as an integer from 1 through 65535. Default: 36412

Usage Guidelines Use this command to assign the SCTP port with SCTP socket to communicate with the eNodeB using S1AP.

Only one SCTP port can be associated with one MME service.

Example

The following command sets the default SCTP port number 699 for to interact with eNodeB using S1AP on S1-MME interface:

```
default s1-mme sctp port
```

s1-ue-context-release

Specifies the cause code to be sent in a UE-CONTEXT-RELEASE message initiated by the MME upon the reception of any unexpected procedure over Initial-UE from the eNodeB, such as TAU, Service Request, Extended Service Request, Attach Request..

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ]s1-ue-context-release reason { { init-ue-from-enodeb cause type { nas value  nas_value  | radio value radio_value } }| { { attach-reject | tau-reject } emm-cause-code { value specific_emm_value | any } s1-nas-cause cause_value [ new-s1-nas-cause cause_value ] } }
default s1-ue-context-release reason init-ue-from-enodeb cause
```

default

Resets the MME Service configuration to the system defaults.

attach-reject

Specifies the ATTACH reject message sent by the MME.

emm-cause code { value *specfic_emm_value* | any }

Specifies the EMM Cause Code value for which mapping needs to be applied. The **value** keyword specifies a specific EMM cause code, and the **any** keyword specifies any one of the available EMM cause code.

nas value *nas_value*

nas_value must be an integer from 0 to 4.

- 0 - Normal Release (default value)
- 1 - Authentication Failure

- 2 - Detach
- 3 - Unspecified
- 4 - CSG Subscription Expiry

new-s1-nas-cause *cause_value*

Specifies the S1 NAS cause code that needs to be sent in the S1-UE-CONTEXT_RELEASE, which is sent from the MME.

radio value *radio_value*

radio_value must be an integer from 0 to 38.

- 0 - Unspecified
- 1 - TX2RELOCOverall Expiry
- 2 - Successful Handover
- 3 - Release due to E-UTRAN Generated Reason
- 4 - Handover Cancelled
- 5 - Partial Handover
- 6 - Handover Failure In Target EPC/eNB Or Target System
- 7 - Handover Target not allowed
- 8 - TS1RELOCoverall Expiry
- 9 - TS1RELOCprep Expiry
- 10 - Cell not available
- 11 - Unknown Target ID
- 12 - No Radio Resources Available in Target Cell
- 13 - Unknown or already allocated MME UE S1AP ID
- 14 - Unknown or already allocated eNB UE S1AP ID
- 15 - Unknown or inconsistent pair of UE S1AP ID
- 16 - Handover desirable for radio reasons
- 17 - Time critical handover
- 18 - Resource optimisation handover
- 19 - Reduce load in serving cell
- 20 - User inactivity
- 21 - Radio Connection With UE Lost
- 22 - Load Balancing TAU Required
- 23 - CS Fallback Triggered
- 24 - UE Not Available For PS Service
- 25 - Radio resources not available
- 26 - Failure in the Radio Interface Procedure
- 27 - Invalid QoS combination
- 28 - Inter-RAT redirection
- 29 - Interaction with other procedure
- 30 - Unknown E-RAB ID
- 31 - Multiple E-RAB ID instances
- 32 - Encryption and/or integrity protection algorithms not supported
- 33 - S1 intra-system Handover triggered
- 34 - S1 inter system Handover triggered

- 35 - X2 Handover triggered ...
- 36 - Redirection towards 1xRTT
- 37 - Not supported QCI value
- 38 - invalid CSG Id

s1-nas-cause *cause_value*

Specifies the S1 NAS cause code that needs to be mapped.

tau-reject

Specifies the TAU reject message sent by MME.

Usage Guidelines

By default, an MME initiates the UE-CONTEXT-RELEASE with cause NAS-Normal-Release whenever the MME receives any procedure Request over Initial-UE if the UE is in the connected state. This command makes it possible for the operator to configure a preferred cause code for the reason of the disconnect.

Important In earlier releases, the keyword was **init-ue-from-enodeb-for-tau**. In release 19.2, the name and behavior associated with this keyword changed. The keyword name is **init-ue-from-enodeb**. In support of backward compatibility, the MME will accept configurations with either form of the keyword. When the operator explicitly saves the configuration, the configuration will save using the new form of the keyword.

Beginning with release 19.2, the **init-ue-from-enodeb** reason instructs the MME to initiate the UE-CONTEXT-RELEASE with cause NAS-Normal-Release whenever the MME receives a request over Initial-UE not just for TAU but for all TAU and non-TAU scenarios (such as Service Request, Attach, and Extended-Service-Request) if the UE is in the connected state.

In release 19.5, MME is modified to include S1 NAS Cause Code mapping. This configuration allows the MME to configure the S1 NAS cause code mapping to be sent in S1-UE-CONTEXT-RELEASE initiated from the MME after an ATTACH or TAU is rejected with a specific EMM cause code or any EMM cause code. The newly configured S1 NAS cause code is sent in the UE-CONTEXT-RELEASE message whenever MME releases the existing S1AP connection with the configured S1 NAS cause after an ATTACH/TAU message gets rejected, along with a specific EMM cause or any EMM cause code based on the configuration.

Example

Include 'Authentication Failure' as the cause included in the UE-CONTEXT-RELEASE:

```
s1-ue-context-release reason init-ue-from-enodeb cause type nas value  1
```

The following configuration for S1 NAS cause code mapping is configured for an ATTACH reject with a specific EMM cause code value:

```
s1-ue-context-release reason attach-reject emm-cause-code value 1
s1-nas-cause 3 new-s1-nas-cause 0
```

The following configuration for S1 NAS cause code mapping is configured for an ATTACH reject with any EMM cause code value:

```
s1-ue-context-release reason attach-reject emm-cause-code any s1-nas-cause
 1 new-s1-nas-cause 0
```

s1-ue-retention

This command enables UE Context Retention during SCTP association recovery. The retention process is controlled by a mandatory retention timer.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

s1-ue-retention retention-timer *timer_value*
no s1-ue-retention

no

Disables the UE Context Retention feature from the MME service.

retention-timer *timer_value*

Configures the retention timer for UE context retention when SCTP is down, in milliseconds. *timer_value* specifies the timer value for retaining SCTP association and must be an integer from 1 to 1200. The configuration must be a minimum of 100 ms and maximum of 120000 ms with granularity of 100 ms.

Usage Guidelines

There is no specific external configuration required to use this feature. The operator can configure the UE Context Retention feature during boot time and runtime, but runtime needs MME service restart. Once the operator completes the configuration, MME enables UE Context Retention during SCTP association failures. There are no specific pre-post configuration requirements for this feature.

Note Enabling the **s1-ue-retention** command takes immediate effect at the MME service level. It is also used to process the S1-Setup Request messages. But, disabling the retention timer affects the SCTP stack whenever SCTP is initialized during start and restart of the MME service. Therefore, disabling and changing the retention timer value needs MME service restart during runtime configuration change. Runtime changes will be reflected in the MME service, but not at the SCTP stack.

The following command enables UE Context Retention during an SCTP association failure for a duration of 200 milliseconds:

s1-ue-retention retention-timer 200

secondary-rat

Enables the Secondary RAT Data Usage Report to support 5G NSA.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

secondary-rat data-usage-report { pgw [sgw] | sgw [pgw] }
[no | remove] secondary-rat data-usage-report

no

Disables the Secondary RAT Usage Report at call-control-profile.

remove

Removes the Secondary-RAT Usage Report configuration from call-control-profile. It fall-back to MME service level configuration.

secondary-rat data-usage-report { pgw [sgw] | sgw [pgw] }

MME sets IR-SGW and IR-PGW flags based on the available options configured for Secondary-RAT data usage report. By default, MME disables the Secondary-RAT data usage reporting towards both SGW and PGW. If the configuration is removed from call-control-profile, then it fall-back to MME-SERVICE level configuration for Secondary-RAT-Data-Usage-Report functionality.

- **secondary-rat data-usage-report pgw**: Disables the Secondary-RAT Usage Report option for S-GW and enables only for PGW.
- **secondary-rat data-usage-report sgw**: Disables the Secondary-RAT Usage Report option for P-GW and enables only for S-GW.
- **secondary-rat data-usage-report pgw sgw**: Enables Secondary-RAT Usage Report option for both SGW and PGW.
- **secondary-rat data-usage-report sgw pgw**: Enables Secondary-RAT Usage Report option for both SGW and PGW.

Usage Guidelines

Use this command to enable the Secondary RAT Data Usage Report to support 5G NSA.

Example

Configures the Secondary-RAT Usage Report option for both SGW and PGW:

```
secondary-rat data-usage-report pgw sgw
```

setup-timeout

Configures the timeout duration for setting up MME calls in this MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

setup-timeout *dur*
default setup-timeout

default

Sets the call setup timeout duration to the default value of 60 seconds.

dur

Specifies the call setup timeout duration (in seconds) for MME calls after which the attempt will be discarded.

dur is an integer from 1 through 10000. Default: 60

Usage Guidelines

Use this command to configured the timeout duration for setting up an MME call with an MME service. One this timer expires, the call setup procedure will be discarded within this MME service.

Example

The following command sets the default setup timeout duration of 60 seconds for MME calls:

default setup-timeout

sgw-blockedlist

This command specifies the configurable parameters required for SGW blockedlisting .

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax

In releases prior to StarOS 21.26:

sgw-blacklist timeout *timer_value* **msg-timeouts-per-min** *number_of_timeouts*
[no] sgw-blacklist

From StarOS 21.26 and later releases:

sgw-blockedlist timeout *timer_value* **msg-timeouts-per-min** *number_of_timeouts*
[no] sgw-blockedlist

no

Disables the SGW Blockedlisting configuration.

timeout *timer_value*

Specifies the period of time the blockedlisted SGW cannot be used for call procedures. The timeout value is an integer ranging from 5 to 86400 seconds.

msg-timeouts-per-min *number_of_timeouts*

Configures the number of message timeouts to wait, before blockedlisting a SGW locally in a session manager instance. Only Create Session Response timeout is considered. The number of message is an integer ranging from 1 to 5000.

Usage Guidelines

Use this command to blockedlist un-accessible or un-responsive SGWs. The MME does not select these blockedlisted SGWs during any procedures that requires SGW selection so that there is minimal latency during the procedures.

Example

In releases prior to StarOS 21.26:

A sample configuration for SGW blacklisting is as follows:

sgw-blacklist timeout 8 msg-timeouts-per-min 8

From StarOS 21.26 and later releases:

A sample configuration for SGW blockedlisting is as follows:

sgw-blockedlist timeout 8 msg-timeouts-per-min 8

sgw-restoration

This command restores PDN connections on the MME after an S-GW failure.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

sgw-restoration session hold-timeout *max_restore_time*
no sgw-restoration

no

This command prefix disables S-GW restoration from the configured MME Service.

session

This keyword specifies the S-GW session having the disconnected PDN to be restored.

hold-timeout*max_restore_time*

This keyword specifies the maximum time available to restore the sessions at S-GW, that is, the number of PDN connections to be restored through the S-GW. *max_restore_time* specifies the time duration for S-GW Restoration in seconds as an integer from 1 to 3600.

Note If S-GW Restoration is enabled at an MME Service level and at an APN Profile level, the **hold-timeout** value of the APN Profile configuration will take precedence over that of the MME Service level.

Usage Guidelines

The T-Release-PDN timer is configured as part of the S-GW Restoration procedure. The MME restores as many PDN connections as it can through an alternative S-GW (in case of S-GW failure) or with the same S-GW (in case of S-GW restart), within the configured T-Release-PDN time. On expiry of the timer, MME detaches the remaining PDN connections of the affected S-GW.

PDN restorations are performed in a paced manner. The pacing rate can be configured using the **network-overload-protection mme-tx-msg-rate** command under the *Global Configuration Commands* mode. If the pacing rate is not configured, the internal default pacing rate of 100 restorations per session manager, per second is applied.

Example

The following command configures a maximum time of 500 seconds to restore the sessions at S-GW:

```
sgw-restoration session hold-timeout 500
```

sgw-retry-max

Sets the maximum number of SGW selection retries to be attempted during Attach/HO/TAU. By default, this functionality is not enabled.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Command Modes

Exec > Global Configuration > MME Service Configuration

configure > mme-service *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-mme-serviceprofile_name)#`

Syntax Description

sgw-retry-max *max_number*

no sgw-retry-max

no

Disables the configuration for the maximum number of retries.

max_number

Sets the maximum number of retries possible. Enter an integer from 0 to 5. If 0 (zero) is configured, then the MME sends Create-Session-Request to the 1st SGW and if that SGW does not reply, the MME does not select any further SGW to retry. The MME then rejects the ongoing procedure (Attach/HO/TAU) and sends a Reject message.

Usage Guidelines

Using the this command sets a limit to the maximum number of SGW selection retries to be attempted during Attach/HO/TAU. This means, the total number of tries would be 1 (the initial try) + the sgw-retry-max value (the maximum number of retries). This command is applicable only to scenarios, where SGW is selected from the DNS pool (i.e. not taken from static configuration of MME). For statically configured SGW nodes the SGW selection takes place only once.

Entering a value with this command overrides the default behavior. If no value is configured, then the MME uses or falls back to the default behavior which is in compliance with 3GPP TS 29.274, Section 7.6. The MME sends Create-Session-Request message to one SGW in the pool. If the SGW node is not available, the MME picks the next SGW from the pool and again sends a Create-Session-Request message. The MME repeats this process. For an Attach procedure, the MME tries up to five (1 + 4 retries) different SGWs from the pool. In the case of a HO procedure, the MME will try every SGW in the entire pool of SGWs sent by the DNS. If there are no further SGW nodes available in the DNS pool or if the guard timer expires, then MME stops trying and sends a Reject with cause "Network-Failure" towards the UE and the UE must restart the Attach/Handover procedure.

Benefits of this configuration -- The amount of signaling at Attach or Handover can be reduced and the amount of time to find an available SGW can be reduced.

If the **sgw-retry-max** command is configured under both the MME service and the Call-Control Profile, then the configuration under Call-Control Profile takes precedence.

Example

Use this command to enable the functionality for limiting the number of SGWs tried during Attach/HO/TAU to 2 retries:

```
sgw-retry-max 2
```

snmp trap

Enables or disables the SNMP trap for S1 interface connection establishment.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default | no ] snmp trap { s1-initial-establishment |
s1-path-establishment }
```

default

Returns the command to its default setting of disabled.

no

Disables the SNMP trap.

s1-initial-establishment

Specifies that the SNMP trap for the initial S1 interface connection establishment is to be enabled or disabled.

s1-path-establishment

Specifies that the SNMP trap for the S1 path establishment is to be enabled or disabled.

Usage Guidelines

Use this command to enable or disabled the SNMP trap for S1 interface connection establishment.

statistics

Configures the statistics collection mode for the MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
statistics collection-mode { enodeb | tai } [ -noconfirm ]
default statistics collection-mode [ -noconfirm ]
```

default

Configures the command to its default setting, where statistics are collected per eNodeB.

collection mode { enodeb | tai }

Configures the collection mode for statistics.

enodeb: Default - Collect statistics per eNodeB.

tai: Collect statistics per TAI.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to collect statistics for this MME service at the eNodeB level (default), or at the TAI level.

Caution Changing this collection mode **will restart the MME service** and will clear all statistics at the MME service and eNodeB level.

When configured to collect statistics per TAI, the MME will collect statistics only for the TAIs that are configured in the LTE TAI Management Database that is associated with the MME service.

If a specific TAI is configured within multiple TAI Management Databases, the records collected for that TAI will be a sum of all counters for all TAI Management Databases to which it belongs.

Refer to the *TAI Schema* chapter in the *Statistics and Counters Reference* for a listing of all bulk statistics impacted by this command.

Refer also to the **show mme-service statistics** command to display TAI statistics.

Example

The following command configures this MME service to collect statistics per TAI, instead of per eNodeB.

```
statistics collection-mode tai -noconfirm
```

tai

Important The **tai** CLI command introduced with the DECOR feature is not fully qualified in this release. It is available only for testing purposes.

This command allows you to configure the non-broadcast Tracking Area Identity (TAI).

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

tai non-broadcast mcc *mcc_id* **mnc** *mnc_id* **tac** *tac_id*
no tai non-broadcast

no

Deletes the non-broadcast TAI configuration.

mcc *mcc_id*

Configures the mobile country code (MCC) for the specified decor profile. *mcc_id* is a 3-digit number between 000 to 999.

mnc *mnc_id*

Configures the mobile network code (MNC) for the specified decor profile. *mnc_id* is a 2- or 3-digit number between 00 to 999.

tac *tac_id*

Configures the tracking area code (TAC) for the specified decor profile. *tac_id* is an integer from 0 to 65535.

Usage Guidelines

Use this command to configure the Tracking Area Identity (TAI) which is not assigned to any area.

MME provides support for HSS Initiated Dedicated Core Network Reselection. When HSS sends ISDR with different UE-Usage-Type value other than what is already used by the subscriber and MME decides to move that UE to a new DCN, MME will send the GUTI Reallocation command with unchanged GUTI and non-broadcast TAI.

Example

The following command configures non-broadcast TAI with MCC set to *123*, MNC set to *456* and TAC set to *1234* for this MME service:

```
tai non-broadcast mcc 123 mnc 456 tac 1234
```

trace cell-traffic

This command allows you to enable realtime cell traffic tracing for eNodeBs in MME service.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
trace cell-traffic [ trace-extension enb-id ue-s1ap-id ]
no trace cell-traffic
```

no

Disables realtime cell traffic tracing for eNodeBs in MME service.

trace

Specifies the trace configuration for MME.

cell-traffic

Specifies the configuration for eNodeB cell traffic tracing

trace-extension

Defines the UE or eNodeB identity extension parameters.

enb-id

ue-s1ap-id

Usage Guidelines

Use this command to enable or disable realtime cell traffic tracing for eNodeBs in MME service.

ue-db

Configures the UE database that is maintained by the MME as a cache of EPS contexts per UE keyed by IMSI/GUTI to allow the UE to attach by a Globally Unique Temporary Identity (GUTI) and reuse previously established security parameters. This cache will be maintained in each session manager where the first attach occurred for the UE.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

ue-db purge-timeout *dur_mins*
default ue-db purge-timeout

default

Resets the UE database purge timer timeout to the default value of 10080 minutes.

purge-timeout *dur_mins*

Sets the timeout duration (in minutes) for MME to store the UE database in cache memory. This timer starts when the UE goes dormant.

dur_mins is an integer from 1 through 20160. Default: 10080

Usage Guidelines

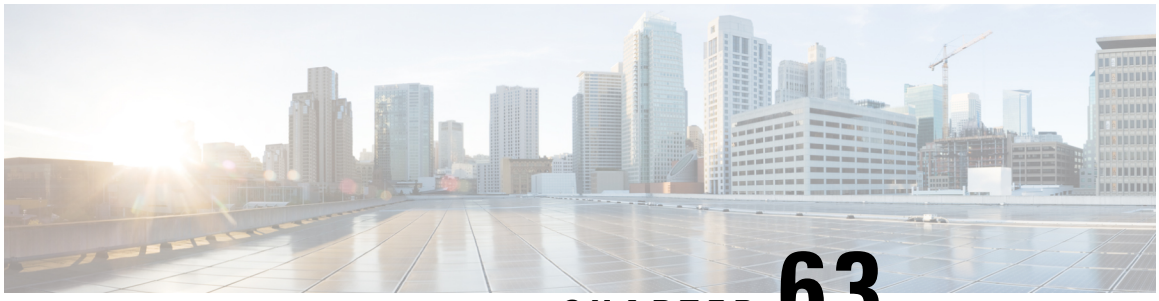
Use this command to set timeout duration for MME to hold UE database information in cache memory.

The MME DB acts as a cache for storing subscriber related information. This subscriber related information helps reduce signaling traffic. The MME DB is a part of the Session Manager and interfaces between the Session Manager Application and Evolved Mobility Management Manager to provide access to the cached data.

Example

The following command configures the MME database cache timer to hold the UE information up to 7 days (10080 minutes) in the MME Database:

default ue-db purge-timeout



CHAPTER 63

MME SGs Service Configuration Mode Commands

The MME SGs Service Configuration Mode is used to create and manage the LTE Mobility Management Entity (MME) SGs services on this system. The SGs service creates an SGs interface between the MME and a Mobile Switching Center/Visitor Location Register (MSC/VLR).

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

associate

Associates or disassociates a Stream Control Transmission Protocol (SCTP) parameter template with the SGs service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

associate sctp-param-template *template_name*
no associate sctp-param-template

no

Removes the SCTP parameter template association.

template_name

Associates an SCTP parameter template with the SGs service.

template_name specifies the name for a pre-configured SCTP parameter template to associate with this SGs service as an alphanumeric string of 1 through 63 characters. For more information on the SCTP parameter template, refer to the **sctp-param-template** command in the *Global Configuration Mode Commands* chapter and the *SCTP Parameter Template Configuration Mode Commands* chapter.

Usage Guidelines

Use this command to associate a pre-configured SCTP parameter template with the SGs service.

Caution This is a critical configuration. Any change to this configuration will cause the SGs service to restart, and the UEs is only supported with EPS Service. In such cases, the UE's are expected to send a COMBINED_IMSI_ATTACH message to the MME to resume the process.

Important If no SCTP parameter template is specified, all default settings for the configurable parameters in the SCTP Parameter Template Configuration Mode apply.

Example

The following command associates a pre-configured SCTP parameter template called *sctp-3* to the SGs service:

```
associate sctp-param-template sctp-3
```

bind

Binds the service to a logical IP interface serving as the SGs interface.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

bind { ipv4-address *ipv4_address* **[ipv4-address** *ipv4_address* **] | ipv6-address** *ipv6_address* **[ipv6-address** *ipv6_address* **] }**
no bind

no

Removes the interface binding from this service.

ipv4-address *ipv4_address* [ipv4-address *ipv4_address*]

Specifies the IPv4 address of the SGs interface in IPv4 dotted-decimal notation.

A secondary IPv4 address can be configured to support SCTP multi-homing.

ipv6-address *ipv6_address* [ipv6-address *ipv6_address*]

Specifies the IPv6 address of the SGs interface in IPv6 colon-separated hexadecimal notation.

A secondary IPv6 address can be configured to support SCTP multi-homing.

Usage Guidelines

Associate the SGs service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an SGs interface that provides the session connectivity for circuit switched fallback (CSFB) to/from a Mobile Switching Center/Visitor Location Register (MSC/VLR). Only one interface can be bound to a service. The interface must be configured prior to issuing this command.

Caution This is a critical configuration. Any change to this configuration will cause the SGs service to restart. Removing or disabling this configuration will stop the SGs service.

Example

The following command binds the logical IP interface with the IPv4 address of *209.165.200.246* to the SGs service:

```
bind ipv4-address 209.165.200.246
```

ip

This command configures the IP parameters on the SGs interface.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ip qos-dscp *dscp_value*

no

Removes IP parameter configuration from the SGs service/interface.

qos-dscp *dscp_value*

The **qos-dscp** keyword designates the Quality of Service - Differentiated Services Code Point value to the packet leaving through the SGs interface.

dscp_value is a value assigned to the packet for DSCP marking. The value can be a pre-defined DSCP value or an arbitrary value ranging from 0x01 to 0x3F.

Usage Guidelines

SGs interface allows Differentiated Services Code Point (DSCP) marking functionality. DSCP marking helps in packet traffic management. DSCP marking can be performed on both IPv4 and IPv6 packets leaving the SGs interface.

Either the pre-defined DSCP values can be used for marking, or any arbitrary value ranging from 0x01 to 0x3F can be assigned. The default DSCP value is 0x00 or be (Best Effort). The default DSCP value is automatically set when the configuration is disabled.

Example

The following command shows the IP configuration for DSCP marking on the SGs service.

```
ip qos-dscp ef
```

lai

This command allows you to configure the non-broadcast Location Area Identity (LAI).

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

lai non-broadcastmcc *mcc_id* **mnc** *mnc_id* **lac** *lac_id*
no lai non-broadcast

no

Removes the non-broadcast LAI configuration.

mcc *mcc_id*

Configures the mobile country code (MCC). mcc_id is a 3-digit number between 000 to 999.

mnc *mnc_id*

Configures the mobile network code (MNC). mnc_id is a 2- or 3-digit number between 00 to 999.

lac *lac_id*

Configures the location area code (LAC). lac_id is an integer from 0 to 65535

Usage Guidelines

Use this command to configure the Location Area Identity (LAI) which is not assigned to any area.

Example

The following command configures non-broadcast LAI with MCC set to 123 , MNC set to 456 and LAC set to 1234 for this MME SGs service:

```
lai non-broadcast mcc 123 mnc 456 lac 1234
```

non-pool-area

Configures a non-pool area where a group of Location Area Code (LAC) values use a specific visitor Location Register (VLR).

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
non-pool-area name use-vlr vlr_name { lac value + | plmnid { any | mcc mcc_value
 mnc mnc_value } }
no non-pool-area name { lac value + }
```

no non-pool-area *name* { lac *value* }

Removes the configured non-pool-area from this service. Optionally, removes a specific LAC or LACs from this non-pool area. *name* is the name of an existing non-pool-area expressed as an alphanumeric string of 1 through 63 characters. *value* is an existing LAC integer value from 1 through 65535.

name

Specifies the name of the non-pool area as an alphanumeric string of 1 through 63 characters.

use-vlr *vlr_name*

Specifies the VLR to be used in this non-pool area configuration as an alphanumeric string of 1 through 63 characters.

lac *value*

Specifies the location area code or codes to be used with the configured VLR in this non-pool area configuration. *value(s)* is an integer from 1 through 65535.

A maximum of 96 areas can be added per non pool area (in a single line, or separately).

plmnid { any | mcc *mcc_value* mnc *mnc_value* }

Specifies the Public Land Mobile Network (PLMN) identifier to be used with the VLR in this non-pool area configuration.

any: Specifies that any PLMN ID can be used with the VLR in this configuration.

mcc *mcc_value* **mnc** *mnc_value*: Specifies the mobile country code (MCC) and mobile network code (MNC) of the PLMN identifier. *mcc_value* must be an integer from 101 through 998. *mnc_value* must be a 2- or 3-digit integer from 00 through 998.

+

Indicates that the LAC value in this command can be entered multiple times. A maximum of 96 areas can be added per non pool area (in a single line or separately).

Usage Guidelines

Use this command to configure a non-pool area where LAC values and/or PLMN IDs are associated with a specific VLR.

A maximum of 48 combined non pool areas and pool areas can be created.

Example

The following command creates a non-pool area named *svlr1* associated with a VLR named *vlr1* and containing LAC values of 1, 2, 3, 4, 5, 6, 7, and 8:

```
non-pool-area svlr1 use-vlr vlr1 lac 1 2 3 4 5 6 7 8
```

pool-area

Creates a location area code (LAC) pool area configuration or specifies an existing pool area and enters the LAC Pool Area Configuration Mode.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] pool-area *pool_name* **[-noconfirm]**

no

Removes the selected pool area configuration from the SGs service.

pool_name

Specifies the name of the LAC pool area configuration. If *pool_name* does not refer to an existing pool, a new pool is created. *pool_name* must be an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to enter the LAC Pool Area Configuration Mode for an existing pool area configuration or for a newly defined pool area configuration. This command is also used to remove an existing pool area configuration.

Note The selection of the pool to use is based on matching PLMN (for Sv) or matching PLMN and LAC (for Sgs).The PLMN used is the one from the TAC/LAC and not from UE (IMSI).

In Release 12.2 and later, a maximum of 48 combined pool areas and non pool areas can be created. In older releases, a maximum of 8 combined pool areas and non pool areas can be created.

Entering this command results in the following prompt:

```
[context_name]hostname(config-sgs-pool-area)#
```

LAC Pool Area Configuration Mode commands are defined in the *MME LAC Pool Area Configuration Mode Commands* chapter.

Example

The following command enters the LAC Pool Area Configuration Mode for a new or existing pool area configuration named *pool1*:

```
pool-area pool1
```

sctp

Configures the Stream Control Transmission Protocol (SCTP) port number for this service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

sctp port *port_number*
no sctp

no

Removes the SCTP configuration for this service.

port *port_number*

Specifies the SCTP port number used to communicate with the MSC/VLR using the SGs interface as an integer from 1 through 65535.

Usage Guidelines

Use this command to assign the SCTP port with SCTP socket to communicate with the MSC/VLR through the SGs interface. A maximum of one SCTP port can be associated with one SGs service.

Example

The following command sets the SCTP port to *29118* for this service:

```
sctp port 29118
```

tac-to-lac-mapping

Maps any Tracking Area Code (TAC) value or a specific TAC value to a LAC value.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

tac-to-lac-mapping { any-tac | tac *value* **} map-to lac** *value* **+**
no tac-to-lac-mapping { any-tac | { tac *value* **} + }**

any-tac | tac *value*

Specifies the TAC to map to the LAC.

any-tac: Specifies that any TAC value is to be mapped to the specified LAC.

tac *value*: Maps a specific TAC value to a LAC value expressed as an integer from 1 through 65535. For specific TAC values, multiple mappings can be entered on the same line (see Example).

map-to lac *value*

Specifies the LAC value that the selected TAC value, or any TAC value is mapped as an integer from 1 through 65535. For specific TAC values, multiple mappings can be entered on the same line (see Example).

For releases 19 and higher, the number of TAC to LAC mappings are increased from 512 to 1024 entries.

Usage Guidelines

Use this command to map TAC values to LAC values.

Enter up to 8 mappings per line.

In Release 12.2 and later, a maximum of 64 mapping lists can be created. In older releases, a maximum of 32 mapping lists can be created.

If no mapping is entered, the default behavior is TAC equals LAC.

Example

The following command maps a TAC value of 2 to a LAC value of 3, a TAC value of 4 to a LAC value of 5, and a TAC value of 6 to a LAC value of 7:

```
tac-to-lac-mapping tac 2 map-to lac 3 tac 4 map-to lac 5 tac 6 map-to lac
 7
```

timer

Configures the SGs-AP timer values.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

timer { ts6-1 *value* **| ts10** *value* **| ts12-1** *value* **| ts12-2** *value* **| ts13** *value* **| ts8** *value* **| ts9** *value* **}**
default timer { ts10 | ts12-1 | ts12-2 | ts13 | ts6-1 | ts8 | ts9 }

default timer { ts10 | ts12-1 | ts12-2 | ts13 | ts6-1 | ts8 | ts9 }

Returns the timer to its default setting.

ts10 *value*

Specifies the Ts10 timer value (in seconds) as an integer from 1 through 30. This timer is used to guard the Implicit IMSI detach from non-EPS services procedure.

Default: 4

ts12-1 *value*

Specifies the Ts12-1 timer value (in seconds) as an integer from 8 through 23048. This timer is used to control the reset of the 'MME-Reset' variable. It is expected to take a value greater than the longest periodic tracking area update timer running on the MME, plus the transmission delay on the radio interface.

Default: 36000

ts12-2 *value*

Specifies the Ts12-2 timer value (in seconds) as an integer from 1 through 120. This timer is used to guard the MME reset procedure. There is one Ts12-2 timer per VLR for which the MME has an SGs association.

Default: 4

ts13 *value*

Specifies the Ts13 timer value (in seconds) as an integer from 1 through 30. This timer configures the retransmission interval for sending SGs message SGsAP-EPS-DETACH-INDICATION to MSC/VLR due to an Implicit IMSI detach from EPS services. If no SGsAP-EPS-DETACH-ACK is received, the MME will resend SGsAP-EPS-DETACH-INDICATION message upon expiry of this timer.

Default: 4

ts6-1 *value*

Specifies the Ts6-1 timer value (in seconds) as an integer from 10 through 90. This timer is used to guard the Location Update procedure. It is expected to take a value greater than 2 times the maximum transmission time in the SGs interface, plus the supervision timer of the Update Location procedure (as defined in 3GPP TS 29.002 [15]).

Default: 15

ts8 *value*

Specifies the Ts8 timer value (in seconds) as an integer from 1 through 30. This timer is used to guard the Explicit IMSI detach from EPS services procedure.

Default: 4

ts9 *value*

Specifies the Ts9 timer value (in seconds) as an integer from 1 through 30. This timer guards the Explicit IMSI detach from non-EPS services procedure.

Default: 4

Usage Guidelines Use this command to configure the SGs-AP timers.

Example

The following command sets the SGs-AP Ts6-1 timer to *20* seconds:

```
timer ts6-1 20
```

vlr

Configures the Visitor Location Register (VLR) to be used by this service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
vlr vlr_name { ipv4-address ipv4_address [ ipv4-address ipv4_address ] |
ipv6-address ipv6_address [ ipv6-address ipv6_address ] } port port_number
no vlr vlr_name
```

no

Removes the configured VLR from this service.

vlr_name

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

ipv4-address *ipv4_address* [ipv4-address *ipv4_address*]

Specifies the IPv4 address of the VLR. *ipv6_address* must be entered in dotted-decimal notation.

A secondary IPv4 address can be configured to support SCTP multi-homing.

ipv6-address *ipv6_address* [ipv6-address *ipv6_address*]

Specifies the IPv6 address of the VLR. *ipv6_address* must be entered in colon-separated hexadecimal notation.

A secondary IPv6 address can be configured to support SCTP multi-homing.

port *port_number*

Specifies the SCTP port number as an integer from 1 to 65535.

Usage Guidelines Use this command to configure the VLR used by this SGs service.

In Release 12.2 and later, a maximum of 48 separate VLRs can be created. In older releases, a maximum of 32 separate VLRs can be created.

Each individual VLR can be defined with up to 10 separate associations to a single MSS pool. Each of these associations support SCTP multi-homing by defining a primary/secondary IP address. Application layer messages are transmitted to the first available association for a particular VLR. If a complete failure of the underlying SCTP layer for a given association (for example, both SCTP paths in a multi-homed configuration) occurs, the VLR association is removed as a candidate for application message transmission until it recovers. A given MMS (VLR) will remain available as long as at least one related association remains available.

When the VLR configuration includes the same pair of peer VLR addresses with different destination port, this results in paging drops. The configuration to support the same IP address and different port is not supported by MME.

Example

The following command configures a VLR to be used by this service with a name of *vlr1*, with an SCTP multi-homed primary IPv4 address of *209.165.200.228*, a secondary IPv4 address of *209.165.200.225* and a port number of *29118*:

```
vlr vlr1 ipv4-address 209.165.200.228 ipv4-address 209.165.200.225 port
29118
```

vlr-failure

Configures automatic VLR failure handling for the SGs service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] vlr-failure duration *minutes* **backoff-timer** *seconds* **detach-rate** *number* **[-noconfirm]**

no

Removes the configuration from this service, which disables automatic detection and offload of VLRs when an SGs association failure occurs.

duration *minutes*

Specifies the amount of time in minutes during which all qualifying UEs will be detached.

The MME splits this duration into *n* intervals, 5 seconds apart. For example, a setting of 2 minutes with 100 subscribers would result in the MME processing all subscribers in the first 2 intervals (10) seconds. Any subscribers remaining at the expiry of the duration will not be processed.

If no detach rate is defined using the **detach-rate** keyword, a maximum of 50 subscribers are processed per interval. Any remaining UEs will remain attached until detached by other means (UE/network detach, etc).

minutes must be an integer from 1 to 3000.

backoff-timer *seconds*

Specifies the period of time that the MME will wait following the detection of a VLR condition before starting the controlled release of affected UEs. The MME begins offloading UEs following the expiry of this backoff timer. If the VLR has recovered before the backoff timer expires, no offloading is performed.

seconds must be an integer from 1 to 3000.

detach-rate *number*

This optional keyword specifies a maximum number of detaches to perform per 5 second cycle.

For example, if 12,000 subscribers are to be detached during a 5 minute window (duration = 5 minutes), the MME calculates 60 cycles (5 minutes / 5-second cycles) which results in 200 UEs to detach per cycle.

If the detach-rate is configured to 100, the MME will only detach 100 per 5 second cycle, resulting in a total of 6000 detaches. Any remaining UEs will remain attached until detached by other means (UE/network detach, etc).

number must be an integer from 1 to 2000.

-noconfirm

Executes the command without additional prompting for command confirmation.

Usage Guidelines

This command requires that a valid MME Resiliency license key be installed. Contact your Cisco account or support representative for information on how to obtain a license.

This command configures the MME to automatically initiate the VLR offload feature when a SGs association failure is detected.

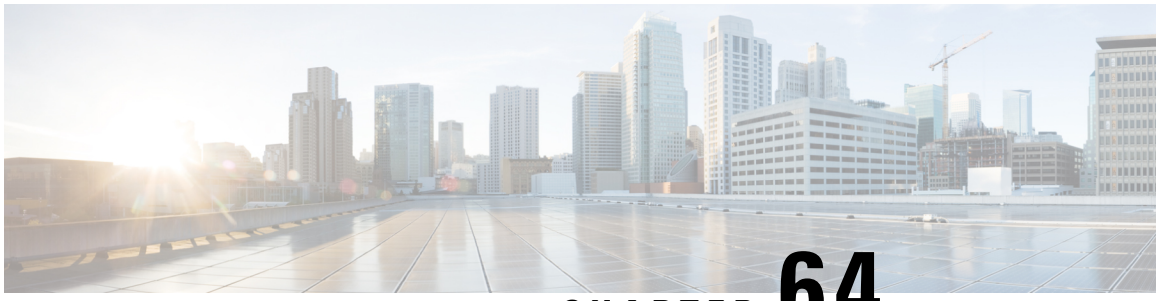
This command provides equivalent functionality to the **sgs vlr-failure** command in the Exec Mode. The differences are that the Exec Mode command must be applied manually, while the command in this mode is applied automatically when a failure condition is detected.

Both commands cannot be enabled simultaneously. An error message is reported to the operator if this is attempted.

Example

The following command enables automatic SGs failure handling functionality. After detecting an SGs association failure, the MME will wait 180 seconds before starting to detach UEs over a 60 minute window, without exceeding a detachment rate of 100 UEs per 5-second cycle:

```
vlr-failure duration 60 backoff-timer 180 detach-rate 100
```



CHAPTER 64

MME SMSC Service Configuration Mode Commands

The MME SMSC Service Configuration Mode is used to create and configure the MME SMSC services on this system. The SMSC peer service allows communication with SMSC peer.

Command Modes

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

configure > context *context_name* **> smsc-service** *smsc_svc_name*

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

diameter

This command configures the Diameter interface to be associated with the SMSC service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SMSC Service Configuration

configure > context *context_name* **> smsc-service** *smsc_svc_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
diameter { dictionary standard | endpoint endpoint_name }
default diameter dictionary
no diameter endpoint
```

default

Configures the default setting.

no

Removes the previous Diameter endpoint configuration.

diameter

Configures the Diameter interface.

dictionary standard

Configures the standard SGd dictionary.

endpoint *endpoint_name*

Enables Diameter to be used for accounting, and specifies which Diameter endpoint to use. *endpoint_name* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure the Diameter interface.

Example

The following command configures the Diameter endpoint named *test* to the SMSC service:

```
diameter endpoint test
```

mme-address

This command configures the MME address to send SMS on the SGd interface.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SMSC Service Configuration

configure > context *context_name* **> smsc-service** *smsc_svc_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

mme-address *mme_address*
no mme-address

no

Removes the previous MME address configuration.

mme_address

Specifies the MME address (ISDN identity) to send SMS on the SGd interface as an integer from 1 to 15.

Usage Guidelines

Use this command to configure the MME address to send SMS on the SGd interface.

Example

The following command configures the MME address with ISDN ID *491720499* to send SMS:

mme-address 491720499

tmsi

This command configures the Temporary Mobile Subscriber Identity (TMSI) for the SMSC service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME SMSC Service Configuration

configure > context *context_name* **> smsc-service** *smsc_svc_name*

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-smsc-service)#

Syntax Description

tmsi *tmsi_value* **non-broadcast mcc** *mcc_value* **mnc** *mnc_value* **lac** *lac_value*
no tmsi

no

Removes the TMSI configuration.

tmsi_value

Specifies the 4-byte M-TMSI as an integer from 1 to 4294967295.

non-broadcast

Configures the non-broadcast Location Area Identifier (LAI).

mcc *mcc_value*

Configures the mobile country code (MCC) portion of non-broadcast LAI for the SMSC service. *mcc_value* must be an integer from 100 through 999.

mnc mnc_value

Configures the mobile network code (MNC) portion of non-broadcast LAI for the SMSC service. *mnc_value* must be a 2- or 3-digit integer from 00 through 999.

lac *lac_value*

Configures the location area code (LAC) value. *lac_value* must be an integer from 1 to 65535.

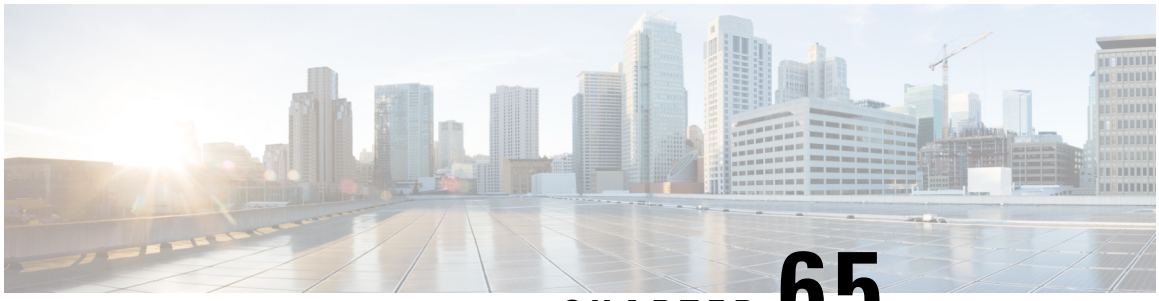
Usage Guidelines

Use this command to configure the TMSI to be sent to UE for the SMSC service.

Example

The following command configures the TMSI for the SMSC service with value set to *123456789012345*, MCC *123*, MNC *456* and LAC *654*:

```
tmsi 123456789012345 non-broadcast mcc 123 mnc 456 lac 654
```



CHAPTER 65

Monitor Group Configuration Mode Commands

Command Modes

The Monitor Group Configuration Mode is used for the configuration of the protocol monitoring peer relations for the group. This mode is entered from the Monitor Protocols Configuration Mode.

Exec > Global Configuration > Context Configuration > Monitor Protocols Configuration > Monitor Group Configuration

configure > context *context_name* **> monitor-protocols > monitor-group** *monitor_group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-monitor-group)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

session-ctx

Configures the protocol monitoring peer relations for the monitor group.

Product

CUPS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Monitor Protocols Configuration > Monitor Group Configuration

configure > context *context_name* **monitor-protocols > monitor-group** *monitor-group-name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-monitor-group)#
```

Syntax Description

session-ctx *session-ctx-name* **local-addr** *IPv4/IPv6_address* **remote-addr** *IPv4/IPv6_address*

session-ctx-name

Specify the name of the context containing the local interfaces over which the protocol monitoring occurs. This must be the same context in which the Sx is configured.

local-addr *IPv4/IPv6_address*

Specify the IPv4 or IPv6 address corresponding to the local interface in the current context.

remote-addr *IPv4/IPv6_address*

Specify the IPv4 or IPv6 address corresponding to the remote peer with which the protocol monitoring occurs.

If the monitor group is configured on the CP, then the remote address is that of the peer UP.

If the monitor group is configured on the UP, then the remote address is that of the peer CP.

Usage Guidelines

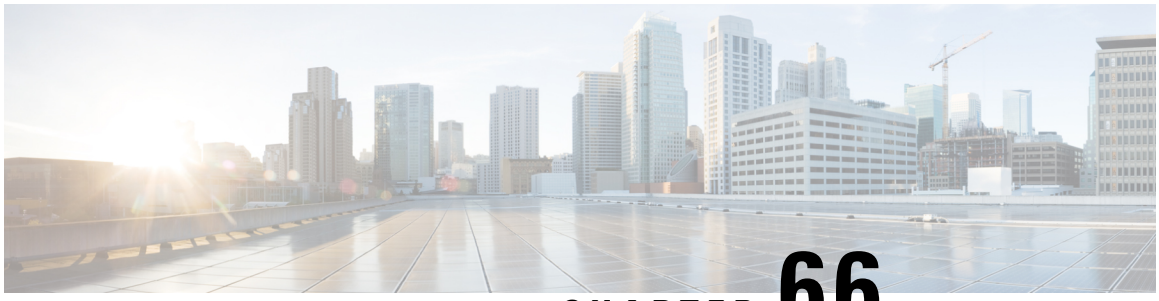
Creates a monitoring relationship within the group for use with CUPS features such as N+2 UP Recovery. Repeat this command to configure multiple relationships.

Configure the monitor protocol groups on both the CP and UP and within the same context as the CUPS Sx interface.

Example

The following command configures a monitoring relationship with UP whose address is *209.165.200.229* and with a local IP address of *209.165.200.228* in a context called *ingress_ctx*:

session-ctx *ingress_ctx* **local-addr** *209.165.200.228* **remote-addr** *209.165.200.229*



CHAPTER 66

Monitor Protocols Configuration Mode Commands

Command Modes

The Monitor Protocols Configuration Mode is used for the configuration of protocol monitoring parameters. This mode is entered from the Context Configuration Mode.

Exec > Global Configuration > Context Configuration > Monitor Protocols Configuration

configure > context *context_name* **> monitor-protocols**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-mon-proto)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

monitor-group

Configures a protocol monitor group and enters the monitor-group configuration mode.

Product CUPS

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Monitor Protocols Configuration

configure > context *context_name* **> monitor-protocols**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-mon-proto)#`

Syntax Description

{ no | default } monitor-group *monitor-group-name* **protocol bfd**

no

Deletes the specified monitor group within the current context.

default

Restores the default state of the monitor group. This keyword is disabled for a specific context.

monitor-group-name

Specify a unique name of the group specifying the BFD monitoring parameters. *monitor-group-name* is an alphanumeric string of 1 through 63 characters.

bfd

Specifies the monitoring protocol as Bidirectional Forwarding Detection (BFD).

Usage Guidelines

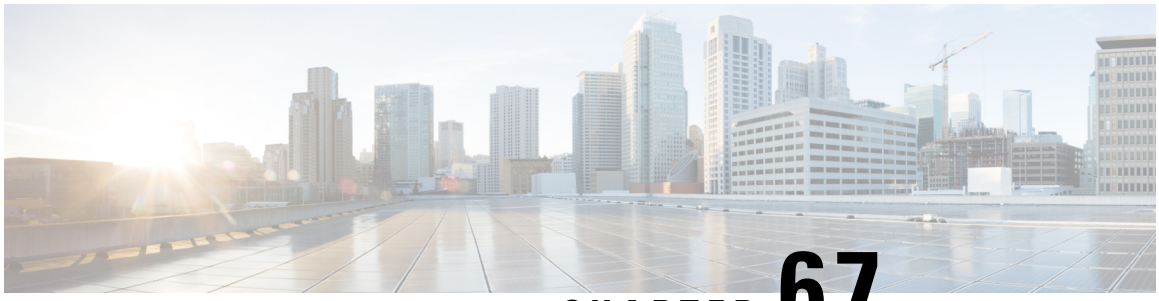
Creates a protocol monitoring group for use with CUPS features such as N+2 UP Recovery.

Use this command to configure multiple monitor-groups specifying unique monitoring group name for each peer relationship.

Example

The following command configures a BFD monitor protocol group named *mp_group_1* within the current context:

monitor-group *mp_group_1* **protocol bfd**



CHAPTER 67

MPLS-IP Configuration Mode Commands

Command Modes

The MPLS-IP Configuration Mode is used for configuration of Multiprotocol Label Switching (MPLS) IP forwarding specific parameters. This mode is entered from the Context Configuration Mode.

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration

configure > context *context_name* **> mpls-ip**

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

protocol ldp

Creates or removes the MPLS label distribution protocol (LDP) configuration, or configures an existing protocol and enters the MPLS-LDP Configuration Mode in the current context. This command configures the protocol parameters for MPLS LDP.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration

configure > context *context_name* **> mpls-ip**

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] protocol ldp

no

Removes the configured MPLS-LDP mode from MPLS-IP Configuration mode.

Usage Guidelines

Use this command to create/ or remove the MPLS LDP configuration, or configure an existing protocol. If required mode already exists it enters the MPLS-LDP Configuration Mode in the current context.

Entering this command results in the following prompt:

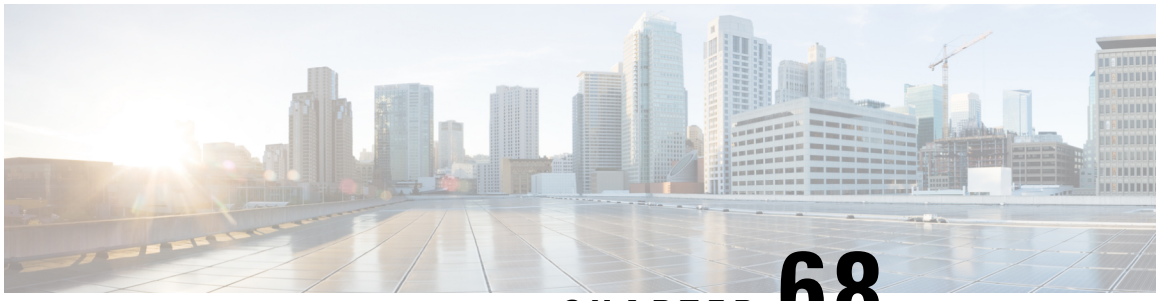
```
[context_name]hostname(config-ldp)#
```

The commands configured in this mode are defined in the *MPLS-LDP Configuration Mode Commands* chapter.

Example

The following command creates and enters the MPLS-LDP Protocol mode:

protocol ldp



CHAPTER 68

MRME Service Configuration Mode Commands

Command Modes

The MRME Service Configuration Mode provides commands to enable a trusted WLAN network to provide access to the Evolved Packet Core (EPC) using a AAA peer functionality.

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

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

Important Available commands or keywords/variables vary based on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

aaa

This command allows you to control the range of EAP-payload size, or restrict the Framed-MTU AVP from being forwarded in the Auth-Request message to the AAA server.

Product SaMOG

Privilege Security Administrator, Administrator

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

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

aaa send framed-mtu *eap_payload_size*
no aaa send framed-mtu

no

Disables SaMOG from forwarding Framed-MTU AVP in the Auth-Request message to the AAA server.

eap_payload_size

Specifies the EAP payload limit for the AAA server to use during the Auth-Response on the link between the NAS and the peer.

twan_profile_name must be an integer from 64 through 1500.

Usage Guidelines This command enables SaMOG to support EAP TLS and EAP TTLS-based authentication. Use this command to control the range of EAP-payload size, or restrict the Framed-MTU AVP from being forwarded in the Auth-Request to the AAA server.

Example

The following command sets the EAP payload size to 1000:

aaa send framed-mtu 1000

associate

This command associates one or more TWAN profile with this MRME service.

Product SaMOG

Privilege Security Administrator, Administrator

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

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] associate twan-profile** *twan_profile_name*

no

Removes the association of the TWAN profile with the MRME service.

twan_profile_name

Specifies the twan profile to associate with the MRME service.

twan_profile_name must be an integer from 1 through 64.

Usage Guidelines

Use this command to associate one or more TWAN profile with the MRME service. Once a TWAN profile is associated with the MRME service, SaMOG uses the Radius clients and access type for the clients configured under the TWAN Profile while processing the Radius messages from WLC.

For more information on configuring the Radius clients and access type, refer the *TWAN Profile Configuration Mode Commands* section.

Example

The following command associates the TWAN profile *twan1* with this MRME service.

```
associate twan-profile twan1
```

attribute

This command allows you to include SSID and Calling-Stationd-Id AVP values as part of DER messages over STa Interfaces.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > **context** *context_name* > **mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
attribute sta { anid { called-station-id | ssid | ssid-wlan-prefix |
wlan-string } | calling-station-id { imsi | ue-mac } }
default attribute sta { anid | calling-station-id }
```

default

Sets the configuration to its default value.

Default calling-station-id: imsi

Default anid: wlan-string

anid { called-station-id | ssid | ssid-wlan-prefix | wlan-string }

Specifies to include the information from the ANID AVP in the DER message.

called-station-id: Include the called station ID from the WLC/AP in the ANID AVP.

ssid: Include the SSID information from the ANID AVP.

ssid-wlan-prefix: Include the SSID WLAN prefix information from the ANID AVP.

wlan-string: Include the WLAN string information from the ANID AVP.

calling-station-id { imsi | ue-mac }

Specifies to include the calling station ID in the DER message.

imsi: Include the IMSI information.

ue-mac: Include the UE MAC information.

Usage Guidelines

Use this command to include the received SSID and Calling-Station-Id values in the ANID/ Calling-Station-Id AVP as part of DER messages over STa Interfaces.

Example

The following command includes ue-mac information from the calling-station-id in the DER message.

```
attribute sta calling-station-id ue-mac
```

bind

This command allows you to configure an IPv4 and/or IPv6 address to be used as the connection point for establishing SaMOG sessions to handle authentication and accounting messages.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

Release 19 and later:

```
bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address
 ipv6_address [ ipv4-address ipv4_address ] }[ auth-port auth_port_number ] [
acct-port acct_port_number ] [ max-subscribers max_subscriber_number ]
no bind { ipv4-address [ ipv6-address ] | ipv6-address [ ipv4-address ]
}
```

Release 18 and earlier:

bind address *ipv4_address* **[auth-port** *auth_port_number* **] [acct-port** *acct_port_number* **] [max-subscribers** *max_subscriber_number* **]**
no bind

no

Removes a previously configured binding.

address *ipv4_address*

Important This option is obsolete from Release 19 onwards.

Specifies the IP address of an interface to be used as the connection point for establishing SaMOG sessions.

ipv4_address must be an IPv4 address expressed in dotted-decimal notation.

Important To define more than one NAS IP address per context, in Global Configuration Mode, use the **aaa large-configuration** command.

ipv4-address *ipv4_address* [ipv6-address *ipv6_address*] | ipv6-address *ipv6_address* [ipv4-address *ipv4_address*]

Important In this release, the configuration of the IPv6 bind address is supported as lab quality only.

Specifies the IPv4 or IPv6 address to be used as the connection point between the WLC and the SaMOG gateway for the RADIUS interface. You can optionally bind a secondary IPv4 address (if the primary bind address is an IPv6 address) or IPv6 address (if the primary bind address is an IPv4 address) to the MRME service.

The second bind address can be bond in the same command or separate commands. When the second bind address is provided, the MRME service restarts and existing sessions are lost for the other bind address.

ipv4_address must be an IPv4 address expressed in dotted-decimal notation.

ipv6_address must be an IPv6 address expressed in colon (or double-colon) notation.

auth-port *auth_port_number*

Specifies the authentication port number of the interface where authentication requests are received. The system binds the default authentication port to 1812.

In addition to the authentication port, the accounting port and maximum subscriber limit can also be configured optionally.

auth_port_number must be an integer from 1 through 65535.

acct-port *acct_port_number*

Specified the accounting port number of the interface where accounting requests are received. The system binds the default accounting port to 1813.

In addition to the accounting port, the maximum subscriber limit can also be configured optionally.

acct_port_number must be an integer from 1 through 65535.

max-subscribers *max_subscriber_number*

Specifies the maximum number of subscriber sessions allowed.

max_subscriber_number must be an integer from 0 through 4,000,000.

Usage Guidelines

Use this command to configure the IPv4 address to be used as the connection point for establishing SAMOG sessions for handling authentication and accounting messages.

Example

Release 19 and later: The following command binds the MRME service with the IPv6 address of 209.165.200.227 and a secondary IPv6 address of 7777::101:1 with an accounting port number of 58 and maximum subscriber limit of 1000.

```
bind ipv4-address 209.165.200.227 ipv6-address 7777::101:1 acct-port 58
max-subscribers 1000
```

Release 18 and earlier: The following command binds the service with an IP address of 209.165.200.227 with an accounting port number of 58 and maximum subscriber limit of 1000.

```
bind address 209.165.200.227 acct-port 58 max-subscribers 1000
```

disconnect

This command allows you to specify the delay duration before which the call is disconnected.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
disconnect { delay-time seconds | preauth-wait-time minutes | wait-time seconds
 }
default disconnect { delay-time | preauth-wait-time | wait-time }
```

default

Configures this command to its default setting.

delay-time default: 30 seconds

preauth-wait-time default: 5 minutes

wait-time default: 10 seconds

delay-time *seconds*

Specifies to configure the timer to retain the session on receiving an Accounting Stop, and for roaming scenarios, session continuity on receiving an Accounting Start.

seconds must be an integer from 1 through 60.

preauth-wait-time *minutes*

Specifies the maximum time (in minutes) to wait in the web authorization pre-authorization phase after which the subscriber's session is cleared, if the post-authorization trigger is not received.

minutes must be an integer from 1 through 60.

wait-time *seconds*

Specifies to configure the timer to wait for accounting start message from the new WLC after processing the accounting stop message from the old WLC.

seconds must be an integer of 10 through 300.

Usage Guidelines

Specifies to configure the timer to wait for accounting stop message after triggering a Disconnect Request Message to WLC for an SaMOG session.

Example

The following command sets the disconnect wait time to 60 seconds.

```
disconnect wait-time 60
```

The following command sets the pre-authorization wait time to 10 minutes:

```
disconnect preauth-wait-time 10
```

dns-P-GW

This command allows you to configure the source context in which the DNS client is configured, or enable/disable P-GW selection based on topology and load-balancing of P-GWs, based on weights from DNS.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

Returns the command to its default value.

default dns-pgw context: MRME will fetch the dns-client configuration from the current context.

default dns-pgw selection topology: MRME will perform P-GW selection based on the topology.

no

If previously configured, removes the dns-pgw configuration.

context *context_name*

Specifies to configure the source context in which the DNS client is configured.

context_name must be an alphanumeric string of 1 through 79 characters.

selection { topology [weight] | weight }

Specifies to enable/disable P-GW selection based on topology and load-balancing of P-GWs based on weights from DNS.

Usage Guidelines

Use this command to configure the source context in which the DNS client is configured, or enable/disable P-GW selection based on topology and load-balancing of P-GWs, based on weights from DNS.

In case of topology-based selection, when the DNS procedure outputs a list of P-GW host names for the APN FQDN, MRME performs the longest suffix match and selects the P-GW which is topologically closest to the MRME/subscriber. In case of weight-based selection, if there are multiple entries with the same priority in the list of P-GW host names for the APN FQDN in the output from the DNS procedure, calls are distributed to the P-GWs according to the weight field in RRs. The weight field specifies a relative weight for entries with the same priority.

Example

This command will configure the source context in which the DNS client is configured to "mrmectx".

```
dns-P-GW context mrmectx
```

fqdn

This command allows you to configure the MRME fully qualified domain name (FQDN) to match the longest suffix during dynamic allocation.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

fqdn *fqdn_name*
{ default | no } fqdn

default

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

no

Removes the configured FQDN from the MRME service configuration.

fqdn_name

Specifies the MRME FQDN name that will be used for the longest suffix match during dynamic allocation.

fqdn_name must be an alphanumeric string of 1 to 255 characters.

Usage Guidelines

Use this command to configure the MRME FQDN under MRME service to match the longest suffix during dynamic allocation.

Example

The following command sets an MRME FQDN value of "topon.eth.mrme.north.blore.3gppnetwork.org".

fqdn topon.eth.mrme.north.blore.3gppnetwork.org

pgw-selection

This command provides P-GW selection related parameters for this MRME service.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] pgw-selection { fallback pgw-id | local-configuration-preferred }

no

Removes the configuration.

local-configuration-preferred

Specifies the SaMOG Gateway to perform P-GW selection based on local configuration.

When this keyword is enabled,

- In the case of dynamic P-GW selection from the AAA server (APN FQDN based selection), the SaMOG Gateway first tries to establish session with the locally configured P-GWs. If the locally configured P-GWs are not reachable, APN FQDN resolution is performed, and SaMOG Gateway tries to establish session with the resolved IP addresses.
- In the case of static P-GW selection from the AAA server (IP address or P-GW FQDN), SaMOG tries to establish session with the AAA server provided P-GW address (IP address or resolved P-GW FQDN). If the AAA server provided P-GW addresses are not reachable, session setup fails.

fallback pgw-id

Specifies the SaMOG Gateway to trigger fall back to locally configured P-GW addresses (or DNS resolved P-GW addresses using APN FQDN) when session establishment with AAA provided P-GW address or DNS provided P-GW address for P-GW FQDN fails.

Usage Guidelines

Use this command to enable SaMOG Gateway to perform P-GW selection based on local configuration.

When the **local-configuration-preferred** keyword is enabled, SaMOG first uses the locally configured P-GW addresses to fall-back to. When the locally configured P-GW addresses are not reachable, SaMOG then uses APN FQDN based P-GW address resolution.

When the **local-configuration-preferred** keyword is not enabled, SaMOG first uses APN FQDN based P-GW address resolution to fall-back to. When the P-GW address resolved using APN FQDN is not reachable, SaMOG then uses the locally configured P-GW addresses.

When session establishment with AAA provided P-GW address or DNS provided P-GW address for P-GW FQDN fails, fall-back is triggered when the **fallback pgw-id** keyword is enabled.

Example

The following command enables the SaMOG Gateway to use locally configured P-GW addresses first for P-GW resolution:

```
pgw-selection local-configuration-preferred
```

radius

This command allows you to specify the IP address and shared secret of the RADIUS accounting and authentication client from which RADIUS accounting and authentication requests are received.

Important From release 16.0 onwards, this command has been deprecated. Instead, use the **radius** command described under the *TWAN Profile Configuration Mode Commands* section.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context *context_name* **> mrme-service** *mrme_service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius client *ipv4_address*[**/***mask*] **{ [encrypted] key** *key* **[[disconnect-message [dest-port** *port_number* **]] [acct-onoff { [aaa-context** *aaa_context_name* **] [aaa-group** *aaa_group_name* **] [clear-sessions] }] }**
no radius client *ipv4_address*[**/***mask*]

no

Removes a previously configured RADIUS client.

ipv4_address[/mask]

Specifies the IP address, and optional subnet mask of the RADIUS client from which RADIUS accounting and authentication requests are received.

ipv4_address[/mask] must be an IPv4 address expressed in dotted-decimal notation.

[encrypted] key *key*

- **encrypted**: Specifies that the shared key between the RADIUS client and this service is encrypted.
- **key** *key*: Specifies the shared key between the RADIUS client and this service.

  key with encryption must be an alphanumeric string of 1 through 288 characters, and without encryption an alphanumeric string of 1 through 127 characters. Note that *key* is case sensitive.

disconnect-message [dest-port *port_number*]

Specifies to send RADIUS disconnect messages to the configured RADIUS accounting client in call failure scenarios.

- **dest-port** *port_number* : Specifies a port number to which the disconnect message must be sent.

  port_number must be an integer from 1 through 65535.

acct-onoff { [aaa-context *context_name*] [aaa-group *group_name*] [clear-sessions] }

Important The **acct-onff** keyword is currently not supported in this release.

Usage Guidelines Use this command to specify the IP address and shared secret of the RADIUS accounting and authentication client from which RADIUS accounting and authentication requests are received.

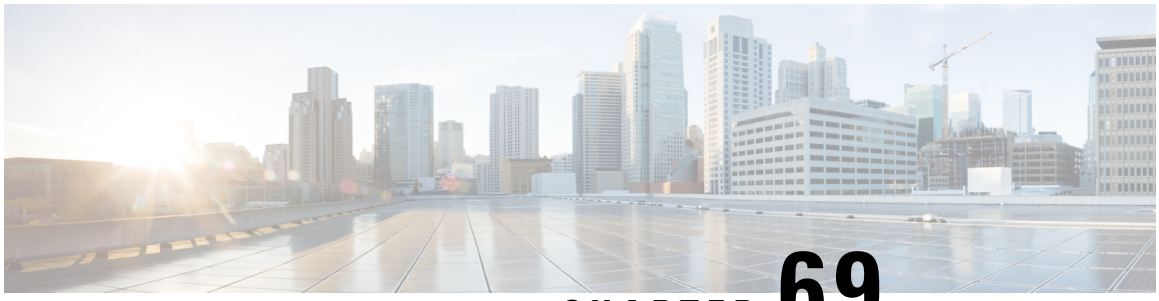
Example

The following command configures the service to communicate with a RADIUS client with an IP address of 209.165.200.244 and an encrypted shared secret of key1234Ax3Z, and clear the session when accounting on/off messages are received:

```
radius client 209.165.200.244 encrypted key 123 4Ax3Z acct-onoff
clear-sessions
```

setup-timeout

This command is currently not supported in this release.



CHAPTER 69

MSISDN Group Configuration Mode Commands

The MSISDN Group Configuration Mode provides commands to configure discrete list and range of Mobile Station International Subscriber Directory Number (MSISDN) numbers.

Command Modes

Exec > Global Configuration > MSISDN Group Configuration

configure > msisdn-group *group_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(msisdn-group)#`

Important Available commands or keywords/variables vary based on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

msisdn cc

This command configures the discrete list of MSISDN numbers.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > MSISDN Group Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(msisdn-group)#
```

Syntax Description

msisdn cc *cc_value* **number** *value*
no msisdn cc *cc_value* **number** *value*

no

Deletes the specified MSISDN numbers.

cc *cc_value*

cc is the country code of the subscriber. *cc_value* is a three digit number between 1 and 999.

number *value*

This keyword allows up to 500 MSISDNs to be configured per group. *value* is 1 to 14 digit MSISDN number.

Usage Guidelines

Use this command to specify the discrete list of MSISDN numbers (Combination of discrete and range line is 20 per group).

Example

The following command configures the CC as *334* and MSISDN as *12345678901234*:

msisdn cc 334 number 12345678901234

range

This command configures the range of MSISDN numbers.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > MSISDN Group Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(msisdn-group)#
```

Syntax Description

range cc *cc_value* **number first** *start_range* **last** *end_range*
no range cc *cc_value* **number first** *start_range* **last** *end_range*

no

Deletes the specified MSISDN numbers.

cc *cc_value*

cc is the country code of the subscriber. *cc_value* is a three digit number between 1 and 999.

number first *start_range* last *end_range*

Specifies the MSISDN range. *start_range* and *end_range* are 1 to 14 digit MSISDN numbers.

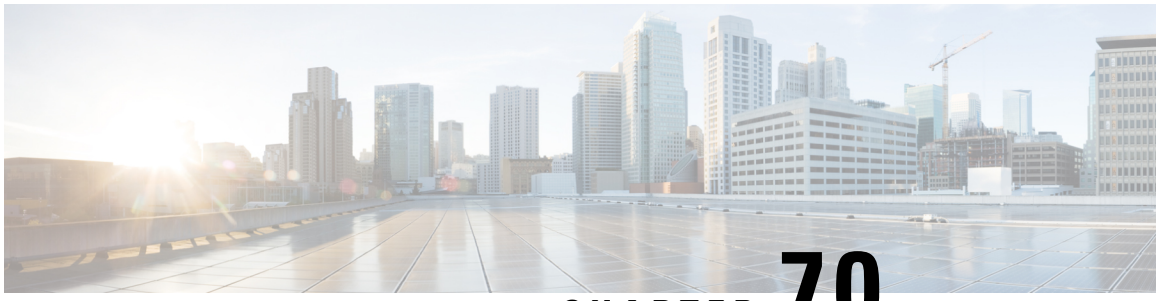
Usage Guidelines

Use this command to configure the MSISDN range.

Example

The following command configures the CC as *334* and MSISDN range as *12345678901234* and *23456789012341*:

```
range cc 334 number first 12345678901234 last 23456789012341
```



CHAPTER 70

NETCONF Protocol Configuration Mode Commands

The NETCONF Protocol Configuration Mode is used to configure the ConfD/NETCONF interface (server confd) with the Cisco Network Service Orchestrator (NSO) and Elastic Services Controller (ESC).

Command Modes

Exec > Global Configuration > Context Configuration >NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

autosave-config

Automatically saves the current ConfD configuration to a specified URL whenever a change is applied by NSO through the ConfD interface. By default, this command is disabled.

Important This command is obsolete in StarOS 21.2 and later releases.

Product All (ASR 5500 and VPC platforms only)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration >NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

`[local]host_name(config-confd)#`

Syntax Description **`[ no ] autosave-config`** *`url`*

no

Disables the autosave configuration.

url

Specifies the URL where the ConfD configuration will be saved as:

`[file:]{/flash | /usb1 | /hd-raid | /sftp}[/`*`<directory>`***`]/`***`<filename>`**

Usage Guidelines Use this command to save the current ConfD configuration to a specified URL whenever a change is applied by NSO through the ConfD interface.

Example

The following command specifies a the URL to which the ConfD configuration will be saved:

`autosave-config /flash/confd.cfg`

bulkstats

Enables bulkstats collection and reporting via REST interface. By default, this command is disabled.

Product All (ASR 5500 and VPC platforms only)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration >NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

`[local]host_name(config-confd)#`

Syntax Description `[ no ] bulkstats`

no

Disables bulkstats gathering on ConfD.

Usage Guidelines Use this command to enable or disable populating ConfD with bulkstats operational data. When enabled, StarOS will send schema information to confdmgr while gathering statistics. Collected bulkstats are stored in the ConfD database for later retrieval over REST interface.

By default, this command is disabled.

For additional information, see the *NETCONF and ConfD* appendix of the *System Administration Guide*.

Example

The following command enables population of bulkstats operational data in ConfD:

```
bulkstats
```

The following command disables populating ConfD with bulkstats operational data:

```
no bulkstats
```

confd-user

Associates a username for all CLI operations via NETCONF. The user will be authenticated with verifiable credentials. This username is used for CLI logging purposes only.

Product All (ASR 5500 and VPC platforms only)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration >NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

Syntax Description `[ no ] confd-user` *username*

no

Disables the ConfD administrative username.

username

Specifies the username as an alphanumeric string of 1 through 144 characters.

Usage Guidelines Use this command to associate a username for all CLI operations via NETCONF.

Important The NETCONF or RESTful session must still be established with verifiable credentials.

For additional information, see the *NETCONF and ConfD* appendix of the *System Administration Guide*.

Example

The following command specifies a name to be associated with all NETCONF operations in the CLI logs:

```
confd-user admin4126
```

kpi

Configures the Key Performance Indicator (KPI) collection interval for Node Selection and Load Balancing (NSLB).

Product All (ASR 5500 and VPC platforms only)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

Syntax Description **kpi** *seconds*

kpi *seconds*

Configures the Key Performance Indicator (KPI) collection interval for NSLB. Default: disabled.

seconds is an integer value of 0 (disabled), or 10 through 120 which sets the time interval in seconds for collecting the following KPIs:

- Percentage session cpu usage
- Percentage session memory usage
- Percentage non session cpu usage
- Percentage non session memory usage
- Percentage session usage

Usage Guidelines Use this command to enable ConfD/REST support for NSLB KPI collection.

For additional information, see the *NETCONF and ConfD* appendix of the *System Administration Guide*.

Example

The following command enables KPI collection with the collection interval of 30 seconds:

```
kpi 30
```

The following command disables KPI collection:

```
kpi 0
```

netconf

Configures the NETCONF interface.

Product

All (ASR 5500 and VPC platforms only)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

Syntax Description

```
netconf { notifications { events level { critical | error | warning |
unusual | info } | snmp } | port port_number }
 no netconf { notifications { events | snmp } |port }
```

no

Restores all the NETCONF parameters to their default values.

notifications events: Disables sending of StarOS events via NETCONF notifications.

notifications snmp: Disables sending of SNMP alerts/alarms via NETCONF notifications.

port: Resets the port number to 830.

notifications events level { critical | error | warning | unusual | info }

When enabled, events logged in StarOS will be sent out as NETCONF notifications on the stream named "StarOS." Level specifies the lowest event severity level that results in a notification. Default: disabled.

- **critical** - Level 1: Reports critical errors contained in log file.
- **error** - Level 2: Reports error notifications contained in log file.
- **warning** - Level 3: Reports warning messages contained in log file.
- **unusual** - Level 4: Reports unexpected errors contained in log file.
- **info** - Level 5: Reports informational messages contained in log file.

Important Any event that is of category "critical-info" (regardless of severity) will also be converted to notifications.

notifications snmp

When enabled, SNMP alerts and alarms will be sent out as NETCONF notifications on the stream named "StarOS_SNMP". Default: disabled.

This configuration setting does not affect the sending of SNMP alarms; if SNMP alarms are configured to be sent to an external server, they will continue to be sent.

The notification will not contain SNMP OIDs but will contain the content used to generate the SNMP alert.

port *port_number*

When **server confd** is enabled, the port is set to the NETCONF default port, 830. This keyword sets the NETCONF interface port number to something other than 830.

port_number must be an integer from 1 through 65535.

Important A change to the NETCONF interface port value will result in a planned restart of ConfD and temporary loss of connectivity over the NETCONF and REST (if enabled) interfaces.

Usage Guidelines

Use this command to configure the NETCONF interface parameters.

For additional information, see the *NETCONF and ConfD* appendix of the *System Administration Guide*.

Example

The following command will generate NETCONF notifications for StarOS events of severity warning, error, or critical:

```
netconf notifications events warning
```

The following command disables NETCONF notifications for all StarOS events:

```
no netconf notifications events
```

The following command sets the NETCONF interface port number to 500:

```
netconf port 500
```

The following command resets the NETCONF interface port number to 830:

```
no netconf port
```

rest

Configures the REST interface.

Product

All (ASR 5500 and VPC platforms only)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration >NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

Syntax Description

```
rest { auth-policy { none | peer | peer-fail } | certificate certificate_name
 | hostname host_name | port port_number }
no rest [ auth-policy | certificate | hostname | port ]
```

no

Restores all the REST parameters to their default values.

auth-policy: none

certificate: Removes any configured certificate and key. REST will not be operational without a valid certificate and key.

hostname: System name is used and matching of hostname is not mandated.

port: Use the default port, 443.

auth-policy { none | peer | peer-fail }

Controls the level of verification the server does on client certificates. CA (certificate authority) certificates can be configured using the existing **ca-certificate** command in Global Configuration mode.

- **none** - No authentication performed.
- **peer** - If the client does not provide a certificate, or the client provides a certificate and it is valid, the connection is allowed. If the client provides a certificate that is not valid, the connection is aborted.

Important If **peer** is selected, CA certificates are recommended; otherwise, a client providing a valid certificate cannot be authenticated and connection will fail.

- **peer-fail** - Server requires the client to supply a client certificate and will fail the connection if certificate is not successfully validated.

Important If **peer-fail** is selected, one or more CA certificates must be present on the device; otherwise, the REST interface will not be enabled.

certificate *certificate_name*

Configures certificate and private-key for REST interface.

certificate_name is an alphanumeric string of 1 to 128 characters.

Important The certificate specified must be present on the device. Certificate and the associated private-key can be configured using the existing **certificate** command in Global Configuration mode.

hostname *host_name*

Specifies a hostname the web server will serve. If configured, mandates the web server to only service requests whose Host field matches the configured hostname.

host_name is an alphanumeric string of 1 to 63 characters.

port *port_number*

Sets the REST interface port number to the specified value.

port_number must be an integer from 1 through 65535.

Usage Guidelines

Use this command to configure the REST interface parameters.

Important Changes to any REST interface parameters may result in a planned restart of ConfD and temporary loss of connectivity over the NETCONF and REST (if still enabled) interfaces.

Changes to global certificates which ConfD is using while REST is enabled will also result in a restart of ConfD.

For additional information, see the *NETCONF and ConfD* appendix of the *System Administration Guide*.

Example

The following command requires the client to supply a client certificate:

```
rest auth-policy peer-fail
```

The following command specifies no client authentication is required:

```
no rest auth-policy
```

The following command specifies existing certificate box1 for the REST interface:

```
rest certificate box1
```

The following command removes any configured certificate and key. REST will not be operational without a valid certificate and key.

```
no rest certificate
```

The following command mandates the web server to only serve URLs adhering to the hostname restconf:

```
rest hostname restconf
```

The following command specifies that the system name is used and matching of hostname is not mandated:

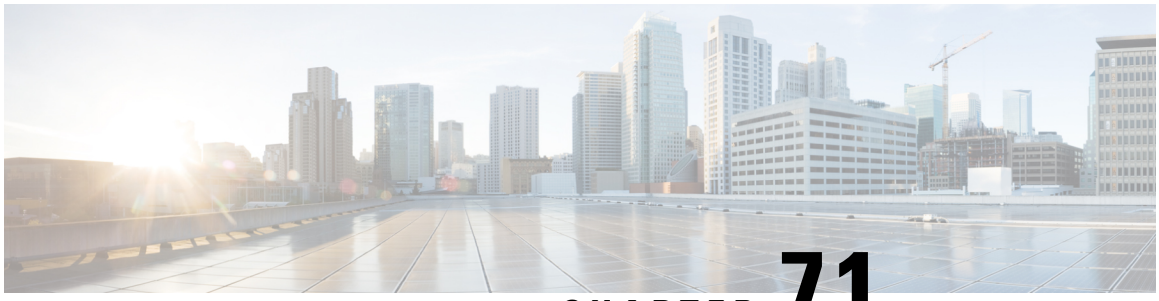
```
no rest hostname
```

The following command sets the REST interface port number to 700:

```
rest port 700
```

The following command resets the REST interface port number to 443:

```
no rest port
```



CHAPTER 71

Network Service Entity- IP Local Configuration Mode Commands

The Network Service Entity (NSE) - IP Local configuration mode is a sub-mode of the Global Configuration mode. This sub-mode configures the local endpoint for NS/IP with the commands and parameters to define the management functionality for the Gb interface between a BSS and an SGSN over a 2.5G GPRS IP network connection.

Command Modes

Exec > Global Configuration > Network Service Entity - IP Configuration

configure > network-service-entity ip-local

Entering the above command sequence results in the following prompt:

```
[local]host_name(nse-ip-local)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

all-nsvc-failure-action

Configure how the SGSN handles the NSE when all NSVCs go down.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Network Service Entity - IP Configuration

configure > network-service-entity ip-local

Entering the above command sequence results in the following prompt:

```
[local]host_name(nse-ip-local)#
```

Syntax Description

all-nsvc-failure-action clear-nse
default all-nsvc-failure-action

default

By default, the NSE is not cleared if all NSVCs go down.

clear-nse

Instructs the SGSN to SGSN to clear NSEs if all NSVCs to the BSC are down. This CLI clears the info only in cases where all the NSVC of NSE go down due to ALIVE time out.

Usage Guidelines

Enable the SGSN to clear NSE information when all NSVCs go down.

Example

Use the following command to configure the SGSN to clear NSEs when all NSVCs go down.

all-nsvc-failure-action clear-nse

associate

This command supports the association of DSCP template at network-service-entity ip local level.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Network Service Entity - IP Configuration

configure > network-service-entity ip-local

Entering the above command sequence results in the following prompt:

```
[local]host_name(nse-ip-local)#
```

Syntax Description

```
associate dscp-template downlink [<template-name>]
no associate dscp-template downlink
```

no

Removes the associate services needed for all IP nses.

dscp-template

Configures DCSP for all IP nses.

downlink *[<template-name>]*

Specifies the DSCP template used for the downlink packets.

template-name: String of size 1 up to 64.

Usage Guidelines

Configuring this command allows the SGSN to send the configured DSCP value to:

- All the GPRS nodal messages.
- All the subscriber specific messages, when dscp template association at gprs-service level and nsei level are absent.

The DSCP template can be defined in sgsn global.

By default, SGSN will apply best effort DSCP value (that is, "0").

Note:

- Atleast one nsvl should be configured, before configuring the DSCP marking at "network-service-entity ip-local" level.
- After the removal of last nsvl, DSCP template association is removed from "network-service-entity ip-local".

Example

The following example associates a DSCP template at network-service-entity ip local level.

```
associate dscp-template downlink DSCP
```

bssgp-timer

This command has been deprecated.

max-ns-retransmissions

This command configures the maximum number of transmission retries counter.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Network Service Entity - IP Configuration

configure > network-service-entity ip-local

Entering the above command sequence results in the following prompt:

`[local]host_name(nse-ip-local)#`

Syntax Description

`[ default ] max-ns-retransmissions { alive` *`count`* `| sns-proc` *`count`* `}`

default

Resets the specified counter configuration to the default value.

alive *count*

Sets the maximum number of alive retries.

count: Must be an integer between 0 and 10. Default is 3.

sns-proc *count*

Sets the maximum number of retries for the SNS procedure

count: Must be an integer between 0 and 5. Default is 3.

Usage Guidelines

Sets the maximum for NS transmission retries.

Example

`max-ns-retransmission alive` *`4`*

ns-timer

This command sets the network service (NS) counters for the SNS procedure and testing.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Network Service Entity - IP Configuration

configure > network-service-entity ip-local

Entering the above command sequence results in the following prompt:

`[local]host_name(nse-ip-local)#`

Syntax Description

`ns-timer { sns-guard` *`timeout_val`* **`| sns-prov`** *`timeout_val`* **`| test`** *`timeout_val`* **`}`**
`default ns-timer { sns-guard | sns-prov | test }`

default

Resets the selected timer configuration to its default value.

sns-guard *timeout_val*

Sets the SNS-guard timer which is used in the auto-learn procedure to clean-up learnt BSC/NSE informtation. Timeout value is in seconds.

timeout_val: Enter an integer from 1 to 300. Default is 60.

sns-prov *timeout_val*

Sets the SNS procedure timeout value in seconds.

timeout_val: Enter an integer from 1 to 10. Default is 5.

test *timeout_val*

Sets the test procedure timeout value in seconds.

timeout_val: Enter an integer from 1 to 60. Default is 30 seconds.

Usage Guidelines

Set NS timers to help manage the NSE-IP connection.

Example

The following example sets the test timer to 4 seconds:

```
ns-timer test 4
```

nsvc-failure-action

This command enables and disables the sending of an NS-STATUS message with cause 'ip-test fail' when NSVC goes down.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Network Service Entity - IP Configuration

configure > network-service-entity ip-local

Entering the above command sequence results in the following prompt:

```
[local]host_name(nse-ip-local)#
```

Syntax Description

```
nsvc-failure-action send-ns-status
default nsvc-failure-action
```

default

Resets the command configuration to its default value. The default action is not to send an NS-STATUS message. This is applicable only to NSVCs that are auto-learned and not configured.

send-ns-status

Enables the sending of the NS-STATUS message.

Usage Guidelines Use this command to enable or disable sending an NS-STATUS messages when an NSVC goes down.

Example

Enable sending of the message:

```
nsvc-failure-action send-ns-status
```

nsvl

This command creates and instance of a network service virtual link (NSVL) and enters the NSVL configuration mode.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Network Service Entity - IP Configuration

configure > network-service-entity ip-local

Entering the above command sequence results in the following prompt:

```
[local]host_name(nse-ip-local)#
```

Syntax Description **[no] nsvl instance** *nsvl_id*

no

Removes the identified NSVL definition from the configuration.

instance *nsvl_id*

Identifies a specific NSVL configuration instance.

nsvl_id: Must be an integer from 0 to 3.

Usage Guidelines Access the NSVL configuration mode.

Example

Enter the NSVL configuration sub-mode to modify the configuration for NSVL instance 2:

```
nsvl instance 2
```

peer-network-service-entity

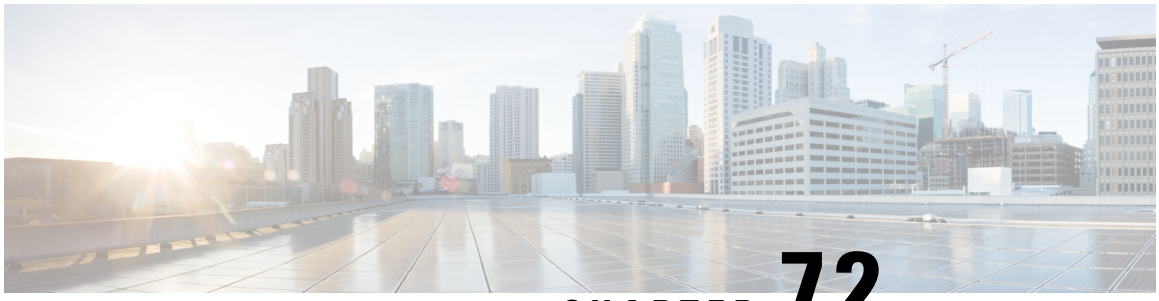
This command has been replaced by the Network Service Entity - Peer NSEI Frame Relay configuration mode.

retry-count

This command has been replaced by the **max-ns-retransmissions** command.

timer

This command has been replaced by the **ns-timer** command.



CHAPTER 72

Network Service Entity - Peer NSEI Configuration Mode Commands

Command Modes

The Network Service Entity (NSE) - Peer NSEI configuration mode configures the Frame Relay parameters for the peer NSE. This mode is a sub-mode of the Global Configuration mode. This sub-mode provides the commands and parameters to define the management functionality for the Gb interface between a BSS and an SGSN over a 2.5G GPRS Frame Relay network connection.

Exec > Global Configuration > Network Service Entity - Frame Relay Peer NSEI Configuration

configure > network-service-entity peer-nsei *nsei_number* **frame-relay**

Entering the above command sequence results in the following prompt:

```
[local]host_name(nse-fr-peer-nsei-nse_id)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

bssgp-timer

This command has been deprecated.

ns-reset-mode

The command configures automatic NS-Reset for a specific Frame Relay peer NSE (network service entity).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Network Service Entity - Frame Relay Peer NSEI Configuration

configure > network-service-entity peer-nsei *nsei_number* **frame-relay**

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(nse-fr-peer-nsei-`*`nse_id`*`)#`

Syntax Description

`ns-reset-mode { active | passive }`
`default ns-reset-mode`

default

Resets the configuration to the passive mode.

active

Configures active mode so that the SGSN is enabled to initiate NS-Reset without manual intervention.

passive

Configures passive mode which means the SGSN continues *not* to initiate NS-Reset.

This is the default mode.

Usage Guidelines

Use this command to configure the SGSN for active mode regarding the peer NSE, so that the SGSN will initiate:

- NS-Reset when NSVC-DLCI binding is done.
- NS-Reset when the link goes down and then comes back.
- NS-Unblock upon receipt of NS-Reset-Ack message.

Active mode is useful in the following scenarios:

- if the SGSN detects LMI down but the BSC does not detect any link failure so does not send NS-Reset.
- if the NS layer can go down and the SGSN will mark the link as 'Blocked-Dead'. If the link comes up later, the NS layer state for that link will remain in the Blocked state.

Example

Configure active mode to perform NS-Reset when the link goes down and comes back up:

`ns-reset-mode active`

ns-vc

This command creates a network service virtual circuit (NSVC) for this frame relay NSE and enters the configuration sub-mode to define the NSVC parameters. These parameters are described in the NSVC Configuration Mode chapter elsewhere in this CLI Reference Guide.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Network Service Entity - Frame Relay Peer NSEI Configuration

configure > network-service-entity peer-nsei *nsei_number* **frame-relay**

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(nse-fr-peer-nsei-`*`nse_id`*`)#`

Syntax Description

`[ no ] ns-vc id` *`ns-vc_id`*

no

Removes the specified NSVC configuration.

id *ns-vc_id*

This keyword defines the NSVC configuration identifier.

ns-vc_id: Must be an integer from 0 to 65535

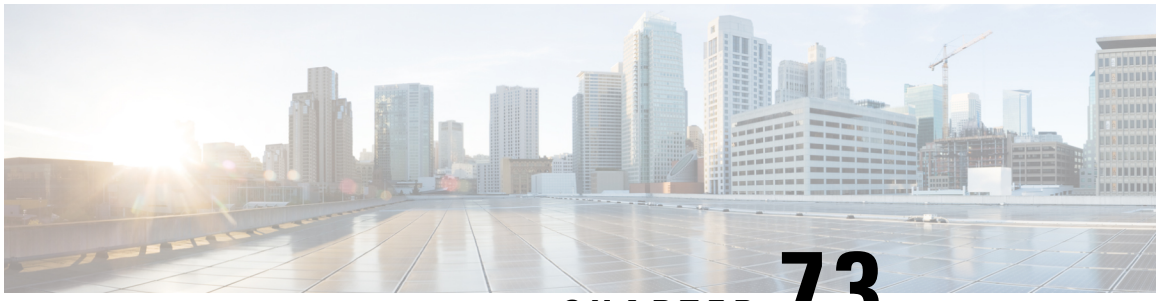
Usage Guidelines

Access the NSVC configuration mode.

Example

Gain access to the NSVC configuration mode to change the 4th instance.

`ns-vc id` *`4`*



CHAPTER 73

Network Service Header - Fields Configuration Mode Commands

The Network Service Header (NSH) - fields configuration mode is a sub-mode of the Global Configuration mode. This sub-mode associates tag values to the nsh-fields.

Command Modes

Exec > Global Configuration > Network Service Header > Network Service Header - Fields Configuration

configure > nsh > nsh-fields

Entering the above command sequence results in the following prompt:

```
[local]host_name(nse-nshfields)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

tag-value

Associates a tag value to a field.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > NSH Configuration > NSH-Fields Configuration

configure > nsh > nsh-fields

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-nshfields)#
```

Syntax Description

[no] tag-value *<value>* **{ content-type | imei | imsi | msisdn | rating-group | rulebase | tdf-app-id }**

no

Disassociates tag-value from the nsh-fields.

content-type

Associates tag-value to the content-type of the payload.

imei

Associates tag-value to the imei of the subscriber.

imsi

Associates tag-value to the imsi of the subscriber.

msisdn

Associates tag-value to the msisdn of the subscriber.

rating-group

Associates tag-value to the rating-group applied to the traffic.

rulebase

Associates tag-value to the rulebase of the subscriber session.

tdf-app-id

Associates tag-value to the tdf application id applied to the traffic.

Usage Guidelines

Use this command to associate a tag value to a field.

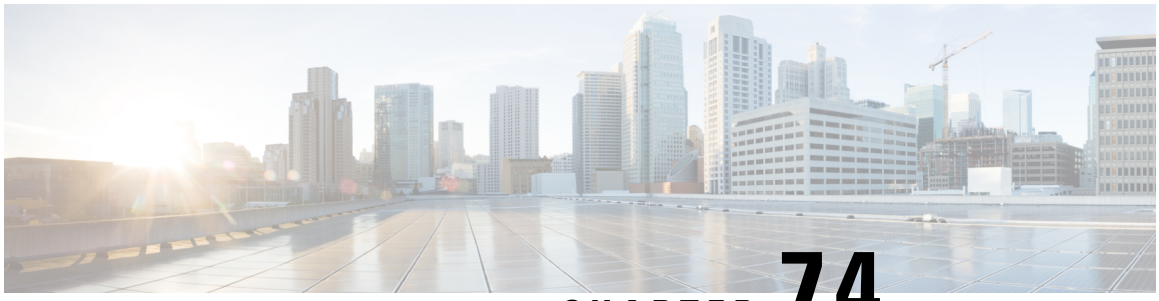
Example

The following commands associates a tag-value to a field:

```
tag-value 10 content-type
tag-value 20 msisdn
```

The following commands disassociates a tag-value from a field:

```
no tag-value 10 content-type
```



CHAPTER 74

Network Service Header - Format Configuration Mode Commands

The Network Service Header (NSH) - format configuration mode is a sub-mode of the Global Configuration mode. This sub-mode defines nsh-format for encoding or decoding NSH header.

Command Modes

Exec > Global Configuration > Network Service Header > Network Service Header - Format Configuration

configure > nsh > nsh-format

Entering the above command sequence results in the following prompt:

```
[local]host_name(nsh-nshformat)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

decode

This command decodes the NSH fields to be associated with the NSH format.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > NSH Configuration > NSH-Format Configuration

configure > nsh > nsh-format

Entering the above command sequence results in the following prompt:

`[local]host_name(config-nshformats)#`

Syntax Description

`[ no ] decode nsh-fields` *`<nsh_fields_name>`*

no

Deletes the nsh-format type.

nsh-fields

Decodes the nsh-fields to be associated with the nsh-format.

Usage Guidelines

Use this command to associate a tag value to a field.

Example

The following commands decodes the nsh-fields to be associated with the nsh-format:

```
decode nsh-fields F1
```

The following commands deletes the nsh-format:

```
no decode nsh-fields F1
```

encode

This command encodes the NSH fields to be associated with the NSH format.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > NSH Configuration > NSH-Format Configuration

configure > nsh > nsh-format

Entering the above command sequence results in the following prompt:

`[local]host_name(config-nshformats)#`

Syntax Description

`[ no ] encode nsh-fields` *`<nsh_fields_name>`*

no

Deletes the nsh-format type.

nsh-fields

Encodes the nsh-fields to be associated with the nsh-format.

Usage Guidelines Use this command to associate a tag value to a field.

Example

The following commands encodes the nsh-fields to be associated with the nsh-format:

```
encode nsh-fields F1
```

The following commands deletes the nsh-format:

```
no encode nsh-fields F1
```

encoding-frequency

This command defines frequency of encoding the NSH fields to be associated with the NSH format.

Product P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > NSH Configuration > NSH-Format Configuration

configure > nsh > nsh-format

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-nshformats)#
```

Syntax Description

```
encoding-frequency { always | once-per-flow }
```

encoding-frequency

Defines frequency of encoding nsh-fields.

always

Encodes nsh fields on every hit.

once-per-flow

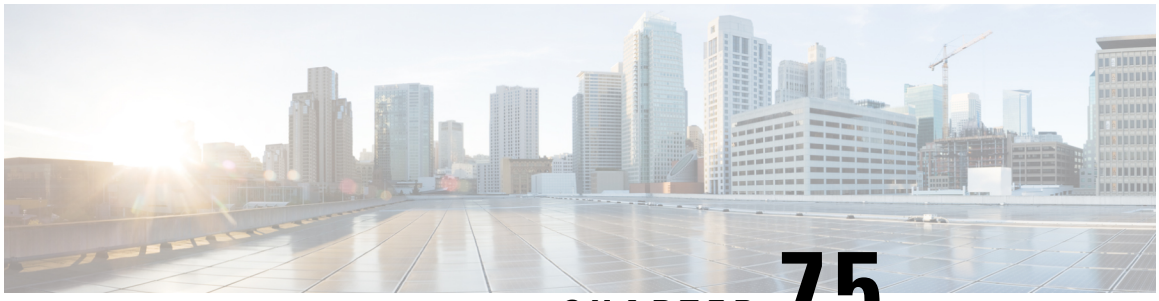
Encodes nsh fields once per flow.

Usage Guidelines Use this command to define the frequency of encoding the nsh fields.

Example

The following commands defines the frequency of encoding the nsh-fields to be associated with the nsh-format:

```
encoding-frequency always
```



CHAPTER 75

Network Service Virtual Connection Configuration Mode Commands

Command Modes

The Network Service Virtual Connection (NSVC) configuration mode is a sub-mode of the Network Service Entity (NSE) - Peer NSEI (for Frame Relay) configuration mode. The NSVC sub-mode creates a configuration instance for a specific NSVC, within the Gb interface, between a BSS and an SGSN in a 2.5G GPRSFrame Relay network connection.

Exec > Global Configuration > Network Service Entity - Frame Relay Peer NSEI Configuration > NSVC Configuration

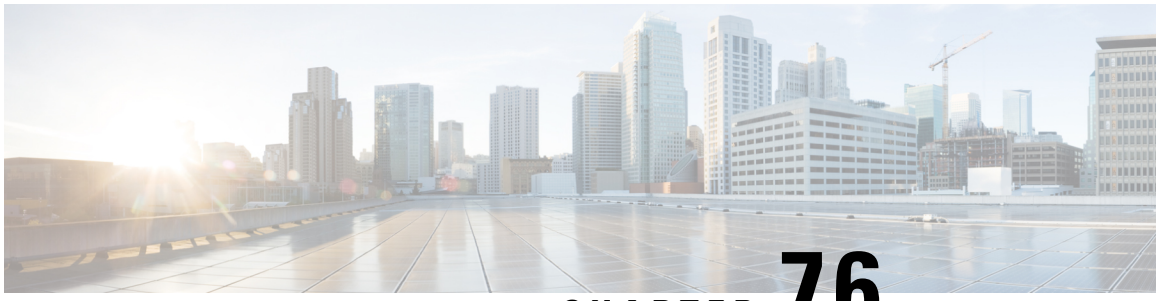
configure > network-service-entity peer-nsei *peer_nsei* **framerelay > ns-vc** *nsvc_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(nse-fr-peer-nsei-nse_id-nsvci-`*`nsvc_instance`*`)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.



CHAPTER 76

Network Service Virtual Link Configuration Mode Commands

Command Modes

The Network Service Virtual Link configuration mode is a sub-mode of the Network Service Entity - IP configuration mode. This sub-mode provides the commands and parameters to define the NSVL of the Gb interface between a BSS and an SGSN in a 2.5G GPRS IP network connection.

Exec > Global Configuration > Network Service Entity - IP Configuration > NSVL Configuration

configure > network-service-entity ip > nsvl instance *nsvl_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(nse-ip-local-nsvl-`*`nsvl_instance`*`)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

nsvl-address

This command configures the IP address of the NSVL. end-point.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Network Service Entity - IP Configuration > NSVL Configuration

configure > network-service-entity ip > nsvl instance *nsvl_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(nse-ip-local-nsvl-nsvl_instance)#
```

Syntax Description

nsvl-address ip-address *ip_address* **context** *ctxt_name* **port** *port_num*

ip-address *ip_address*

Identifies the address of the NSVL.

ip_address: Must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6.

context *ctxt_name*

Identifies the specific context associated with this NSVL address.

ctxt_name: Enter up to 79 alphanumeric characters.

port *port_num*

Specifies the UDP port to associate with the NSVL end-point.

port_num: Must be an integer from 1 to 65535.

Usage Guidelines

Use this command to configure the IP address, context name and port number for the NSVL end-point.

Example

nsvl-address ip-address *209.165.200.225* **context** *sgsn2* **port** *3735*

weight

This command configures the signaling or data weight for NSVL.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Network Service Entity - IP Configuration > NSVL Configuration

configure > network-service-entity ip > nsvl instance *nsvl_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(nse-ip-local-nsvl-nsvl_instance)#
```

Syntax Description

weight { data *data_weight* **| signaling** *signaling_weight* **}**

data *data_weight*

Defines the data weight for the NSVL.

data_weight: Must be an integer from 0 to 255. Default is 1.

signaling *signaling_weight*

Defines the signaling weight for the NSVL.

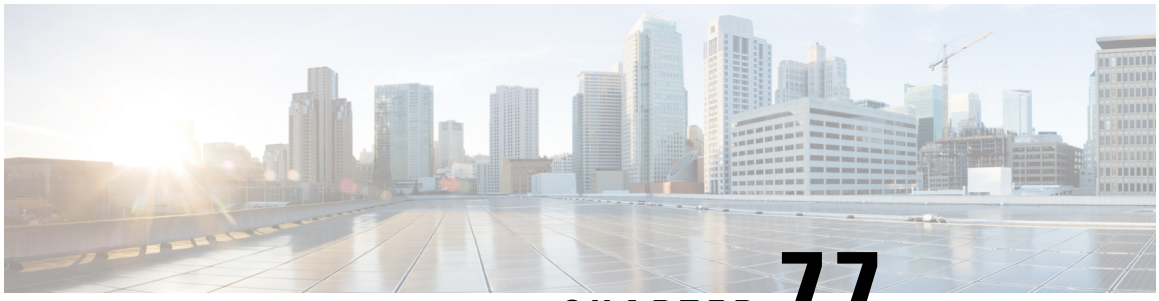
signaling_weight: Must be an integer from 0 to 255. Default is 1.

Usage Guidelines

Configure the weight of the signaling or data for the NSVL.

Example

```
weight data 234
```



CHAPTER 77

NTP Configuration Mode Commands

The NTP Configuration Mode is used to manage the Network Time Protocol (NTP) options for the entire system.

Command Modes

Exec > Global Configuration > NTP Configuration

configure > ntp

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ntp)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

enable

Enables the use of the Network Time Protocol (NTP) for synchronizing the system clock. By default, NTP is not enabled externally and should be configured when the system is initially installed. When enabled, the active ASR 5000 SMC or ASR 5500 MIO will synchronize with external sources. If not enabled, the active SMC or MIO will use its local clock as a time source. In the event of an NTP server or network outage, an already running SMC or MIO will continue to use NTP to maintain time accuracy, but in a holdover mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > NTP Configuration

configure > ntp

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ntp)#
```

Syntax Description

enable [*context* **]**

context

Default: local

Specifies the context for which NTP is to be enabled as an alphanumeric string of 1 through 79 characters.

Important NTP must be configured for use in the local context only. Use of other contexts will cause issues.

Usage Guidelines

Sets the NTP server to be used for the system. Only one NTP server may be active at any given time.

The system uses NTP to synchronize internal clocks on the chassis to external time sources (typically GPS NTP sources, or other Stratum 2 or 3 servers, switches or routers).

All cards with CPUs synchronize to the active SMC or MIO internally. This occurs even if an external NTP server is not configured. In the event of a SMC or MIO switchover, all other cards will start synchronizing with the newly active SMC or MIO automatically.

If any NTP server is enabled, the chassis system clock will be synchronized to the active NTP server which covers all contexts for timing synchronization.

Refer to the *System Administration Guide* for additional information on configuring NTP.

Example

The following command enables use of NTP for the *local* context.

enable

server

Configures a Network TIme Protocol (NTP) server for use by the local NTP client in synchronizing the system clock.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > NTP Configuration

configure > ntp

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ntp)#
```

Syntax Description

server *ip_address* **[prefer] [version** *number* **] [minpoll** *poll_period* **] [maxpoll** *poll_period* **]**
no server *ip_address*

no

Indicates the server specified is to be removed from the list of NTP servers for clock synchronization.

ip_address

Specifies the IP address of the NTP server to be used for clock synchronization in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

NTP should be configured for at least three external NTP servers. With three or more servers, outlyers and broken or misconfigured servers can be detected and excluded. Generally, the more servers the better (within reason).

prefer

Indicates the NTP server specified to be the preferred server. Only one server can be set to preferred. The preferred server is the first one contacted for clock synchronization.

Important Use of the **prefer** keyword is not recommended.

Important Do not change the **version**, **minpoll** or **maxpoll** keyword settings unless instructed to do so by Cisco TAC.

version *number*

Specifies the network timing protocol version to use for server communications as an integer from 1 to 4. Default: 4 (RFC 5905)

minpoll *poll_period*

Specifies the minimum polling interval (in seconds) for NTP messages as a power of 2. *poll_period* is the exponent (power of) expressed as an integer from 6 through 17. For example, if you specify the number 6, the value is 2^6 and the resultant poll period is 64 seconds. Default: 6

maxpoll *poll_period*

Specifies the maximum polling interval (in seconds) for NTP messages as a power of 2. *poll_period* is the exponent (power of) expressed as an integer from 6 through 17. For example, if you specify the number 10, the value is 2^10 and the resultant poll period is 1024 seconds. Default: 10

Usage Guidelines

Configure the NTP servers in response to network changes.

Refer to the *System Administration Guide* for important information on configuring NTP servers with local sources, and using a load balancer to communicate with external NTP servers.

Important Adding, removing, or modifying an NTP server configuration entry causes the NTP client to restart itself and resynchronize with all configured NTP servers.

Example

The following command adds the NTP server with address *209.165.200.228* to the list of NTP servers.

```
server 209.165.200.228
```

vlan

Use the NTP Configuration Mode to enable Network TIme Protocol (NTP) on tagged interface.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > NTP Configuration

configure > ntp

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ntp)#
```

Syntax Description

```
[ no ] vlan vlan_id
```

vlan_id is the vlan where the local context interface is bound to. After configuration the NTP daemon starts listening on the tagged interface.

no

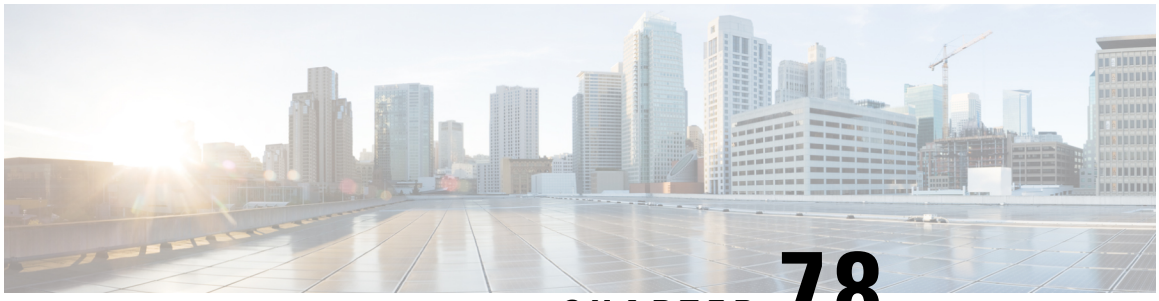
Resets the NTP configuration to default. The NTP daemon will start listening on the default untagged interface.

Usage Guidelines Configure the NTP vlan on a tagged interface.

Example

The following command makes the NTP daemon to listen on the interface bound to vlan *101*.

```
config
  ntp
    enable
    vlan 101
    exit
  exit
```



CHAPTER 78

NTSR Pool Configuration Mode Commands

MME restoration is a 3GPP specification-based feature designed to gracefully handle the sessions at S-GW once S-GW detects that the MME has failed or restarted. If the S-GW detects an MME failure based on a different restart counter in the Recovery IE in any GTP Signaling message or Echo Request / Response, it will terminate sessions and not maintain any PDN connections.

As a part of this feature, if a S-GW detects that a MME or S4-SGSN has restarted, instead of removing all the resources associated with the peer node, the S-GW shall maintain the PDN connection table data and MM bearer contexts for some specific S5/S8 bearer contexts eligible for network initiated service restoration, and initiate the deletion of the resources associated with all the other S5/S8 bearers.

The S5/S8 bearers eligible for network initiated service restoration are determined by the S-GW based on operator's policy, for example, based on the QCI and/or ARP and/or APN.

The benefit of this feature is that it provides support for the geo-redundant pool feature on the S4-SGSN/MME. In order to restore session when the MME receives a DDN, the S-GW triggers restoration when the serving MME is unavailable, by selecting another MME and sending DDN. This helps in faster service restoration/continuity in case of MME/S4-SGSN failures.

Command Modes

This mode is used to configure a pool of IP addresses associated with a pool ID and pool type (either MME or S4-SGSN) for Network Triggered Service Restoration (NTSR).

Exec > Global Configuration > NTSR Pool Configuration

configure > ntsr pool pool-id *id* **> pool-type** *type*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ntsr-pool)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

- peer-ip-address, on page 780

peer-ip-address

Configures a pool of IP addresses associated with a pool ID and pool type (either MME or S4-SGSN) for Network Triggered Service Restoration (NTSR).

Product

S-GW

Privilege

Administrator, Security Administrator

Command Modes

Exec > Global Configuration > NTSR Pool Configuration

configure > ntsr pool pool-id *id* **> pool-type** *type*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ntsr-pool)#
```

Syntax Description

[no] peer-ip-address { ipv4-address *ipv4_address* **| ipv6-address** *ipv6_address*

no

Removes the specified IP address configuration.

ipv4 ***ipv4_address***

Specifies an IPv4 address to use with an associated NTSR pool ID and pool type (either MME or S4-SGSN).

ipv6 ***ipv6_address***

Specifies an IPv6 address to use with an associated NTSR pool ID and pool type (either MME or S4-SGSN).

Usage Guidelines

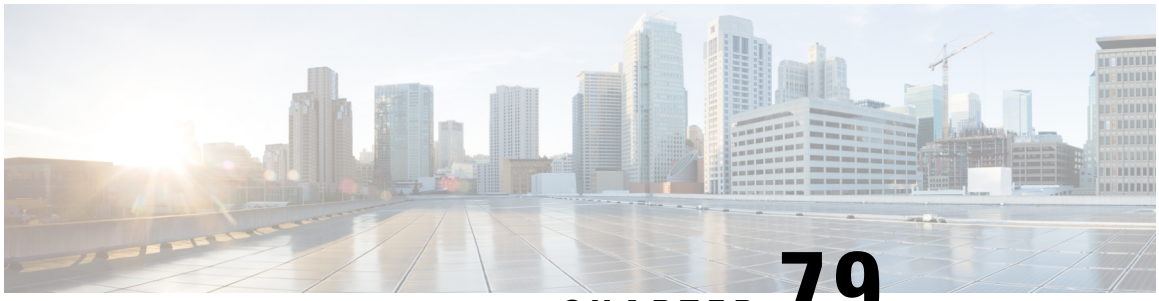
Use this command to configure a pool of IP addresses associated with a pool ID and pool type (either MME or S4-SGSN) for Network Triggered Service Restoration (NTSR).

Before using this command, operators must configure an NTSR pool ID and pool type by executing the **ntsr pool** command in Global Configuration Mode

Example

To configure a an IPv4 address associated with a pool ID and pool type (either MME or S4-SGSN) for Network Triggered Service Restoration (NTSR).

peer-ip-address ipv4-address *209.165.200.225*



CHAPTER 79

Operator Policy Configuration Mode

The Operator Policy Configuration Mode is used to create and manage operator policies for MME, S-GW, SAEGW, and SGSN configurations.

- A maximum of 1,000 operator policies can be defined, including the "default" operator policy.
- A maximum of 128 APN profiles can be associated with a single operator policy.
- A maximum of 128 IMEI profiles can be associated with a single operator policy (SGSN-only).
- Only one APN remap table can be associated with a single operator policy.
- Only one call control profile can be associated with a single operator policy.

Using the Operator Policy feature allows the operator to fine-tune any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers across IMSI ranges.

Command Modes

Operator Policy configuration mode associates APNs, APN profiles, IMEI ranges, IMEI profiles, an APN remap table and a call control profile to an operator policy. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies.

Exec > Global Configuration > Operator Policy Configuration

configure > operator-policy *policy_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-opr-policy-policy_name)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

apn

This command identifies an APN (access point name) and associates it with an APN profile (created separately in the APN Profile Configuration mode).

Product

MME

SAEGW

SaMOG

S-GW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Operator Policy Configuration

configure > operator-policy *policy_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-opr-policy-policy_name)#`

Syntax Description

apn { default-apn-profile *apn_profile_name* **| network-identifier** *apn_net_id* **[apn-profile** *apn_profile_name* **| congestion-control] | operator-identifier** *apn_op_id* **apn-profile** *apn_profile_name* **| webauth-apn-profile** *apn_webauth_name* **}**
no apn { default-apn-profile | network-identifier *apn_net_id* **[congestion-control] | operator-identifier** *apn_op_id* **| webauth-apn-profile** *apn_webauth_name* **}**

no

Disables the specified APN to APN Profile correspondence.

default-apn-profile *apn_profile_name*

Enables the use of a default APN profile comprised of default values for all parameters. this profile will be used when none of the configured APNs match the APN in the incoming Request.

apn_profile_name must be an alphanumeric string of 1 through 64 characters.

apn-profile *apn_profile_name*

apn_profile_name must be an alphanumeric string of 1 through 64 characters.

network-identifier *apn_net_id* [congestion-control]

Links the specified APN network ID with the specified APN profile.

apn_net_id must be an alphanumeric string of 1 through 63 characters, including dots (.) and dashes (-).

congestion-control: MME or SGSN only. This optional keyword configures the MME or SGSN to apply congestion control actions for this specific APN. Refer to the **drop** and **reject** commands within the [SGSN] Congestion Action Profile Configuration Mode for more information on configuring APN-based congestion control.

operator-identifier *apn_op_id*

Links the specified APN operator ID with the specified APN profile.

apn_op_id: must be a string of size string of size 1 to 39, in format of [MNCxxx.MCCyyy.GPRS] / [ABCD.DEF.MNCxxx.MCCyyy.ZZZZ].

Important With release 21.15 Operator Identifier can be configured in [ABCD.DEF.MNCxxx.MCCyyy.ZZZZ] format in addition to existing [MNCxxx.MCCyyy.GPRS] format.

webauth-apn-profile *apn_webauth_name*

Specify the APN profile to be used for SaMOG web authorization.

apn_webauth_name must be an alphanumeric string of 1 through 64 characters.

Important The SaMOG Web Authorization feature is license dependent. Contact your Cisco account representative for more information on license requirements.

Usage Guidelines

Use this command, to associate APNs with APN profiles. This command can be repeated to associate multiple APNs with profiles.

Example

Associate the APN profile named *apnprof1* to APN network ID *starflash.com*:

```
apn apnprof1 network-identifier starflash.com
```

Associate congestion control with APN network ID *starflash.com*:

```
apn network-identifier starflash.com congestion-control
```

associate

Associate an APN remap table and a call control profile with the operator policy.

Product

MME

SAEGW

S-GW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Operator Policy Configuration

configure > operator-policy *policy_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-opr-policy-policy_name)#`

Syntax Description

`associate { apn-remap-table` *`table_id`* **`| call-control-profile`** *`profile_id`* **`}`**
`no associate { apn-remap-table | call-control-profile }`

no

Removes the association definition from the policy configuration.

apn-remap-table *table_id*

Identifies the APN remap table to be associated with the operator policy.

table_id must be an alphanumeric string of 1 through 65 characters.

call-control-profile *profile_id*

Identifies a call control profile to be associated with the operator policy.

profile_id must be an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to associate an APN remap table and/or a call control profile with this Operator Policy. The APN remap table and the call control profile contain the definitions that instruct the SGSN or MME how to handle calls. Only one of each of these can be associated with an operator policy.

Example

Associate the *stardust.net_APNremap1* APN remap table with this operator policy:

`associate apn-remap-table stardust.net_APNremap1`

description

Associates a description with or names an operator policy.

Product

MME

SAEGW

S-GW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Operator Policy Configuration

configure > operator-policy *policy_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-opr-policy-policy_name)#
```

Syntax Description

```
description description
no description
```

description

Enter an alphanumeric string of 1 through 100 characters. If the string includes spaces, punctuation, and case-sensitive letters, it must be bracketed with double quotation marks (" ").

no

Removes the existing description from this operator policy.

Usage Guidelines

Identity this particularly operator policy using descriptive text.

Example

```
description "sgsn1 operator policy carrier1"
```

imei

Defines a range of IMEI (International Mobile Equipment Identity) numbers and associates an IMEI profile with the range definition.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Operator Policy Configuration

configure > operator-policy *policy_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-opr-policy-policy_name)#
```

Syntax Description

```
imei range IMEI_number to IMEI_number { imei-profile profile_name | sv ##
imei-profile profile_name }
no imei range IMEI_number to IMEI_number sv ##
```

no

Removes the IMEI definition from the policy configuration.

range *IMEI_number* to *IMEI_number*

Defines the beginning and end of a range of IMEIs.

IMEI_number must be a numerical string of up to 14 digits.

sv ##

Identifies the software version to fine-tune the IMEI definition. This keyword should only be included if the IMEISV is retrievable.

must be a 2-digit integer.

imei-profile *profile_name*

Identify the IMEI profile that defines the actions appropriate to the devices identified within the specified range.

profile_name must be an alphanumeric string of 1 through 64 characters.

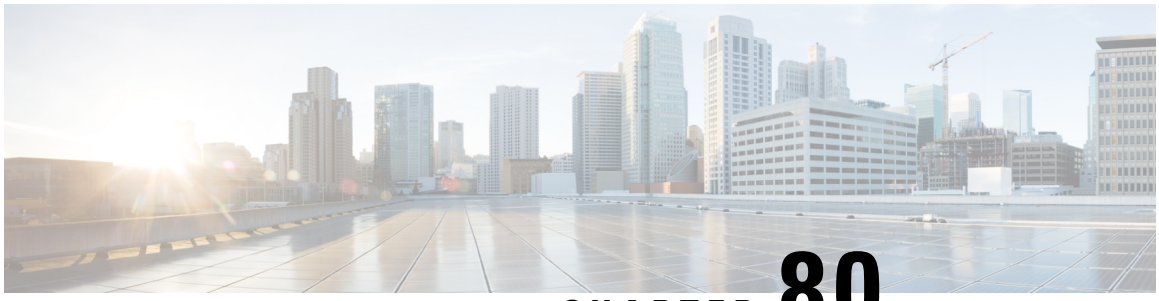
Usage Guidelines

This command defines the IMEI ranges that will be used by the operator policy to determine if the device is appropriately selected for actions defined in the specified IMEI profile.

Example

All devices with an IMEI of *123123** requesting Attach shall be subject to actions in the *blacklist_profile1*

```
imei range 1231230 to 1231239 imei-profile name blacklist_profile1
```



CHAPTER 80

ORBEM Force Configuration Mode Commands

Attention

- With Release 21.16 onwards, the **force** keyword has to be appended to the **orbem** CLI command to enter the ORBEM mode and enable the feature. The **orbem** keyword is now hidden.
- Support for the end-of-life ORBEM/WEM feature will be fully discontinued in future releases.

The ORBEM Configuration Mode is used to manage the Object Request Broker Element Manager (ORBEM) server options for the current context.

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem force

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

activate client id

Activates/deactivates a Common Object Request Broker Architecture (CORBA) client for the ORBEM interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

`[ no ] activate client id` *`name`*

no

Deactivates the specified client

id *name*

Specifies the client to be activated. *name* must refer to a previously configured CORBA client expressed as an alphanumeric string of 1 through 10 characters.

Usage Guidelines

Activates CORBA clients after they have been configured or deactivated by the system or by configuration.

Example

The following command activates the CORBA *ems* client.

```
activate client id ems
```

client id

Configures or removes a CORBA client from the ORBEM interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

```
client id name { encrypted password | password } pwd
no client id name
```

no

Removes the specified client from the configuration.

id *name*

Specifies the client to be configured. *name* must be an alphanumeric string of 1 through 10 characters.

encrypted password

Specifies the use of an encrypted password for use by the chassis while saving configuration scripts. Signifies that ORBEM messages are transported using SSL encryption techniques. StarOS 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.

password

Specifies the plain text password for the CORBA client. *pwd* must be an alphanumeric string of 1 through 35 characters.

pwd

Specifies the password for the CORBA client.

For an encrypted password, *pwd* must be an alphanumeric string of 1 through 212 characters.

For an unencrypted password, *pwd* must be an alphanumeric string of 1 through 35 characters.

Usage Guidelines

Use this command to configure or remove a CORBA client from the ORBEM interface.

CORBA clients must be configured prior to being activated.

Example

The following command sets a plain text password for CORBA client *ems*:

```
client id ems password ems1001
```

event-notif-iiop-port

Configures the port number for Internet inter-ORB event notifications.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

event-notif-iiop-port *number*
default event-notif-iiop-port

default

Restores the port number for the inter-ORB event notifications to the system default: 7778.

number

Specifies the port number to use as an integer from 1 through 65535. Default: 7778

Usage Guidelines

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for standardized inter-ORB communications.

Event notification port configured is only used if the Internet inter-ORB transport is enabled via the **iiop-transport** command with the event notification service being enabled as well.

Example

The following command sets the IIOP port number to 5466:

event-notif-iiop-port 5466

event-notif-service

Enables or disables the ORB Notification Service and allows the configuration of filters dictating which event notifications are sent.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

[no] event-notif-service [filter { event-id *event_id* **[to** *final_event_id* **] | facility** *event_facility* **level** *event_level* **}]**
default event-notif-service filter

default

Restores the ORB Notification Service filter to its default behavior of sending all "error" level and higher events, and "info" level events for the orbs facility, CLI command logs, and license change logs.

no

Disables the event notification service.

filter

Specifies a filter that determines for which events the system sends notifications.

event-id *event_id* [to *final_event_id*]

Specifies an event filter based on event identification (event ID) number.

event_id is a specific event ID to filter or is the initial event ID in range if the **to** keyword is used.

In 14.1 and earlier releases, *event_id* is an integer from 1 through 202699.

In 15.0 and later releases, *event_id* is an integer from 1 through 204999.

to allows the specification of a range of event IDs to filter. When used, *final_event_id* specifies the last event ID in the range to be filtered. It can be configured to an integer from 1 through 204999, but must be a value greater than the initial event ID.

facility *event_facility* level *event_level*

Specifies an event filter based on facility type and notification severity level.

event_facility specifies the facility type and can be any one of the following:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: Authentication, Authorization and Accounting (AAA) client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
- **acl-log**: Access Control List (ACL) logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: ACS Manager facility
- **afctrl**: Fabric Controller facility [ASR 5500 only]
- **afmgr**: Fabric Manager logging facility [ASR 5500 only]
- **alarmctrl**: Alarm Controller facility
- **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility

- **alcapmgr**: ALCAP manager logging facility
- **all**: All facilities
- **asngwmgr**: Access Service Network (ASN) Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-Demux Manager logging facility
- **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **callhome**: Call Home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]

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

- **cdf**: Charging Data Function (CDF) logging facility
- **cgw**: Converged Access Gateway (CGW) logging facility
- **cli**: Command Line Interface (CLI) logging facility
- **cmp**: Certificate Management Protocol (IPSec) logging facility
- **connectedapps**: SecGW ASR 9000 oneP communication procotol
- **connproxy**: Controller Proxy logging facility
- **credit-control**: Credit Control (CC) facility
- **csp**: Card/Slot/Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: CSS RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility [CSCF <--> HSS]
- **data-mgr**: Data Manager Framework logging facility
- **dcardctrl**: IPSec Daughter Card Controller logging facility

- **dcardmgr**: IPSec Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diactrl**: Diameter Controller proclet logging facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-engine**: Diameter version2 engine logging facility
- **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSec Data Path facility
- **drvctrl**: Driver Controller facility
- **dpath**: IPSec Data Path logging facility
- **drvctrl**: Driver Controller logging facility
- **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
- **eap-diameter**: Extensible Authentication Protocol (EAP) IP Sec urity facility
- **eap-ipsec**: Extensible Authentication Protocol (EAP) IPSec facility
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
- **egtpu**: eGTP-U logging facility
- **embms**: evolved Multimedia Broadcast Multicast Service facility
- **embms**: eMBMS Gateway Demux facility
- **epdg**: evolved Packet Data (ePDG) gateway logging facility

- **event-notif**: Event Notification Interface logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: Femto Network Gateway (FNG) logging facility
- **gbmgr**: SGSN Gb Interface Manager facility
- **gmm**:
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  - For 3G: Logs the access application layer (above the RANAP layer)
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol manager logging facility
- **gtpp**: GTP-prime protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTP-U Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **h248prt**: H.248 port manager facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **henbapp**: Home Evolved NodeB (HENB) App facility

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

- **henbgw**: HENB-GW facility

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
- **igmp**: Internet Group Management Protocol (IGMP)
- **ikev2**: Internet Key Exchange version 2 (IKEv2)
- **ims-authorizatn**: IP Multimedia Subsystem (IMS) Authorization Service facility
- **ims-sh**: HSS Diameter Sh Interface Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMS User Equipment (IMSUE) facility
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
- **ipne**: IP Network Enabler (IPNE) facility
- **ipsec**: IP Security logging facility
- **ipsecdemux**: IPSec demux logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: Key/Value Store (KVSTORE) Store facility
- **l2tp-control**: Layer 2 Tunneling Protocol (L2TP) control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: Link Aggregation Group (LAG) manager logging facility

- **lcs**: Location Services (LCS) logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **location-service**: Location Services facility
- **m3ap**: M3 Application Part facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: Mobile Application Part (MAP) protocol logging facility
- **megadiammgr**: MegaDiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity (MME) Application logging facility
- **mme-embms**: MME evolved Multimedia Broadcast Multicast Service facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
- **mrme**: Multi Radio Mobility Entity (MRME) logging facility
- **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
- **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
- **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
- **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
- **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
- **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility

- **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
- **netwstrg**: Network Storage facility
- **npuctrl**: Network Processor Unit Control facility
- **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-drv**: NPUMGR DRV logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-lc**: NPUMGR LC logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **npumgr-rri**: NPUMGR RRI (Reverse Route Injection) logging facility
- **npumgr-vpn**: NPUMGR VPN logging facility
- **npusim**: NPUSIM logging facility [ASR 5500 only]
- **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
- **ocsp**: Online Certificate Status Protocol logging facility.
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pagingmgr**: PAGINGMGR logging facility
- **pccmgr**: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
- **pdg**: Packet Data Gateway (PDG) logging facility
- **pdgdmgr**: PDG Demux Manager logging facility
- **pdif**: Packet Data Interworking Function (PDIF) logging facility
- **pgw**: Packet Data Network Gateway (PGW) logging facility
- **pmm-app**: Packet Mobility Management (PMM) application logging facility
- **ppp**: Point-To-Point Protocol (PPP) link and packet facilities
- **pppoe**: PPP over Ethernet logging facility
- **proclet-map-frwk**: Proclet mapping framework logging facility
- **push**: VPNMGR CDR push logging facility

- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Diameter Rf interface messages facility
- **rip**: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
- **rlf**: Rate Limiting Function (RLF) logging facility
- **rohc**: Robust Header Compression (RoHC) facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
- **s102**: S102 protocol logging facility
- **s102mgr**: S102Mgr logging facility
- **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
- **sabp**: Service Area Broadcast Protocol (SABP) logging facility
- **saegw**: System Architecture Evolution (SAE) Gateway facility
- **sbc**: SBc protocol logging facility
- **sccp:** Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **sct**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef_ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN "glue" interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).

- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSN System Components logging facility (used infrequently)
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sls**: Service Level Specification (SLS) protocol logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
- **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
- **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
- **ssl**: Secure Socket Layer (SSL) message logging facility
- **stat**: Statistics logging facility
- **supserv**: Supplementary Services logging facility [H.323]
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility

- **threshold**: threshold logging facility
- **ttg**: Tunnel Termination Gateway (TTG) logging facility
- **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
- **udr**: User Data Record (UDR) facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User Layer 3 tunnel logging facility
- **usertcp-stack**: User TCP Stack
- **vim**: Voice Instant Messaging (VIM) logging facility
- **vinfo**: VINFO logging facility
- **vmgctrl**: Virtual Media Gateway (VMG) controller facility
- **vmgctrl**: VMG Content Manager facility
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6
- **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)
- **x2gw-app**: X2GW (X2 proxy Gateway, eNodeB) application logging facility
- **x2gw-demux**: X2GW demux task logging facility

event_level

specifies the severity level of the event notification to filter and can be configured to one of the following:

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

Usage Guidelines

This command is used to enable or disable the ORB Notification Service. Additionally, it can be used to configure filters dictating which events are sent. This service is disabled by default.

Filters can be configured for a specific event identification number (event ID), a range of event IDs, or specific severity levels for events for particular facilities.

When no filters are configured and the service is enabled, the ORB Notification Service sends all "error" level and higher events, and "info" level events for the orbs facility, CLI command logs, and license change logs.

Multiple instance of this command can be executed to configure multiple filters.

Example

The following command enables the ORB Notification service:

event-notif-service

The following command disables the ORB Notification service:

no event-notif-service

The following command configures a filter for the ORB Notification Service allowing only event IDs *800* through *805* to be sent:

event-notif-service filter event-id 800 to 805

The following command configures a filter for the ORB Notification Service allowing only *critical* level notifications for all facilities:

event-notif-service filter facility all level critical

event-notif-siop-port

Configures the port to use for secure socket layer (SSL) inter-ORB event communication.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

event-notif-siop-port *number*
default event-notif-siop-port

default

Restores the port to use for secure socket layer inter-ORB event communication to the system default: 7777.

number

Specifies the port number to use as an integer from 1 through 65535. Default: 7777

Usage Guidelines

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for inter-ORB communications using SSL.

Example

event-notif-siop-port 25466

iiop-port

Configures the port number for Internet Inter-ORB Protocol (IIOP) communications.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

[no] iiop-port *number*

default

Restores the port number for inter-ORB communications to the system default: 14132.

no

Disables the IIOP port.

number

Specifies the port number to use as an integer from 1 through 65535. Default: 14132

Usage Guidelines

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for standardized inter-ORB communications.

Internet inter-ORB port is only used if IIOP transport is enabled via the **iiop-transport** command.

Example

The following commands sets the IIOP port number to 2546:

```
iiop-port 2546
```

iiop-transport

Enables/disables use of the Internet Inter-ORB Protocol (IIOP) for management across the network.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

[no] iiop-transport

no

Disables internet inter-ORB protocol communication across the network.

Usage Guidelines

Enables the transport of IIOP messages to support remote management across the network.

The default is IIOP transport disabled.

Example

The following command enables ORB-based management across the network:

iiop-transport

iop-address

Sets the IP address used by the ORBEM Server to advertise service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

[default] iop-address *ip_address*

default

Restores the IP address for inter-ORB communications to the system default: IP address of the current context.

ip_address

Specifies the IP address to use for inter-ORB communications using IPv4 dotted-decimal notation.

Usage Guidelines

Change the inter-ORB IP address when the IP address of the current context should not be used. The IP address of the local context may not be appropriate when the ORB configuration across nodes would cause conflicts with the IP addresses.

The default inter-ORB IP address is the IP address of the current context.

Example

The following command sets the inter-ORB IPv4 address to 209.165.200.228:

```
iop-address 209.165.200.228
```

max-attempt

Configures the maximum number of failed login attempts after which the client is deactivated.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

max-attempt *count*
default max-attempt

default

Restores the maximum number of failed login attempts before which the client is deactivated to the system default: 3 attempts.

count

Specifies the number of failed login attempts prior to deactivating a client. The value must be an integer from 1 through 10. Default: 3 attempts

Usage Guidelines

Adjust the maximum number of attempts to a smaller value to increase the security level of the system.

Example

The following command sets the maximum number of attempts to 5:

```
max-attempt 5
```

session-timeout

Configures the amount of idle time (no activity) before a client session is terminated.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

session-timeout *seconds*
default session-timeout

default

Restores the amount of idle time (no activity) before a session is terminated to the system default: 300 seconds.

seconds

Specifies the number of seconds of idle time before a client session is terminated. The value must be must be an integer from 1 through 86400. Default: 300 seconds

Usage Guidelines

Reduce the session timeout when the maximum number of sessions allowed is frequently being reached. Setting this to a lower value will help release idle sessions faster to allow use by other clients.

Example

The following sets the session timeout value to 150 seconds:

session-timeout 150

siop-port

Configures the SSL I/O port for inter-ORB events.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

siop-port *number*
[default | no] siop-port

default

Restores the secure socket layer I/O port for inter-ORB events to the system default: 14131.

default

Restores the secure socket layer I/O port for inter-ORB events to the system default: 14131.

number

Specifies the port number to use as an integer from 1 through 65535. Default: 14131

Usage Guidelines

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for inter-ORB communications.

Example

The following command sets the SIOP port number to 2466:

```
siop-port 2466
```

ssl-auth-policy

Configures the SSL peer authentication policy used by the ORBEM server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

```
ssl-auth-policy { auth-none | auth-once | auth-once-fail | auth-peer |
auth-peer-fail }
```

auth-none

Specifies that the ORBEM server does not authenticate the peer. This is the default setting.

auth-once

Specifies that the ORBEM server authenticates the peer once (no fail).

auth-once-fail

Specifies that the ORBEM server authenticates the peer once (fail if no certificate).

auth-peer

Specifies that the ORBEM server authenticates the peer every time (no fail).

auth-peer-fail

Specifies that the ORBEM server authenticates the peer every time (fail if no certificate).

Usage Guidelines Use to configure the peer authentication policy used by the SSL transport of ORBEM.

Example

The following command sets the policy to authenticate the peer once without failure.

```
ssl-auth-policy auth-once
```

ssl-certificate

Defines the certificate to be used by the SSL transport of ORBEM.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description **ssl-certificate { string** *certificate* **| file** *url* **}**

string *certificate*

Specifies an ORBEM SSL certificate. *certificate* is an alphanumeric string of up to 4096 characters.

file *url*

Default: /usr/ssl/certs/orbscert.pem

Specifies an ORBEM SSL certificate file and location. *url* is an alphanumeric string of up to 1024 characters.

Usage Guidelines Use to configure the certificate to be used by the SSL transport of ORBEM. Note that if the **file** option is used, the certificate content is read from the *url* and converted into a quoted string.

Example

The following command defines the certificate *cert3.pem* file as being located in the **/usr/ssl/certs** directory:

```
ssl-certificate file /usr/ssl/certs/cert3.pem
```

The following command defines the certificate string (the string shown is abbreviated):

```
ssl-certificate string
```

"-----BEGIN CERTIFICATE-----\n\
MIIELDCCA5WgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBsTELMAkGA1UEBhMCVVMx\n\
FjAUBgNVBAgTDU1hc3NhY2h1c2V0dHMxEjAQBgNVBAcTCVRld2tzYnVyeTEeMBwG\n\
A1UEChMVU3RhcmVudCBOZXR3b3JrcyBJbmMuMSIwIAYDVQQLExlFbGVtZW50IE1h\n\
bmFnZW1lbnQgU3lzdGVtMQ4wDAYDVQQDEwVPUkJFTTEiMCAGCSqGSIb3DQEJARYT\n\
b3JiZW1AbnVsaW5raW5jLmNvbTAeFw0wMjA5MDYxMjE5MTNaFw0yMjA5MDExMjE5\n\
MTNaMIGxMQswCQYDVQQGEwJVUzEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czESMBAG\n\
A1UdDgQWBBSpuGGMTwgaq8H+e70ZPIFHVZjiWDCB3gYDVR0jBIHWMIHTgBRkVBzy\n\
4zW5Gv0pXcwT07PtzCm53qGBt6SBtDCBsTELMAkGA1UEBhMCVVMxFjAUBgNVBAgT\n\
DU1hc3NhY2h1c2V0dHMxEjAQBgNVBAcTCVRld2tzYnVyeTEeMBwGA1UEChMVU3Rh\n\
cmVudCBOZXR3b3JrcyBJbmMuMSIwIAYDVQQLExlFbGVtZW50IE1hbmFnZW1lbnQg\n\
U3lzdGVtMQ4wDAYDVQQDEwVPUkJFTTEiMCAGCSqGSIb3DQEJARYTb3JiZW1AbnVs\n\
aW5raW5jLmNvbYIBADANBgkqhkiG9w0BAQQFAAOBgQATOdeDWikcoUIU8Gth9wr4\n\
Z5Fi8akXHhKhN7UMKyiW/Nn5NyfqPIA+9JwYMqwVOG8ybtfBQIGRCQodbXUm6Z9Z\n\
cM3XxWKVKHVolGS83f/JfpSLnuGkBIW8m3p/snHBH2BtgNT8OLItlTdBHedTKL72\n\
ZIxGF9/ok9hUqU4ikzQcEQ==\n\
-----END CERTIFICATE-----\n"

ssl-private-key

Configures the SSL private key used by the ORBEM server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

Syntax Description

ssl-private-key { string *key* **| file** *url* **}**

string *key*

Specifies an ORBEM SSL private key. *key* is an alphanumeric string of up to 4096 characters.

file *url*

Default: /usr/ssl/certs/orbscert.pem

Specifies the ORBEM SSL private key file location. *url* is an alphanumeric string of up to 1024 characters.

Usage Guidelines

Use to configure the private key for the SSL transport of ORBEM. Note that if **file** option is used, the private key is read from the *url* and converted into a quoted string.

Example

The following command defines the private-key *cert3.pem* file as being located in the **/usr/ssl/certs** directory:

```
ssl-private-key file /usr/ssl/certs/cert3.pem
```

The following command defines the private-key string (the string shown is abbreviated):

```
ssl-private-key string
```

"-----BEGIN RSA PRIVATE KEY-----\n\

MIICXQIBAAKBgQC6Dh79iaK/zZG/Kwme2XS6G8/n3/+sac6huxI1WNyammyYZKZp\n\

XTjHUlS92fvn0UUM4tFjN4XoqveSiqy3IqUhnVKS3+0L7s9beanQUJuR9MdLy9Ho\n\

7qh720wpN4isqN7YfGLoqGslLQjhS8z6ZT0ZUhyusY0rE6yHTV23nHKNtQIDAQAB\n\

9br1iVWvy/N23WXwZIiH+e1tBfHqlSd/0wJBANEEOgH/vJse/YdHeYjlT76IcGRp\n\

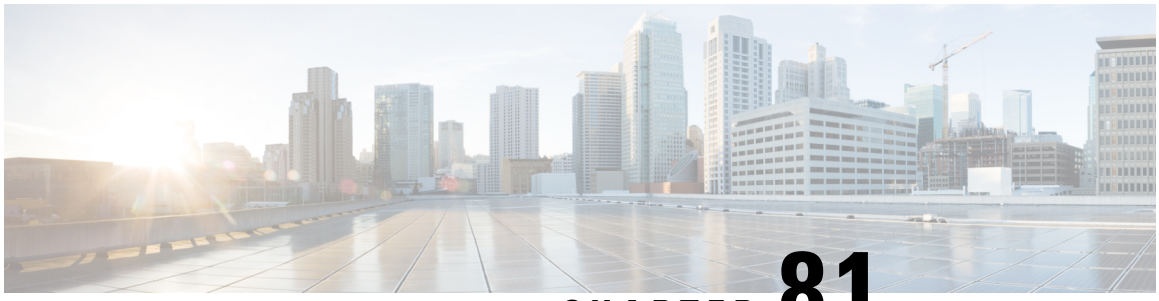
Tq6ldBXdoLRDGUF2AqdboJ7wWCOJQO34XbBtmWFfTkqz48Mi6uh3/5kDfH8CQGAl\n\

XObwPFRztvkXprZfh7IekxAIuoHiT1JsEKSIGPzEqDY2rmoWDghOvPETO+5zWEQk\n\

TXzLaRHgbIy9MKnXSt8CQQCcBfT7VndEfG9VWyPzeL4vx4ZhUMZQ6FIJdXo7Xq9x\n\

mzX8hgIcfdg3tahlNt35gL/DjUY7d14+MgLrRf3Udbk9\n\

-----END RSA PRIVATE KEY-----\n"



CHAPTER 81

OSPF Configuration Mode Commands

The OSPF Configuration sub-mode is used to configure the Open Shortest Path First (OSPF) routing protocol. This mode includes commands that configure OSPF routing parameters.

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ospf)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

- area authentication, on page 812
- area default-cost, on page 813
- area nssa, on page 814
- area stub, on page 815
- area virtual-link, on page 816
- area virtual link authentication, on page 817
- area virtual-link authentication-key, on page 818
- area virtual link intervals, on page 819
- area virtual link message-digest-key, on page 821
- bfd-all-interfaces, on page 822
- capability graceful-restart, on page 823
- default-information originate, on page 823
- default-metric, on page 824
- distance, on page 825
- distribute-list, on page 826
- ip vrf, on page 827

area authentication

Enables authentication for the specified OSPF area.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

```
[ no ] area { ip_address | decimal_value } authentication [ message-digest ]
```

no

Disables authentication for the specified area.

ip_address

Specifies the IP address of the area where authentication will be enabled in IPv4 dotted-decimal notation.

decimal_value

Specifies the identification number of the area where authentication will be enabled. This must be an integer from 0 through 4294967295.

authentication

Sets the OSPF authentication type to use the simple authentication method.

message-digest

Sets the OSPF authentication type to use the message digest 5 (MD5) authentication method.

Usage Guidelines Use this command to enable authentication of OPSF areas.

Example

The following command enables authentication for an OSPF area defined by the IP address *209.165.200.234* and the OSPF authentication type to MD5:

```
area 209.165.200.234 authentication message-digest
```

area default-cost

Configures the default cost for an area.

Product PDSN

HA

GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description `[ no ] area { ip_address | decimal_value } default-cost cost_value`

no

Deletes the default cost for the area.

ip_address

Specifies the IP address of the area in IPv4 dotted-decimal notation.

decimal_value

Specifies the identification number of the area as an integer from 0 through 4294967295.

cost_value

Sets the default cost to be configured for the specified area as an integer from 0 through 16777215.

Usage Guidelines Use this command to configure the default cost for an OSPF area.

Example

The following command sets the default cost for an OSPF area defined by the IP address *209.165.200.234* to *300*:

```
area 209.165.200.234 default-cost 300
```

area nssa

Defines an area as an NSSA (Not So Stubby Area) and configures OSPF parameters for it.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

[no] area { *ip_address* | *decimal_value* } **nssa** [**default-information-originate**] [**no-redistribution**] [**no-summary**] [**translate-always**] [**translate-candidate**] [**translate-never**]

ip_address

Specifies the IP address of the NSSA in IPv4 dotted-decimal notation.

decimal-value

Specifies the identification number of the NSSA area as an integer from 0 through 4294967295.

default-information-originate

Originates default information to the NSSA area.

no-redistribution

Does not redistribute external routes to the NSSA area.

no-summary

Does not inject inter-area routes into NSSA.

translate-always

Configures the NSSA-ABR (Area Border Router) to always translate

translate-candidate

Configure NSSA-ABR for translate election. (This is enabled by default.)

translate-never

Configure NSSA-ABR to never translate.

Usage Guidelines Use this command to define NSSA areas.

Example

The following command defines the area designated by the IP address *209.165.200.234* as an NSSA area:

```
area 209.165.200.234 nssa
```

area stub

Defines an area as an OSPF stub area.

Product PDSN

HA

GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description `[ no ] area { ip_address | decimal_value } stub [ no-summary ]`

ip_address

Specifies the IP address of the stub area in IPv4 dotted-decimal notation.

decimal_value

Specifies the identification number of the stub area as an integer from 0 through 4294967295.

stub

Specifies this is a stub area.

no-summary

Disables (stops) the ABR (Area Border Router) from sending summary link state advertisements (LSAs) into the stub area.

Usage Guidelines Use this command to define an OPSF area as a stub area.

Example

The following command defines the OSPF area defined by the IP address *209.165.200.234* as a stub area:

```
area 209.165.200.234 stub
```

area virtual-link

Configures a virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

```
[ no ] area { ip_address | decimal_value } virtual-link router_id_address
```

no

Disables area virtual-link.

ip_address

Specifies the IP address of the transit area in IPv4 dotted-decimal notation.

decimal_value

Specifies The identification number of the transit area as an integer from 0 through 4294967295.

router_id_address

Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

Usage Guidelines

Use this command to create a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command creates a virtual link between the OSPF areas defined by the IP address *209.165.200.234* and the IP address *209.165.200.244*:

```
area 209.165.200.234 virtual-link 209.165.200.244
```

area virtual link authentication

Configures the OSPF authentication method to be used by the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

```
[ no ] area { ip_address | decimal_value } virtual-link router_id_address
authentication { message-digest | null | text }
```

no

Disables area virtual link authentication.

ip_address

Specifies the IP address of the transit ares in IPv4 dotted-decimal notation.

decimal_value

Specifies the identification number of the transit area as an integer from 0 through 4294967295.

router_id_address

Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

authentication

Sets the OSPF authentication type to use the simple authentication method.

message-digest

Sets the OSPF authentication type to use the message digest (MD) authentication method.

null

Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.

text

Set the OSPF authentication type to use the clear text authentication method.

Usage Guidelines

Use this command to set the authentication method for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command sets the authentication method for a virtual link between the OSPF areas defined by the IP address *209.165.200.234* and the IP address *209.165.200.244* to use no authentication:

```
area 209.165.200.234 virtual-link 209.165.200.244 null
```

area virtual-link authentication-key

Configures the authentication password for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

area { *ip_address* | *decimal_value* } **virtual-link** *router_id_address* **authentication-key** { **encrypted password** *encrypted_key* **| password** *password_key* }
no area { *ipaddress* | *decimal_value* } **virtual-link** *router_id_address* **authentication-key**

no

Disables the area virtual link authentication key.

ipaddress

Specifies the IP address of the transit area in IPv4 dotted-decimal notation.

decimal-value

Specifies the identification number of the transit area as an integer from 0 through 4294967295.

router_id_address

Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

encrypted password

encrypted_key is an alphanumeric string of 1 through 523 characters.

Use this if you are pasting a previously encrypted authentication key into the CLI command.

password *password_key*

The password to use for authentication. *password_key* is an alphanumeric string of 1 through 16 characters that denotes the authentication password. This variable is entered in clear text format.

Usage Guidelines

Use this command to specify the authentication password for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command creates an authentication password of *123456* for a virtual link between the OSPF areas defined by the IP address *209.165.200.234* and the IP address *209.165.200.244*:

```
area 209.165.200.234 virtual-link 209.165.200.244 authentication-key
password 123456
```

area virtual link intervals

Configures the interval or delay type, and the delay time in seconds, for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

[no] area { *ip_address* | *decimal_value* } **virtual-link** *router_id_address* [**dead-interval** *dead_value*] [**hello-interval** *hello_value*] [**retransmit-interval** *rt_value*] [**transmit-delay** *td_value*]

no

Disables the area virtual link intervals.

ipaddress

Specifies the IP address of the area in IPv4 dotted-decimal notation.

decimal_value

Specifies the identification number of the transit area as an integer from 0 through 4294967295.

router_id_address

Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

dead-interval *dead_value*

Specifies The interval (in seconds) that the router should wait, during which time no packets are received and after the router considers a neighboring router to be off-line. *dead_value* must be an integer from 1 through 65535.

hello-interval *hello_value*

Specifies the interval (in seconds) before sending a hello packet. *hello_value* must be an integer from 1 through 65535.

retransmit-interval *rt_value*

Specifies the interval (in seconds) that router should wait before retransmitting a packet. *rt_value* must be an integer from 1 through 3600.

transmit-delay *td_value*

Specifies the interval (in seconds) that the router should wait before transmitting a packet. *td_value* must be an integer from 1 through 3600.

Usage Guidelines

Use this command to set the intervals or delay types for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command sets the retransmit interval for a virtual link between the OSPF areas defined by the IP address 209.165.200.234 and the IP address 209.165.200.244 to 60 seconds:

```
area 209.165.200.234 virtual-link 209.165.200.244 retransmit-interval 60
```

area virtual link message-digest-key

Enables the use of MD5-based OSPF authentication for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

area { *ip_address* | *decimal_value* } **virtual-link** *router_id_address* **message-digest-key** *key_id* **md5** { **encrypted password** *encrypted__key* **| password** *password_key* }
no area { *ipaddress* | *decimal_value* } **virtual-link** *router_id_address* **message-digest-key** *key_id*

no

Disables the area virtual link message digest key.

ip_address

Specifies the IP address of the transit area in IPv4 dotted-decimal notation.

decimal_value

Specifies the identification number of the transit area as an integer from 0 through 4294967295.

router_id_address

Specifies the router id of the ABR to be linked to in IPV4 dotted-decimal notation.

message-digest-key *key_id*

Specifies the key identifier number. *key_id* must be an integer from 1 through 255.

encrypted password *encrypted_key*

Specifies the use of an encrypted password. *encrypted_key* is an alphanumeric string of 1 through 523 characters.

Used this if you are pasting a previously encrypted authentication key into the CLI command.

password *password_key*

Specifies the password to use for authentication. *password_key* is an alphanumeric string from 1 through 16 characters that is entered in clear text format.

Usage Guidelines

Use this command to enable the use of MD5-based OSPF authentication for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command enables the use of MD5-based OSPF authentication for a virtual link between the OSPF areas defined by the IP address 209.165.200.234 and the IP address 209.165.200.244, sets the MD5 Key ID to 25, and the password to 123456:

```
area 209.165.200.234 virtual-link 209.165.200.244 message-digest-key 25
md5 password 123456
```

bfd-all-interfaces

Enables or disables Bidirectional Forwarding Detection (BFD) on all OSPF interfaces.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

[no] bfd-all-interfaces

no

Disables BFD capability on all interfaces.

Usage Guidelines

Use this command to configure BFD on all OSPF interfaces. See the *System Administration Guide* for additional information on how to configure BFD.

Example

The following command configures BFD on all OSPF interfaces:

```
bfd-all-interfaces
```

capability graceful-restart

Configures graceful-restart. By default, this capability is set to enabled.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ospf)#`

Syntax Description

`[ no | default ] capability graceful-restart`

no

Disables the graceful-restart capability.

default

Enables the graceful-restart capability if it has been disabled.

Usage Guidelines

Use this command to configure graceful-restart.

Example

The following command configures graceful-restart:

`capability graceful-restart`

default-information originate

Creates a default external route into an OSPF routing domain.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

```
default-information originate
default-information originate [ always ] [ metric metric_value ] [ metric-type { 1 | 2 } ] [ route-map route_map_name ]
no default-information originate
```

no

Disables the default external route.

always

Always advertise the route regardless of whether or not the software has a default route.

metric *metric_value*

Sets the OSPF metric used in creating the default rout as an integer from 1 through 16777214.

metric-type { 1 | 2 }

Sets the default route metric type.

1: Sets the OSPF external link type for default routes to Type 1.

2: Sets the OSPF external link type for default routes to Type 2.

route-map *route_map_name*

Specifies the name of the default route-map to be use as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to set the default external route into an OSPF routing domain.

Example

The following command sets the default external route to originate from the route map named *rmap1*:

```
default-information originate route-map rmap1
```

default-metric

Configures the default metric value for the OSPF routing protocol. All OSPF interfaces have a cost, which is a routing metric that is used in the link-state calculation. Routes with lower total path metrics are preferred over those with higher path metrics. When several equal-cost routes to a destination exist, traffic is distributed equally among them. The default metric is a global parameter that specifies the cost applied to all OSPF routes by default.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

default-metric *metric_value*
no default-metric

metric-value

Sets the metric value expressed as an integer from 1 through 16777214. Default: 26385.

no

Enables or disables the default metric value for OSPF.

Usage Guidelines

Use this command to set the default metric for routes.

Example

The following command sets the default metric to *235*:

```
default-metric 235
```

distance

Configures the OSPF route administrative distances for all OSPF route types or based on specific route type. Administrative distance is the measure used by Cisco routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) using an administrative distance value. A lower numerical value is preferred.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

`[ no ] distance { distance_value | ospf { [ external distance_value ] [ inter-area distance_value ] [ intra-area distance_value ] } }`

no

Disables the OSPF route administrative distances for all OSPF route types.

distance_value

Specifies the OSPF route administrative distances as an integer from 1 to 255. The default distance value is 110.

ospf { [external *distance_value*] [inter-area *distance_value*] [intra-area *distance_value*] }

Set the distance value for the specified route type.

external *distance_value*: Set the OSPF route administrative distance for routes from other routing domains, learned by redistribution. This must be an integer from 1 through 255. The default is 110.

inter-area *distance_value*: sets the OSPF route administrative distance for routes from one routing area to another. This must be an integer from 1 through 255. The default is 110.

intra-area *distance_value*: sets the OSPF route administrative distance for all routes within an area. This must be an integer from 1 through 255. The default is 110.

no

Enables or disables the specified option.

Usage Guidelines

Use this command to set the administrative distance for OSPF routes.

Example

The following command sets the administrative distance for all OSPF route types to *30*:

```
distance 30
```

distribute-list

Enables or disables the filtering of networks in outgoing routing updates.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

[no] distribute-list *route_access_list* **out { connected | rip | static }**

no

Disables the filtering of networks in outgoing routing updates.

route_access_list

Specifies the name of the OSPF route access list to use for filtering as an alphanumeric string of 1 through 63 characters.

connected

Filters connected routes.

rip

Filters RIP routes. (RIP is not supported at this time.)

static

Filters static routes.

no

Disables the specified option.

Usage Guidelines

Use this command to enable the filtering of outgoing route updates by using the specified route access list.

Example

The following command uses the route access list named *ral1* to filter outgoing routing updates for all connected routes:

```
distribute-list ral1 out connected
```

ip vrf

Configures the Virtual Routing and Forwarding (VRF) instances for OSPF routing protocol.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

`[ no ] ip vrf vrf_name`

no

Disables the VRF instances and removes the configured VRF context association for OSPF routing.

vrf*vrf_name*

Configures Virtual Routing & Forwarding (VRF) parameters.

vrf_name is name of a preconfigured VRF context configured in Context Configuration Mode via the **ip vrf** command. It is an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure the IP VRF forwarding also to associate the preconfigured VRF context with the specific tunnel interface.

This command creates and enters the OSPF VRF Configuration Mode if required to configure the VRF context instances for OSPF routing.

Example

The following command enables preconfigured VRF context instance *ospf_vrf1* for OSPF routing and enters the OSPF VRF Configuration mode:

```
ip vrf ospf_vrf1
```

neighbor

Configures OSPF routers that interconnect to non-broadcast networks.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

`[ no ] neighbor ip_address [ poll-interval poll_interval_value ] [ priority priority_value ]`

no

Disables OSPF routers that interconnect to non-broadcast networks.

ip_address

Specifies the interface IP address of the OSPF neighbor expressed using IPv4 dotted-decimal notation.

poll-interval *poll_interval_value*

Default: 120

Sets the number of seconds in the dead neighbor polling interval as an integer from 1 through 65535

priority *priority_value*

Default: 0

Sets the 8-bit number that represents the router priority value of the non-broadcast neighbor associated with the specified IP address. This must be an integer from 0 through 255. This keyword does not apply to point-to-multipoint interfaces.

Usage Guidelines

Use this command to configure OSPF routers that connect to non-broadcast networks.

Example

The following command specifies an OSPF router neighbor with the IP address of *209.165.200.234*:

```
neighbor 209.165.200.234
```

network area

Enables OSPF on an interface and defines the OSPF area for that network.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

```
[ no ] network network_ip_address / network_mask area { area_id | area_ip_address }
```

no

Disables OSPF on an interface and defines the OSPF area for that network.

network_ip_address/network_mask

Specifies the network address and mask as well as the interface on which OSPF will be enabled. *network_ip_address* in entered in IPv4 dotted-decimal notation, followed by the "/" and the mask (CIDR).

area_id

Specifies the OSPF area identification number for the specified network as an integer from 0 through 4294967295.

area_ip_address

Specifies the IP address of the OSPF area for this network. This must be entered in IPv4 dotted-decimal notation.

Usage Guidelines

Use this command to specify the IP address of the network interface that the OSPF router will use.

Example

The following command specified that the OSPF router will use the interface at IP address *209.165.200.224* with a netmask of *24*:

```
network 209.165.200.224/27
```

ospf graceful-restart

Configures OSPF graceful-restart settings.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

ospf graceful-restart { **grace-period** *grace_period* | **helper** { **never** | **policy** { **only-reload** | **only-upgrade** } } }

grace-period grace-period

Specifies the OSPF graceful restart grace period (in seconds) as an integer from 1 through 1800. Default grace period is 60 seconds.

helper { never | policy { only-reload | only-upgrade } }

Helps configure OSPF helper settings.

never: Do not allow helper mode.

policy { only-reload | only-upgrade }: Allows ospf graceful-restart helper mode.

- **only-reload**: Allows ospf graceful-restart helper mode only for a reload.
- **only-upgrade**: Allows ospf graceful-restart helper mode only for an upgrade.

Default is ospf graceful-restart grace-period.

Usage Guidelines Use this command to configure graceful-restart specific settings.

Example

The following command sets the graceful restart grace period to *60* seconds:

```
ospf graceful-restart grace-period 60
ospf graceful-restart helper policy only-reloadL
ospf graceful-restart helper policy only-upgrade
```

ospf router-id

This command configures the router ID for the OSPF process.

Product PDSN

HA

GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description `[ no ] ospf router-id ip_address`

no

Disables the router ID for the OSPF process.

router-id *ip_address*

Specifies the router ID for the OSPF process. *ip_address* is entered using IPv4 dotted-decimal notation.

Usage Guidelines Use this command to set the router ID for the current OSPF router process.

Example

The following command sets the router ID to *192.168.200.1*:

```
ospf router-id 192.168.200.1
```

passive-interface

Enables or disables the suppression of OSPF routing updates on the specified interface.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

```
[ no ] passive-interface interface_name
```

no

Disables the name assigned to a logical interface within the specific context.

interface_name

Specifies the name assigned to a logical interface within the specific context as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to suppress router updates on an interface in the current context.

Example

The following command suppresses OSPF routing updates on the interface named *Intfc1*:

```
passive-interface Intfc1
```

redistribute

Redistributes routes from other protocols to OSPF neighbors using the OSPF protocol.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

redistribute { **connected** | **rip** | **static** } [**metric** *metric_value*] [**metric-type** { **1** | **2** }] [**route-map** *route_map_name*]
no redistribute { **connected** | **rip** | **static** }

no

Disables the redistributed routes.

connected

Redistributes connected routes.

rip

Specifies that RIP routes will be redistributed. (RIP is not supported at this time.)

static

Redistributes static routes.

metric *metric_value*

Sets the OSPF metric used in the redistributed route. This must be an integer from 1 through 16777214.

metric-type { 1 | 2 }

Default: 2

Sets route metric type that is applied to redistributed routes.

1: Sets the OSPF external link type for routes to Type 1.

2: Sets the OSPF external link type for routes to Type 2.

route-map *route_map_name*

Filter routes through the specified route map before redistribution. *route_map_name* specifies the name of the route-map to use as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to define what routing protocols should have their routes redistributed into OSPF.

Example

The following command defines that BGP routes should be redistributed:

```
redistribute connected
```

refresh timer

Adjusts settings for the OSPF refresh timer.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

Syntax Description

```
[ no ] refresh  timer value
```

no

Disables the refresh timer.

value

Default: 10

Specifies the minimum amount of time (in seconds) to wait before refreshing a Link-state Advertisement (LSA). This must be an integer from 10 through 1800.

Usage Guidelines

Use this command to define the amount of time to wait before refreshing an LSA.

Example

The following command sets the refresh timer to *90* seconds:

```
refresh timer 90
```

router-id

Configures the router ID for the OSPF process.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ospf)#`

Syntax Description

`[ no ] router-id` *`ip_address`*

no

Disables the router ID for the OSPF process.

ip_address 196

Specifies the router ID for the OSPF process in IPv4 dotted-decimal notation.

Usage Guidelines

Use this command to set the router ID for the current OSPF router process.

Example

The following command sets the router ID to *192.168.200.1*:

```
router-id 192.168.200.1
```

timers spf

Sets the Shortest Path First (SPF) timers.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context *context_name* **> router ospf**

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ospf)#`

Syntax Description

timers spf *delay_value hold_time_value*
no timers spf

no

Disables SPF timers.

delay_value

Default: 5

Specifies the delay time (in seconds) between receiving changes to an SPF calculation. This must be an integer from 0 through 4294967295.

hold_time_value

Default: 10

Specifies the hold time (in seconds) between consecutive SPF calculations. This must be an integer from 0 through 4294967295.

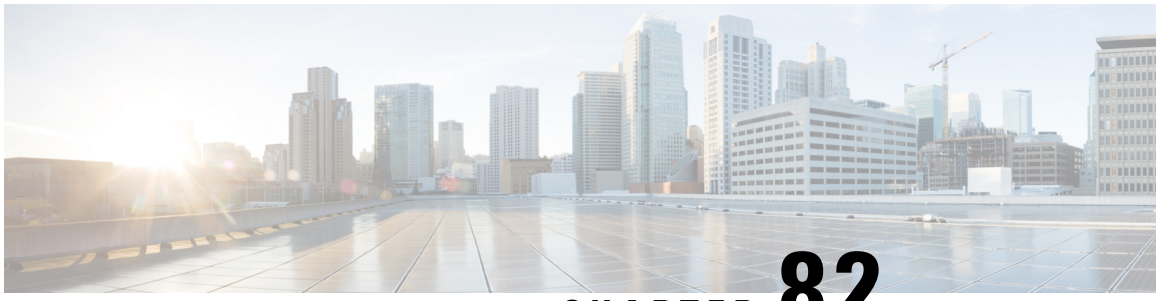
Usage Guidelines

Use this command to set the SPF delay and hold timers for the current OSPF router process.

Example

The following command sets the delay timer to *15* and the hold timer to *15*:

```
timers spf 15 15
```



CHAPTER 82

OSPFv3 Configuration Mode Commands

The OSPFv3 Configuration sub-mode is used to configure the OSPFv3 routing protocol. This mode includes commands that configure OSPFv3 routing parameters.

Command Modes

Exec > Global Configuration > Context Configuration > OSPFv3 Configuration

configure > context *context_name* **> router ospfv3**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospfv3)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

area

Configures an Open Shortest Path First Version 3 (OSPFv3) area and enables authentication for that area.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPFv3 Configuration

configure > context *context_name* **> router ospfv3**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospfv3)#
```

Syntax Description

```
[ no ] area { decimal_value | ipv4address } default-cost default_integer_value |
stub [ no-summary ] | virtual-link virtuallink_neighbour_Ipv4_address [
dead-interval virtuallink_dead_interval ] [ hello-interval virtuallink_hello_interval
 ] [ retransmit-interval virtuallink_retransmit_interval ] [ transmit-delay
virtuallink_transmit_delay ]
```

no

Disables authentication for the specified area.

decimal_value | ipv4address

decimal_value: Specifies the identification number of the area where authentication will be enabled as an integer from 0 through 4294967295.

ipv4address: Specifies the IP address of the area where authentication will be enabled in IPv4 dotted-decimal notation.

default-cost *default_integer_value*

Sets the OSPFV3 authentication area's default cost as an integer from 1 through 16777215.

stub [no-summary]

Sets the OSPFV3 stub area. Only Router-LSAs, Network-LSAs, Inter-area Prefix-LSAs, Intra-area Prefix-LSAs and Link-LSAs are allowed in a Stub area.

no-summary Does not inject inter-area routes into stub area.

virtual-link *virtuallink_neighbour_Ipv4_address*

Configures a virtual link to the authentication area.

virtuallink_neighbour_Ipv4_address is the IPv4 address for the virtual link of the authenticated area in dotted-decimal notation.

The following interval timers can be set for the virtual link:

- **dead-interval** *virtuallink_dead_interval*: Sets the virtual link dead-interval (in seconds) as an integer from 1 through 65535.
- **hello-interval** *virtuallink_hello_interval*: Sets the virtual link hello interval (in seconds) as an integer from 1 through 65535.
- **retransmit-interval** *virtuallink_retransmit_interval*: Sets the virtual link retransmit interval (in seconds) as an integer from 1 through 3600.

- **transmit-delay** *virtuallink_transmit_delay*: Sets the virtual link transmit delay (in seconds) as n integer from 1 through 3600.

Usage Guidelines Use this command to establish OPSFv3 areas and enable authentication.

Example

The following command enables authentication for an OSPFv3 area defined by the IP address 192.168.100.10 with default cost of 256

```
area 192.168.100.10 default-cost 256
```

default-metric

Configures the default metric value for routes redistributed from another protocol into Open Shortest Path First Version 3 (OSPFv3).

Product PDSN

HA

GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > OSPFv3 Configuration

configure > context *context_name* **> router ospfv3**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospfv3)#
```

Syntax Description

```
[ no ]  default-metric default_metric_integer_value
```

no

Disables the default metric.

default_metric_integer_value

Specifies the default metric as an integer from 1 through 16777214.

Usage Guidelines Use this command to configure OPSFv3 default metric.

Example

The following command configures OSPFv3 default metric to 256

```
default-metric 256
```

passive-interface

Configures an interface as being OSPFv3 passive. If a network interface is configured as passive, it will not receive or send any OSPFv3 packets.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPFv3 Configuration

configure > context *context_name* **> router ospfv3**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospfv3)#
```

Syntax Description

`[ no ] passive-interface` *`interface_name`*

no

Disables the passive interface.

interface_name

Specifies an OSPFv3 passive interface as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to configure an OPSFv3 passive interface in this context.

Example

The following command configures the *OSPF-if1* interface to be OSPFv3 passive.

```
passive-interface OSPF-if1
```

redistribute

Redistributes routes from other protocols to OSPFv3 neighbors using the OSPFv3 protocol.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPFv3 Configuration

configure > **context** *context_name* > **router ospfv3**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospfv3)#
```

Syntax Description

[no] redistribute { connected | static } redistribute connected [**metric** *metric_value* [**metric-type** *external_metric_type*] [**route-map** *route_map_name*]] [**metric-type** *external_metric_type* [**route-map** *route_map_name*]] [**route-map** *route_map_name*] **static** [**metric** *metric_value* [**metric-type** *external_metric_type*] [**route-map** *route_map_name*]] [**metric-type** *external_metric_type* [**route-map** *route_map_name*]] [**route-map** *route_map_name*]

no

Disables the route redistribution.

connected

Redistributes connected routes.

static

Redistributes static routes.

metric ***metric_value***

Specifies the OSPFv3 default metric value as an integer from 0 through 16777214.

metric-type ***external_metric_type***

Specifies the OSPFv3 external metric type as the integer 1 or 2

route-map ***route_map_name***

Specifies a route map as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to configure OPSFv3 redistribution of connected or static routes.

Example

The following command configures OSPFv3 redistribution of connected routes.

```
redistribute connected metric 45 metric-type 1 route-map rt
```

router-id

Sets the OSPFv3 router ID for the Open Shortest Path First Version 3 (OSPFv3) routing process.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPFv3 Configuration

configure > context *context_name* **> router ospfv3**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospfv3)#
```

Syntax Description

[no] router-id *router_id_ipaddress*

no

Disables the router-id.

router_id_ipaddress

Specifies the router-id an IPv4 address in dotted-decimal notation.

Usage Guidelines

Use this command to configure OPSF v3 router id to the given IPv4 address.

Example

The following command configures OSPFv3 router id to the given IPv4 address.

```
router-id 11.22.22.21
```

timers spf

Sets OSPFv3 the delay in the time between the detection of a topology change and when the SPF algorithm actually runs.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPFv3 Configuration

configure > context *context_name* **> router ospfv3**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospfv3)#
```

Syntax Description

[no] timers spf *spf_delay_timer_value spf_hold_timer_value*

no

Disables the SPF delay timer.

spf_delay_timer_value

Sets the Shortest Path First (SPF) delay timer (in milliseconds) as an integer from 0 through 4294967295.

spf_hold_timer_value

Specifies the hold time (in milliseconds) between consecutive SPF calculations. This must be an integer from 0 through 4294967295.

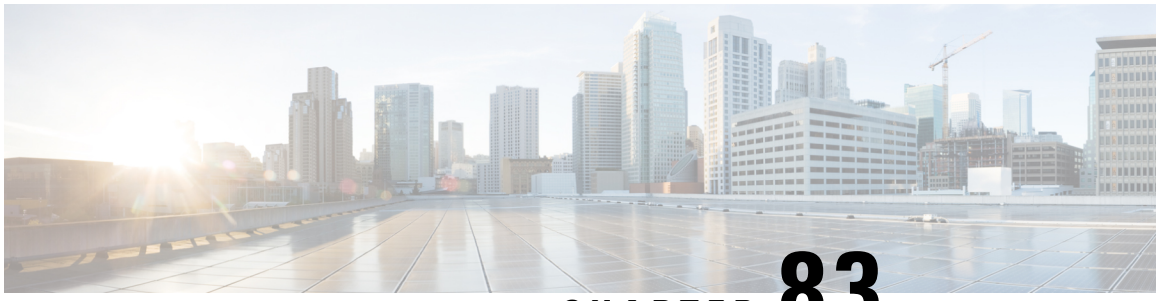
Usage Guidelines

Use this command to configure the OPSFv3 SPF delay timer.

Example

The following command sets OSPFv3 SPF timer.

```
timers spf 256
```



CHAPTER 83

OSPF VRF Configuration Mode Commands

Command Modes

The OSPF VRF Configuration sub-mode is used to configure the virtual routing and forwarding (VRF) context instances for OSPF routing protocol. This mode includes commands that configure VRF instance for OSPF routing parameters.

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

area

Configures various parameters, including authentication, area identification, virtual link ID, and delay/interval values for the specified OSPF area using a specific VRF instance.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

[no] area { *decimal_value* **|** *ip_address* **} {authentication [message-digest] | default-cost** *cost_value* **| nssa [default-information-originate] [no-redistribution] [no-summary] [translate-always] [translate-candidate] [translate-never] | stub [no-summary] | virtual-link** *router_ip_address* **[authentication {message-digest | null | text}| authentication-key {encrypted password** *encrypted_string* **| password** *password_string***}| message-digest-key** *key_id* **md5 [encrypted password** *encrypted_string* **| password** *password_string***]} [dead-interval] [hello-interval] [retransmit-interval] [transmit-delay]**

no

Disables or removes configured parameters for the specified OSPF area using a specific VRF instance.

ip_address

Specifies the IP address of the area where authentication will be enabled in IPv4 dotted-decimal notation.

decimal_value

Specifies the identification number of the area where parameters to be configured as an integer from 0 through 4294967295.

authentication

Sets the OSPF authentication type to use the simple authentication method.

message-digest

Sets the OSPF authentication type to use the message digest 5 (MD5) authentication method.

default-cost *cost_value*

Sets the default cost for an OSPF area. *cost_value* must be an integer from 0 through 16777215.

nssa [default-information-originate] [no-redistribution no-summary] [translate-always] [translate-candidate] [translate-never]

Configures and defines an area as an NSSA (Not So Stubby Area) and configures OSPF parameters for it.

default-information-originate: Configures the OSPF VRF instances to originate default information to the NSSA area.

no-redistribution: Configures the OSPF VRF instance to not to redistribute external routes to the NSSA area.

no-summary: Configures the OSPF VRF instance to not to inject the inter-area routes into NSSA.

translate-always: Configures the NSSA-ABR (Area Border Router) always to translate. By default this is disabled.

translate-candidate: Configures the NSSA-ABR always to translate election. By default this is enabled.

translate-never: Configures the NSSA-ABR never to translate. By default this is disabled.

stub [no-summary]

Specifies an OSPF area as an stub area configures the NSSA-ABR never to translate. By default this is disabled.

no-summary: Disables (stops) the ABR from sending summary LSAs into the stub area.

virtual-link *router_id*

Specifies the router identifier which provides a virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

router_id must be an IP address in IPv4 dotted-decimal notation of the ABR to be linked to.

authentication {message-digest | null | text}

Configures the OSPF authentication method to be used by the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

message-digest: Set the OSPF authentication type to use the message digest (MD) authentication method.

null: Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.

text: Set the OSPF authentication type to use the clear text authentication method.

authentication-key

Configures the authentication password for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

message-digest-key *key_id*

Specifies the MD key identifier number for virtual link connection. *key_id* must be an integer from 1 through 255.

md5

Sets the message digest to MD5 for virtual link connection.

[encrypted] password *passwd_string*

Specifies the password required for virtual link connection authentications. The keyword **password** is optional and if specified *passwd_string* must be an alphanumeric string of 1 through 63 characters. The password specified must be in an encrypted format if the optional keyword **encrypted** was specified.

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 **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file. *encrypted_string* is an alphanumeric string of 1 through 523 characters.

dead-interval *value*

Specifies the dead interval (in seconds) that the router should wait, during which time no packets are received and after the router considers a neighboring router to be off-line. *value* must be an integer from 1 through 65535.

hello-interval *value*

Specifies the hello interval (in seconds) before sending a hello packet. *value* must be an integer from 1 through 65535.

retransmit-interval *value*

Specifies the delay between retransmission (in seconds) that router should wait before retransmitting a packet. *value* must be an integer from 1 through 3600.

transmit-delay *value*

Specifies the interval (in seconds) that the router should wait before transmitting a packet. *value* must be an integer from 1 through 3600.

Usage Guidelines

Use this command to configure/set the various network/connection/authentication parameters of OPSF areas using specific VRF instance.

Example

The following command enables authentication for an OSPF area defined by the IP address *192.168.100.10* and the OSPF authentication type to MD5:

```
area 192.168.100.10 authentication message-digest
```

The following command defines the area designated by the IP address *192.168.100.10* as an NSSA area where translation of NSSA candidate is enabled by default:

```
area 192.168.100.10 nssa
```

The following command defines the OSPF area defined by the IP address *192.168.100.10* as a stub area:

```
area 192.168.100.10 stub
```

The following command creates a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20*:

```
area 192.168.100.10 virtual-link 192.168.200.20
```

The following command sets the authentication method for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20* to use no authentication:

```
area 192.168.100.10 virtual-link 192.168.200.20 null
```

The following command creates an authentication password of *123456* for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20*:

```
area 192.168.100.10 virtual-link 192.168.200.20 authentication-key password
 123456
```

The following command enables the use of MD5-based OSPF authentication for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20*, sets the MD5 Key ID to *25*, and the password to *123456*:

```
area 192.168.100.10 virtual-link 192.168.200.20 message-digest-key 25 md5
 password 123456
```

The following command sets the retransmit interval for a virtual link between the OSPF areas defined by the IP address *192.168.100.10* and the IP address *192.168.200.20* to *60* seconds:

```
area 192.168.100.10 virtual-link 192.168.200.20 retransmit-interval 60
```

default-information originate

Creates a default external route into an OSPF routing domain.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

default-information originate [**always**] [**metric** *metric_value*] [**metric-type** { **1** | **2** }] [**route-map** *route_map_name*]
no default-information originate

no

Disables the default external route.

always

Always advertise the route regardless of whether or not the software has a default route.

metric *metric_value*

Sets the OSPF metric used in creating the default rout as an integer from 1 through 16777214.

metric-type { 1 | 2 }

Sets the default route metric type.

1: Sets the OSPF external link type for default routes to Type 1.

2: Sets the OSPF external link type for default routes to Type 2.

route-map *route_map_name*

Specifies the name of the default route-map to be use as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to set the default external route into an OSPF routing domain.

Example

The following command sets the default external route to originate from the route map named *rmap1*:

```
default-information originate route-map rmap1
```

default-metric

Configures the default metric value for the OSPF routing protocol.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

```
default-metric metric_value
no default-metric
```

metric_value

Sets the metric value expressed as an integer from 1 through 16777214. The default metric value setting is 26385.

no

Enables or disables the default metric value for OSPF.

Usage Guidelines

Use this command to set the default metric for routes.

Example

The following command sets the default metric to *235*:

```
default-metric 235
```

distance

Configures the OSPF route administrative distances for all OSPF route types or based on specific route type. Administrative distance is the measure used by Cisco routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) using an administrative distance value. A lower numerical value is preferred.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

```
[ no ] distance { distance_value | ospf { [ external distance_value ] [ inter-area
 distance_value ] [ intra-area distance_value ] } }
```

no

Disables the soecified option.

distance_value

Specifies the OSPF route administrative distances as an integer from 1 to 255. The default distance value is 110.

external *ext_distance_value*

Sets the OSPF route administrative distance for routes from other routing domains, learned by redistribution. *ext_distance_value* must be an integer from 1 through 255. The default is 110.

inter-area *inter_distance_value*

Sets the OSPF route administrative distance for routes from one routing area to another. *inter_distance_value* must be an integer from 1 through 255. The default is 110.

intra-area *intra_distance_value*

Sets the OSPF route administrative distance for all routes within an area. *intra_distance_value* must be an integer from 1 through 255. The default is 110.

Usage Guidelines

Use this command to set the administrative distance for OSPF routes.

Example

The following command sets the administrative distance for all OSPF route types to *30*:

```
distance 30
```

distribute-list

Enables or disables the filtering of networks in outgoing routing updates.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

```
[ no ] distribute-list route_access_list out { connected | rip | static }
```

no

Disables the filtering of networks in outgoing routing updates.

route_access_list

Specifies the name of the OSPF route access list to use for filtering as an alphanumeric string of 1 through 63 characters.

connected

Filters connected routes.

rip

Filters RIP routes. (RIP is not supported at this time.)

static

Filters static routes.

Usage Guidelines

Use this command to enable the filtering of outgoing route updates by using the specified route access list.

Example

The following command uses the route access list named *ral1* to filter outgoing routing updates for all connected routes:

```
distribute-list ral1 out connected
```

neighbor

Configures OSPF routers that interconnect to non-broadcast networks.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

```
[ no ] neighbor  ip_address  [ poll-interval poll_interval_value ] [ priority priority_value ]
```

no

Disables OSPF routers that interconnect to non-broadcast networks.

ip_address

Specifies the interface IP address of the OSPF neighbor expressed using IPv4 dotted-decimal notation.

poll-interval *poll_interval_value*

Default: 120

Sets the number of seconds in the dead neighbor polling interval as an integer from 1 through 65535

priority *priority_value*

Default: 0

Sets the 8-bit number that represents the router priority value of the non-broadcast neighbor associated with the specified IP address. This must be an integer from 0 through 255. This keyword does not apply to point-to-multipoint interfaces.

Usage Guidelines

Use this command to configure OSPF routers that connect to non-broadcast networks.

Example

The following command specifies an OSPF router neighbor with the IP address of *192.168.100.10*:

```
neighbor 192.168.100.10
```

network

Enables OSPF on an interface and defines the OSPF area for that network.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

`[ no ] network` *`network_ip_address/mask`* `area {` *`area_id`*`|` *`area_ip_address`* `}`

no

Disables OSPF on an interface and defines the OSPF area for that network.

network_ip_address/mask

Specifies the network address and mask as well as the interface on which OSPF will be enabled. *network_ip_address* in entered in IPv4 dotted-decimal notation, followed by the "/" and the mask in CIDR notation.

area_id

Specifies the OSPF area identification number for the specified network as an integer from 0 through 4294967295.

area_ip_address

Specifies the IP address of the OSPF area for this network. This must be entered in IPv4 dotted-decimal notation.

Usage Guidelines

Use this command to specify the IP address of the network interface that the OSPF router will use.

Example

The following command specified that the OSPF router will use the interface at IP address 192.168.1.0 /24 an area ID 2345 and IP address 192.168.1.5:

```
network 192.168.1.0/24 area 2345 192.168.1.5
```

ospf router-id

Configures the router ID for the OSPF process.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

`[ no ] ospf router-id` *`ip_address`*

no

Disables the specified OSPF router.

ip_address

Specifies the router ID for the OSPF process as an IP address entered using IPv4 dotted-decimal notation

Usage Guidelines

Use this command to set the router ID for the current OSPF router process.

Example

The following command sets the router ID to *192.168.200.1*:

```
ospf router-id 192.168.200.1
```

passive-interface

Enables or disables the suppression of OSPF routing updates on the specified interface.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

[no] passive-interface *interface_name*

no

Disables the name assigned to a logical interface within the specific context.

interface_name

Specifies the name assigned to a logical interface within the context as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to suppress router updates on an interface in the current context.

Example

The following command suppresses OSPF routing updates on the interface named *Intfc1*:

passive-interface Intfc1

redistribute

Redistributes routes from other protocols to OSPF neighbors using the OSPF protocol.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > **context** *context_name* > **router ospf** > **ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

```
redistribute { connected | rip | static } [ metric metric_value ] [ metric-type { 1 | 2 } ] [ route-map route_map_name ]
no redistribute { connected | rip | static }
```

no

Disables the redistributed routes.

connected

Redistributes connected routes.

rip

Specifies that RIP routes will be redistributed. (RIP is not supported at this time.)

static

Redistributes static routes.

metric *metric_value*

Sets the OSPF metric used in the redistributed route. This must be an integer from 1 through 16777214.

metric-type { 1 | 2 }

Default: 2

Sets route metric type that is applied to redistributed routes.

1: Sets the OSPF external link type for routes to Type 1.

2: Sets the OSPF external link type for routes to Type 2.

route-map *route_map_name*

Filter routes through the specified route map before redistribution. *route_map_name* specifies the name of the route-map to use as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to define what routing protocols should have their routes redistributed into OSPF.

Example

The following command defines that BGP routes should be redistributed:

```
redistribute connected
```

refresh timer

Adjusts settings for the OSPF refresh timer.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

```
[ no ] refresh  timer value
```

no

Disables the refresh timer.

value

Default: 10

Specifies the minimum amount of time (in seconds) to wait before refreshing a Link-state Advertisement (LSA). This must be an integer from 10 through 1800.

Usage Guidelines

Use this command to define the amount of time to wait before refreshing an LSA.

Example

The following command sets the refresh timer to *90* seconds:

```
refresh timer 90
```

router-id

Configures the router ID for the OSPF process.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

```
[ no ] router-id ip_address
```

no

Disables the router ID for the OSPF process.

ip_address 92

Specifies the router ID for the OSPF process in IPv4 dotted-decimal notation.

Usage Guidelines

Use this command to set the router ID for the current OSPF router process.

Example

The following command sets the router ID to *192.168.200.1*:

```
router-id 192.168.200.1
```

timers spf

Sets the Shortest Path First (SPF) timers.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context *context_name* **> router ospf > ip vrf** *vrf_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

Syntax Description

```
timers spf delay_value hold_time_value
no timers spf
```

no

Disables SPF timers.

delay_value

Default: 5

Specifies the delay time (in seconds) between receiving changes to an SPF calculation. This must be an integer from 0 through 4294967295.

hold_time_value

Default: 10

Specifies the hold time (in seconds) between consecutive SPF calculations. This must be an integer from 0 through 4294967295.

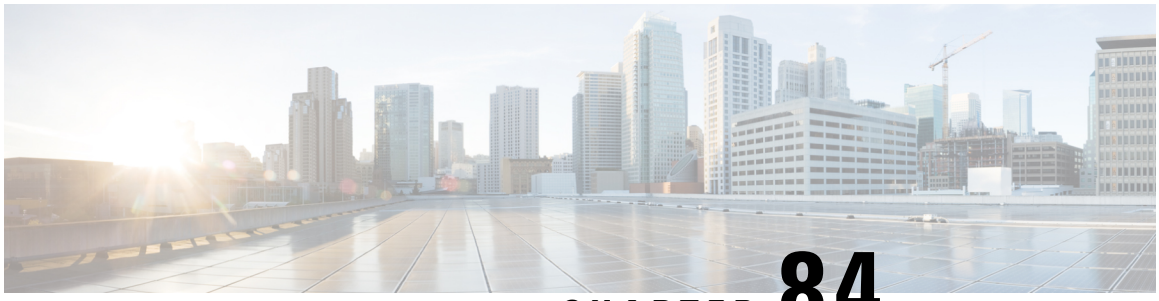
Usage Guidelines

Use this command to set the SPF delay and hold timers for the current OSPF router process.

Example

The following command sets the delay timer to *15* and the hold timer to *15*:

```
timers spf 15 15
```



CHAPTER 84

Out-Address Configuration Mode Commands

Command Modes

The Out-Address configuration mode provides the commands to configure the outbound parameters for the SCCP entities as part of the gtt-address-map configuration.

Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

configure > gtt address-map *map_id* **> out-address** *address_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-gtt-addrmap-outaddr-`*`out_address`*`)#`

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

gt-address

Configures the SCCP short address.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

configure > **gtt address-map** *map_id* > **out-address** *address_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-gtt-addrmap-outaddr-out_address)#`

Syntax Description

gt-address *gt_address*

gt_address

A string of 1 to 15 digits to define the GT-address

Usage Guidelines

Define the GT-address

Example

gt-address *010405525397*

gt-format

The GT-format provides four formats that can be used during GTT.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

configure > **gtt address-map** *map_id* > **out-address** *address_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-gtt-addrmap-outaddr-out_address)#`

Syntax Description

gt-format *format_num*

format_num

1: Selects GT-format 1 options which include **nature-of-address** and **odd/even.** Once selected, the system enters GT-Format1 configuration mode.

2: Selects GT-format2 options which include **translation-type**. Once selected, the system enters GT-Format2 configuration mode.

3: Selects GT-format3 options which include **encoding-scheme**, **numbering-plan3** and **translation-type**. Once selected, the system enters GT-Format1 configuration mode.

4: Selects GT-format4 options which include **encoding-scheme**, **nature-of-address**, **numbering-plan**, and **translation-type**. Once selected, the system enters GT-Format4 configuration mode.

Usage Guidelines

Select the a GT-format that include encoding-scheme as part of the GTT process.

Example

gt-format *3*

ni-indicator

Configures the National and International indicator to use during the GTT process.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

configure > gtt address-map *map_id* **> out-address** *address_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-gtt-addrmap-outaddr-`*`out_address`*`)#`

Syntax Description

ni-indicator *ni_ind*

ni_ind

Select one of the following as the appropriate type of national indicator for the address structure:

- **national**
- **international**

Usage Guidelines

Select the international indicator to be used for out-going addresses.

Example

ni-indicator *international*

point-code

Selects and configures the SS7-type point code for use with the out-going address.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

configure > gtt address-map *map_id* **> out-address** *address_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-addrmap-outaddr-out_address)#
```

Syntax Description **point-code** *pt_code*

pt_code

Enter 1 to 11 digits in the point code format predefined during variant selection of GTT association.

Usage Guidelines Define an ITU point code to be used for out-going address processing.

Example

point-code *6.255.6*

routing-indicator

Selects the type of routing and the indicator to be included in the out-going message.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

configure > gtt address-map *map_id* **> out-address** *address_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-addrmap-outaddr-out_address)#
```

Syntax Description **routing-indicator** *routing_ind*

routing_ind

Select one of the following options:

- **gt**: Inserts an indicator that identifies routing based on global title.
- **ssn**: Inserts an indicator that identifies routing based on the subsystem number.

Usage Guidelines Select global title as the appropriate routing indicator.

Example

routing-indicator *gt*

ssf

Selects the subservice field as factor in the out-going address processing. **ssf** sets the network indicator in the subservice field for SS7 Message Signal Units (MSUs). The indicator carried in the message's routing information typically identifies the structure of the point code as a message from within a nation or as a message coming from outside the national - international.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

configure > gtt address-map *map_id* **> out-address** *address_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-addrmap-outaddr-out_address)#
```

Syntax Description

ssf *sub_svc_fld*

sub_svc_fld

Select one of the following options:

- **international:** The network indicator identifies the message as international with a point code structure that does not match the national point code structure,
- **national:** The network indicator identifies the messages as having a national point code structure.
- **reserved:** Provides an alternate network indicator for national messages.
- **spare:** Provides an alternate network indicator for international messages.

Usage Guidelines

Select the international NI for inclusion in out-going address subservice fields.

Example

ssf *international*

ssn

Selects the subsystem number to be included in the out-going message.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

configure > gtt address-map *map_id* **> out-address** *address_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-addrmap-outaddr-out_address)#
```

Syntax Description

ssn *sub_sys_num*

sub_sys_num

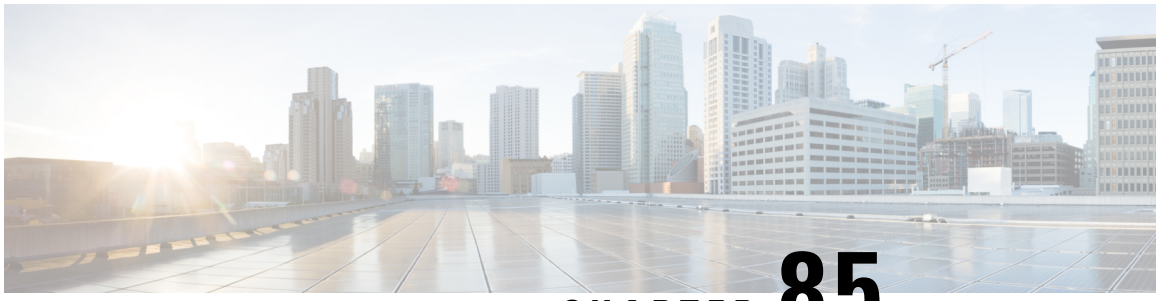
Enter an integer from 1 to 255.

Usage Guidelines

Use subsystem number 44 in the out-going address.

Example

ssn *44*



CHAPTER 85

P2P Advertisement Server Group Configuration Mode Commands

The P2P Advertisement Server Group Configuration Mode is used to configure the P2P ad-server group and the application(s) to which advertisements need to be matched. The type of advertisement flow will be configured per application.

Command Modes

Exec > ACS Configuration > P2P Advertisement Server Group Configuration

active-charging service *service_name* **> p2p-ads-group** *ads_group_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-p2p-ads)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

ad-source

This command allows to configure the P2P advertisement source that can be a HTTP host or SSL server.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > P2P Advertisement Server Group Configuration

active-charging service *service_name* **> p2p-ads-group** *ads_group_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-p2p-ads)#
```

Syntax Description

`[ no ] ad-source` *operator http_host_name/ssl_server_name*

no

If previously configured, disables the configured ad-source.

operator

Specifies how to match.

operator must be one of the following:

- =: Equals
- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

http_host_name/ssl_server_name

Specifies the name of the HTTP host or SSL server to match and must be an alphanumeric string of 1 through 127 characters. SSL supports the Server Name indication (SNI) field.

Usage Guidelines

This command allows to configure the P2P advertisement source that can be a HTTP host or SSL server when the user runs an active application session. The ad-source can be server name indication for HTTPS flows and host name for HTTP-based ad flows.

Important The maximum number of ad-source lines that can be configured is 32.

Example

The following command matches the ad-source string ending with *admob.com*:

```
ad-source ends-with admob.com
```

map-to-application

This command allows to configure the P2P advertisement application that will map the advertisement group to the corresponding application/protocol.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > P2P Advertisement Server Group Configuration

active-charging service *service_name* **> p2p-ads-group** *ads_group_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-p2p-ads)#
```

Syntax Description

[no] map-to-application { *p2p_list* } +

no

If previously configured, disables the application/protocol mapping.

p2p_list

Specifies the list of protocols/applications supported in the P2P plugin.

+

More than one protocol/application supported in the P2P plugin can be entered within a single command.

Usage Guidelines

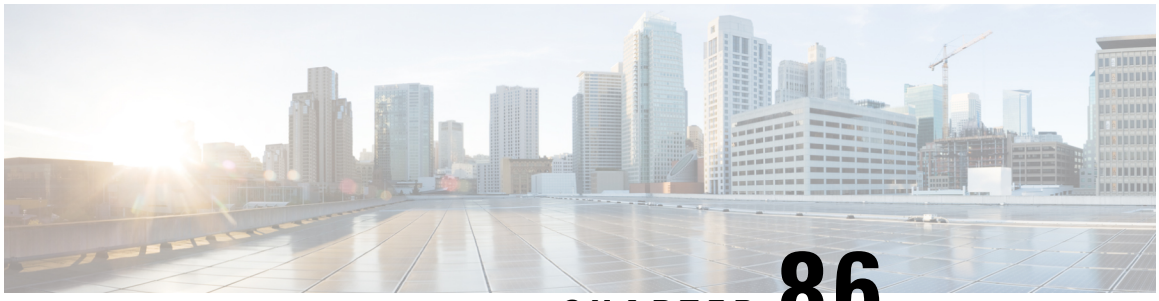
This command allows to configure the P2P advertisement application that will map the advertisement group to the application protocol.

The maximum number of map-to-application rule lines that can be configured is equal to the number of the applications present in *p2p_list* supported by P2P plugin.

Example

The following command maps the ads-group to the *slacker-radio* application:

```
map-to-application slacker-radio
```



CHAPTER 86

PCC-Action-Set Configuration Mode Commands

Important This configuration mode is supported from StarOS Release 12.1 onward.

Command Modes

The PCC- Action-Set Configuration Mode provides the parameters to indicate the policy and charging as well as event generation related decisions that will get activated when the corresponding PCC-Condition-Group is evaluated to TRUE within a profile. A maximum of 32 actions can be configured in an instance of PCC-Action-Set.

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

af-media-type

This command is used to set the action to be taken when specific media type is received from Application Function (AF) over Rx interface.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

[no] af-media-type {application | audio | control | data | message | other | text | video} {qos-profile *qos_profile_value***[gate-status { disabled | enabled | enabled-downlink | enabled-uplink] } | {gate-status {disabled | enabled | enabled-downlink | enabled-uplink [qos-profile** *qos_profile_value***] }[monitoring-key** *mon_key_id*

no

Removes the configured action set for different type of AF media in a PCC-Action-Set configuration instance for PCC-Service configuration.

application

Sets the AF media type to 'application' data traffic for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

audio

Sets the AF media type to 'audio' data traffic for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

control

Sets the AF media type to 'control' signal for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

data

Sets the AF media type to 'data' for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

message

Sets the AF media type to 'message' data for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

other

Sets the AF media type to 'other', out of AF media type configured here, for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

text

Sets the AF media type to 'text' for various action configured under PCC-Action-Set configuration instance for PCC-Service configuration.

video

Sets the AF media type to 'video' for various action configured under PCC-Action-Set configuration instance for PCC-Service configuration.

qos-profile *qos_profile_value*

Associate the pre-defined PCC-QoS-Profile for specific AF media type for various action configured for PCC-Service configuration.

qos_profile_value is name of the pre-defined PCC-QoS-Profile in PCC-Service Configuration instance.

gate-status {disabled | enabled | enabled-downlink | enabled-uplink}

Default: Enabled

Associate the status of Gate for specific AF media type for various action configured for PCC-Service configuration.

disabled: disables the Gate status in downlink and uplink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance.

enabled: Enables the Gate status in downlink and uplink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance. This is the default status of Gate.

enabled-downlink: Enables the Gate status in downlink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance.

enabled-uplink: Enables the Gate status in uplink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance.

monitoring-key *mon_key_id*

Specifies the Monitoring Key identifier to be associated with AF-Media-type under PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id must be a preconfigured monitoring key having integer between 1 through 65535.

Usage Guidelines

Use this command to set the action to be taken when specific media type is received from Application Function (AF) over Rx interface.

It also associates the pre-defined PCC-QoS-Profile and **Gate** function and monitoring key with specific media type.

Example

The following command sets the AF media type to 'video' with PCC-QoS-Profile named *video_qos1* with gate status enabled in downlink and uplink traffic for various action configured under PCC-Action-Set configuration instance for PCC-Service configuration:

af-media-type video qos-profile *video_qos1* **gate-status enabled**

associate monitoring-key

This command associates a Monitoring Key id with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

[no] associate monitoring-key *mon_key_id* **usage-monitor** *usage_mon_name*

no

Removes the associated Monitoring Key id configuration along with the association to PCC-Usage-Monitor from a PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id

Specifies the Monitoring Key identifier to be associated with PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id must be an integer between 1 through 65535.

usage-monitor *usage_mon_name*

Specifies the PCC-Usage-Monitor associated with Monitoring Key *mon_key_id* under PCC-Action-Set configuration instance for PCC-Service configuration.

usage_mon_name is a pre-configured PCC-Usage-Monitor instance in PCC-Service Profile Configuration for PCC-Service configuration.

Usage Guidelines

Use this command to associate a Monitoring Key with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

There is a Many-To-Many relationship between Usage-Monitor and Monitoring-Key. Operator can change this relationship using required command.

When usage is reported to IPCF for a particular Monitoring Key, the usage is added to all the Usage Monitoring to which the Monitoring Key is associated.

Operator can break the relationship between Monitoring Key and Usage Monitor by **dissociate monitoring-key** command.

Example

The following command associates Monitoring Key id *102* with pre-defined PCC-Usage-Monitor named *usage_mon1* under PCC-Action-Set configuration instance for PCC-Service configuration:

associate monitoring-key *102* **usage-monitor** *usage_mon1*

authorize

This command sets an action to change the various authorization parameters used for the IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

[no] authorize {**apn-mbr** | **default-eps-bearer** | **qci** *qci_value*} **qos-profile** *qos_prof_name*

no

Removes the configured action for QoS Profile authorization parameters from PCC-Action-Set configuration instance for PCC-Service configuration.

apn-mbr

Sets the action for QoS authorization of Maximum Bit Rate (MBR) at APN through a pre-configured QoS profile name *qos_prof_name* which is to use for the authorization at different level in an PCC-Service instance.

This keyword is applicable only to EPS access type. MBR Download and MBR Upload values of the QoS profile is used with this authorization.

default-eps-bearer

Sets the action QoS authorization of the Default EPS bearer in an EPS access network through a pre-configured QoS profile name *qos_prof_name* which is to use for the authorization at different level in an PCC-Service instance.

This keyword is applicable only to EPS access type. QoS Class Identifier (QCI) and Allocation and Retention Priority (ARP) values of the QoS profile is used with this authorization.

qci *qci_value*

Sets the action QoS authorization per QCI in case of PCEF binding through a pre-configured QoS profile name *qos_prof_name* which is to use for the authorization at different level in an PCC-Service instance.

qci_value must be an integer value between 1 through 255.

Important This keyword is applicable only in case of PCEF binding. QCI defined in QoS profile is not used when this keyword is active, so this keyword is repeated per QCI that has to be authorized by IPCF. For each QCI authorization Maximum Bit Rate Upload/Download (MBR DL/MBR UL) or Guaranteed Bit Rate Upload/Download (GBR DL/MBR UL) and ARP values of the QoS profile is used with this authorization.

qos-profile *qos_prof_name*

This keyword associate the action configured for authorization with a pre-configured PCC-QoS-Profile named *qos_prof_name* and uses configured values from specific PCC-QoS-Profile during authorization.

qos_prof_name specifies the pre-configured QoS profile name which is to use for the authorization at different level in an PCC-Service instance.

Usage Guidelines Use this command to define an action for the authorization parameters in PCC-QoS-Profile which is to be used under PCC-Action-Set configuration instance for PCC-Service configuration.

Example

Following command sets the action for QoS authorization for APN MBR with PCC-QoS-Profile *apn_qos_prof1* under PCC-Action-Set configuration instance for PCC-Service configuration.

```
authorize apn-mbr qos-profile apn_qos_prof1
```

dissociate monitoring-key

This command dissociates a Monitoring Key id with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

```
[no] dissociate monitoring-key mon_key_id usage-monitor usage_mon_name
```

no

Removes the dissociated Monitoring Key id configuration from a PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id

Specifies the Monitoring Key identifier to be dissociated with PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id must be an integer between 1 through 65535.

usage-monitor *usage_mon_name*

Specifies the PCC-Usage-Monitor need to be dissociated with Monitoring Key *mon_key_id* under PCC-Action-Set configuration instance for PCC-Service configuration.

usage_mon_name is a pre-configured PCC-Usage-Monitor instance in PCC-Service Profile Configuration for PCC-Service configuration.

Usage Guidelines

Use this command to dissociate a Monitoring Key with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

There is a Many-To-Many relationship between Usage-Monitor and Monitoring-Key. Operator can change this relationship using required commands.

When usage is reported to IPCF for a particular Monitoring Key, the usage is added to all the Usage Monitoring to which the Monitoring Key is associated.

Operator can reassociate the relationship between Monitoring Key and Usage Monitor by **associate monitoring-key** command.

Example

The following command dissociates a associated pair of Monitoring Key id *102* and PCC-Usage-Monitor named *usage_mon1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
dissociate monitoring-key 102 usage-monitor usage_mon1
```

dynamic-rule-install

This command sets an action to install a PCC Dynamic rule for the specified PCC-Data-service in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

[no] dynamic-rule-install data-service *data_svc_name* [**qos-profile** *qos_prof_name*] [**precedence** *preced_value*] [**monitoring-key** *mon_key_id* [**rating-group** *rating_grp_id*] [**gate-status** {**disabled** | **enabled** | **enabled-downlink** | **enabled-uplink**}] [**defer-by interval** *delayed_dur*] [**metering-method** {**both-duration-volume** | **duration** | **volume**}] [**reporting-level** {**service-identifier-level** | **rating-group-level**}] [**failure-policy** { **continue** | **terminate**}]

no

Removes the Dynamic Rule install action configured for specific PCC-Data-Service from a PCC-Action-Set configuration instance for PCC-Service configuration.

data-service *data_svc_name*

Specifies the name of the pre-configured PCC-Data-Service for which Dynamic Rules to be installed under PCC-Action-Set configuration instance for PCC-Service configuration.

data_svc_name is a pre-configured PCC-Data-Service instance in PCC-Service Configuration mode.

metering-method {both-duration-volume | duration | volume}

Specifies the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-service instance on IPCF node.

- **both-duration-volume** sets the metering method as based on volume of data usage and duration of session, both for offline charging in a PCC-Data-service instance on IPCF node.
- **duration** sets the metering method as based on duration of session usage for offline charging in a PCC-Data-service instance on IPCF node.
- **volume** sets the metering method as based on the volume of data usage for offline charging in a PCC-Data-service instance on IPCF node.

If no metering method is defined, the reporting level preconfigured at PCEF is considered.

monitoring-key *mon_key_id*

Specifies the pre-defined Monitoring Key identifier which is to be used in Dynamic Rule for specific PCC-Data-service under PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id is a pre-defined Monitoring Key identifier in PCC-Service Configuration mode.

precedence *preced_value*

Specifies the precedence value for the Dynamic Rule for specific PCC-Data-service under PCC-Action-Set configuration instance for PCC-Service configuration.

preced_value must be an integer between 1 through 65535.

qos-profile *qos_prof_name*

Specifies the name of the pre-configured PCC-QoS-Profile which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.

qos_prof_name is a pre-configured PCC-QoS-Profile instance in PCC-Service Configuration mode.

rating-group *rating_grp_id*

Specifies the pre-defined Rating Group identifier which is to be used in Dynamic Rule for specific PCC-Data-service under PCC-Action-Set configuration instance for PCC-Service configuration.

rating_grp_id is a pre-defined Rating Group identifier in PCC-Service Configuration mode.

reporting-level {service-identifier-level | rating-group-level

Specifies the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-service instance on IPCF node.

- **service-identifier-level** sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the Service Identifier level which is configured in a PCC-Data-service instance on IPCF node.
- **rating-group-level** sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the Rating Group level which is configured in a PCC-Data-service instance on IPCF node.

If no reporting level is defined, the reporting level preconfigured at PCEF is considered.

gate-status {disabled | enabled | enabled-downlink | enabled-uplink}

Default: Enabled

Sets the Gate-status which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.

disabled: disables the Gate status in downlink and uplink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.

enabled: Enables the Gate status in downlink and uplink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration. This is the default status of Gate.

enabled-downlink: Enables the Gate status in downlink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.

enabled-uplink: Enables the Gate status in uplink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for dynamic rule installation.

delayed_dur configures the relative delay time by which the corresponding dynamic rule installation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.

delayed_dur specifies the delayed interval in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- *SS* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

failure-policy { continue | terminate}

Default: Continue

This optional keyword configures the rule failure policy action when failure occurs on PCEF for PCC rules.

- **Continue**: If this option enabled, the IPCF continues even if PCEF reports rule failure through charging rule report. This is the default action.
- **Terminate**: If this option enabled, the IPCF triggers PCC session termination on receiving rule failure through charging rule report.

Usage Guidelines

Use this command to set an action to install a PCC Dynamic rule for the specified PCC-Data-Service in PCC-Action-Set configuration for PCC-Service instance

Operator can override parameters such as, QoS profile, Precedence, Gate-status, Monitoring Key and PCC-Rating-id.

The same command is used to modify already installed PCC Dynamic-rule for the PCC-Data-Service by overriding required parameters only.

Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding dynamic rule installation is deferred.

IPCF handles operation of PCC Rule and activate/deactivate/install/modify/remove the PCC rules at PCEF through this configuration. PCC rule operation may fail on PCEF due to various reasons. In such failure cases PCEF sends back a Charging Rule Report containing name of the failed PCC rule and corresponding failure cause.

The IPCF handles these charging rule report and take appropriate actions based on configuration done through **failure-policy** keyword.

Charging Rule Report comes through CCA or RAA messages in a call flow used for handling the charging-rule-report.

IPCF supports following charging rule failure codes in report:

- Out-of-credit
- Reallocation-of-credit
- Unknown rule name
- Invalid Rating Group
- Invalid Service Identifier
- GW/PCEF Malfunction
- Limited Resources
- Max No. of Bearers Reached
- Unknown Bearer Id
- Missing Bearer Id
- Missing Flow Description
- Resource Allocation Failure

- QoS Validation Failure

Charging rule status can any one of the following in this scenario:

- Active
- Inactive
- Temporarily Inactive

A charging rule report can occur in CCR message multiple times and maximum of 16 charging rule reports per CCR message is supported by IPCF.

Example

The following command sets the action for PCC-Data-Service named *temp_data1* for Dynamic Rule install with PCC-QoS-Profile named *temp_qos1* having precedence *22* and Gate-status as **Enabled** under PCC-Action-Set configuration instance for PCC-Service configuration:

dynamic-rule-install data-service *temp_data1* **qos-profile** *temp_qos1* **precedence** *22*

dynamic-rule-uninstall

This command sets an action to uninstall a Dynamic Rule for the specified PCC-Data-Service in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

[no] dynamic-rule-uninstall data-service *data_svc_name* **[defer-by interval** *delayed_dur*]

no

Removes the Dynamic Rule Uninstall action configured for specific PCC-Data-Service from a PCC-Action-Set configuration instance for PCC-Service configuration.

data-service *data_svc_name*

Specifies the name of the pre-configured PCC-Data-Service for which Dynamic Rules to be uninstalled under PCC-Action-Set configuration instance for PCC-Service configuration.

data_svc_name is a pre-configured PCC-Data-Service instance in PCC-Service Configuration mode.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for dynamic rule removal.

delayed_dur configures the relative delay time by which the corresponding dynamic rule uninstallation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.

delayed_dur specifies the delayed interval in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- *SS* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage Guidelines

Use this command to set an action to uninstall a PCC Dynamic rule for the specified PCC-Data-Service in PCC-Action-Set configuration for PCC-Service instance

Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding dynamic rule uninstallation is deferred.

Example

The following command sets the action of Dynamic Rule uninstall for PCC-Data-Service named *temp_data1* under PCC-Action-Set configuration instance for PCC-Service configuration:

dynamic-rule-uninstall data-service *temp_data1*

log-event

This command allows operator to specify a string to be logged at Subscriber Service Controller (SSC) when the corresponding action set is triggered under PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pcc-action-set)#`

Syntax Description

[no] log-event msg-text *message_string*

no

Removes the notification message configured for specific action under a PCC-Action-Set configuration instance for PCC-Service configuration.

msg-text *message_string*

Specifies the message notification text string to be logged at the SSC when a particular PCC-Action-Set triggered for PCC-Service instance.

message_string is a string of alphanumerical characters of 1 through 255 characters

Usage Guidelines

Use this command to allow operator to specify a string to be logged at Subscriber Service Controller (SSC) when the corresponding action set is triggered under PCC-Action-Set configuration for PCC-Service instance.

Example

The following command sets the notification message for an action under PCC-Action-Set configuration instance for PCC-Service configuration:

```
log-event msg-text "This Action is Applicable for EPS Session Only."
```

notify-user

This command allows operator to specify a string template-id at SSC under PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

```
[no] notify-user message-id message_id [parameter value_pair]
```

no

Removes the user notification message id configured for specific action under a PCC-Action-Set configuration instance for PCC-Service configuration.

message-id *message_id*

Specifies the message template id stored at SSC to be used for user notification for action under PCC-Action-Set configuration for PCC-Service instance.

message_id is a string of alphanumerical characters of 1 through 255 characters

parameter *value_pair*

Specifies the parameters in the form of name value pairs separated by comma. A maximum of 16 name value pairs can be defined for action under PCC-Action-Set configuration for PCC-Service instance.

The name value pairs is encoded into **xml** data like other parameters and sent out to SSC for user notification.

value_pair is a string of alphanumerical characters of 1 through 255 characters which can accommodate up to 16 name value pair separated by comma (,).

Usage Guidelines

Use this command to allow operator to specify a string template-id under PCC-Action-Set configuration for PCC-Service instance.

The template description exists at SSC and when the corresponding action set is hit, the subscriber is notified with the specified template configured via this command.

The action set makes a XML remote procedure call towards SSC. The XML contains information like IMSI, template-id of the SMS/E-mail template and other details like MSISDN, NAI if available. To give more flexibility to the operator, now the this command accepts name value pairs, which are also sent along with the said data.

Example

The following command sets the message id *"Invalid User."* for user notification message to an action under PCC-Action-Set configuration instance for PCC-Service configuration:

```
notify-user message-id "Invalid User."
```

offline-charging-server

This command sets the action to change the offline charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

```
[no] offline-charging-server primary pri_serv_address [secondary sec_serv_address]
```

no

Removes the action set to change the offline charging server under PCC-Action-Set configuration instance for PCC-Service configuration.

primary *pri_serv_address*

Identifies the name of the primary offline charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration.

The *pri_serv_address* must be the address of an offline charging server in Diameter URI format (*FQDN* [*port*] [*transport*] [*protocol*]).

secondary *sec_serv_address*

Identifies the name of the secondary offline charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration.

The *sec_serv_address* must be the address of an offline charging server in Diameter URI format (*FQDN* [*port*] [*transport*] [*protocol*]).

Usage Guidelines

Use this command to set an action to change the offline charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

Example

Following command configures an action change the offline charging server to primary server *aaa://host.abc.com:6666;transport=tcp;protocol=diameter* and secondary server *aaa://host.xyz.com:6666;transport=sctp;protocol=radius* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
offline-charging-server primary
aaa://host.abc.com:6666;transport=tcp;protocol=diameter secondary
aaa://host.xyz.com:6666;transport=sctp;protocol=radius
```

online-charging-server

This command sets the action to change the online charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

```
[no] online-charging-server primary pri_serv_address [secondary sec_serv_address]
```

no

Removes the action set to change the online charging server under PCC-Action-Set configuration instance for PCC-Service configuration.

primary *pri_serv_address*

Identifies the name of the primary online charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration.

The *pri_serv_address* must be the address of an online charging server in Diameter URI format (*FQDN* [*port*] [*transport*] [*protocol*]).

secondary *sec_serv_address*

Identifies the name of the secondary online charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration.

The *sec_serv_address* must be the address of an online charging server in Diameter URI format (*FQDN* [*port*] [*transport*] [*protocol*]).

Usage Guidelines

Use this command to set an action to change the online charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

Example

Following command configures an action change the online charging server to primary server *aaa://host.abc.com:6666;transport=tcp;protocol=diameter* and secondary server *aaa://host.xyz.com:6666;transport=sctp;protocol=radius* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
online-charging-server primary aaa://host.abc.com:6666;transport=tcp;protocol=diameter
 secondary aaa://host.xyz.com:6666;transport=sctp;protocol=radius
```

request-usage-report monitoring-key

This command configures the action to allow operator to explicitly request usage report for the specified Monitoring Key or all Monitoring Keys under PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

```
[no] request-usage-report monitoring-key {mon_key_id | any}
```

no

Removes the usage request action configuration for Monitoring Key id from a PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id

Specifies the Monitoring Key identifier for which usage report action is to be set under PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id must be an integer between 1 through 65535.

any

Specifies the Monitoring Key identifier to "ANY" value for which usage report action is to be set under PCC-Action-Set configuration instance for PCC-Service configuration.

Usage Guidelines

Use this command to configure the action to allow operator to explicitly request usage report for the specified Monitoring Key or all Monitoring Keys under PCC-Action-Set configuration for PCC-Service instance.

Example

The following command sets an action to request the usage report for Monitoring Key id *102* under PCC-Action-Set configuration instance for PCC-Service configuration:

request-usage-report monitoring-key *102*

rule-activate

This command sets an action to activate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-pcc-action-set)#

Syntax Description

[**no**] **rule-activate** *rule_name*[**defer-by interval** *delayed_dur*]

no

Removes the action to activate a pre-configured Rule from a PCC-Action-Set configuration instance for PCC-Service configuration.

rule_name

Specifies the name of the pre-configured Rule on PCEF for an activation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.

rule_name is a pre-configured Rule in PCEF.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for rule activation.

delayed_dur configures the relative delay time by which the corresponding rule activation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.

delayed_dur specifies the delayed interval in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- *SS* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage Guidelines

Use this command to set an action to activate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.

Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding rule activation is deferred.

Example

The following command sets an action to activate for Rule *rule1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
rule-activate rule1
```

rule-deactivate

This command sets an action to deactivate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

```
[no] rule-deactivate rule_name [defer-by interval delayed_dur]
```

no

Removes the action to deactivate a pre-configured Rule from a PCC-Action-Set configuration instance for PCC-Service configuration.

rule_name

Specifies the name of the pre-configured Rule on PCEF for a deactivation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.

rule_name is a pre-configured Rule in PCEF.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for rule deactivation.

delayed_dur configures the relative delay time by which the corresponding rule deactivation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.

delayed_dur specifies the delayed interval in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- *SS* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage Guidelines

Use this command to set an action to deactivate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.

Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding rule deactivation is deferred.

Example

The following command sets an action to deactivate for Rule *rule1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
rule-deactivate rule1
```

rulebase-activate

This command sets an action to activate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

`[no] rulebase-activate rulebase_name [defer-by interval delayed_dur]`

no

Removes the action to activate a pre-configured Rulebase from a PCC-Action-Set configuration instance for PCC-Service configuration.

rulebase_name

Specifies the name of the pre-configured Rulebase on PCEF for an activation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.

rulebase_name is a pre-configured Rulebase in PCEF.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for Rulebase activation.

delayed_dur configures the relative delay time by which the corresponding Rulebase activation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.

delayed_dur specifies the delayed interval in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- *SS* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage Guidelines

Use this command to set an action to activate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.

Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding Rulebase activation is deferred.

Example

The following command sets an action to activate for Rulebase *rulebase1* under PCC-Action-Set configuration instance for PCC-Service configuration:

`rulebase-activate rulebase1`

rulebase-deactivate

This command sets an action to deactivate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

[no] rulebase-deactivate *rulebase_name* **[defer-by interval** *delayed_dur*]

no

Removes the action to deactivate a pre-configured Rulebase from a PCC-Action-Set configuration instance for PCC-Service configuration.

rulebase_name

Specifies the name of the pre-configured Rulebase on PCEF for a deactivation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.

rule_name is a pre-configured Rulebase in PCEF.

defer-by interval *delayed_dur*

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for Rulebase deactivation.

delayed_dur configures the relative delay time by which the corresponding Rulebase deactivation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.

delayed_dur specifies the delayed interval in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *delayed_dur*:

- *HH* specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- *MIN* specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- *SS* specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage Guidelines

Use this command to set an action to deactivate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.

Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding Rulebase deactivation is deferred.

Example

The following command sets an action to deactivate for Rulebase *rulebase1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
rulebase-deactivate rulebase1
```

service-tag

This command sets an action to activate/deactivate a pre-configured Service Tag rule in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

[no] service-tag *svc_tag* {**activate-rule** | **activate-rule**}

no

Removes the action to activate/deactivate a pre-configured Service Tag rule in PCC-Action-Set configuration for PCC-Service instance.

svc_tag

Specifies the name of the pre-configured Service Tag rule for an activation/deactivation is set under PCC-Action-Set configuration instance for PCC-Service configuration.

svc_tag is a pre-configured Service Tag name.

activate-rule

Specifies that action to be set for Service Tag activation rule under PCC-Action-Set configuration instance for PCC-Service configuration.

deactivate-rule

Specifies that action to be set for Service Tag deactivation rule under PCC-Action-Set configuration instance for PCC-Service configuration.

Usage Guidelines

Use this command to set an action to activate/deactivate a pre-configured Service Tag rule in PCC-Action-Set configuration for PCC-Service instance.

Example

The following command sets the an activation rule for Service Tag named *service_1* under PCC-Action-Set configuration instance for PCC-Service configuration:

service-tag *service_1* **activate-rule**

terminate-session

This command sets an action to terminate a Bearer based on **bearer-id** or unique combination of QCI and ARP received through current CCR message in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

```
[no] terminate-session
```

no

Removes the action to terminate a Bearer based on **bearer-id** from a PCC-Action-Set configuration instance for PCC-Service configuration.

Usage Guidelines

Use this command to set an action to terminate a Bearer based on **bearer-id** or unique combination of QCI and ARP received through current CCR message in PCC-Action-Set configuration for PCC-Service instance.

Termination of Bearer is possible only in case of PCRF binding and limited to Dynamic rules.

Important This action is only applicable to IP-CAN sessions with access type as GPRS. When terminate Bearer is initiated, IPCF triggers **Bearer Termination Procedure** for the **bearer-id** received through current CCR message.

Caution This command triggers termination of **Gx** and SPR sub session active under PCC-Service instance.

Example

The following command sets an action to terminate a Bearer based on **bearer-id** received through current CCR message under PCC-Action-Set configuration instance for PCC-Service configuration:

```
terminate-session
```

usage-monitor

This command sets an action to allow operator to stop, reset or start the counting for a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context *context_name* **> pcc-service** *service_name* **> action-set** *action_set_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

Syntax Description

[no] usage-monitor *usage_mon_name* {**reset-counter** | **start-counter** | **stop-counter**}

no

Removes the action to allow operator to stop, reset or start the counting for a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

usage_mon_name

Specifies the name of the pre-configured PCC-Usage-Monitor for which counter action is configured under PCC-Action-Set configuration instance for PCC-Service configuration.

usage_mon_name is a pre-configured PCC-Usage-Monitor.

reset-counter

Resets the usage counts for PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

start-counter

Starts the accumulation of usage counts for PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

stop-counter

Stops the accumulation of usage counts for PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

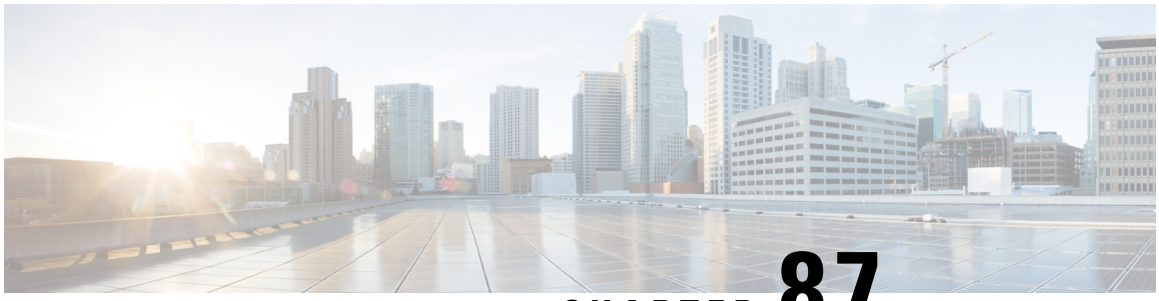
Usage Guidelines

Use this command to set an action to allow operator to stop, reset or start the counting for a usage monitor in PCC-Action-Set configuration for PCC-Service instance.

Example

The following command sets the an action to stop the accumulation of usage counts for PCC-Usage-Monitor named *usage_1* under PCC-Action-Set configuration instance for PCC-Service configuration:

usage-monitor *usage_1* **stop-counter**



CHAPTER 87

PCC-AF-Service Configuration Mode Commands

An Application Function (AF) provides Application (layer 7) proxies for client server applications. It also provides enforcement of operator and subscriber QoS, Charging, and Security policies to subscriber session and represents the network element that supports applications that require dynamic policy and/or charging control. In the IMS model, the AF is implemented by the Proxy Call Session Control Function (P-CSCF).

Important This configuration mode is supported from StarOS Release 12.1 onward.

Command Modes

The PCC-AF-Service Configuration mode provides a mechanism to IPCF to manage the external interfaces required for media and application function management. The PCC-AF-Service manages **Rx** interface which would be based on the dictionary used.

Exec > Global Configuration > Context Configuration > PCC AF Service Configuration

configure > context *context_name* **> pcc-af-service** *service_name*

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

associate pcc-service

This command is used to associate a pre-configured PCC-Service with a PCC-AF-Service for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC AF Service Configuration

configure > **context** *context_name* > **pcc-af-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
associate pcc-service pcc_svc_name
[no] associate pcc-service
```

no

Removes/disassociate the configured PCC-service from this PCC-AF-Service instance configured for IPCF configuration.

pcc_svc_name

Specifies the name of a pre-configured PCC-service configured in Context Configuration mode for IPCF configuration.

The *pcc_svc_name* is name of a predefined PCC-Service instance and must be an alphanumerical string from 1 through 63 characters.

Usage Guidelines

Use this command to associate a pre-configured PCC-Service instance for IPCF configuration.

Important For more information on PCC-Service configuration, refer *PCC-Service Configuration Mode Commands*.

Example

Following command binds a PCC-Service named *pcc_svc1* with in a PCC-AF-Service.

```
associate pcc-service pcc_svc1
```

Following command removes an associated PCC-Service named *pcc_svc1* from a PCC-AF-Service.

```
no associate pcc-service pcc_svc1
```

diameter dictionary

This command is used to assign a Diameter dictionary for **Rx** messaging with a PCC-AF-Service for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC AF Service Configuration

configure > context *context_name* **> pcc-af-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
diameter dictionary {r8-standard | standard}
default diameter dictionary
```

default

Sets the Diameter **Rx** dictionary to default dictionary **r8-standard** (3GPP Rel. 8 standard) for a PCC-AF-Service instance configured for IPCF configuration.

r8-standard

Default: Enabled

Sets the Diameter **Rx** dictionary to be used by a PCC-AF-Service instance configured for IPCF configuration over **Rx** interface to 3GPP Rel. 8 standard.

standard

Default: Disabled

Sets the Diameter **Rx** dictionary to be used by a PCC-AF-Service instance configured for IPCF configuration over **Rx** interface to 3GPP Rel. 7 standard.

Usage Guidelines

Use this command to configure the PCC-AF-Service to determine which of the 3GPP dictionary to be used for **Rx** interface messaging for media and application function management.

Example

Following command sets the PCC-AF-Service to use 3GPP Rel. 8 standard dictionary for **Rx** interface and application function management related messaging in a PCC-AF-Service.

```
default diameter dictionary
```

diameter origin end-point

This command is used to bind/associate a pre-configured Diameter host/realm (AF) over **Rx** interface with a PCC-AF-Service to be used for subscriber service control and AF profile management.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC AF Service Configuration

configure > context *context_name* **> pcc-af-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter origin endpoint *dia_endpoint_name*
no diameter origin endpoint

no

Removes the associated Diameter Origin Endpoint configuration from PCC-AF-Service instance configured for IPCF configuration.

any

Sets the PCC-AF-Service instance to use any available AF node over **Rx** interface for AF support.

dia_endpoint_name

The *dia_endpoint_name* is a predefined Diameter origin endpoint node and must be an alphanumerical string from 1 through 63 characters.

Usage Guidelines

Use this command to bind the AF node over **Rx** interface by associating a pre-configured Diameter Origin Endpoint with a PCC-AF-Service.

The Diameter origin endpoint must be a pre-configured instance in the Context Configuration Mode. For more information on Diameter origin endpoint configuration, refer *Diameter Endpoint Configuration Mode Commands* chapter.

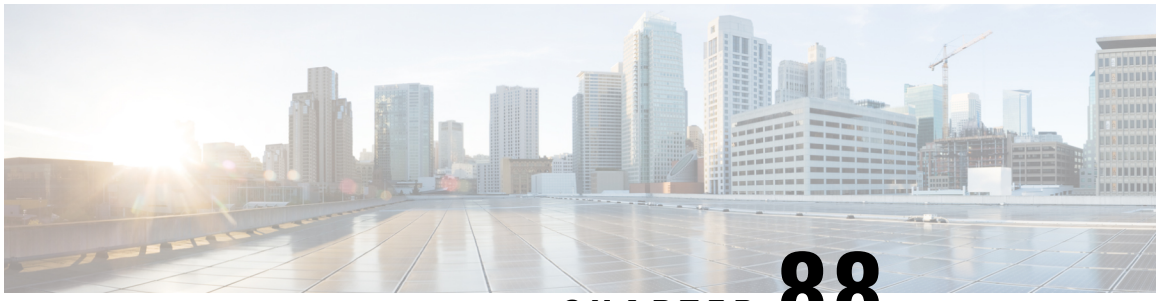
Example

Following command associates a pre-configured Diameter endpoint node configuration named *af_pcscf1* with a PCC-AF-Service for AF profile management.

diameter origin endpoint *af_pcscf1*

Following command removes the pre-associated Diameter endpoint node configuration named *af_pcscf1* with a PCC-AF-Service.

no diameter origin endpoint



CHAPTER 88

PCC-Condition-Group Configuration Mode Commands

Important This configuration mode is supported from StarOS Release 12.1 onward.

Command Modes

The PCC-Condition-Group Configuration Mode is used to configure the various rating parameters under a logical identifier name in the PCC-Service. A PCC-Condition-Group is a collection of conditions that identify a network or state constraint represented as a logical expression. A maximum of 128 conditions can be configured in one PCC-Condition-Group.

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

af-application-id

This command defines a condition based on the application id of an Application Function service through the **Rx** interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] af-application-id operator value af_app_id
[ no ] af-application-id operator profile-attribute spr_attr_value
[ no ] af-application-id operator subscription-attribute subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the AF-Application id.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

af_app_id

Specifies the identity string for AF-Application identifier over **Rx** interface.

af_app_id must be an alphanumeric string of 1 to 256 characters.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with application id of an Application Function service condition validation in an IP-CAN session.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with application id of an Application Function service condition validation in an IP-CAN session.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the application id of an Application Function service through the **Rx** interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the AF Application id is not equal to *pcc_af_1*:

```
af-application-id != pcc_af_1
```

af-media-codec

This command defines a condition based on the media Codec used by AF application in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] af-media-coded operator value {g722 | g726 | ilbc | pcma | pcmu}
[ no ] af-media-coded operator profile-attribute spr_attr_value
[ no ] af-media-coded operator subscription-attribute subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the AF-media Codec.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

g722

Specifies the media Codec as G.722 used for user traffic from AF server over **Rx** interface.

G.722 is a ITU-T standard 7 kHz wideband speech codec operating at 48, 56 and 64 kbit/s.

g726

Specifies the media codec as G.726 used for user traffic from AF server over **Rx** interface.

G.726 is an ITU-T ADPCM speech codec standard covering the transmission of voice at rates of 16, 24, 32, and 40 kbit/s.

ilbc

Specifies the media codec as Internet Low Bitrate Codec (iLBC) used for user traffic from AF server over **Rx** interface.

iLBC is a narrowband speech codec suitable for VoIP applications, streaming audio, archival and messaging. The encoded blocks encapsulated in Real-time Transport Protocol (RTP) protocol for transport.

pcma

Specifies the media codec as Pulse Code Modulation A-law scaling (PCMA) used for user traffic from AF server over **Rx** interface.

PCMA is an ITU-T Recommendation G.711 audio data encoding in eight bits per sample, after A-law logarithmic scaling.

pcmu

Specifies the media codec as Pulse Code Modulation mu-law scaling (PCMU) used for user traffic from AF server over **Rx** interface.

PCMU is an ITU-T Recommendation G.711 audio data encoding in eight bits per sample, after mu-law logarithmic scaling.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with application media codec of an Application Function service condition validation in an IP-CAN session.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with application media codec of an Application Function service condition validation in an IP-CAN session.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the media codecs used by AF service through the **Rx** interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the AF Media codec is equal to PCMA:

```
af-media-codec = pcma
```

af-media-type

This command defines a condition based on the media type used by AF application in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] af-media-type operator value {application | audio | control | data |
message | other | text | video}
[ no ] af-media-type operator profile-attribute spr_attr_value
[ no ] af-media-type operator subscription-attribute subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the media type in user traffic.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

application

Specifies the media type as Application in user traffic from AF server over **Rx** interface.

audio

Specifies the media type as Audio in user traffic from AF server over **Rx** interface.

control

Specifies the media type as Control in user traffic from AF server over **Rx** interface.

data

Specifies the media type as Data in user traffic from AF server over **Rx** interface.

message

Specifies the media type as Message in user traffic from AF server over **Rx** interface.

text

Specifies the media type as Text in user traffic from AF server over **Rx** interface.

video

Specifies the media type as Video in user traffic from AF server over **Rx** interface.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with application media type of an Application Function service condition validation in an IP-CAN session.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with application media type of an Application Function service condition validation in an IP-CAN session.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines Use this command to define a condition based on the media type used by AF service through the **Rx** interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the AF Media type is equal to Video:

```
af-media-type = video
```

af-service-urn

This command defines a condition based on the service Uniform Resource Names (URNs) used by AF application in an IP-CAN session.

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] af-service-urn operator value urn_string
[ no ] af-service-urn operator profile-attribute spr_attr_value
[ no ] af-service-urn operator subscription-attribute subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

urn_string

Specifies the URN in user traffic from AF server over **Rx** interface.

urn_string must be an alphanumeric string of 1 through 256 characters.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with URN used by AF service condition validation in an IP-CAN session.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with URN used by AF service condition validation in an IP-CAN session.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the URN used by AF service through the **Rx** interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Uniform Resource Names (URNs) serves as persistent, location-independent resource identifiers and are designed to make it easy to map other namespaces into URN-space.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the AF service URN is equal to *ietf:rfc:4003*:

```
af-service-urn = ietf:rfc:4003
```

an-gw-address

This command defines a condition based on the IP address of Access Node Gateway (AN-GW) on which subscriber is attached in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] an-gw-address {operator value angw_ip/mask | {in-range | !in-range}
range_start_ip to range_end_ip}
[ no ] an-gw-address operator profile-attribute spr_attr_value
[ no ] an-gw-address operator subscription-attribute subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

in-range

Specifies the condition to accept the IP address which are in range as argument to define the Access Node Gateway address which is used by subscriber in IP-CAN session.

!in-range

Specifies the condition to accept the IP address which are NOT in range as argument to define the Access Node Gateway address which is used by subscriber in IP-CAN session.

range_start_ip

Specifies the starting IP address which is used for defining the range of AN-GW IP addresses which is used by subscriber in IP-CAN session.

range_start_ip is an IP address and must be lesser than *end_start_ip* address.

range_end_ip

Specifies the ending IP address which is used for defining the range of AN-GW IP addresses which is used by subscriber in IP-CAN session.

range_end_ip is an IP address and must be greater than *end_start_ip* address.

angw_ip/mask

Specifies the IP address of the Access Node Gateway which is used by subscriber in IP-CAN session along with IP mask as well.

angw_ip must be an IP address in IPv4 or IPv6 notation.

mask Specifies the IP address mask bits to determine the number of IP addresses of AN-GW in condition. *mask* must be specified using the standard IPv4 dotted decimal notation.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with AN gateway IP address condition validation in an IP-CAN session.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with AN gateway IP address condition validation in an IP-CAN session.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the AN-GW IP address used by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on AN-GW IP address *209.165.200.228* in an IP-CAN session:

an-gw-address = *209.165.200.228*

authorized-qci

This command defines a condition based on the authorized QoS Class Identifier used in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pcc-condition-group)#`

Syntax Description

[no] authorized-qci *operator* **value** *qci*
[no] authorized-qci *operator* **profile-attribute** *spr_attr_value*
[no] authorized-qci *operator* **subscription-attribute** *subs_prof_attr_value*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

qci

Specifies the authorized QoS class identifier in user traffic for condition validation.

qci must be an integer between 1 through 255.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with authorized QoS class identifier condition validation in an IP-CAN session.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with authorized QoS class identifier condition validation in an IP-CAN session.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the authorized QCI used by the subscriber in an IP-CAN session.

The condition evaluates to TRUE, if Bearer Control Mode is UE and network (PCEF bearer binding) and IPCF has authorized the specified QCI earlier.

QCI is a number which describes the error rate and delay that are associated with the service. It includes bearer parameters including scheduling weights and queue management thresholds.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the authorized QCI is greater than or equal to *4*:

```
authorized-qci >= 4
```

base-station-id

This command defines a condition based on the various parameters used in base-station id by subscriber in an IP-CAN session between PCEF (PDSN) and IPCF over **Gx** interface.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

[no] base-station-id {[**sid** *operator sys_identifier*] | **range** *start_range* **to** *end_range*]] [**nid** *operator netwrk_identifier*] | **range** *start_range* **to** *end_range*]] [**cellid** *operator cell_identifier*] | **range** *start_range* **to** *end_range*]]}

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- <: Lesser than
- <=: Lesser than or equals
- =: Equals
- >: Greater than
- >=: Greater than or equals

sid *operator sys_identifier*

Specifies the system identifier in base-station id of subscriber for condition validation in an IP-CAN session.

sys_identifier must be an integer between 0 through 65535.

nid *operator netwrk_identifier*

Specifies the network identifier in base-station id, which is used by subscriber, for condition validation in an IP-CAN session.

netwrk_identifier must be an integer between 0 through 65535.

cellid *operator cell_identifier*

Specifies the cell identifier in base-station id, which is used by subscriber, for condition validation in an IP-CAN session.

cell_identifier must be an integer between 0 through 65535.

range *start_range* to *end_range*

This optional keyword specifies range of the identifiers (SID, Cell id, Network Id) to be used for condition validation in an IP-CAN session.

start_range is the start value of range having integer between 0 through 65535 and it must be lesser than *end_range*.

end_range is the end value of range having integer between 0 through 65535 and it must be greater than *start_range*.

Usage Guidelines

User this command to define a condition based on the parameters used in base-station id of subscriber, which is composition of SID, Cell Id, and/or Network Id, in an IP-CAN session between PCEF (PDSN) and IPCF over **Gx** interface.

This condition is defined for PCC functionality support to CDMA users over **Gx** interface.

Example

The following command creates a condition definition to analyze the condition based on base-station id of subscriber where SID is *1001* and cell id is in range of *2001* to *2069* in an IP-CAN session between PDSN and IPCF having network id as *3989*:

```
base-station-id sid = 1001 nid = 3989 cellid = range 2001 to 2069
```

bearer-count

This command defines a condition based on the number of bearers allowed in a subscriber session on IPCF to accept bearer-count in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] bearer-count operator value num_bearer
[ no ] bearer-count operator profile-attribute spr_attr_value
[ no ] bearer-count operator subscription-attribute subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

num_bearer

Specifies the number of bearers in user traffic for condition validation.

num_bearer indicates a condition based on the number of bearer established in a IP-CAN session and must be an integer between 1 through 11.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with number of bearers allowed for a subscriber in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with number of bearers allowed for a subscriber in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the number of bearers allowed for a subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for bearers allowed in a subscriber session is equal to *4*:

```
bearer-count = 4
```

connectivity-access-network

This command defines a condition based on the access network type used by subscriber in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] connectivity-access-network operator value {3gpp-gprs | 3gpp2 |
3gpp2-eps | docsis | non-3gpp-eps | wimax | xdsl }
[ no ] connectivity-access-network operator profile-attribute spr_attr_value
[ no ] connectivity-access-network operator subscription-attribute
subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the media type in user traffic.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

3gpp-gprs

Specifies the network access connectivity type as 3GPP-GPRS for user traffic in condition definition.

3gpp2

Specifies the network access connectivity type as 3GPP2 (CDMA) for user traffic in condition definition.

3gpp2-eps

Specifies the network access connectivity type as 3GPP2-EPS for user traffic in condition definition.

docsis

Specifies the network access connectivity type as Data Over Cable Service Interface Specification (DOCSIS) for user traffic in condition definition.

non-3gpp-eps

Specifies the network access connectivity type as non-3GPP-EPS to connect with Gxa based HSGW for user traffic in condition definition.

wimax

Specifies the network access connectivity type as Wi-MAX for user traffic in condition definition.

xdsl

Specifies the network access connectivity type as xDSL (ADSL/SDSL) or user traffic in condition definition.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with type of connectivity used for network access by subscriber in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with type of connectivity used for network access by subscriber in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the type of connectivity used for network access by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the network type is equal to Wi-MAX:

```
connectivity-access-network = wimax
```

eval-condition-group

This command defines a condition based on the TRUE or FALSE setting of a configured PCC-Condition-Group for subscriber in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[no] eval-condition-group cond_grp_name operator {FALSE | TRUE}
```

no

Removes the specified condition definition.

cond_grp_name

Specifies the name of the configured PCC-Condition-Group which is used for evaluation with in this PCC-Condition-Group for user traffic.

cond_grp_name must be a pre-configured PCC-Condition-Group in this configuration mode.

operator

Specifies how to logically match the media type in user traffic.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

FALSE

Sets the evaluation condition for specified PCC-Condition-Group to FALSE.

With this keyword system rejects all conditions defined in specific PCC-Condition-Group and match the same in user traffic.

TRUE

Sets the evaluation condition for specified PCC-Condition-Group to TRUE.

With this keyword system accepts all conditions defined in specific PCC-Condition-Group and match the same in user traffic.

Usage Guidelines

Use this command to define a condition based on the acceptance or rejection of specific pre-configured PCC-Condition-Group for user traffic in an IP-CAN session.

This command allows the operator to use configured PCC-Condition-Group in another PCC-Condition-Group as subset of PCC-Condition-Group.

Important A maximum of 3 level of recursion depth is allowed for PCC-Condition-Group evaluation in a PCC-Condition-Group.

Example

The following command creates a condition definition to accept the all conditions defined in PCC-Condition-Group named *af_1*:

```
eval-condition-group af_1 = TRUE
```

event-time

This command defines a condition based on the event-trigger time as per the time specified by the named Time definition (Timedef) configured for subscriber session in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[no] event-time operator timedef_name
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **<=**: Lesser than or equals
- **=**: Equals
- **>=**: Greater than or equals

timedef_name

Specifies the name of the configured time definition (start and end timer of session) which is used for evaluation with this PCC-Condition-Group for user traffic.

timedef_name must be a pre-configured Time definition in *PCC-Service Configuration Mode*.

Usage Guidelines

Use this command to define a condition based on the start and end time defined in a Time Definition configuration in *PCC-Service Configuration Mode* for user traffic in an IP-CAN session.

Event trigger in this command indicates a condition when the event-trigger time was as per the time specified by the named Time Definition.

This command allows the operator to use configured time period as event trigger for this PCC-Condition-Group.

Example

The following command creates a condition definition to trigger the condition based on the start and end time defined in Timedef named *timedef_night*:

```
event-time = timedef_night
```

event-trigger

This command defines a condition based on the event triggers due to various conditions for subscriber in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

[no] event-trigger *operator event_trigger*

no

Removes the specified condition definition.

operator

Specifies how to logically match the media type in user traffic.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

event_trigger

Specifies the network events as condition definition for user traffic in an IP-CAN session.

Following event triggers are supported with this command:

- **an-gw-change**
- **bearer-qos-change**
- **bearer-setup**
- **bearer-termination**
- **default-eps-bearer-qos-change**
- **ip-can-change**
- **loss-of-bearer**
- **out-of-credit**
- **pgw-trace-control**
- **plmn-change**
- **qos-change**
- **qos-change-exceeding-authorization**
- **rai-change**
- **rat-change**
- **reallocation-of-credit**
- **recover-of-bearer**
- **resource-modification-request**
- **revalidation-timeout**
- **session-setup**
- **session-termination**
- **sgsn-change**
- **successful-resource-allocation**
- **tft-change**
- **ue-ip-address-allocate**
- **ue-ip-address-release**
- **ue-time-zone-change**
- **user-location-change**

Usage Guidelines Use this command to define a condition based on the event triggered in network for user traffic.

Example

The following command creates a condition definition when there is a change in traffic flow template for subscriber:

```
event-trigger = tft-change
```

imsi

This command defines a condition based on the International Mobile Station Identification number (IMSI) of a subscriber in an IP-CAN session.

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] imsi operator value imsi
[ no ] imsi operator profile-attribute spr_attr_value
[ no ] imsi operator subscription-attribute subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- =: Equals

imsi

Specifies the IMSI of subscriber to be used for condition validation in an IP-CAN session.

imsi must be a string of between 8 to 15 digits which starts with 3 digit of MCC then 2 to 3 digit of MNC.

Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ('). For example; '$'.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with IMSI in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with IMSI in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the IMSI of a subscriber used in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on subscriber IMSI as *12334566434* in an IP-CAN session:

```
imsi = 12334566434
```

msisdn

This command defines a condition based on the Mobile Station International Subscriber Directory Number (MSISDN) of a subscriber in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] msisdn operator value msisdn
[ no ] msisdn operator profile-attribute spr_attr_value
[ no ] msisdn operator subscription-attribute subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal

- =: Equals

imsi

Specifies the MSISDN of subscriber to be used for condition validation in an IP-CAN session.

msisdn must be a string of between 1 to 16 digits which contains CC + NDC/NPA + SN.

Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ('). For example; '$'.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with MSISDN in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with MSISDN in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the MS ISDN of a subscriber used in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on subscriber MSISDN as *380561234567* in an IP-CAN session:

```
msisdn = 380561234567
```

multi-line-or

This command enables/disables the "OR" relation across all conditions exist in PCC-Condition-Group Configuration Mode.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[no] multi-line-or
```

no

Sets the PCC-Condition-Group to "AND" relation across all conditions exist in a PCC-Condition-Group Configuration Mode.

Usage Guidelines

Use this command to enable the "OR" relation across all conditions exist in PCC-Condition-Group Configuration Mode.

In absence of this command the default relation of "AND" applies across all conditions exist in PCC-Condition-Group Configuration Mode.

Example

The following command enables the "OR" relation across all conditions exist in *PCC-Condition-Group Configuration Mode*:

```
multi-line-or
```

The following command enables the default "AND" relation across all conditions exist in *PCC-Condition-Group Configuration Mode*:

```
no multi-line-or
```

nai

This command defines a condition based on the Network Access Identifier (NAI) of a subscriber in an IP-CAN session between PCEF (PDSN) and IPCF over **Gx** interface.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] nai operator {username user_name [domain domain] | domain domain}
[ no ] nai operator profile-attribute spr_attr_value
[ no ] nai operator subscription-attribute subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

username *user_name*

Specifies the subscriber user name to be used for condition validation in an IP-CAN session.

user_name must be an alpha and/or numeric string of 1 through 128 characters in length. The user name can contain all special characters.

domain *domain*

Specifies the domain (Realm) of subscriber to be used for condition validation in an IP-CAN session.

domain must be an alpha and/or numeric string of 1 through 128 characters in length. The domain name can contain all special characters.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with NAI in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with NAI in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

User this command to define a condition based on the NAI, which contains of user name and domain name, of a subscriber in an IP-CAN session between PCEF (PDSN) and IPCF over **Gx** interface.

This condition is defined for PCC functionality support to CDMA users over **Gx** interface.

Example

The following command creates a condition definition to analyze the condition based on subscriber user name as *cdma2000_subs1* in an IP-CAN session between PDSN and IPCF having *xyz.com* as domain:

```
nai = username cdma2000_subs1 domain xyz.com
```

out-of-credit rulename

This command defines a condition based on the exhaustion of credit for subscriber Rulename at PCEF in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

[no] out-of-credit rulename *operator rule_name*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

rule_name

Specifies the name of the Rulename for which out of credit condition is to match in an IP-CAN session.

rule_name is a pre-configured Rulename on PCEF and must be an alphanumeric string of from 1 through 63 characters.

Usage Guidelines

Use this command to define a condition based on the exhaustion of credit for subscriber Rulename at PCEF in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on the exhaustion of credit for subscriber Rulename *rule_101* at PCEF in an IP-CAN session:

out-of-credit rulename = *rule_101*

out-of-credit rulebase-name

This command defines a condition based on the exhaustion of credit for subscriber Rulebase name at PCEF in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[no] out-of-credit rulebase-name operator rulebase_name
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

rulebase_name

Specifies the name of the Rulebase for which out of credit condition is to match in an IP-CAN session.

rulebase_name is a pre-configured Rulebase on PCEF and must be an alphanumeric string of from 1 through 63 characters.

Usage Guidelines

Use this command to define a condition based on the exhaustion of credit for subscriber Rulebase name at PCEF in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on the exhaustion of credit for subscriber Rulebase name *rulebase_101* at PCEF in an IP-CAN session:

```
out-of-credit rulebase-name = rulebase_101
```

pcef-address

This command defines a condition based on the IP address of Policy and Charging Enforcement Function (PCEF) which is served by IPCF and through which subscriber is attached to an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] pcef-address {operator value pcef_ip/mask | {in-range | !in-range} value
 range_start_ip to range_end_ip}
[ no ] pcef-address operator profile-attribute spr_attr_value
[ no ] pcef-address operator subscription-attribute subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

in-range

Specifies the condition to accept the IP address which are in range as argument to define the PCEF address which is used by subscriber in IP-CAN session.

!in-range

Specifies the condition to accept the IP address which are NOT in range as argument to define the PCEF address which is used by subscriber in IP-CAN session.

range_start_ip

Specifies the starting IP address which is used for defining the range of PCEF IP addresses which is used by subscriber in IP-CAN session.

range_start_ip is an IP address and must be lesser than *end_start_ip* address.

range_end_ip

Specifies the ending IP address which is used for defining the range of PCEF IP addresses which is used by subscriber in IP-CAN session.

range_end_ip is an IP address and must be greater than *end_start_ip* address.

pcef_ip/mask

Specifies the IP address of the PCEF which is used by subscriber in IP-CAN session along with IP mask as well.

pcef_ip must be an IP address in IPv4 or IPv6 notation.

mask Specifies the IP address mask bits to determine the number of IP addresses of PCEF in condition. *mask* must be specified using the standard IPv4 dotted decimal notation.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with PCEF address in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with PCEF address in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the PCEF IP address used by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on PCEF P address *209.165.200.228* in an IP-CAN session:

pcef-address = *209.165.200.228*

pdn-id

This command defines a condition based on the PDN or calling station id in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-pcc-condition-group)#

Syntax Description

[no] pdn-id [case-insensitive] *operator* **value** *pdn_id*
[no] pdn-id [case-insensitive] *operator* **profile-attribute** *spr_attr_value*
[no] pdn-id [case-insensitive] *operator* **subscription-attribute** *subs_prof_attr_value*

no

Removes the specified condition definition.

case-insensitive

This optional keyword sets the condition to not to consider the case of argument phrase for condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals
- **contains**: Contains
- **!contains**: Does not contain
- **starts-with**: Starts with
- **!starts-with**: Does not start with
- **ends-with**: Ends with
- **!ends-with**: Does not end with

pdn_id

Specifies the PDN or calling station id to be used for condition validation in an IP-CAN session.

pdn_id must be an alphanumeric string of between 1 to 128 characters.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with PDN id in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with PDN id in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the PDN or calling station id used in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on calling station id *ggsn_all_102* in an IP-CAN session:

```
pdn-id = ggsn_all_102
```

profile-attribute

This command defines a condition based on the matching between subscriber profile attribute value and SPR attribute value in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

[no] profile-attribute parameter *subs_prof_attr_value operator spr_attr_value*

no

Removes the specified condition definition.

parameter *subs_prof_attr_value*

Specifies the attribute parameter value to match with SPR attribute for condition validation in an IP-CAN session.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Important This keyword deprecated in StarOS Release 14.0 and onward.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

spr_attr_value

Specifies the attribute value in SPR to match with Subscriber profile attribute for condition validation in an IP-CAN session.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

Usage Guidelines

Use this command to define a condition based on the matching parameters between subscriber profile attribute and SPR attribute parameters used in an IP-CAN session and provides a generic way of specifying and triggering actions based on any of the subscriber profile attribute received from SPR interactions.

Example

The following command creates a condition definition to analyze the condition based on matching of subscriber profile attribute value *subs_gold_102* with SPR attribute value *spr_gold_102*in an IP-CAN session:

profile-attribute parameter *subs_gold_102* **=** *spr_gold_102*

radio-access-technology

This command defines a condition based on the radio access technology used by subscriber in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

[no] radio-access-technology *operator* **value** *RAT*
[no] radio-access-technology *operator* **profile-attribute** *spr_attr_value*
[no] radio-access-technology *operator* **subscription-attribute** *subs_prof_attr_value*

no

Removes the specified condition definition.

operator

Specifies how to logically match the media type in user traffic.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

RAT

Specifies the radio access technology used by subscriber to access the network as condition definition for user traffic in an IP-CAN session.

Following RAT are supported with this command:

- **cdma2000-1x**: 3GPP2 CDMA 2000 - 1x RTT

- **eutran**: Evolved Universal Terrestrial Radio Access Network (eUTRAN)
- **gan**: Generic Access Network (GAN)
- **geran**: GSM Edge Radio Access Network (GERAN)
- **hrpd**: High Rate Packet Data (CDMA 2000 1xEV-DO)
- **hspa-evolution**: Evolved High-Speed Packet Access (eHSPA/HSPA+)
- **umb**: Ultra-Mobile Broadband
- **utran**: Universal Terrestrial Radio Access Network (UTRAN)
- **wlan**: Wireless Local Area Network (WLAN/xDSL)

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with type of RAT in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with type of RAT in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the type of radio technology used for network access by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the radio access technology type as WLAN:

```
radio-access-technology = wlan
```

sgsn-ip

This command defines a condition based on the IP address of SGSN on which subscriber is attached in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

[no] sgsn-ip {*operator* **value** *sgsn_ip/mask* | {**in-range** | **!in-range**} *range_start_ip* **to** *range_end_ip*}

```
[ no ] sgsn-ip operator profile-attribute spr_attr_value
[ no ] sgsn-ip operator subscription-attribute subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

in-range

Specifies the condition to accept the IP address which are in range as argument to define the SGSN address which is used by subscriber in IP-CAN session.

!in-range

Specifies the condition to accept the IP address which are NOT in range as argument to define the SGSN address which is used by subscriber in IP-CAN session.

range_start_ip

Specifies the starting IP address which is used for defining the range of SGSN IP addresses which is used by subscriber in IP-CAN session.

range_start_ip is an IP address and must be lesser than *end_start_ip* address.

range_end_ip

Specifies the ending IP address which is used for defining the range of SGSN IP addresses which is used by subscriber in IP-CAN session.

range_end_ip is an IP address and must be greater than *end_start_ip* address.

sgsn_ip/mask

Specifies the IP address of the SGSN which is used by subscriber in IP-CAN session along with IP mask as well.

sgsn_ip must be an IP address in IPv4 or IPv6 notation.

mask Specifies the IP address mask bits to determine the number of IP addresses of SGSN in condition. *mask* must be specified using the standard IPv4 dotted decimal notation.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with SGSN IP address in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with SGSN IP address in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the SGSN IP address used by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on SGSN IP address *209.165.200.228* in an IP-CAN session:

sgsn-ip = *209.165.200.228*

sgsn-mcc-mnc

This command defines a condition based on the PLMN (MCC+MNC) of SGSN on which subscriber is attached in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

[no] sgsn-mcc-mnc *operator* {**mcc** *mcc_value* [**mnc** *mnc_value*] | [**mcc** *mcc_value*] **mnc** *mnc_value*}
[no] sgsn-mcc-mnc *operator* **profile-attribute** *spr_attr_value*
[no] sgsn-mcc-mnc *operator* **subscription-attribute** *subs_prof_attr_value*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

mcc *mcc_value*

Specifies the Mobile Country Code in PLMN of SGSN which is used by subscriber in IP-CAN session.

mcc_value must be an integer between 101 and 998.

mnc *mnc_value*

Specifies the Mobile Network Code in PLMN of SGSN which is used by subscriber in IP-CAN session.

mnc_value must be an integer between 1 and 998.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with PLMN of SGSN used by subscriber in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with PLMN of SGSN used by subscriber in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the PLMN of SGSN used by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on PLMN of SGSN with MCC as *102* and MNC as *99*in an IP-CAN session:

```
sgsn-mcc-mnc = mcc 102 mnc 99
```

subscription-attribute

This command defines a condition based on the matching between subscriber subscription attribute value and SPR attribute value in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description `[no] subscription-attribute subsription_attr_value operator spr_attr_value`

no

Removes the specified condition definition.

subsription_attr_value

Specifies the subscriber subscription attribute value to match with SPR attribute for condition validation in an IP-CAN session.

subsription_attr_value must be an alphanumeric string of from 1 through 31 characters.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

spr_attr_value

Specifies the attribute value in SPR to match with subscriber subscription attribute for condition validation in an IP-CAN session.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

Usage Guidelines Use this command to define a condition based on the matching parameters between subscriber subscription attribute and SPR attribute value used in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on matching of subscriber subscription attribute value *subs_gold_102* with SPR attribute value *spr_gold_101*in an IP-CAN session:

```
subscription-attribute subscribe_gold_102 = spr_gold_101
```

spr-profile-not-found

This command defines a condition based on the availability of SPR profile for s subscriber in an IP-CAN session.

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[no] spr-profile-not-found
```

no

Removes the specified condition definition.

Usage Guidelines

Use this command to define a condition based on the availability of SPR profile for a subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition if SPR profile is not available for a subscriber in an IP-CAN session:

```
spr-profile-not-found
```

threshold-condition usage-monitor

This command defines a condition based on the threshold conditions in usage of traffic by subscriber session in an IP-CAN session. It is used to support usage tracking and dynamic Policy control based on subscriber usage.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] threshold-condition usage-monitor usage_mon_name { time | vol-or-time
 | volume } usage operator { absolute value volume | subscription-limit |
subscription-threshold subs_thres_limit}
```

no

Removes the specified condition definition.

usage_mon_name

Specifies a unique name for configured usage monitor condition which is used for evaluation with this condition group for user traffic in IP-CAN session.

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

usage

This keyword specifies the condition as usage for threshold condition which is used for evaluation with this condition group for user traffic in IP-CAN session.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

{time | vol-or-time | volume }

This keywords sets the type of thresold; time or volume or both as condition definition for user traffic in IP-CAN session.

- **time**: This keyword sets the threshold condition to use time as condition definition for a user traffic in IP-CAN session.
- **vol-or-time**: This keyword sets the threshold condition to use time or volume as condition definition for a user traffic in IP-CAN session. The condition is matched if either of the two usage values fulfills the condition.
- **volume**: This keyword sets the threshold condition to use volume as condition definition for a user traffic in IP-CAN session.

absolute value *volume*

Specifies the threshold limit condition definition based on absolute usage volume *volume* in Kilo Bytes which is used for evaluation with this condition group for user traffic in IP-CAN session.

volume must be an integer between 1 through 4294967295.

subscription-limit

Specifies the threshold limit condition based on Subscriber's subscription limit which is used for evaluation with this condition group for user traffic in IP-CAN session.

In this condition the system takes Subscriber's subscription limit as defined in subscriber subscription policy for threshold limit monitoring.

subscription-threshold *subs_thres_limit*

Specifies the condition definition for threshold limit based on a configured usage monitor threshold named *subs_thres_limit* in IP-CAN session.

subs_thres_limit is a pre-configured subscription limit in this configuration mode.

This command allows the operator to use configured subscription limit as subset of a threshold condition.

Usage Guidelines

Use this command to define a condition based on the duration of usage of service in seconds or volume usage in Bytes for user traffic in an IP-CAN session. This usage monitor is used to support usage tracking and dynamic Policy control based on subscriber usage.

IPCF supports the concept of Monitoring Key. PCEF, when instructed by PCRF, keeps track of usage per Monitoring Key. PCEF reports the usage when thresholds are reached or requested by PCRF.

To allow operator to have dynamic Policy control, IPCF uses Usage Monitor. This Usage Monitor has attribute of volume-limit, time-limit or both. Operator can "associate" different Monitoring Keys to these usage monitors. It can be a Many-To-Many relationship between Usage-Monitor and Monitoring-Key. Operator can use Usage conditions on Usage Monitors instead of Monitoring Keys directly.

IPCF tracks usage per usage-monitor. Different monitoring keys associated to a Usage-Monitor. When monitoring key is associated to a Usage-Monitor, the usage reported for that particular monitoring key is added to all the usage monitoring to which it is associated.

IPCF supports 2 types of usage monitors; it can be defined on IPCF or SSC supplied usage monitors. The name *usage_mon_name* identifies an usage-monitor, which is locally defined or received from SSC. The **absolute** value applies to both types of usage monitors.

This command allows the operator to use configured threshold condition with another threshold condition as subset.

A maximum of 8 thresholds can be configured per usage monitor.

Example

The following command creates a threshold condition with usage monitor name *threshold1* as usage monitor to trigger the condition based on the **subscription limit** as provide in Subscriber policy:

threshold-condition usage-monitor *threshold1* **usage** = **subscription-limit**

user-access-network

This command defines a condition based on the access location type of the subscriber in an IP-CAN session as received on **Gx** interface.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

[no] user-access-network *operator* **value { home | roaming | visiting }**
[no] user-access-network *operator* **profile-attribute** *spr_attr_value*
[no] user-access-network *operator* **subscription-attribute** *subs_prof_attr_value*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

value home

Specifies the subscriber network access type as Home for condition validation in an IP-CAN session.

This condition contains all subscribers active in Home networks in this condition.

value roaming

Specifies the subscriber network access type as Roaming for condition validation in an IP-CAN session.

This condition contains all subscribers active in Roaming networks in this condition.

value visiting

Specifies the subscriber network access type as Visiting for condition validation in an IP-CAN session.

This condition contains all subscribers active in Visiting networks in this condition.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with user access network condition validation in an IP-CAN session.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with user access network condition validation in an IP-CAN session.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the location of the user as defined in SPR attribute or subscriber profile attribut or location of user in Home, Roaming, Visiting in an IP-CAN session as received on **Gx** interface.

This configuration compares ULI and other location information from Gx data with the Home/roaming/visiting location as received from SSC. IPCF will also use global data as received from SSC in determining user access network through Subscriber profile attribute or SPR attribute in profile attribute.

Example

The following command creates a condition definition to analyze the condition based on location of the subscribes as **roaming** in an IP-CAN session:

```
user-access-network = value roaming
```

user-equipment-info esn

This command defines a condition based on the Electronic Serial Number (ESN) used for the identification of mobile device (UE) in a Non-3GPP IP-CAN session received over **Gx** interface between PDSN and IPCF.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

[no] user-equipment-info esn *operator* **value** *esn*
[no] user-equipment-info esn *operator* **profile-attribute** *spr_attr_value*
[no] user-equipment-info esn *operator* **subscription-attribute** *subs_prof_attr_value*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

esn

Specifies the Electronic Serial Number used for the identification of UE in 64 bit format as condition value for UE information received over **Gx** interface in a Non-3GPP IP-CAN session.

esn must be a 15 character long string of Hexadecimal numbers only.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with ESN of the UE in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with ESN of the UE in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the ESN of the UE received over **Gx** interface in a Non-3GPP IP-CAN session between PDSN and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the ESN of the UE as *1234567890120AF* in a Non-3GPP IP-CAN session:

```
user-equipment-info esn = 1234567890120AF
```

user-equipment-info eui64

This command defines a condition based on the Extended Unique Identifier in 64 bit (EUI-64) used for the identification of mobile device (UE) in an IP-CAN session received over **Gx** interface.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] user-equipment-info eui64 operator value eui64
[ no ] user-equipment-info eui64 operator profile-attribute spr_attr_value
[ no ] user-equipment-info eui64 operator subscription-attribute
subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

eui64

Specifies the Extended Unique Identifier in 64 bit format as a condition value for UE information received over **Gx** interface in an IP-CAN session.

eui64 is a 16 character long string of Hexadecimal numbers only.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with EUI-64 value of the UE in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with EUI-64 value of the UE in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the EUI-64 value of the UE received over **Gx** interface in an IP-CAN session between PCEF and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the EUI-64 of the UE as *0012989099832345* in an IP-CAN session:

```
user-equipment-info eui64 = 0012989099832345
```

user-equipment-info imeisv

This command defines a condition based on the International Mobile Equipment Identity Software Version (IMEI-SV) used for the identification of mobile device (UE) in an IP-CAN session received over **Gx** interface.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] user-equipment-info imeisv  operator value imei_sv
[ no ] user-equipment-info imeisv operator profile-attribute spr_attr_value
[ no ] user-equipment-info imeisv operator subscription-attribute
subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

imei_sv

Specifies the International Mobile Equipment Identity Software Version (IMEI-SV) as a condition value for UE information received over **Gx** interface in an IP-CAN session.

imei_sv is a 16 digit long string of decimal numbers only.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with IMEI-SV value of the UE in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with IMEI-SV value of the UE in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the IMEI-SV value of the UE received over **Gx** interface in an IP-CAN session between PCEF and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the IMEI-SV of the UE as *0012989099832345* in an IP-CAN session:

```
user-equipment-info eui64 = 0012989099832345
```

user-equipment-info mac

This command defines a condition based on the Media Access Control (MAC) address used for the UE information in an IP-CAN session as received over **Gx** interface.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

[no] user-equipment-info mac *operator* **value** *mac_value*
[no] user-equipment-info mac *operator* **profile-attribute** *spr_attr_value*
[no] user-equipment-info mac *operator* **subscription-attribute** *subs_prof_attr_value*

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

mac_value

Specifies the Media Access Control (MAC) address as condition value for UE information received over **Gx** interface in an IP-CAN session.

mac_value is a 17 character long string of Hexadecimal numbers in *xx:xx:xx:xx:xx:xx* format only.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with MAC value of the UE in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with MAC value of the UE in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the MAC address value as UE information received over **Gx** interface in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on the MAC value of the UE as *00:12:98:90:99:83* in an IP-CAN session:

```
user-equipment-info mac = 00:12:98:90:99:83
```

user-equipment-info meid

This command defines a condition based on the Mobile Equipment Id (MEID) used for the identification of CDMA mobile device (UE) in a Non-3GPP IP-CAN session received over **Gx** interface between PDSN and IPCF.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] user-equipment-info meid operator value me_id
[ no ] user-equipment-info meid operator profile-attribute spr_attr_value
[ no ] user-equipment-info meid operator subscription-attribute
subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- =: Equals

me_id

Specifies the Mobile Equipment identifier used for the identification of UE in 64 bit format as condition value for UE information received over **Gx** interface in a Non-3GPP IP-CAN session.

me_id must be a 14 character long string of Hexadecimal numbers only.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with Mobile Equipement id of the UE in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with Mobile Equipement id of the UE in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the MEID of the CDMAUE received over **Gx** interface in a Non-3GPP IP-CAN session between PDSN and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the MEID of the CDMA UE as *123456780120AF* in a Non-3GPP IP-CAN session:

```
user-equipment-info meid = 123456780120AF
```

user-equipment-info modified-eui64

This command defines a condition based on the modified-Extended Unique Identifier in 64 bit (EUI-64) used for the identification of mobile device (UE) in an IP-CAN session received over **Gx** interface.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

```
[ no ] user-equipment-info modified-eui64 operator value meui64
[ no ] user-equipment-info modified-eui64 operator profile-attribute
spr_attr_value
[ no ] user-equipment-info modified-eui64 operator subscription-attribute
subs_prof_attr_value
```

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

meui64

Specifies the modified Extended Unique Identifier (EUI) in 64 bit format as condition value for UE information received over **Gx** interface in an IP-CAN session.

meui64 is a 16 character long string of Hexadecimal numbers only.

profile-attribute*spr_attr_value*

Specifies the profile attribute value in SPR to match with modified EUI-64 value of the UE in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute *subs_prof_attr_value*

Specifies the subscriber profile attribute parameter value to match with modified EUI-64 value of the UE in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage Guidelines

Use this command to define a condition based on the modified EUI-64 value of the UE received over **Gx** interface in an IP-CAN session between PCEF and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the EUI-64 of the UE as *0012989099832345* in an IP-CAN session:

```
user-equipment-info modified-eui64 = 0012989099832345
```

user-location-info

This command defines a condition based on the UE location used in an IP-CAN session as received on **Gx** interface.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context *context_name* **> pcc-service** *service_name* **> condition group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax Description

[no] user-location-info {**cgi** *operator* **mcc** *mcc_value* **mnc** *mnc_value* **lac** *lac_value* **ci** *ci_value* | **ecgi** *operator* **mcc** *mcc_value* **mnc** *mnc_value* **ecgi** *ecgi_value* | **rai** *operator* **mcc** *mcc_value* **mnc** *mnc_value* **lac** *lac_value* **rai** *rai_value*| **sai** *operator* **mcc** *mcc_value* **mnc** *mnc_value* **lac** *lac_value* **sac** *sac_value*| **tai** *operator* **mcc** *mcc_value* **mnc** *mnc_value* **tai** *tai_value*}

no

Removes the specified condition definition.

cgi

Specifies the Cell Global Identifier in UE location received over **Gx** interface in an IP-CAN session.

ecgi

Specifies the E-UTRAN Cell Global Identifier in UE location received over **Gx** interface in an IP-CAN session.

rai

Specifies the Routing Area Identifier in UE location received over **Gx** interface in an IP-CAN session.

sai

Specifies the Service Area Identifier in UE location received over **Gx** interface in an IP-CAN session.

tai

Specifies the Tracking Area Identifier in UE location received over **Gx** interface in an IP-CAN session.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- **!=**: Does not equal
- **=**: Equals

mcc *mcc_value*

Specifies the Mobile Country Code used in UE location information received over **Gx** interface in IP-CAN session.

mcc_value must be an integer between 101 through 998.

mnc *mnc_value*

Specifies the Mobile Network Code used in UE location information received over **Gx** interface in IP-CAN session.

mnc_value must be an integer between 1 through 998.

lac *lac_value*

Specifies the Location Area Code used in UE location information received over **Gx** interface in IP-CAN session.

lac_value must be an integer between 1 through 65535.

ci *ci_value*

Specifies the Cell Identifier used in UE location information received over **Gx** interface in IP-CAN session.

ci_value must be an integer between 1 through 65535.

ecgi *ecgi_value*

Specifies the E-UTRAN Cell Global Identifier used in UE location information received over **Gx** interface in IP-CAN session.

ecgi_value must be an integer between 1 through 1048575.

rai *rai_value*

Specifies the Routing Area Identifier used in UE location information received over **Gx** interface in IP-CAN session.

rai_value must be an integer between 1 through 65535.

sac *sac_value*

Specifies the Service Area Code used in UE location information received over **Gx** interface in IP-CAN session.

sac_value must be an integer between 1 through 65535.

tai *tai_value*

Specifies the Tracking Area Code used in UE location information received over **Gx** interface in IP-CAN session.

tai_value must be an integer between 1 through 65535.

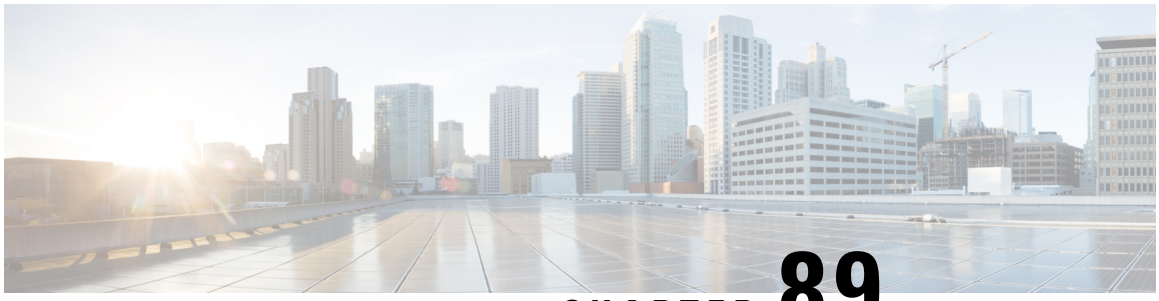
Usage Guidelines

Use this command to define a condition based on the UE location information received over **Gx** interface in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on the RAI received for UE location in an IP-CAN session:

```
user-location-info rai  = mcc 102 mnc 99 lac 1003 rai 3521
```



CHAPTER 89

PCC-Data-Service Configuration Mode Commands

Important This configuration mode is supported from StarOS Release 12.1 onward.

Command Modes

The PCC-Data-Service Configuration Mode is used to configure the data flow parameters for the media data, as well as corresponding attributes that are necessary for charging and policy enforcement decisions for the media parameters represented by its service flows in the PCC-service. A maximum of ten service data flows can be configured in a PCC-Data-Service instance.

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context *context_name* **> pcc-service** *service_name* **> data-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-data-service)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

• service-identifier, on page 959

flow direction in

This command configures the flow service parameters for incoming data flow in PCC-Data-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **data-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-data-service)#
```

Syntax Description

[no] flow direction in protocol {**ip** | **tcp** | **udp**} **from** {*src_ip_addr*[*/maskbit*] | **any**} **port** {*src_port_num* | **any**} **to** {*dest_ip_addr/maskbit* | **any**} **port** {*dest_port_num* | **any**}

no

Removes the configured data service flow parameters from PCC-Data-Service instance for IPCF configuration.

protocol {ip | tcp | udp}

This keyword configures the data flow parameters for specific protocol.

Following protocols are supported through this keyword:

- **ip**: Sets the parameters for IP traffic.
- **tcp**: Sets the parameters for TCP traffic.
- **UDP**: Sets the parameters for UDP traffic.

from {*src_ip_addr*[*/maskbit*] | any} port {*src_port_num* | any}

This keyword configures the data flow condition parameters for specific protocol through IP address and port as source of flow.

Following parameters are defined with this keyword:

- *src_ip_addr*: specifies the specific IP address in IPv4/IPv6 notation as source of flow.
- *maskbit*: Specifies the IP address suffix in IPv4 or IPv6 notation.
- **any**: specifies that flow from any source IP address/port can be analyzed or considered.
- **port** *src_port_num*: specifies the specific source port parameter for flow.

  src_port_num is the source port number of flow and must be an integer from 1 through 65535.

to {*dest_ip_addr*[*/maskbit*] | any} port {*dest_port_num* | any}

This keyword configures the data flow condition parameters for specific protocol through IP address and port as source of flow.

Following parameters are defined with this keyword:

- *dest_ip_addr*: specifies the specific IP address in IPv4/IPv6 notation as destination of flow.
- *maskbit*: Specifies the IP address suffix in IPv4 or IPv6 notation.
- **any**: specifies that flow to any destination IP address/port can be analyzed or considered.
- **port** *dest_port_num*: specifies the specific destination port parameter for flow.

  dest_port_num is the destination port number of flow and must be an integer from 1 through 65535.

Usage Guidelines

Use this command to configure the flow service parameters for incoming data flow in PCC-Data-Service instance for IPCF Configuration.

Example

Following command sets the data service parameters for **tcp** type protocol from **any** IP/port source to **any** IP/port in incoming direction with in a PCC-Data-Service.

```
flow direction in protocol tcp from any port any to any port any
```

flow direction out

This command configures the flow service parameters for outgoing data flow in PCC-Data-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context *context_name* **> pcc-service** *service_name* **> data-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-data-service)#
```

Syntax Description

```
[no] flow direction in protocol {ip | tcp | udp} from {src_ip_addr[ /maskbit] |
any} port {src_port_num | any} to {dest_ip_addr[ /maskbit] | any} port {dest_port_num
 | any}
```

no

Removes the configured data service flow parameters from PCC-Data-Service instance on IPCF node.

protocol {ip | tcp | udp}

This keyword configures the data flow parameters for specific protocol.

Following protocols are supported through this keyword:

- **ip**: Sets the parameters for IP traffic.
- **tcp**: Sets the parameters for TCP traffic.
- **UDP**: Sets the parameters for UDP traffic.

from {*src_ip_addr* | any} port {*src_port_num* | any}

This keyword configures the data flow condition parameters for specific protocol through IP address and port as source of flow.

Following parameters are defined with this keyword:

- *src_ip_addr*: specifies the specific IP address in IPv4/IPv6 notation as source of flow.
- *maskbit*: Specifies the IP address suffix in IPv4 or IPv6 notation.
- **any**: specifies that flow from any source IP address/port can be analyzed or considered.
- **port** *src_port_num*: specifies the specific source port parameter for flow.

  src_port_num is the source port number of flow and must be an integer from 1 through 65535.

to {*dest_ip_addr* | any} port {*dest_port_num* | any}

This keyword configures the data flow condition parameters for specific protocol through IP address and port as source of flow.

Following parameters are defined with this keyword:

- *dest_ip_addr*: specifies the specific IP address in IPv4/IPv6 notation as destination of flow.
- *maskbit*: Specifies the IP address suffix in IPv4 or IPv6 notation.
- **any**: specifies that flow to any destination IP address/port can be analyzed or considered.
- **port** *dest_port_num*: specifies the specific destination port parameter for flow.

  dest_port_num is the destination port number of flow and must be an integer from 1 through 65535.

Usage Guidelines

Use this command to configure the flow service parameters for outgoing data flow in PCC-Data-Service instance on IPCF node.

Example

Following command sets the data service parameters for **tcp** type protocol from **any** IP/port source to **any** IP/port in outgoing direction with in a PCC-Data-Service.

```
flow direction out protocol tcp from any port any to any port any
```

metering-method

This command specifies the metering method to be used by PCEF for offline charging in a PCC-Data-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context *context_name* **> pcc-service** *service_name* **> data-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pcc-data-service)#`

Syntax Description

[no] metering-method {both-duration-volume | duration | volume}

no

Removes the configured metering method from PCC-Data-Service instance on IPCF node.

In such scenario, the metering method pre-configured at PCEF is considered.

both-duration-volume

Specifies the metering method as based on volume of data usage and duration of session, both for offline charging in a PCC-Data-Service instance on IPCF node.

duration

Specifies the metering method as based on the duration of session usage for offline charging in a PCC-Data-Service instance on IPCF node.

volume

Specifies the metering method as based on the volume of data usage for offline charging in a PCC-Data-Service instance on IPCF node.

Usage Guidelines

Use this command to define the metering method to be used for offline charging in a PCC-Data-Service instance on IPCF node.

If no metering method is defined, the metering method preconfigured at PCEF is considered.

Example

Following command sets the metering method as based on volume of data usage and duration of session, both for offline charging in a PCC-Data-Service instance on IPCF node.

metering-method both-duration-volume

monitoring-key

This command defines the monitoring key under which data is monitored for the PCC-Data-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context *context_name* **> pcc-service** *service_name* **> data-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-data-service)#
```

Syntax Description

monitoring-key *mon_key_value*
[**no**] **monitoring-key**

no

Removes the configured monitoring-key from PCC-Data-Service instance on IPCF node.

mon_key_value

Specifies the monitoring key value under which data usage is monitored for the PCC-Data-Service instance and must be an integer from 1 through 65535.

Usage Guidelines

Use this command to define the monitoring key under which data is monitored for the PCC-Data-Service instance on IPCF node.

Example

Following command sets the monitoring key *123* for data monitoring in PCC-Data-Service instance on IPCF node.

monitoring-key *123*

precedence

This command defines the precedence that is assigned to the Dynamic PCC rule created for a PCC-Data-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context *context_name* **> pcc-service** *service_name* **> data-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-data-service)#
```

Syntax Description

precedence *preced_value*
[**no**] **precedence**

no

Removes the configured precedence value from PCC-Data-Service instance on IPCF node.

preced_value

Specifies the precedence that is assigned to the dynamic PCC rule created for a PCC-Data-Service instance and must be an integer from 1 through 65535.

Usage Guidelines Use this command to define the precedence value that is assigned to the Dynamic PCC rule created for a PCC-Data-Service instance on IPCF node.

Example

Following command sets the precedence value*2* to assign to the dynamic PCC rule created for a PCC-Data-Service instance on IPCF node.

```
precedence 2
```

qos-profile

This command defines the PCC-QoS-Profile which is to use for the PCC-Data-Service instance on IPCF node.

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **data-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-data-service)#
```

Syntax Description

```
qos-profile qos_prof_name
[no] qos-profile
```

no

Removes the configured PCC-QoS-Profile from PCC-Data-Service instance on IPCF node.

qos_prof_name

Specifies the pre-configured PCC-QoS-Profile name which is to use for the PCC-Data-Service instance.

Usage Guidelines Use this command to define the PCC-QoS-Profile for a PCC-Data-Service instance on IPCF node.

Example

Following command sets the PCC-QoS-Profile *ipcf_qos_prof1* for PCC-Data-Service instance on IPCF node.

qos-profile *ipcf_qos_prof1*

rating-group

This command defines the PCC-Rating-Group that is assigned for a PCC-Data-Service instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context *context_name* **> pcc-service** *service_name* **> data-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-data-service)#
```

Syntax Description

rating-group *rating_grp_id*
[**no**] **rating-group**

no

Removes the configured PCC-Rating-Group Id from PCC-Data-Service instance on IPCF node.

rating_grp_id

Specifies the PCC-Rating-Group Id that is assigned to the PCC-Data-Service instance and must be an integer from 1 through 99.

Usage Guidelines

Use this command to define the PCC-Rating Id value for a PCC-Data-Service instance on IPCF node.

Example

Following command sets the Rating Group id *11* for a PCC-Data-Service instance on IPCF node.

rating-group *11*

reporting-level

This command specifies the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-Service instance on IPCF node.

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context *context_name* **> pcc-service** *service_name* **> data-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-data-service)#
```

Syntax Description `[no] reporting-level {service-identifier-level | rating-group-level}`

no

Removes the configured usage reporting level from PCC-Data-Service instance on IPCF node.

In such scenario, the reporting level configured at PCEF is considered.

service-identifier-level

Sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the service identifier level in a PCC-Data-Service instance on IPCF node.

rating-group-level

Sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the Rating-group level in a PCC-Data-Service instance on IPCF node.

Usage Guidelines Use this command to define the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-Service instance on IPCF node.

If no reporting level is defined, the reporting level preconfigured at PCEF is considered.

Example

Following command sets the reporting level at 'Rating-group' level which is to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-Service instance on IPCF node.

```
reporting-level rating-group-level
```

service-identifier

This command defines the service identifier for a PCC-Data-Service instance.

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **data-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-data-service)#
```

Syntax Description

service-identifier *svc_id*
[**no**] **service-identifier**

no

Removes the configured Service Identifier from PCC-Data-Service instance on IPCF node.

svc_id

Specifies the Service Identifier that is assigned to the PCC-Data-Service instance and must be an integer from 1 through 65535.

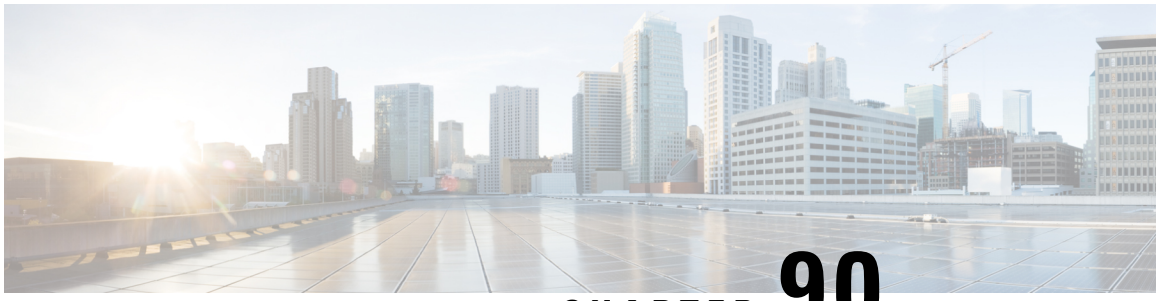
Usage Guidelines

Use this command to define the Service Identifier for a PCC-Data-Service instance on IPCF node.

Example

Following command sets the Service Identifier *1011* for a PCC-Data-Service instance on IPCF node.

service-identifier *1011*



CHAPTER 90

PCC-Event-Notification-Interface-Endpoint Configuration Mode Commands

Important This configuration mode is supported from StarOS Release 12.1 onward.

Command Modes

The PCC-Event-Notification-Interface-Endpoint configuration mode is used to enable the event notification interface mechanism for the Intelligent Policy Control Function (IPCF) and to configure the Event Notification collection server endpoint related parameters.

Exec > Global Configuration > Context Configuration > Event Notification Interface Endpoint Configuration

configure > context *context_name* **> event-notif-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ntfyintf-endpoint)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

address

This command binds an IP address to the local IPCF node which is to be used for event notification processing with remote event collection server endpoint during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Event Notification Interface Endpoint Configuration

configure > context *context_name* **> event-notif-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ntfyintf-endpoint)#
```

Syntax Description

address *ip_address*

ip_address

Specifies the IP address bind with local IPCF node to be used by the event collection server endpoint for event message processing during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Usage Guidelines

Use this command to bind an IP address to interact with the remote event notification collection server endpoint to which the event messages are sent for IP-CAN session events.

Example

Following command binds the *1.2.3.4* for event notification message with remote event notification endpoint.

address*1.2.3.4*

peer name

This command binds/associates a remote Event Notification collection server as peer having specified IP address and optionally port for event notification during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Event Notification Interface Endpoint Configuration

configure > context *context_name* **> event-notif-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ntfyintf-endpoint)#
```

Syntax Description **peer name** *peer_name* **address** *ip_address* [**port** *port_num*]

name *peer_name*

Sets the in PCC-Event-Notification-Interface-Endpoint instance to use a particular peer node configured by a peer name *peer_name* for event notification interface.

The *peer_name* is name of the peer node to be sued for event collection and must be an alphanumerical string from 1 through 31 characters. *peer_name* allows punctuation marks.

ip-address *ip_address*

Sets the PCC-Event-Notification-Interface-Endpoint instance to bind the particular peer node name with IP address *ip_address* in IPv4 or IPv6 notation for event notification message processing.

The *ip_address* is an IP address in IPv4/IPv6 notation.

port *port_num*

This optional keyword sets a particular port number to be used with in the PCC-Event-Notification-Interface-Endpoint instance to configure a particular peer node having a pre assigned IP address *ip_address* in IPv4 or IPv6 notation for event notification message processing.

The *port_num* must be an integer between 1 and 65535.

Usage Guidelines Use this command to bind/associate a remote Event Notification collection server as peer having specified IP address and optionally port for event notification during IP-CAN session in the PCC-Event-Notification-Interface-Endpoint instance.

Multiple peers can be configured using this command and peer selection methods, **primary-secondary** or **round-robin** can be applied using **peer select-algorithm** command for event notification during IP-CAN session in this configuration mode.

Example

Following command configures and associates an Event Notification peer node named *event_peer_1* having an IP address *209.165.200.228* with port number as *2345* in an PCC-Event-Notification-Interface-Endpoint instance.

peer name *event_peer_1* **ip-address** *209.165.200.228* **port** *2345*

peer select-algorithm

This command applies the peer selection algorithm to select the configured remote Event Notification collection server during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Event Notification Interface Endpoint Configuration

configure > context *context_name* **> event-notif-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ntfyintf-endpoint)#
```

Syntax Description

peer select-algorithm {**primary-secondary** | **round-robin**}

primary-secondary

Sets the PCC-Event-Notification-Interface-Endpoint peer selection algorithm to select the configured remote peer servers in primary and secondary method during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

This mode is applicable only when multiple peers are configured and primary and secondary peer is defined using **peer select-peer** command in this configuration mode.

round-robin

Sets the PCC-Event-Notification-Interface-Endpoint peer selection algorithm to select the configured remote peer servers in round-robin method mode during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

This mode is applicable only when multiple peers are configured in this configuration mode.

Usage Guidelines

Use this command apply the peer selection algorithm to select the configured remote Event Notification collection server during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Example

Following command configures the peer selection algorithm to select the configured remote peer in **round-robin** method in PCC-Event-Notification-Interface-Endpoint instance.

```
peer select-algorithm round-robin
```

Following command configures the peer selection algorithm to select the configured primary and secondary remote peers in **primary-secondary** method in PCC-Event-Notification-Interface-Endpoint instance.

```
peer select-algorithm primary-secondary
```

peer select-peer

This command sets the configured remote Event Notification collection server as primary and secondary servers for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Event Notification Interface Endpoint Configuration

configure > context *context_name* **> event-notif-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ntfyintf-endpoint)#
```

Syntax Description

peer select-peer *pri_peer_name* **secondary** *sec_peer_name*

pri_peer_name

Sets the configured remote PCC-Event-Notification-Interface-Endpoint peer as primary peer for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

pri_peer_name must be a pre-configured peer name configured with **peer name** command in this configuration mode.

secondary *sec_peer_name*

Sets the configured remote PCC-Event-Notification-Interface-Endpoint peer as secondary peer for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

sec_peer_name must be a pre-configured peer name configured with **peer name** command in this configuration mode.

Usage Guidelines

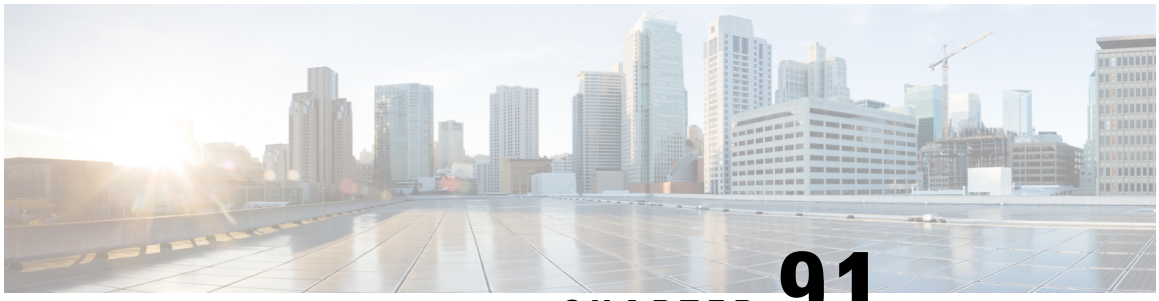
Use this command to set the configured remote Event Notification collection server as primary and secondary node for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

This configuration is used when peer selection algorithm is set to **primary-secondary** using **peer select-algorithm** command in this configuration mode.

Example

Following command configures the specified peer *event1* as primary and *event2* as secondary node for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

peer select-peer *event1* **secondary** *event2*



CHAPTER 91

PCC-Policy-Service Configuration Mode Commands

Important This configuration mode is supported from StarOS Release 12.1 onward.

Command Modes

The PCC-Policy-Service Configuration mode provides a mechanism for the Intelligent Policy Control Function (IPCF) to manage the external interfaces required for policy authorization purpose between IPCF and PCEF Bearer Binding and Event Reporting Function (BBERF). The PCC-Policy-Service manages **Gx**/**Gx** based on the Diameter dictionary used.

Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context *context_name* **> pcc-policy-service** *service_name*

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

associate pcc-service

This command associates a pre-configured PCC-Service with a PCC-Policy-Service for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context *context_name* **> pcc-policy-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

associate pcc-service *pcc_service_name*
[no] associate pcc-service

no

Removes/disassociate the configured PCC-Service from this PCC-Policy-Service instance configured for IPCF configuration.

pcc_service_name

Specifies the name of a pre-configured PCC-Service configured in Context Configuration mode for IPCF configuration.

The *pcc_service_name* is name of a predefined PCC-Service instance and must be an alphanumerical string from 1 through 63 characters.

Usage Guidelines

Use this command to associate a pre-configured PCC-Service instance for IPCF configuration.

Important For more information on PCC-Service configuration, refer *PCC-Service Configuration Mode Commands*.

Example

Following command binds a PCC-Service named *pcc_svc1* with in a PCC-Policy-Service.

associate pcc-service *pcc_svc1*

Following command removes an associated PCC-Service named *pcc_svc1* from a PCC-Policy-Service.

no associate pcc-service *pcc_svc1*

diameter dictionary

This command assigns a Diameter dictionary for **Gx**/**Gxa** messaging with a PCC-Policy-Service for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context *context_name* **> pcc-policy-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter dictionary {**gxa-standard** | **r7-standard** | **standard**}
default diameter dictionary

default

Sets the Diameter **Gx** dictionary to default dictionary **standard** (3GPP Rel. 8 standard) for a PCC-Policy-Service instance configured for IPCF configuration.

gxa-standard

Default: Disabled

Sets the Diameter **Gxa** dictionary to be used by a PCC-Policy-Service instance configured for IPCF configuration over **Gxa** interface to 3GPP Rel. 8 standard.

r7-standard

Default: Disabled

Sets the Diameter **Gx** dictionary to be used by a PCC-Policy-Service instance configured for IPCF configuration over **Gx** interface to 3GPP Rel. 7 standard.

standard

Default: Enabled

Sets the Diameter **Gx** dictionary to be used by a PCC-Policy-Service instance configured for IPCF configuration over **Gx** interface to 3GPP Rel. 8 standard.

Usage Guidelines

Use this command to configure the PCC-Policy-Service to determine which of the 3GPP dictionary to be used for **Gx** or **Gxa** interface messaging for policy and/or quota management.

Example

Following command sets the PCC-Policy-Service to use 3GPP Rel. 8 standard dictionary for **Gx** interface and policy management related messaging in a PCC-Policy-Service.

default diameter dictionary

diameter origin end-point

This command binds/associates a pre-configured Diameter host/realm (PCEF/BBERF) over **Gx/Gxa** interface with a PCC-Policy-Service to be used for subscriber service control and policy profile management.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context *context_name* **> pcc-policy-service** *service_name*

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pccpolicy-service)#

Syntax Description

diameter origin endpoint *dia_endpoint_name*
no diameter origin endpoint

no

Removes the associated Diameter Origin Endpoint configuration from PCC-Policy-Service instance configured for IPCF configuration.

any

Sets the PCC-Policy-Service instance to use any available PCEF/BBERF node for policy interfaces (**Gx**/**Gx**-like) support.

dia_endpoint_name

The *dia_endpoint_name* is a predefined Diameter origin endpoint node and must be an alphanumerical string from 1 through 63 characters.

Usage Guidelines

Use this command to bind the PCEF/BBERF node over **Gx**/**Gx**-like interface by associating a pre-configured Diameter Origin Endpoint with a PCC-Policy-Service.

The Diameter origin endpoint must be a pre-configured instance in the Context Configuration Mode. For more information on Diameter origin endpoint configuration, refer *Diameter Endpoint Configuration Mode Commands* chapter.

Example

Following command associates a pre-configured Diameter endpoint node configuration named *pcef_1* with a PCC-Policy-Service for policy profile management.

diameter origin endpoint*pcef_1*

Following command removes the pre-associated Diameter endpoint node configuration named *pcef_1* with a PCC-Policy-Service.

```
no diameter origin endpoint
```

ehrpd-access-bcm

This command configures the PCC-Policy-Service to accept the applicable Bearer-Control-Mode for eHRPD access over **Gxa** interface on IPCF.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context *context_name* **> pcc-policy-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ehrpd-access-bcm {**as-requested** | **ue-nw** | **ue-only**}
default ehrpd-access-bcm

default

Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from Application Server (AS) for eHRPD access over **Gxa** interface on IPCF node.

as-requested

Default: Enabled.

Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from Application Server (AS) for eHRPD access over **Gxa** interface on IPCF node.

ue-nw

Default: Disabled.

Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE and/or network element for eHRPD access over **Gxa** interface on IPCF node.

ue-only

Default: Disabled.

Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE only for eHRPD access over **Gxa** interface on IPCF node.

Usage Guidelines

Use this command to set the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS or UE or Network for eHRPD access over **Gxa** interface on IPCF node.

Example

Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS for eHRPD access over **Gxa** interface on IPCF node.

```
default ehrpd-access-bcm
```

Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request only from UE for eHRPD access over **Gxa** interface on IPCF node.

```
ehrpd-access-bcm ue-only
```

gprs-access-bcm

This command configures the PCC-Policy-Service to accept the applicable Bearer-Control-Mode for GPRS access over **Gx** interface on IPCF.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context *context_name* **> pcc-policy-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gprs-access-bcm {as-requested | ue-nw | ue-only}
default gprs-access-bcm
```

default

Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from Application Server (AS) for GGSN access over **Gx** interface on IPCF node.

as-requested

Default: Enabled.

Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from Application Server (AS) for GGSN access over **Gx** interface on IPCF node.

ue-nw

Default: Disabled.

Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE and/or network element for GGSN access over **Gx** interface on IPCF node.

ue-only

Default: Disabled.

Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE only for GGSN access over **Gx** interface on IPCF node.

Usage Guidelines

Use this command to set the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS or UE or Network for GGSN access over **Gx** interface on IPCF node.

Example

Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS for GGSN access over **Gx** interface on IPCF node.

```
default gprs-access-bcm
```

Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request only from UE for GGSN access over **Gx** interface on IPCF node.

```
gprs-access-bcm ue-only
```

max policy-sessions

This command configures the maximum limit of the policy sessions allowed in a PCC-Policy-Service instance on IPCF.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context *context_name* **> pcc-policy-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
max policy-sessions max_session
default max policy-sessions
```

default

Sets the maximum policy sessions allowed in PCC-Policy-Service instance to default value of 10000 sessions.

max_session

Default: 10000

Specifies the maximum number of policy sessions configured in PCC-Policy-Service to allow to be connected in PCC-Quota service instance.

max_session must be an integer between 0 and 4000000.

Usage Guidelines

Use this command to set the maximum number of policy sessions allowed by a PCC-Policy-Service instance on IPCF.

Example

Following command sets the maximum number of policy sessions allowed in PCC-Policy-Service instance to 10000.

default max policy-sessions

subscriber-binding-identifier

This command specifies the subscriber binding identifier to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context *context_name* **> pcc-policy-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

subscriber-binding-identifier {**imsi** | **msisdn** | **nai** | **sip-uri**}
default subscriber-binding-identifier

default

Sets the subscriber binding identifier to default value; i.e. IMSI, to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

imsi

Default: Enabled.

Sets the subscriber binding identifier as IMSI to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

msisdn

Default: Disabled.

Sets the subscriber binding identifier as MSISDN to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

nai

Default: Disabled.

Sets the subscriber binding identifier as Network Access Identifier (NAI) to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

sip-uri

Default: Disabled.

Sets the subscriber binding identifier as SIP URI (Uniform Resource Identifier) to be used by **bindmux** for binding different subscriber session to PCC-Policy-Service on IPCF node.

Usage Guidelines Use this command to configure the **bindmux** in PCC-Policy-Service instance on IPCF node to use specific subscriber identifier for binding different subscriber session to IP-CAN session.

Example

The following command sets the PCC-Policy-Service to use IMSI as subscriber binding identifier for IP-CAN session on an IPCF node.

```
default subscriber-binding-identifier
```

subscription-id-absence-action

This command configures the PCC-Policy-Service instance to handle the Initial Credit Control Request (CCR-I) messages during initial authentication over **Gx** interface when CCR-I message received by IPCF node is without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.).

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context *context_name* **> pcc-policy-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
{default} subscription-id-absence-action initial-auth {continue | reject}
```

default

Sets the PCC-Policy-Service instance to reject the CCR-I message during initial authentication over **Gx** interface if received without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.) on IPCF node.

continue

Default: Disabled.

Sets the PCC-Policy-Service instance to accept the CCR-I message and continue with the session if CCR-I is received without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.) on IPCF node.

In this case, IPCF accepts the CCR-I message and will do the PCC provisioning as per the operator configuration in associated PCC-Service.

reject

Default: Enabled.

Sets the PCC-Policy-Service instance to reject the CCR-I message and continue with the session if CCR-I is received without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.) on IPCF node.

In this case, IPCF will send CCA-I message with Result-code as **Permanent Error** and rejects the session establishment with PCEF.

Usage Guidelines

Use this command to configure the PCC-Policy-Service instance to handle the Initial Credit Control Request (CCR-I) message processing during the initial authentication over **Gx** interface if CCR-I message received by IPCF node has no valid Subscription-Id AVP.

Example

The following command sets the PCC-Policy-Service to reject the CCR-I request and terminations the session establishment with PCEF.

```
default subscription-id-absence-action initial-auth
```

unsolicited-provisioning

This command is used to enable/disable the support for unsolicited time-of-day-based procedures to PCC-Policy-Service on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context *context_name* **> pcc-policy-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[no | default] unsolicited-provisioning time-of-day
```

default

Sets the support for unsolicited time-of-day-based procedures to default mode; i.e. disabled, in PCC-Policy-Service instance on IPCF node.

no

Removes the configured support for unsolicited time-of-day-based procedures in PCC-Policy-Service instance on IPCF node.

Usage Guidelines

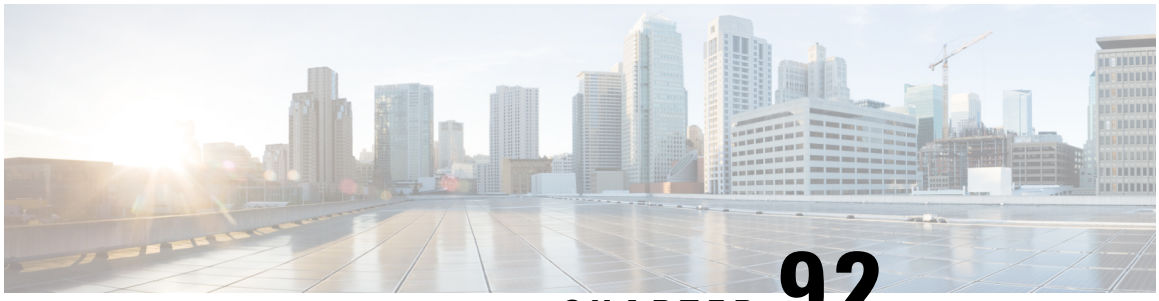
Use this command to enable/disable the support for unsolicited time-of-day-based procedures to PCC-Policy-Service on IPCF node.

By default this command is disabled.

Example

The following command enables the unsolicited time-of-day-based procedures to PCC-Policy-Service on an IPCF node.

```
unsolicited-provisioning time-of-day
```



CHAPTER 92

PCC-Service-Profile Configuration Mode Commands

Important This configuration mode is supported from StarOS Release 12.1 onward.

Command Modes

The PCC-Service-Profile Configuration Mode is used to define the business logic used by the operator for managing the policy requirements and objectives for the network specific to a group of subscribers in the network. A PCC-Service-Profile manages multiple PCC-Conditions-Groups and associated PCC-Action-Sets pairs in an ordered manner. A maximum of 32 PCC-Service-Profile can be configured in a PCC-Service instance.

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

configure > context *context_name* **> pcc-service** *service_name* **> profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

default-rulebase-name

This command is used to associate the default PCC-Rulebase with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

configure > context *context_name* **> pcc-service** *service_name* **> profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

Syntax Description

[no] default-rulebase-name *rulebase_name*

no

Removes the configured default PCC-Rulebase from PCC-Service-Profile instance on IPCF node.

rulebase_name

This keyword specifies the default PCC-Rulebase name to be associated with PCC-Service-Profile instance.

rulebase_name is the Rulebase name configured at PCEF and must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to associate the default PCC-Rulebase configured on PCEF with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Example

Following command associates the PCC-Rulebase named *pcc_rulebase1* for PCC-Profile instance on IPCF node.

default-rulebase-name *pcc_rulebase1*

eval-priority

This command sets the priority for evaluation of PCC-Condition-Group with corresponding PCC-Action-Set in a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

configure > context *context_name* **> pcc-service** *service_name* **> profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

Syntax Description

```
[no] eval-priority last action-set actionset_name
[no] eval-priority priority_value timedef timedef_name [condition-group
cond_grp_name] action-set actionset_name
[no] eval-priority priority_value condition-group cond_grp_name action-set
actionset_name
```

no

Removes the configured evaluation priority for PCC-Condition-Group with corresponding PCC-Action-Set from PCC-Service-Profile instance on IPCF node.

last

Sets last evaluation priority action-set configured for the PCC-Service-Profile instance.

no removes the last evaluation priority action-set.

priority_value

Specifies the priority to be set for PCC-Condition-Group with corresponding PCC-Action-Set in a PCC-Service-Profile instance.

priority_value must be an integer from 1 through 1023.

timedef *timedef_name*

Specifies a pre-configured time definition in *PCC-Timedef Configuration mode* and to be set for evaluation priority in a PCC-Service-Profile instance.

timedef_name is a pre-configured PCC-Timedef and must be an alphanumerical string of 1 through 63 characters.

condition-group *cond_grp_name*

Specifies a pre-configured PCC-Condition-Group to be set for evaluation priority in a PCC-Service-Profile instance.

cond_grp_name is a pre-configured PCC-Condition-Group and must be an alphanumerical string of 1 through 63 characters.

Important An special PCC-Condition-Group "none" can be used to set the default PCC-Condition-Group for **any-match** typically used for a default condition for a session which does not match any of the conditions specified with higher evaluation priority.

action-set *actionset_name*

Specifies a pre-configured PCC-Action-Set for PCC-Condition-Group to be set for evaluation priority in a PCC-Service-Profile instance.

actionset_name is a pre-configured PCC-Action-Set and must be an alphanumerical string of 1 through 63 characters.

Usage Guidelines

Use this command to set the priority for evaluation of PCC-Condition-Group with corresponding PCC-Action-Set in a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Additionally **timedef** is used to accept the Timedefs to support the time-of-day-based procedures to trigger an evaluation priority. The action is triggered only when the time of session lies in the time span defined in specific PCC-Timedef *timedef_name*.

Default **eval-priority** has the lowest priority in the PCC-Service-Profile and as default **eval-priority** does not have any PCC-Condition-Group associated with it, all the actions in the **action-set** always be applied.

A maximum of 64 PCC-Evaluation-Priorities can be configured in a PCC-Service-Profile.

Example

Following command sets the evaluation priority value as *1* for PCC-Condition-Group *cond_1* along with PCC-Action-Set *act_cond1* for PCC-Service-Profile instance on IPCF node:

eval-priority *1* **condition-group** *cond_1* **action-set** *act_cond1*

Following command sets the evaluation priority value as *2* for PCC-Condition-Group *none* for **any-match** typically used for a default condition for a session which does not match any of the conditions specified with higher evaluation priority.along with PCC-Action-Set *act_cond1* for PCC-Service-Profile instance on IPCF node:

eval-priority *1* **condition-group** *none* **action-set** *act_cond1*

service-tag

This command configures the PCC-Service Tags to be used for PCC-Rulename or PCC-Rule-base in a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

configure > context *context_name* **> pcc-service** *service_name* **> profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

Syntax Description

[no] service-tag *svc_tag* {**rule-name** *rule_name* | **rulebase-name** *rulebase_name*}

no

Removes the configured PCC-Service Tags for PCC-Rulename and PCC-Rulebase from PCC-Service-Profile instance on IPCF node.

svc_tag

Specifies the name of the PCC-Service Tag to be used for PCC-Rulename and PCC-Rulebase in a PCC-Service-Profile instance.

svc_tag must be an alphanumerical string of 1 through 63 characters.

rule-name *rule_name*

Specifies a pre-defined PCC-Rulename on PCEF to be used with PCC-Service Tag *svc_tag* in a PCC-Service-Profile instance.

rule_name is a pre-defined PCC-Rulename on PCEF and must be an alphanumerical string of 1 through 63 characters.

rulebase-name *rulebase_name*

Specifies a pre-defined PCC-Rulebase name pre-defined on PCEF to be used with PCC-Service Tag *svc_tag* in a PCC-Service-Profile instance.

rulebase_name is a pre-defined PCC-Rulebase name on PCEF and must be an alphanumerical string of 1 through 63 characters.

Usage Guidelines

Use this command to set the PCC-Service Tag for PCC-Rulename and PCC-Rulebase which are defined on PCEF with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance.

Example

Following command sets the PCC-Service Tag named *Rule1* for PCC-Rulebase named *pcc_rulebase1* for PCC-Service-Profile instance on IPCF node:

```
service-tag Rule1 rulebase-name pcc_rulebase1
```

Following command sets the PCC-Service Tag named *Rule11* for PCC-Rulename *pcc_rule1* for PCC-Service-Profile instance on IPCF node:

```
service-tag Rule11 rule-name pcc_rule1
```

timeout long-duration

Configures the long duration timeout and inactivity duration for subscriber session before system notifies or terminates session in PCC Profile instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

configure > context *context_name* **> pcc-service** *service_name* **> profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

Syntax Description

```
timeout long-duration ldt_timeout [action {detection | disconnect}]
no timeout long-duration
default timeout long-duration
```

no

Removes the configured long duration timeout value and action in PCC Profile instance.

default

Sets the the long duration timeout value to the default value of '0' which disables the long duration timeout configuration in PCC Profile instance.

long-duration *ldt_timeout*

Default: 0

Designates the maximum duration of the session, in seconds, before the system automatically reports/terminates the session.

Specifies the maximum amount of time, in seconds, before the specified timeout action is activated.

ldt_timeout must be a value in the range from 0 through 4294967295.

The special value 0 disables the timeout specified.

action {detection | disconnect}

Default: Detection

Specifies the action to be taken on expiry of long duration timeout duration *ldt_timeout* set with **timeout long-duration** command.

- **detection**: sets the system to detect the sessions for which long duration timeout timer is exceeded and sends the SNMP TRAP and CORBA notification. This is the default behavior.
- **disconnect**: sets the system to send SNMP TRAP and CORBA notification and disconnect the subscriber session once the long duration timeout timer is expired.

Usage Guidelines

Use this command to set the long duration timeout period and actions to be taken on expiry of duration of timer for subscriber session.

Important Reduce the timeout duration to free session resources faster for use by new requests.

Important In case of long-duration timeout configured at PCC Service Configuration mode as well as at the PCC-Profile Configuration mode level, the long-duration timeout and action set in PCC-Profile Configuration mode will prevail. This enables defining session behavior as per profile provisioning.

Example

Following command sets the system to detect the subscriber sessions that exceeds the long duration timer of 6000 seconds and sends SNMP TRAP and CORBA notification:

```
timeout long-duration 6000 action detection
```

Following command sets the system to detect and disconnect the subscriber sessions that exceeds the long duration timer of 6000 seconds and disconnect the session after sending SNMP TRAP and CORBA notification:

```
timeout long-duration 6000 action disconnect
```

usage-monitor

This command creates/modifies/deletes the PCC-Usage-Monitor Configuration instance to track the usage volume across the PCC-services based on the usage monitor settings in a PCC-service instance for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

Syntax Description

```
[no] usage-monitor usage_mon_name [-noconfirm]
```

no

Removes the configured PCC-Usage-Monitor from PCC-Service-Profile instance for IPCF configuration.

usage_mon_name

Identifies the name of the PCC-Usage-Monitor instance which is to be created or modified through this command.

The *usage_mon_name* must be an alphanumerical string from 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Caution If this keyword option is used with **no usage-monitor** *usage_mon_name* command, the PCC-Usage-Monitor instance named *usage_mon_name* is deleted with all configured parameters without prompting any warning or confirmation.

Usage Guidelines

Use this command to create and configure a PCC-Usage-Monitor for PCC-Service-Profile in a PCC-service instance of IPCF configuration.

A maximum number of 8 PCC-Usage-Monitors can be configured per PCC-Service-Profile.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-profile-usage-mon)#
```

The commands configured in this mode are defined in the *PCC-Usage-Monitor Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution This is a critical configuration. The PCC-Usage-Monitor for volume usage can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

Example

Following command configures the PCC-Usage-Monitor named *pcc_usage1* to track the usage of service with in a PCC-Service-Profile instance.

usage-monitor *pcc_usage1*

unknown-services-treatment

This command configures the PCC-Service for handling of unknown services at IPCF which is to be used in Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

configure > context *context_name* **> pcc-service** *service_name* **> profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

Syntax Description

```
[default] unknown-services-treatment {not-allowed | qos-profile qos_prof_name
 precedence from start_preced to end_preced order {ascending | descending}}
```

default

Sets the configured PCC-Service for handling of unknown services at IPCF to default value of "**Not allowed**" which is to be used in Subscriber profile in PCC-Service instance on IPCF node.

not-allowed

Sets the PCC-Service-Profile instance to reject the packet filters and does not installs any dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list.

qos-profile *qos_prof_name*

Specifies a pre-defined PCC-QoS profile name to be used to create dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list.

qos_prof_name is a pre-defined PCC-QoS Profile and must be an alphanumerical string of 1 through 63 characters.

precedence from *start_preced* to *end_preced*

Specifies the precedence parameters to install dynamic rules for selection of QoS profile when QoS profile is configured to create dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list.

start_preced is an integer between 1 through 65535 and must be less than *end_preced* value where *end_preced* is an integer between 1 through 65535 and must be more than *start_preced* value

order {ascending | descending}

Specifies the order of precedence for QoS profile to be used to install dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list.

- **ascending** sets the precedence setting in ascending order.
- **descending** sets the precedence setting in descending order.

Usage Guidelines

Use this command to set the PCC-Service Tag for PCC-Rulename and PCC-Rulebase which are defined on PCEF with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance.

Whenever IPCF receives any request to authorize Packet Filters from PCEF, it does a lookup in data service list to find a match. If **No** service flow is found matching then the requested filters are treated as **unknown service request** and handled as per the mentioned configuration.

When unknown-service-treatment is set to **not-allowed**, then Packet Filters are rejected and no dynamic rule is installed. Otherwise, dynamic rule is created using the requested packet filters, data rates mentioned in the QoS profile name *qos_prof_name* and precedence value derived from the configured values.

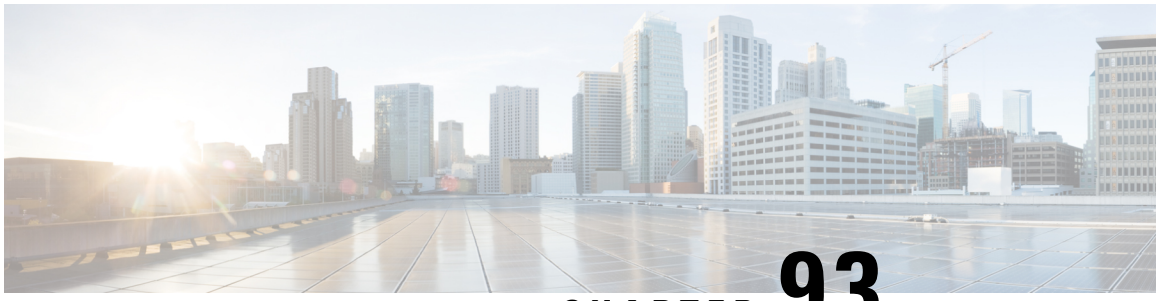
The precedence configuration works in following manner:

- If precedence limits are configured as 1000 to 2000 with order **ascending** then precedence of subsequent dynamic rules will go from 1000 to 2000.
- If precedence limits are configured as 1000 to 2000 with order **descending** then precedence of subsequent dynamic rules will go from 2000 to 1000.

Example

Following command sets the PCC-Service for handling of unknown services for PCC-Service-Profile instance on IPCF node to default action of **not allowed**:

```
default unknown-services-treatment
```



CHAPTER 93

PCC-QoS-Profile Configuration Mode Commands

Important This configuration mode is supported from StarOS Release 12.1 onward.

Command Modes

The PCC-QoS-Profile Configuration Mode is used to define the QoS logic used by the operator for managing the QoS policy requirements and objectives for the network specific to a group of subscribers in the network. A QoS Profile represents a resource requirement identified by means of the corresponding QoS attributes like QCI, MBR, GBR, ARP etc.

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC QoS Profile Configuration

configure > context *context_name* **> pcc-service** *service_name* **> qos-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-qos-profile)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

arp-priority

This command is used to define the Allocation and Retention Priority (ARP) values of the QoS profile in PCC-QoS-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC QoS Profile Configuration

configure > context *context_name* **> pcc-service** *service_name* **> qos-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-qos-profile)#
```

Syntax Description

[no] arp-priority *arp_priority* **pre-emption** {**capable** | **not-capable**} {**not-vulnerable** | **vulnerable**}

no

Removes the configured ARP priority set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

arp_priority

Specifies the priority value for ARP in a PCC-QoS-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

arp_priority must be an integer from 1 through 15.

pre-emption {capable | not-capable}

Sets the Pre-emption capability related parameters with ARP priority in PCC-QoS-Profile name which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Pre-emption capability determines whether a bearer with a lower ARP priority level should be dropped to free up the required resources.

capable: This keyword indicates that the service data flow is allowed to get resources that were already assigned to another service data flow with a lower priority level.

non-capable: This keyword indicates that the service data flow is not allowed to get resources that were already assigned to another service data flow with a lower priority level.

{not-vulnerable | vulnerable}

Sets the Pre-emption vulnerability related parameters with ARP priority in PCC-QoS-Profile name which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Pre-emption vulnerability determines whether a bearer is applicable for dropping by a pre-emption capable bearer with a higher ARP priority value.

not-vulnerable: This keyword indicates that the resources assigned to the service data flow shall not be pre-empted and allocated to a service data flow with a higher priority level.

vulnerable: This keyword indicates that the resources assigned to the service data flow can be pre-empted and allocated to a service data flow with a higher priority level.

Usage Guidelines

Use this command to define the ARP priority and pre-empt parameters in PCC-QoS-Profile which is to be used in Subscriber profile in PCC-Service instance on IPCF node.

ARP controls how the IPCF reacts when there are insufficient resources to establish the new RAB. Typically it manages it by; 1) Deny the RAB request and 2) Preempt an existing RAB and accept the new RAB request.

Example

Following command sets the ARP Priority *2* with preemption capability and vulnerability in PCC-QoS-Profile instance on IPCF node.

arp-priority *2* **pre-emption capable vulnerable**

guaranteed-bitrate

This command defines the Guaranteed Bit Rate (GBR) value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC QoS Profile Configuration

configure > context *context_name* **> pcc-service** *service_name* **> qos-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-qos-profile)#
```

Syntax Description

[no] guaranteed-bitrate downlink *downlink_gbr* **uplink** *uplink_gbr*

no

Removes the configured GBR value set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

downlink *downlink_gbr*

Sets the Guaranteed Bit Rate allowed in downlink direction (from PCEF to UE) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

downlink_gbr must be an integer from 0 through 104857600. A 'zero' value disables the downlink in specified PCC-QoS-Profile.

uplink *uplink_gbr*

Sets the Guaranteed Bit Rate allowed in uplink direction (from PCEF to PDN) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

uplink_gbr must be an integer from 0 through 104857600. A 'zero' value disables the uplink in specified PCC-QoS-Profile.

Usage Guidelines

Use this command to define the Guaranteed Bit Rate value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Example

Following command sets the *1024* bits per seconds as uplink GBR and *2048* bits per second as downlink GBR in PCC-QoS-Profile instance on IPCF node.

guaranteed-bitrate downlink *2048* **uplink** *1024*

max-bitrate

This command defines the Maximum Bit Rate (MBR) value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC QoS Profile Configuration

configure > context *context_name* **> pcc-service** *service_name* **> qos-profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pcc-qos-profile)#`

Syntax Description

[no] max-bitrate downlink *downlink_mbr* **uplink** *uplink_mbr*

no

Removes the configured Maximum Bit Rate value set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

downlink *downlink_mbr*

Sets the Maximum Bit Rate allowed in downlink direction (from PCEF to UE) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

downlink_mbr must be an integer from 0 through 104857600. A 'zero' value disables the downlink in specified PCC-QoS-Profile.

uplink *uplink_mbr*

Sets the Maximum Bit Rate allowed in uplink direction (from PCEF to PDN) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

uplink_mbr must be an integer from 0 through 104857600. A 'zero' value disables the uplink in specified PCC-QoS-Profile.

Usage Guidelines

Use this command to define the Maximum Bit Rate value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Example

Following command sets the *1024* bits per seconds as uplink MBR and *2048* bits per second as downlink MBR in PCC-QoS-Profile instance on IPCF node.

max-bitrate downlink *2048* **uplink** *1024*

qci

This command sets the QoS Class Identifier (QCI) for PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC QoS Profile Configuration

configure > context *context_name* **> pcc-service** *service_name* **> qos-profile** *profile_name*

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-pcc-qos-profile)#

Syntax Description

[**no**] **qci** *qci_id*

no

Removes the configured QCI value set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

qci *qci_id*

Sets the QoS Class Identifier for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

qci_id must be an integer from 1 through 255.

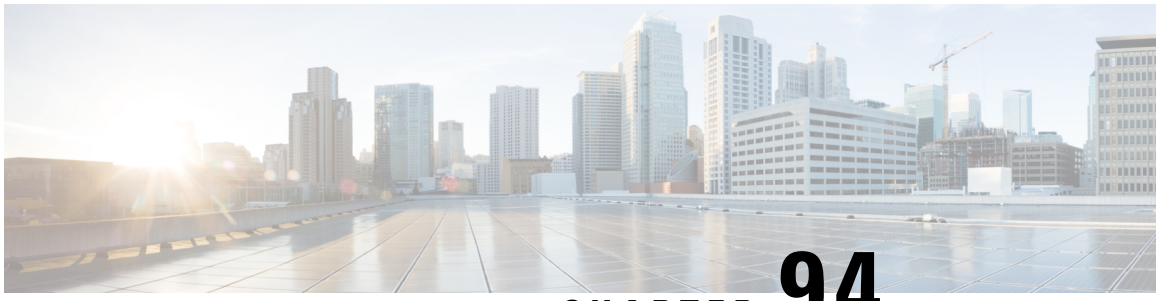
Usage Guidelines

Use this command to set the QoS Class Identifier for PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Example

Following command sets the QCI *101* for PCC-QoS-Profile instance on IPCF node.

qci *101*



CHAPTER 94

PCC-Quota Service Configuration Mode Commands

Important This configuration mode is supported from StarOS Release 12.1 onward.

Command Modes

The PCC-Quota Service Configuration mode provides a mechanism for Intelligent Policy Control Function (IPCF) to manage the external interfaces required for quota management purpose. The PCC-Quota service uses **Gx** interface towards PCEF/DPI node for Volume-Reporting-Over-Gx (VRoGx) for Quota management and messaging based on a Diameter dictionary. This mode exists within Context Configuration mode.

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Quota Service Configuration

configure > context *context_name* **> pcc-quota-service** *service_name*

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

associate pcc-service

This command is used to associate a pre-configured PCC-Service with a PCC-Quota service for IPCF configuration.

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Quota Service Configuration

configure > **context** *context_name* > **pcc-quota-service** *service_name*

Syntax Description

```
associate pcc-service pcc_service_name
[no] associate pcc-service
```

no

Removes/disassociate the configured PCC-service from this PCC-Quota service instance configured for IPCF configuration.

pcc_service_name

Specifies the name of a pre-configured PCC-service configured in Context Configuration mode for IPCF configuration.

The *pcc_service_name* is name of a predefined PCC-Service instance and must be an alphanumerical string from 1 through 63 characters.

Usage Guidelines Use this command to associate a pre-configured PCC-Service instance for IPCF configuration.

Important For more information on PCC-Service configuration, refer *PCC-Service Configuration Mode Commands*.

Example

Following command binds a PCC-Service named *pcc_svc1* with in a PCC-Quota service.

```
associate pcc-service pcc_svc1
```

Following command removes an associated PCC-Service named *pcc_svc1* from a PCC-Quota service.

```
no associate pcc-service pcc_svc1
```

diameter dictionary

This command is used to assign a 3GPP Rel. 8 Gx standard Diameter dictionary for **VRoGx** messaging with a PCC-Quota service for IPCF configuration.

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Quota Service Configuration

configure > **context** *context_name* > **pcc-quota-service** *service_name*

Syntax Description

`[no]diameter dictionary standard`

no

Removes the assigned a 3GPP Rel. 8 Gx standard Diameter dictionary for **VRoGx** messaging with a PCC-Quota service for IPCF configuration.

Usage Guidelines

Use this command to assign a 3GPP Rel. 8 Gx standard Diameter dictionary for **VRoGx** messaging in PCC-Quota service for quota management.

Example

Following command sets the PCC-Quota service to use 3GPP Rel. 8 standard dictionary over **Gx** interface and **VRoGx** supported quota management related messaging in a PCC-Quota service:

```
diameter dictionary standard
```

diameter origin end-point

This command is used to bind/associate a pre-configured Diameter host/realm (SSC/SPR) over **Sp** interface with a PCC-Quota service to be used for subscriber quota management.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Quota Service Configuration

configure > **context** *context_name* > **pcc-quota-service** *service_name*

Syntax Description

```
diameter origin endpoint dia_endpoint_name
no diameter origin endpoint
```

no

Removes the associated Diameter Origin Endpoint configuration from PCC-Quota service instance configured for IPCF configuration.

any

Sets the PCC-Quota service instance to use any available PCEF/DPI node over **Sp** interface for quota management.

dia_endpoint_name

The *dia_endpoint_name* is a predefined Diameter origin endpoint node and must be an alphanumerical string from 1 through 63 characters.

Usage Guidelines

Use this command to bind the SSC/SPR node over **Sp** interface by associating a pre-configured Diameter Origin Endpoint with a PCC-Quota service.

The Diameter origin endpoint must be a pre-configured instance in the Context Configuration Mode. For more information on Diameter origin endpoint configuration, refer *Diameter Endpoint Configuration Mode Commands* chapter.

Example

Following command associates a pre-configured Diameter endpoint node configuration named *ssc1* with a PCC-Quota service for subscriber quota management.

diameter origin endpoint*ssc1*

Following command removes the pre-associated Diameter endpoint node configuration named *ssc1* with a PCC-Quota service.

no diameter origin endpoint

max total-charging-sessions

This command is used configure the maximum limit of the charging sessions allowed in a PCC-Quota service instance on IPCF.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Quota Service Configuration

configure > context *context_name* **> pcc-quota-service** *service_name*

Syntax Description

max total-charging-sessions *max_session*
default max total-charging-sessions

default

Sets the maximum charging sessions allowed in PCC-Quota service instance to default value of charging sessions.

max_session

Default: 1

Specifies the maximum number of charging sessions configured in PCC-Quota service to allow to be connected in PCC-Quota service instance.

max_session must be an integer between 0 and 113.

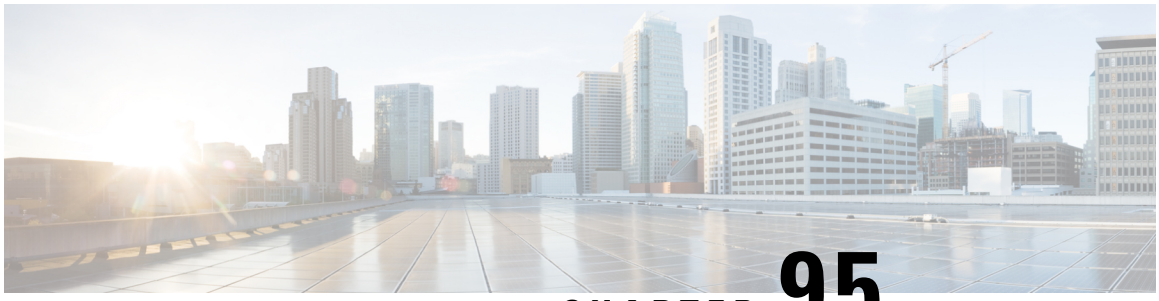
Usage Guidelines

Use this command to set the maximum number of charging sessions allowed by a PCC-Quota service instance on IPCF.

Example

Following command sets the maximum number of charging sessions allowed in PCC-Quota service instance to 10000.

```
default max total-charging-sessions
```



CHAPTER 95

PCC-Sp-Endpoint Configuration Mode Commands

Important This configuration mode is supported from StarOS Release 12.1 onward.

Command Modes

The PCC-Sp-Endpoint Configuration mode provides a mechanism for Intelligent Policy Control Function (IPCF) to support the **Sp** interface endpoint. It represents a client end for SSC interactions. The PCC-Sp-Endpoint configuration mode facilitates the configuration of **Sp** interface, and manages the connection and operational parameters related to its peer.

Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

configure > context *context_name* **> pcc-sp-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

access-type

This command is used to define the type of access protocol to be used with a PCC-Sp-Endpoint instance for IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

configure > context *context_name* **> pcc-sp-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
access-type {diameter | ldap}
default access-type
```

default

Sets access type protocol to be used by endpoints to default protocol of **Diameter** protocol in a PCC-Sp-Endpoint instance for IPCF configuration.

diameter

Default: Enabled

Sets access type protocol to be used by endpoints to Diameter protocol in a PCC-Sp-Endpoint instance for IPCF configuration.

ldap

Default: Disabled

Sets access type protocol to be used by endpoints to Lightweight Directory Access Protocol (LDAP) in a PCC-Sp-Endpoint instance for IPCF configuration.

Usage Guidelines

Use this command to define the type of access protocol to be used with a PCC-Sp-Endpoint instance for IPCF configuration.

Example

Following command sets the access type of protocol to **Diameter** for a PCC-Sp-Endpoint instance.

```
default access-type
```

diameter dictionary

This command is used to assign a Diameter dictionary for interaction with SSC and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

configure > context *context_name* **> pcc-sp-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`diameter dictionary {sh-custon-starent | sh-custom2 | sh-standard }`
`default diameter dictionary`

default

Sets the Diameter **Sh** dictionary to default dictionary **sh-custon-starent** (3GPP Rel. 8 Sh standard) for **Sh** interaction and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration.

sh-custom-starent

Default: Enabled

Sets the Diameter **Sh** dictionary to default dictionary **sh-custom-starent** for **Sh** interaction and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration.

sh-custom2

Default: Disabled

Sets the Diameter **Sh** dictionary to **sh-custom2**with Cisco ULI AVP support for **Sh** interaction and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration.

sh-standard

Default: Disabled

Sets the Diameter **Sh** dictionary to default dictionary **sh-standard** (3GPP Rel. 8 standard) for **Sh** interaction and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration.

Usage Guidelines

Use this command to assign a Diameter dictionary for **Sh** interaction and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration.

Example

Following command sets the Diameter dictionary for **Sh** interaction and messaging over **Sp** interface in a PCC-Sp-Endpoint instance of IPCF configuration to 3GPP Rel. 8 standard.

diameter dictionary sh-standard

diameter origin end-point

This command is used to bind/associate a pre-configured Diameter host/realm (SSC) over **Sp** interface for SPR interactions with a PCC-Sp-Endpoint instance to be used for subscriber profile and policy management.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

configure > context *context_name* **> pcc-sp-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter origin endpoint *ssc_node_name*
no diameter origin endpoint

no

Removes the associated Diameter Origin Endpoint configuration from PCC-Sp-Endpoint instance configured for IPCF configuration.

ssc_node_name

The *ssc_node_name* is a predefined Diameter origin endpoint node (SSC) and must be an alphanumerical string from 1 through 63 characters.

Usage Guidelines

Use this command to bind the SSC node over **Sp** interface by associating a pre-configured Diameter Origin Endpoint configuration with a PCC-Sp-Endpoint instance.

The Diameter origin endpoint must be a pre-configured instance in the Context Configuration Mode. For more information on Diameter origin endpoint configuration, refer *Diameter Endpoint Configuration Mode Commands* chapter.

Example

Following command associates a pre-configured Diameter endpoint node configuration named *ssc_1* with a PCC-Sp-Endpoint instance for subscriber policy profile management.

diameter origin endpoint *ssc_1*

Following command removes the pre-associated Diameter endpoint node configuration named *ssc_1* from a PCC-Sp-Endpoint instance.

no diameter origin endpoint

diameter peer-select

This command nominates primary and secondary Diameter peers amongst the peers configured under Diameter Endpoint Configuration instance which is associated with a PCC-Sp-Endpoint configuration.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

configure > context *context_name* **> pcc-sp-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter peer-select peer *pri_peer_name* **[row-precedence** *row_prec_name* **selection-condition imsi {mcc** *mcc-string* **[mnc** *mnc-string*] **[msin** *msin-string*] | **mnc** *mnc-string* **[msin** *msin-string*] | **msin** *msin-string*}] **[realm** *realm_name*] **[secondary-peer** *sec_peer_name* **[realm** *sec_realm_name*]]
no diameter peer-select
no diameter peer-select row-precedence

no

To remove all the configuration parameters.

To remove a particular selection-condition, a row-precedence value is specified.

peer *pri_peer_name*

Sets a configured Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, as **primary** in Diameter peer selection process for IPCF configuration.

The *pri_peer_name* is a pre-configured Diameter peer in Diameter Endpoint configuration which is associated with a PCC-Sp-Endpoint configuration and must be an alphanumerical string from 1 through 63 characters. *pri_peer_name* allows punctuation marks.

row-precedence *row_prec_name*

The row-precedence decides order of evaluation of the selection conditions.

The *row_prec_name* is an integer between 1 and 63. Lower the value, higher is the priority of evaluation.

selection-condition

The selection-condition parameter is used to define Diameter SPR peer selection conditon.

imsi

It indicates that the selection condition is based on subscriber IMSI.

mcc *mcc-string*

It indicates that the selection condition is based on MCC component of subscriber IMSI.

The *mcc-string* can have one of the following formats: *mccval1* or *mccval1-mccval2*. The first format compares single MCC value and second one incorporates the range with mccval1 <= mccval2.

The values for both mccval1 and mccval2 must be between 100 to 999.

mnc *mnc-string*

It indicates that the selection condition is based on MNC component of subscriber IMSI.

The *mnc-string* can have one of the following formats: *mncval1* or *mncval1-mncval2*. The first format compares single MNC value and second one incorporates the range with mncval1 <= mncval2.

The values for both mncval1 and mncval2 must be between 1 to 999.

msin *msin-string*

It indicates that the condition is based on MSIN component of subscriber IMSI.

The *msin-string* can have following format: *msinval1-msinval2*. The format incorporates the range with mccval1 <= mccval2.

The values for both mccval1 and mccval2 must be of maximum of 10 digits.

realm *realm-name*

This keyword optionally defines the realm (domain) of a configured **primary** Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, in Diameter peer selection process for IPCF configuration.

realm_name is the realm (domain) of the associated primary Diameter peer in Diameter Endpoint configuration which associated with a PCC-Sp-Endpoint configuration. The *realm_name* must be an alpha and/or numeric string of 1 to 127 characters. The realm may typically be a company or service name and it allows punctuation marks.

secondary-peer *sec_peer_name*

Sets a configured Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, as **secondary** in Diameter peer selection process for IPCF configuration.

The *sec_peer_name* is a pre-configured Diameter peer in Diameter Endpoint configuration which is associated with a PCC-Sp-Endpoint configuration and must be an alphanumerical string from 1 through 63 characters. *sec_peer_name* allows punctuation marks.

realm *sec_realm-name*

This keyword optionally defines the realm (domain) of a configured **secondary** Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, in Diameter peer selection process for IPCF configuration.

sec_realm_name is the realm (domain) of the associated primary Diameter peer in Diameter Endpoint configuration which associated with a PCC-Sp-Endpoint configuration. The *sec_realm_name* must be an alpha and/or numeric string of from 1 to 127 characters. The realm may typically be a company or service name and it allows punctuation marks.

Usage Guidelines

Use this command to nominate primary and secondary Diameter peers amongst the peers configured under Diameter Endpoint Configuration instance which is associated with a PCC-Sp-Endpoint configuration. When both primary and secondary are down, the remaining Diameter peers are chosen based on their configured weight in round robin manner.

When row-precedence and selection-conditions are not defined for peer selection configuration, the row precedence value is assumed to be 64 (which is the lowest). This is a deafult peer selection when all the other configured selection conditions fail.

Multiple Diameter peers can be configured in a PCC-Sp-Endpoint instance by entering this command multiple times.

Example

Assume the operator has two MCC-MNC combinations: 123-456 and 123-457 respectively for subscriber IMSI values. If operator wishes to divert subscribers with these two different combinations to different SSC peers (say ssc123456 and ssc123457) then the operator needs to use following commands under PCC-Sp-Endpoint :

```
diameter peer-select row-precedence 4 selection-condition imsi mcc 123 mnc
 456 peer ssc123456
diameter peer-select row-precedence 6 selection-condition imsi mnc 123 mnc
 456 peer ssc223457
```

Following command nominates a pre-configured Diameter peer *dia1* as primary and *dia2* as secondary for Diameter peer selection process in a PCC-Sp-Endpoint configuration instance.

```
diameter peer-select peer dia1 secondary peer dia2
```

profile-data

This command allows the operator to specify data-reference and service indication AVP values used in UDR/SNR message for profile data sent over **Sp** endpoint when access type is set to Diameter.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

configure > context *context_name* **> pcc-sp-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
profile-data key data-reference data_ref_value [service-indication svc_ind_value]
default profile-data key
```

default

Specifies the data-reference value used in UDR/SNR message for profile data sent over **Sp** endpoint to default value of '*0*' (zero) and service indication AVP value to *profile data* when access type is set to Diameter in PCC-Sp-Endpoint instance.

data-reference *data_ref_value*

Default: 0

Specifies the data-reference values used in UDR/SNR message for profile data sent over **Sp** endpoint when access type is set to Diameter in PCC-Sp-Endpoint instance.

The data reference value *data_ref_value* must be an integer from 1 through 65535.

service-indication *svc_ind_value*

Specifies the service indication AVP value used in UDR/SNR message for profile data sent over **Sp** endpoint when access type is set to Diameter in PCC-Sp-Endpoint instance.

Important The Service-Indication values are set as per application logic and are supposed to be used only with SSC.

The service indication value *svc_ind_value* must be a string of alpha and/or numeric characters from 1 to 32 characters.

Usage Guidelines

Use this command to allow the operator to specify data-reference and service indication AVP values used in UDR/SNR message for profile data sent over **Sp** endpoint when access type is set to Diameter in PCC-Sp-Endpoint configuration instance.

Default service-indication value varies as per other interface configuration **default profile-data key** is used to set the service indication value.

Example

Following command set the data-reference value used in UDR/SNR message for profile data sent over **Sp** endpoint to default value of '*0*' (zero) and service-indication value as per application logic when access type is set to Diameter in PCC-Sp-Endpoint instance.

```
default profile-data key
```

profile-update-notification

This command sets the system to indicate whether SSC and IPCF are capable of supporting profile update notifications in a PCC-Sp-Endpoint instance.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

configure > **context** *context_name* > **pcc-sp-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
profile-update-notification {allow | disallow}
default profile-update-notification
```

default

Set the PCC-Sp-Endpoint instance default mode for supporting profile update notifications in a PCC-Sp-Endpoint instance and also to use the same in a PCC-Sp-Endpoint configuration instance.

allow

Default: Enabled

Set the PCC-Sp-Endpoint instance to support the profile update notifications and also allow to use the same in **Sp** interaction.

disallow

Default: Disabled

Set the PCC-Sp-Endpoint instance to not to support the profile update notifications and also does not allow to use the same in **Sp** interaction.

Usage Guidelines

Use command to set to indicate whether SSC and IPCF are capable of supporting profile update notifications in a PCC-Sp-Endpoint instance. It also sets that whether profile update notification should be used or not for a PCC-Sp-Endpoint configuration instance.

Example

Following command indicates that SSC and IPCF are capable of supporting profile update notifications in a PCC-Sp-Endpoint instance and also allow to use it for a PCC-Sp-Endpoint configuration instance.

```
default profile-update-notification
```

spr subscriber identifier

This command sets the PCC-Sp-Endpoint instance to indicate how a subscriber is uniquely identified in SPR database while requesting subscriber data from SSC.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

configure > **context** *context_name* > **pcc-sp-endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
spr subscriber identifier {imsi | msisdn | nai}
default spr subscriber identifier
```

default

Sets the PCC-Sp-Endpoint instance to use subscriber IMSI to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.

imsi

Default: Enabled

Sets the PCC-Sp-Endpoint instance to use subscriber IMSI to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.

msisdn

Default: Disabled

Sets the PCC-Sp-Endpoint instance to use subscriber MSISDN to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.

nai

Default: Disabled

Sets the PCC-Sp-Endpoint instance to use Network Address Identifier as token to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.

This token facilitates CDMA users for Policy Control and Charging functions.

Usage Guidelines

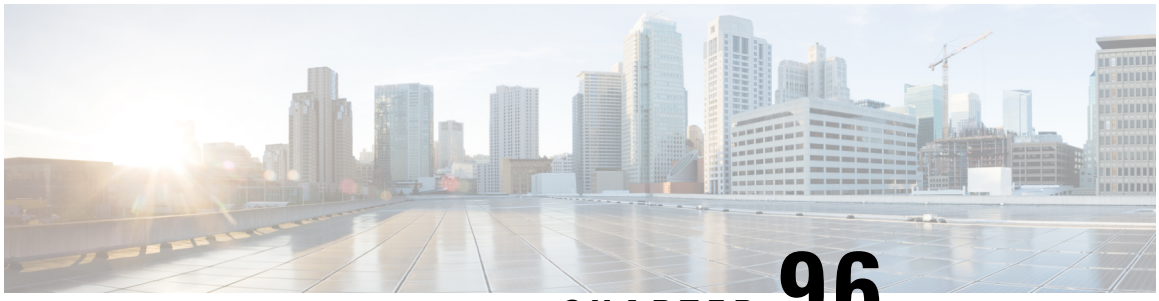
Use command to set the PCC-Sp-Endpoint instance to indicate how a subscriber is uniquely identified in SPR database on SSC while requesting subscriber data. By default it uses Subscriber IMSI for identification in SPR database.

For IP-CAN session between PDSN and IPCF the subscriber token NAI facilitates the Policy Control and Charging functions to subscribers.

Example

Following command sets the PCC-Sp-Endpoint instance to use a subscriber IMSI to uniquely identified in SPR database at SSC.

```
default spr subscriber identifier
```



CHAPTER 96

PCC-Service Addon Configuration Mode Commands

The PCC-Service Configuration Mode is used to link, consolidate and manage the policy logic for the network. The Addon mode specifies the commands related to addon instances for PCC-service.

Important This configuration mode is supported from StarOS Release 15.0 onwards.

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > Addon Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **addon** *addon_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-addon)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

associate-addon-state

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > Addon Configuration

configure > context *context_name* **> pcc-service** *service_name*> **addon** *addon_name*

Syntax Description

associate-addon-state {**expired** | **grace** | **not-started** | **started**} {**action-set** *act_set_name* [**notification-template** *not_temp_name*] | **notification-template** *not_temp_name*}
no associate-addon-state {**expired** | **grace** | **not-started** | **started**}

no

Removes the configured associated addon state from this PCC service addon instance for IPCF configuration.

expired

grace

not-started

started

action-set *act_set_name*

The *act_set_name* must be an alphanumerical string from 1 through 63 characters.

notification-template *not_temp_name*

Usage Guidelines

Use this command to create/remove/configure an action-set in a PCC-service instance for IPCF Configuration.

An Action-set indicates the policy and charging as well as event generation related decisions that will get activated when the corresponding *Condition-Group* is evaluated to *TRUE* within a subscriber policy/profile.

A maximum of 512 PCC-Action-Sets can be configured in 1 instance of PCC-Service.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-action-set)
```

Important For more information on PCC-Action-Set configuration, refer *PCC-Action-Set Configuration Mode Commands*.

Example

Following command creates a PCC-action-set named *pcc_act1* with in a PCC-service.

action-set *pcc_act1*

Following command removes a pre-configured PCC-action-set named *pcc_act1* from a PCC-service.

no action-set *pcc_act1*

description

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > Addon Configuration

configure > context *context_name* **> pcc-service** *service_name*> **addon** *addon_name*

Syntax Description

action-set *act_set_name* [**-noconfirm**]
no action-set *act_set_name*

no

Removes the configured PCC-Action-Set from this PCC-service instance for IPCF configuration.

act_set_name

Identifies the name of the PCC-Action-Set which is to be created or modified through this command.

The *act_set_name* must be an alphanumerical string from 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create/remove/configure an action-set in a PCC-service instance for IPCF Configuration.

An Action-set indicates the policy and charging as well as event generation related decisions that will get activated when the corresponding *Condition-Group* is evaluated to *TRUE* within a subscriber policy/profile.

A maximum of 512 PCC-Action-Sets can be configured in 1 instance of PCC-Service.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-action-set)
```

Important For more information on PCC-Action-Set configuration, refer *PCC-Action-Set Configuration Mode Commands*.

Example

Following command creates a PCC-action-set named *pcc_act1* with in a PCC-service.

action-set *pcc_act1*

Following command removes a pre-configured PCC-action-set named *pcc_act1* from a PCC-service.

no action-set *pcc_act1*

duration

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > Addon Configuration

configure > context *context_name* **> pcc-service** *service_name*> **addon** *addon_name*

Syntax Description

action-set *act_set_name* [**-noconfirm**]
no action-set *act_set_name*

no

Removes the configured PCC-Action-Set from this PCC-service instance for IPCF configuration.

act_set_name

Identifies the name of the PCC-Action-Set which is to be created or modified through this command.

The *act_set_name* must be an alphanumerical string from 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create/remove/configure an action-set in a PCC-service instance for IPCF Configuration.

An Action-set indicates the policy and charging as well as event generation related decisions that will get activated when the corresponding *Condition-Group* is evaluated to *TRUE* within a subscriber policy/profile.

A maximum of 512 PCC-Action-Sets can be configured in 1 instance of PCC-Service.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-action-set)
```

Important For more information on PCC-Action-Set configuration, refer *PCC-Action-Set Configuration Mode Commands*.

Example

Following command creates a PCC-action-set named *pcc_act1* with in a PCC-service.

action-set *pcc_act1*

Following command removes a pre-configured PCC-action-set named *pcc_act1* from a PCC-service.

no action-set *pcc_act1*

status active

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > Addon Configuration

configure > context *context_name* **> pcc-service** *service_name*> **addon** *addon_name*

Syntax Description

action-set *act_set_name* [**-noconfirm**]
no action-set *act_set_name*

no

Removes the configured PCC-Action-Set from this PCC-service instance for IPCF configuration.

act_set_name

Identifies the name of the PCC-Action-Set which is to be created or modified through this command.

The *act_set_name* must be an alphanumerical string from 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create/remove/configure an action-set in a PCC-service instance for IPCF Configuration.

An Action-set indicates the policy and charging as well as event generation related decisions that will get activated when the corresponding *Condition-Group* is evaluated to *TRUE* within a subscriber policy/profile.

A maximum of 512 PCC-Action-Sets can be configured in 1 instance of PCC-Service.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-pcc-action-set)

Important For more information on PCC-Action-Set configuration, refer *PCC-Action-Set Configuration Mode Commands*.

Example

Following command creates a PCC-action-set named *pcc_act1* with in a PCC-service.

action-set *pcc_act1*

Following command removes a pre-configured PCC-action-set named *pcc_act1* from a PCC-service.

no action-set *pcc_act1*

time-allowance

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > Addon Configuration

configure > context *context_name* **> pcc-service** *service_name*> **addon** *addon_name*

Syntax Description

action-set *act_set_name* [**-noconfirm**]
no action-set *act_set_name*

no

Removes the configured PCC-Action-Set from this PCC-service instance for IPCF configuration.

act_set_name

Identifies the name of the PCC-Action-Set which is to be created or modified through this command.

The *act_set_name* must be an alphanumerical string from 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create/remove/configure an action-set in a PCC-service instance for IPCF Configuration.

An Action-set indicates the policy and charging as well as event generation related decisions that will get activated when the corresponding *Condition-Group* is evaluated to *TRUE* within a subscriber policy/profile.

A maximum of 512 PCC-Action-Sets can be configured in 1 instance of PCC-Service.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-action-set)
```

Important For more information on PCC-Action-Set configuration, refer *PCC-Action-Set Configuration Mode Commands*.

Example

Following command creates a PCC-action-set named *pcc_act1* with in a PCC-service.

action-set *pcc_act1*

Following command removes a pre-configured PCC-action-set named *pcc_act1* from a PCC-service.

no action-set *pcc_act1*

volume-allowance

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > Addon Configuration

configure > context *context_name* **> pcc-service** *service_name*> **addon** *addon_name*

Syntax Description

action-set *act_set_name* [**-noconfirm**]
no action-set *act_set_name*

no

Removes the configured PCC-Action-Set from this PCC-service instance for IPCF configuration.

act_set_name

Identifies the name of the PCC-Action-Set which is to be created or modified through this command.

The *act_set_name* must be an alphanumerical string from 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create/remove/configure an action-set in a PCC-service instance for IPCF Configuration.

An Action-set indicates the policy and charging as well as event generation related decisions that will get activated when the corresponding *Condition-Group* is evaluated to *TRUE* within a subscriber policy/profile.

A maximum of 512 PCC-Action-Sets can be configured in 1 instance of PCC-Service.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-action-set)
```

Important For more information on PCC-Action-Set configuration, refer *PCC-Action-Set Configuration Mode Commands*.

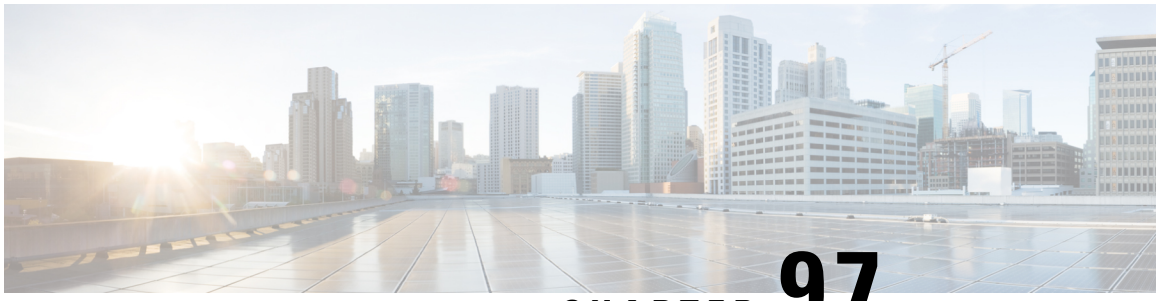
Example

Following command creates a PCC-action-set named *pcc_act1* with in a PCC-service.

action-set *pcc_act1*

Following command removes a pre-configured PCC-action-set named *pcc_act1* from a PCC-service.

no action-set *pcc_act1*



CHAPTER 97

PCC-TimeDef Configuration Mode Commands

Important This configuration mode is supported from StarOS Release 12.1 onward.

Command Modes

The PCC-TimeDef Configuration Mode is used to configure various time definitions (TimeDefs) in the PCC-service instance. A PCC-TimeDef specifies the start and end time for triggering policy-related procedures or conditions.

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC TimeDef Configuration

configure > context *context_name* **> pcc-service** *service_name* **> timedef** *timedef_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-timedef)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

start date

This command defines PCC-TimeDefs with a start and end dates with time for an event to trigger a procedure or condition in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC TimeDef Configuration

configure > context *context_name* **> pcc-service** *service_name* **> timedef** *timedef_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-timedef)#
```

Syntax Description

[no] start date *start_date* **time** *start_time* **end date** *end_date* **time** *end_time*

no

Removes the specified time definition.

date *start_date*

Specifies the start date *start_date* in *MM*/*DD*/*YY* format.

Following format is used for *MM*/*DD*/*YY* in *start_date*:

- *MM* specifies the month of the start date from January through December and must be an integer between 1 through 12.
- *DD* specifies the date of month of the start date 1 through 31 and must be an integer between 1 through 31.
- *YY* specifies the year of the start date from 2010 through 2037 and must be an integer between 10 through 37.

time *start_time*

Specifies the start time *start_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *start_time*:

- *HH* specifies the hour of the start date in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the start date must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the start date must be an integer between 00 through 59.

end date *end_date*

Specifies the end date *end_date* in *MM*/*DD*/*YY* format.

Following format is used for *MM*/*DD*/*YY* in *end_date*:

- *MM* specifies the month of the end date from January through December and must be an integer between 1 through 12.
- *DD* specifies the date of month of the end date 1 through 31 and must be an integer between 1 through 31.
- *YY* specifies the year of the end date from 2010 through 2037 and must be an integer between 10 through 37.

time *end_time*

Specifies the end time *end_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *end_time*:

- *HH* specifies the hour of the end date in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the end date must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the end date must be an integer between 00 through 59.

Usage Guidelines

Use this command to define a PCC-TimeDef with a start and end dates with time for an event to trigger a procedure or condition in an IP-CAN session.

Example

The following command defines a PCC-TimeDef with start date as December 31st 2010 at 00 Hrs. 30 mins. and 00 seconds and end date as January 31st 2011 at 23 Hrs. 59 mins. and 59 seconds:

```
start date 12/31/10 time 00 30 00 end date 01/31/11 time 23 59 59
```

start day

This command defines PCC-TimeDefs with a start and end week days with time for an event to trigger a procedure or condition in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC TimeDef Configuration

configure > context *context_name* **> pcc-service** *service_name* **> timedef** *timedef_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-timedef)#
```

Syntax Description

```
[no] start day start_weekdays time start_time end day end_weekdays time end_time
```

no

Removes the specified time definition.

day *start_weekdays*

Specifies the start day as week days.

Following days are used as *start_weekdays*:

- **friday** specifies Friday of the week as start day.
- **monday** specifies Monday of the week as start day.
- **saturday** specifies Saturday of the week as start day.
- **sunday** specifies Sunday of the week as start day.

- **thrusday** specifies Thursday of the week as start day.
- **tuesday** specifies Tuesday of the week as start day.
- **wednesday** specifies Wednesday of the week as start day.

time *start_time*

Specifies the start time *start_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *start_time*:

- *HH* specifies the hour of the start day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the start day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the start day must be an integer between 00 through 59.

end day *end_weekdays*

Specifies the end day as week days.

Following days are used as *end_weekdays*:

- **friday** specifies Friday of the week as end day.
- **monday** specifies Monday of the week as end day.
- **saturday** specifies Saturday of the week as end day.
- **sunday** specifies Sunday of the week as end day.
- **thrusday** specifies Thursday of the week as end day.
- **tuesday** specifies Tuesday of the week as end day.
- **wednesday** specifies Wednesday of the week as end day.

time *end_time*

Specifies the end time *end_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *end_time*:

- *HH* specifies the hour of the end day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the end day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the end day must be an integer between 00 through 59.

Usage Guidelines

Use this command to define a PCC-TimeDef with a start and end weekdays with time for an event to trigger a procedure or condition in an IP-CAN session.

Example

The following command defines a PCC-TimeDef with start day as Friday at 00 Hrs. 30 mins. and 00 seconds and end day as Sunday at 23 Hrs. 59 mins. and 59 seconds:

```
start day friday time 00 30 00 end day sunday time 23 59 59
```

start time

This command defines PCC-TimeDefs with a start and end time of a day for an event to trigger a procedure or condition in an IP-CAN session.

Product IPCF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC TimeDef Configuration

configure > context *context_name* **> pcc-service** *service_name* **> timedef** *timedef_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-timedef)#
```

Syntax Description **[no] start time** *start_time* **end time** *end_time*

no

Removes the specified time definition.

time *start_time*

Specifies the start time *start_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *start_time*:

- *HH* specifies the hour of the day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the day must be an integer between 00 through 59.

end time *end_time*

Specifies the end time *end_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *end_time*:

- *HH* specifies the end hour of the day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the end hour of the day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the end hour must be an integer between 00 through 59.

Usage Guidelines Use this command to define a PCC-TimeDef with a start and end time for an event to trigger a procedure or condition in an IP-CAN session.

Example

The following command defines a PCC-TimeDef with start at 00 Hrs. 30 mins. and 00 seconds and end at 23 Hrs. 59 mins. and 59 seconds:

```
start time 00 30 00 end time 23 59 59
```

time-slot

This command defines PCC-TimeDefs with a start and end week days with time for an event to trigger a procedure or condition in an IP-CAN session.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC TimeDef Configuration

configure > **context** *context_name* > **pcc-service** *service_name* > **timedef** *timedef_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-timedef)#
```

Syntax Description

[no] time-slot *slot_num* **{ start date** *start_date* **time** *start_time* **end date** *end_date* **time** *end_time* **| start day** *start_weekdays* **time** *start_time* **end day** *end_weekdays* **time** *end_time* **| start time** *start_time* **end time** *end_time*
[no] time-slot *slot_num*

no

Removes the specified time slot definition.

slot_num

Specifies the time slot number to be configured with this command and it must be an integer between 1 through 64.

date *start_date*

Specifies the start date *start_date* in *MM*/*DD*/*YY* format.

Following format is used for *MM*/*DD*/*YY* in *start_date*:

- *MM* specifies the month of the start date from January through December and must be an integer between 1 through 12.
- *DD* specifies the date of month of the start date 1 through 31 and must be an integer between 1 through 31.
- *YY* specifies the year of the start date from 2010 through 2037 and must be an integer between 10 through 37.

time *start_time*

Specifies the start time *start_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *start_time*:

- *HH* specifies the hour of the start date in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the start date must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the start date must be an integer between 00 through 59.

end date *end_date*

Specifies the end date *end_date* in *MM*/*DD*/*YY* format.

Following format is used for *MM*/*DD*/*YY* in *end_date*:

- *MM* specifies the month of the end date from January through December and must be an integer between 1 through 12.
- *DD* specifies the date of month of the end date 1 through 31 and must be an integer between 1 through 31.
- *YY* specifies the year of the end date from 2010 through 2037 and must be an integer between 10 through 37.

time *end_time*

Specifies the end time *end_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *end_time*:

- *HH* specifies the hour of the end date in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the end date must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the end date must be an integer between 00 through 59.

day *start_weekdays*

Specifies the start day as week days.

Following days are used as *start_weekdays*:

- **friday** specifies Friday of the week as start day.
- **monday** specifies Monday of the week as start day.
- **saturday** specifies Saturday of the week as start day.
- **sunday** specifies Sunday of the week as start day.
- **thrusday** specifies Thursday of the week as start day.
- **tuesday** specifies Tuesday of the week as start day.
- **wednesday** specifies Wednesday of the week as start day.

time *start_time*

Specifies the start time *start_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *start_time*:

- *HH* specifies the hour of the start day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the start day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the start day must be an integer between 00 through 59.

end day *end_weekdays*

Specifies the end day as week days.

Following days are used as *end_weekdays*:

- **friday** specifies Friday of the week as end day.
- **monday** specifies Monday of the week as end day.
- **saturday** specifies Saturday of the week as end day.
- **sunday** specifies Sunday of the week as end day.
- **thrusday** specifies Thursday of the week as end day.
- **tuesday** specifies Tuesday of the week as end day.
- **wednesday** specifies Wednesday of the week as end day.

time *end_time*

Specifies the end time *end_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *end_time*:

- *HH* specifies the hour of the end day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the end day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the end day must be an integer between 00 through 59.

time *start_time*

Specifies the start time *start_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *start_time*:

- *HH* specifies the hour of the day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the hour of the day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the day must be an integer between 00 through 59.

end time *end_time*

Specifies the end time *end_time* in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *end_time*:

- *HH* specifies the end hour of the day in 24 hour format and must be an integer between 00 through 23.
- *MIN* specifies the minutes of the end hour of the day must be an integer between 00 through 59.
- *SS* specifies the seconds of the minute of the end hour must be an integer between 00 through 59.

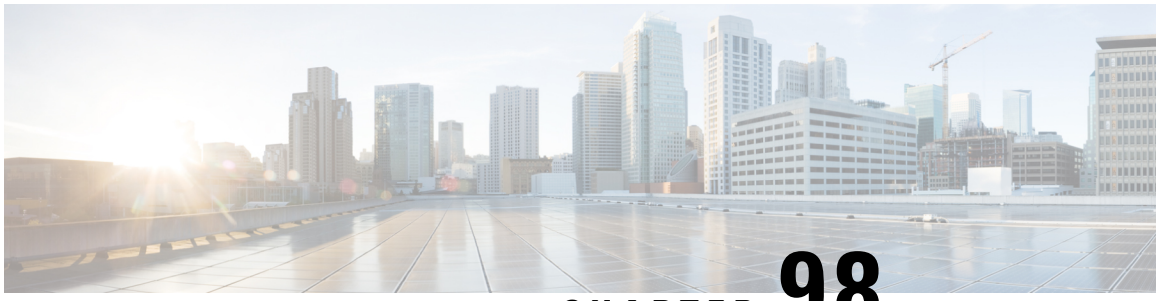
Usage Guidelines

Use this command to define a time slot with a start day, start time, and start date optiion for an event to trigger a procedure or condition in an IP-CAN session. A maximum of 12 time-slots can be configured through this command.

Example

The following command defines a time slot 2 which will start on Friday at 00:30:00 and ends on Saturday at 23:00:00:

```
start day friday start time 00 30 00 end day saturday time 23 00 00
```



CHAPTER 98

PCP Configuration Mode Commands

The Port Control Protocol Service Configuration Mode is used to manage Port Control Protocol (PCP) service related configurations.

Important This configuration mode is customer specific. For more information, contact your Cisco account representative.

Command Modes

Exec > ACS Configuration > Port Control Protocol Service Configuration

active-charging service *service_name* > **pcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-pcp-service)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

policy-control

This command enters the PCP Policy Control Configuration mode to configure policy control parameters for PCP service.

Important This command is customer specific. For more information, contact your Cisco account representative.

Product

ACS

NAT

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Port Control Protocol Service Configuration

active-charging service *service_name* **> pcp-service** *service_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-pcp-service)#`

Syntax Description

[default] policy-control

default

Configures this command with the default setting.

Default: Enabled

Usage Guidelines

Use this command to enter the PCP Policy Control Configuration Mode to configure the policy control parameters for the PCP service.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-pcp-policy-control)#

Also see the *PCP Policy Control Configuration Mode Commands* chapter.

server

Configures the IP address of the PCP server to receive PCP packets.

Important This command is customer specific. For more information, contact your Cisco account representative.

Product

ACS

NAT

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Port Control Protocol Service Configuration

active-charging service *service_name* **> pcp-service** *service_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-pcp-service)#`

Syntax Description

```
server ipv4-address ipv4_address [ port port_number ]
no server ipv4-address
```

server *ipv4_address*

Specifies the IPv4 address of the server to receive PCP packets.

ipv4_address must be specified using the IPv4 dotted-decimal notation.

port *port_number*

Specifies the UDP port number where PCP Request messages are received by the PCP service.

port_number must be an integer from 1 through 65535.

Default: 5351

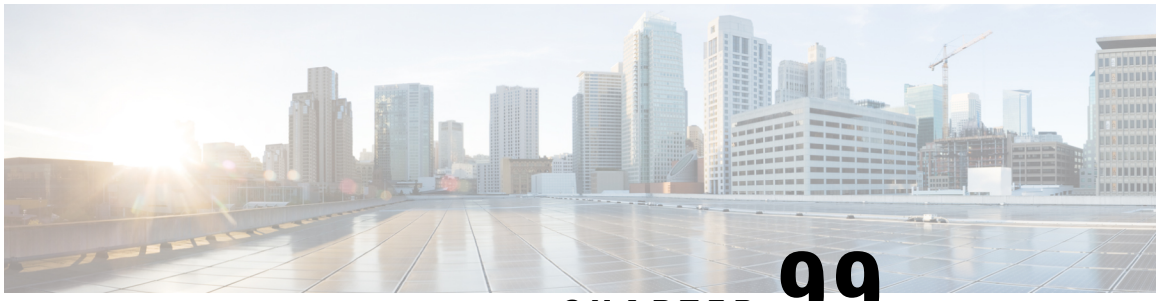
Usage Guidelines

Use this command to configure the IPv4 address on which the PCP service will receive PCP packets and the port on which PCP Request messages will be received from the PCP service.

Example

The following command configures the IPv4 address *209.165.200.228* with port number *5351* for the PCP service:

```
server ipv4-address 209.165.200.228 port 5351
```



CHAPTER 99

PCP Policy Control Configuration Mode Commands

The PCP Policy Control Configuration Mode is used to manage PCP policy control related configurations.

Important This configuration mode is customer specific. For more information, contact your Cisco account representative.

Command Modes

Exec > ACS Configuration > PCP Configuration > Port Control Protocol Service Policy Control Configuration

active-charging service *service_name* **> pcp-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-pcp-policy-control)#
```

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

request-opcode

This command allows you to configure various PCP Request Opcode options.

Important This command is customer specific. For more information, contact your Cisco account representative.

Product

ACS

NAT

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > PCP Configuration > Port Control Protocol Service Policy Control Configuration

active-charging service *service_name* **> pcp-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-pcp-policy-control)#
```

Syntax Description

```
[ no ] request-opcode [ announce | map [ filter | prefer-failure ] | peer
 ] +
default request-opcode [ announce | map | peer ] +
```

no

Deletes the specific PCP opcode settings.

announce

Configures PCP ANNOUNCE opcode to process Announce Request messages.

map [filter | prefer-failure]

Configure PCP MAP opcode to process MAP Request messages.

- **filter**: MAP opcode received with this option contains remote IP/port. Processing will be the same as MAP without option but NAT binding will be 5-tuple if remote port is non-zero or 4-tuple if remote port is zero.
- **prefer-failure**: MAP opcode received with this option contains mapping IP/port which will be non-zero. Processing will be the same as MAP without option but if NAT binding allocation fails with the suggested mapping IP/port, then error will be returned.

peer

Configures PCP PEER opcode to process Peer Request messages.

Usage Guidelines

Use this command to configure various PCP Request Opcode options.

response-opcode

This command allows you to configure various PCP Response Opcode options.

Product

ACS

NAT

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > PCP Configuration > Port Control Protocol Service Policy Control Configuration

active-charging service *service_name* **> pcp-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-pcp-policy-control)#
```

Syntax Description

response-opcode { map | peer } [error { long life-time *long_life_time* **| short life-time** *short_life_time* **} | success life-time** *succ_life_time* **] +**
{ default | no } response-opcode [map | peer] +

default

Configures this command with its default setting.

map

Configures the lifetime for which Map mappings are available.

peer

Configures the lifetime for which Peer mappings are available.

error { long life-time *long_life_time* | short life-time *short_life_time* }

Configures the lifetime for long and short error cases, in seconds.

long_life_time and *short_life_time* must be an integer from 30 through 7200.

success life-time *succ_life_time*

Configures the lifetime for successful long and short cases, in seconds.

succ_life_time must be an integer from 30 through 7200.

peer

Configures this command with its default setting.

Usage Guidelines

Use this command to configure the PCP Response Opcode options.

Example

The following command configures the MAP opcode with lifetime for long and short error cases set to *600* and *30* respectively:

response-opcode map error long life-time 600 short life-time 30

CHAPTER 100

PDIF Service Configuration Mode Commands

The PDIF Service Configuration Mode is used to configure the properties required for a mobile station to interface with a Packet Data Interworking Function (PDIF).

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

aaa attribute

Sets the system attributes for AAA messages.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa attribute { 3gpp2-bsid string | 3gpp2-service-option integer |
calling-station-id integer  | 3gpp2-serving-pcf ip-address }
no aaa attribute
default aaa attribute 3gpp2-service-option integer
```

no

Removes a previously configured AAA attribute.

default

Returns the specified aaa attribute to the original default system settings.

3gpp2-bsid *string*

Specifies the base-station ID and consists of the SID + NID + CELLID.

string must contain 12 hexadecimal upper-case ASCII characters.

3gpp2-service-option *integer*

Specifies the radius attribute value when sending authentication and accounting messages as an integer from 0 through 32767. Default: 4095

calling-station-id *integer*

Specifies the calling station phone number as a sequence of 1 through 15 digits.

3gpp2-serving-pcf *ip-address*

Use this command to generate attribute values without creating a new ASR 5000ASR 5500 image.

Usage Guidelines

If the RADIUS protocol is being used, accounting messages can be sent over a AAA interface to the RADIUS server.

3gpp2-serving-pcf attribute value (if configured) is sent in both RADIUS authentication and accounting messages. If the attribute value is not configured (or explicitly "not configured" using the **no** keyword), RADIUS attributes are still included with just type and length. This is because inclusion/exclusion of RADIUS attributes are still controlled through the dictionary, not via the CLI.

Example

The following command identifies the base station ID:

```
aaa attribute 3gpp2-bsid 0ab2389acb3
```

aaa authentication

Sets the aaa authentication for first and second phase authentication when multiple authentication is configured on the system.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa authentication { { first-phase | second-phase } | { context-name name
 aaa-group name } }
no aaa authentication { first-phase | second-phase }
```

no aaa authentication { first-phase | second-phase }

Removes any existing authentication configuration.

first-phase context-name *name* aaa-group *name*

Specifies the context name and the aaa group name configured in the context for the first authentication phase.

Important First phase authentication is mandatory when multiple authentication is configured on the system.

- **context-name** *name*: Specifies the context where the aaa server group is defined as an alphanumeric string of 1 through 79 characters.
- **aaa-group** *name*: Specifies the name of the aaa-group to be used for authentication as an alphanumeric string of 1 through 79 characters.

second-phase context-name *name* aaa-group *name*

Specifies the context name and the aaa group name configured in the context for the second authentication phase.

- **context-name** *name*: Specifies the context where aaa server group is defined as an alphanumeric string of 1 through 79 characters.
- **aaa-group** *name*: Specifies the name of the aaa-group to be used for authentication as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Two phase-authentication happens in IKEv2 setup for setting up the IPSec session. The first authentication uses Diameter AAA EAP method and second authentication uses RADIUS AAA authentication. The same

AAA context may be used for both authentications. PDIF service allows you to specify only a single AAA group, which could normally be used for the first authentication method.

A given AAA group only supports either Diameter or RADIUS authentication. If the NAI in the first authentication is different from NAI in the second authentication each NAI can point to a different domain profile in the PDIF. Each domain profile may be configured with each AAA group, one for Diameter and the other for RADIUS.

Example

Use the following to configure first-phase authentication for an aaa group named *aaa-10* in the PDIF context:

```
first-phase context-name pdif aaa-group aaa-10
```

bind

Binds the service IP address to a crypto template and configures the number of sessions the PDIF can support.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
bind address address { crypto-template string } [ max-sessions number ]
no bind
```

no

Removes a previously configured binding.

address

Specifies the IP address of the service.

crypto-template *string*

Specifies the name of the crypto template to be bound to the service as an alphanumeric string of 0 through 127 characters.

max-sessions *number*

Specifies the maximum number of sessions to be supported by the service as an integer from 0 to 3000000. Default: 3000000

If the max-sessions value is changed on an existing system, the new value takes effect immediately if it is higher than the current value. If the new value is lower than the current value, existing sessions remain established, but no new sessions are permitted until usage falls below the newly-configured value.

Usage Guidelines

Binds the IP address used as the connection point for establishing the IKEv2 sessions to the crypto template. It can also define the number of sessions the PDIF can support.

Example

The following command binds a service with the IP address *13.1.1.1* to the crypto template *T1* and sets the maximum number of sessions to *2000000*:

```
bind address 13.1.1.1 crypto-template T1 max-sessions 200000
```

default

Sets or restores the default condition for the selected parameter.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
default { { aaa attribute 3gpp2-service-option } |
duplicate-session-detection | hss { failure-handling
mac-address-validation-failure | mac-address-validation | update-profile
 } | ip source-violation { drop-limit | period } | setup-timeout |
subscriber name | username mac-address-stripping } }
```

aaa attribute 3gpp2-service-option

Configures the default value 4095.

duplicate-session-detection

Configures the default to be NAI-based.

hss { failure-handling mac-address-validation-failure | mac-address-validation | update-profile }

Configures the HSS server defaults:

failure-handling mac-address-validation-failure: By default, the MAC address is validated by IMS-Sh interface.

- **mac-address-validation**: By default, validating the MAC address is disabled.
- **update-profile**: By default, updating the PDIF profile is disabled.

ip source-violation { drop-limit | period }

Configures IP source-violation detection defaults.

- **drop-limit**: Default number of ip source violations permitted in detection period before the call is dropped is 10.
- **period**: Default detection period is 120 seconds.

setup-timeout

Default call setup time limit is 60 seconds.

subscriber *name*

Configures the default subscriber name. *name* is a string of 1-127 characters.

username mac-address-stripping

Default is to disable stripping the MAC address from the username.

Usage Guidelines

Configures the default settings for a given parameter.

Example

Use the following example to configure the default call setup time limit:

```
default setup-timeout
```

duplicate-session-detection

Configures the PDIF to detect duplicate call sessions using old IMSI or NAI addresses and clear old call information.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no | default ] duplicate-session-detection { imsi-based | nai-based }
```

no

Stops duplicate session detection.

default

Configures the default setting, which is NAI-based detection.

imsi-based

Configures the PDIF to detect duplicate call sessions based on the IMSI address.

nai-based

Configures the PDIF to detect duplicate call sessions based on the NAI address. This is the default setting.

Usage Guidelines

If an MS leaves the Wi-Fi coverage area and subsequently comes back online, it may initiate a new session setup procedure. After both the device authentication with HSS and the subscriber authentication with AAA server are completed, PDIF runs the internal mechanism to see whether there was any other session bound with the same IMSI. If an old session is detected, PDIF starts clearing this old session by sending a proxy-MIP Deregistration request to the HA. PDIF resumes new session setup by sending a proxy-MIP registration request. When the old session is aborted, PDIF sends Diameter STR messages and RADIUS Acct STOP messages to corresponding AAA servers.

PDIF allows duplicate session detection based on either the NAI or IMSI addresses. When detecting based on NAI, it is the first-phase (device authentication) NAI that is used.

Example

The following command configures duplicate session detection to use IMSI addressing:

```
duplicate-session-detection imsi
```

hss

Configures the Home Subscriber Server (HSS) parameters.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
hss { failure-handling { { mac-address-validation-failure | update-profile
 } action { terminate | continue } } | update-profile |
mac-address-validation }
[ no | default ] hss { failure-handling | update-profile |
mac-address-validation }
```

no

Removes a previously configured HSS profile.

default

Resets the defaults for this command.

failure-handling mac-address-validation-failure

Configures how the HSS is to handle errors.

If HSS returns a list of MAC addresses and if PDIF fails to match the subscriber MAC address against the list, the session is always terminated.

action { continue | terminate }

Configures the action to be performed depending on the failure type.

- **continue**: Ignores a mac-address-validation-failure and continue the session.
- **terminate**: Terminates the session on a mac-address-validation-failure.

mac-address-validation

If mac-address-validation is enabled, the PDIF queries the HSS for a list of MAC addresses associated with the Mobile Directory Number (MDN). Default: Disabled

update-profile

Update the HSS with the subscriber profile. Default: Disabled

Usage Guidelines

An HSS provides MAC address validation and store part of the subscriber profile. This command enables or disables validation and profile updates, and configures how the system responds to failures: terminate or continue a session.

An ims-sh-service and Diameter interface need to be configured to communicate with the HSS.

Example

The following example enables *mac-address* validation:

```
hss mac-address-validation
```

ims-sh-service

Associates the IMS-Sh-service parameters.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

ims-sh-service name *name*
no ims-sh-service name *name*

no

Removes a previously configured IMS-Sh-service.

name

Names the IMS-Sh-service in the pdif-service context.

Usage Guidelines

This command is used to name the IMS-Sh-service.

Example

The following command names the IMS-Sh-service ims1:

ims-sh-service name imsi1

ip source-violation

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

Source validation requires that the source address of the received packets matches the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

ip source-violation { **clear-on-valid-packet** | **drop-limit** *num* | **period** *secs* }
no ip source-violation clear-on-valid-packet

clear-on-valid-packet

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

drop-limit *num*

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

num is an integer from 1 to 1000000. Default: 10

period *secs*

Sets the length of time (in seconds) for a source violation detection period to last.

If *secs* is not specified, the value is set to the default.

secs is an integer from 1 to1000000. Default: 120

Usage Guidelines

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

This function operates in the following manner:

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

For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The period timer continues to count throughout this process.

Example

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

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

mobile-ip

Sets the MIP FA context for the specific PDIF service.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
mobile-ip foreign-agent context string [ fa-service string ]
no mobile-ip
```

no

Removes previously configured parameters.

foreign-agent context *string*

Specifies the context name in which the FA is configured as an alphanumeric string of 1 through 79 characters.

fa-service *string*

Specifies the name of the FA service in the FA context as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Shows in which context the FA is located and names the FA service.

Example

This command configures MIP for the FA context named *fa1*:

```
mobile-ip foreign-agent context fa1
```

setup-timeout

Configures the maximum time allowed to set up a session.

Product

PDIF

Privilege

Security-Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
setup-timeout integer
default setup-timeout
```

setup-timeout *integer*

Specifies the session setup timer (in seconds) as an integer from 2 through 300. Default: 60

default setup-timeout

Defaults the session setup timer to 60 seconds.

Usage Guidelines

PDIF clears both user session and tunnels if a call does not initiate successfully before the timer expires.

Example

The following command sets the setup-timeout to the default 30 seconds:

```
default setup-timeout
```

username

Configures mac-address-stripping on a username coming in from a mobile station session.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
username mac-address-stripping
[ default | no ] username mac-address-stripping
```

username mac-address-stripping

Configures mac-address stripping from the Network Access Identifier (NAI).

default

Configures the default parameter which is **disabled**.

no

Returns the configuration to the default condition.

Usage Guidelines

When enabled, PDIF strips the MAC address from a mobile username NAI before sending to the RADIUS AAA server.

Example

The following example disables mac-address-stripping.

```
no username mac-address-stripping
```

CHAPTER 101

PDG Service Configuration Mode Commands

The PDG Service Configuration Mode is used to specify the properties required for the UEs in the WLAN (Wireless Local Access Network) to interface with the Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG).

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

aaa attribute

Sets the attributes that the system uses in AAA messages.

Product PDG/TTG

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa attribute { 3gpp-negotiated-qos-profile string }
no aaa attribute
```

3gpp-negotiated-qos-profile *string*

Specifies the 3GPP negotiated QoS profile to use in AAA messages during IMS emergency call handling as an alphanumeric string of 1 through 31 characters.

no aaa attribute

Removes a previously configured AAA attribute.

Usage Guidelines Specifies the 3GPP negotiated QoS profile to use in AAA messages during IMS emergency call handling.

Example

The following command specifies the 3GPP negotiated QoS profile to use during IMS emergency call handling:

```
aaa attribute 3gpp-negotiated-qos-profile 100
```

associate sgtp-service

Identifies the SGTP service to be associated with the PDG service to enable TTG functionality on the PDG/TTG. TTG functionality supports GTP-C (GTP control plane) messaging and GTP-U (GTP user data plane) messaging between the TTG and the GGSN over the Gn' interface.

Important This command can be used before the associated service instance is created and configured but care should be used to match the service names.

Product PDG/TTG

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] associate sgtp-service` *`sgtp_service_name`* **`[ context`** *`sgtp_context_name`* **`]`**

no

Removes the service association definition from the configuration.

sgtp-service *sgtp_service_name*

Specifies which SGTP service configuration, by naming the SGTP service instance, to associate with this PDG service.

sgtp_service_name is an alphanumeric string of 1 through 63 characters with no spaces.

context *sgpt_context_name*

Defines the context in which the SGTP service was created. If no context is specified, the current context is used.

sgtp_context_name is an alphanumeric string of 1 through 63 characters with no spaces.

Usage Guidelines

Use this command to associate the SGTP service to be associated with the PDG service to enable TTG functionality on the PDG/TTG.

Example

The following command associates SGTP service *sgtp_service_1* with this PDG service:

```
associate sgtp-service sgtp_service_1 context sgtp_context_1
```

certificate-selection

Configures the PDG/TTG to select the trusted certificate (and the private key for calculating the AUTH payload) to be included in the first IKE_AUTH message from the PDG/TTG based on the APN (Access Point Name). The selected certificate is associated with the APN included in the IDr payload of the first IKE_AUTH message from the UE.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] certificate-selection apn-based
default certificate-selection
```

certificate-selection apn-based

Selects a trusted certificate for the first IKE-AUTH message based on the APN.

no certificate-selection

Disables APN-based certificate selection and resumes sending a certificate bound to a crypto template.

default certificate-selection

Sets the default certificate selection method to a certificate bound to a crypto template.

Usage Guidelines

Configures the PDG/TTG to select the trusted certificate to be included in the first IKE_AUTH message based on the APN.

Example

Use the following example to enable APN-based certificate selection:

```
certificate-selection apn-based
```

bind

Binds the PDG service IP address to a crypto template and specifies the maximum number of sessions the PDG service supports.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] bind address` *`ipv4_address`* **`{ crypto-template`** *`string`* **`} mode { ttg | pdg } [ max-sessions`** *`number`* **`]`**

no

Removes a previously configured binding.

bind address *ipv4_address*

Specifies the IPv4 address of the PDG service with which the UE attempts to establish an IKEv2/IPSec tunnel. This address must be a valid IP address within the context.

This is a mandatory parameter.

crypto-template *string*

Specifies the name of the crypto template to be bound to the PDG service. This is the name of the IPSec policy to be used as a template for PDG/TTG subscriber session IPSec policies. The crypto template includes most of the IPSec and IKEv2 parameters for keepalive, lifetime, NAT-T, and cryptographic and authentication algorithms. There must be one crypto template per PDG service.

This is a mandatory parameter.

string is an alphanumeric string of 0 through 127 characters.

mode { ttg | pdg }

Default: There is no default value.

Specifies whether the PDG service provides TTG or PDG functionality, as follows:

- In TTG mode, PDN connectivity is provided through the GGSN. PDG functionality is provided by the combined TTG and GGSN.
- In PDG mode, PDN connectivity and PDG functionality are provided directly through the PDG service.

This is a mandatory parameter.

Important PDG mode is not supported in this software release.

Dependencies:

When you configure the PDG service to be in TTG mode, you must also configure the SGTP service using the **associate sgtp-service** command, as the TTG needs to connect with the GGSN to complete the PDG functionality.

The following behaviors occur when the PDG service operates in TTG mode:

- If the SGTP service associated with PDG service is not configured, the PDG service is not started.
- If the SGTP service associated with PDG service is not started, the PDG service is not started.
- If the SGTP service associated with PDG service is stopped, the PDG service is stopped.
- If the SGTP service associated with PDG service is re-started, the PDG service is re-started.
- If the SGTP service is not yet configured, whenever the SGTP service is started, the PDG service is started.

Note that starting or stopping the PDG service has no impact on the SGTP service.

max-sessions *number*

Specifies the maximum number of sessions to be supported by the PDG service as an integer from 0 through 1000000. Default: 1000000

If the max-sessions value is changed on an existing system, the new value takes effect immediately if it is higher than the current value. If the new value is lower than the current value, existing sessions remain established, but no new sessions are permitted until usage falls below the newly-configured value.

Usage Guidelines

Use this command in PDG Service Configuration Mode to bind the IP address used as the connection point for establishing IKEv2/IPSec sessions to a crypto template. You can also use it to define the maximum number of sessions the PDG service supports.

Example

The following command binds a PDG service with an IP address of *209.165.200.228* to the crypto template *crypto_template_1*, sets the mode to TTG, and sets the maximum number of sessions to *500000*:

```
bind address 209.165.200.228 crypto-template crypto_template_1 mode ttg
max-sessions 500000
```

ip gnp-qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Gn' interface in the uplink direction.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ip gnp-qos-dscp { background *dscp* **| conversational***dscp* **| interactive** *dscp* **| streaming** *dscp* **| interactive [traffic-handling-priority** *traffic_priority* **] { allocation-retention-priority** *allocation_retention_priority* **} } +**
default ip gnp-qos-dscp

no

Disables the overriding of the ToS (Type of Service) field and enables the pass-through option.

background *dscp*

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP background class, in which the data transfer is not time-critical (for example, in e-mail exchanges). This traffic class is the lowest QoS.

dscp: Sets the DSCP for the specified traffic class. See the *dscp* section below.

conversational *dscp*

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP conversational class, in which there is a constant flow of traffic in both the uplink and downlink direction. This traffic class is the highest QoS.

dscp: Sets the DSCP for the specified traffic pattern. See the dscp section below.

interactive [traffic-handling-priority *traffic_priority*]

Specifies the DSCP marking to be used for packets of sessions subscribed to three possible traffic priorities in the 3GPP interactive class, in which there is an intermittent flow of packets in the uplink and downlink direction. This traffic class has a higher QoS than the background class, but not as high as the streaming class.

traffic_priority is the 3GPP traffic handling priority and can be the integers 1, 2 or 3.

allocation-retention-priority *allocation_retention_priority*

Specifies the DSCP for the interactive class if the allocation priority is present in the QoS profile.

allocation-retention-priority can be the integers 1, 2, or 3.

DSCP uses the values in the following table based on the traffic handling priority and allocation/retention priority if the allocation priority is present in the QOS profile.

Allocation Priority	1	2	3
Traffic Handling Priority			
1	ef	ef	ef
2	af21	af21	af21
3	af21	af21	af21

Important If you only configure DCSP marking for interactive traffic classes without specifying ARP, it may not properly take effect. The CLI allows this scenario for backward compatibility however, it is recommended that you configure all three values.

streaming *dscp*

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP streaming class, in which there is a constant flow of data in either in the uplink or downlink direction. This traffic class has a higher QoS than the interactive class, but not as high as the conversational class.

dscp: Set the DSCP for the specified traffic pattern. See the dscp section below.

dscp

Default:

- background: be
- interactive
- Traffic Priority 1: ef
- Traffic Priority 1: af21
- Traffic Priority 1: af21
- streaming: af11
- conversational: ef

Specifies the DSCP for the specified traffic pattern. *dscp* can be configured to any one of the following:

- af11: Assured Forwarding 11 per-hop-behavior (PHB)
- af33: Assured Forwarding 33 PHB

- af12: Assured Forwarding 12 PHB
- af13: Assured Forwarding 13 PHB
- af21: Assured Forwarding 21 PHB
- af22: Assured Forwarding 22 PHB
- af23: Assured Forwarding 23 PHB
- af31: Assured Forwarding 31 PHB
- af32: Assured Forwarding 32 PHB
- af41: Assured Forwarding 41 PHB
- af42: Assured Forwarding 42 PHB
- af43: Assured Forwarding 43 PHB
- be: Best effort forwarding PHB
- ef: Expedited forwarding PHB

+

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

Usage Guidelines

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they're tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the Gn' interface(s).

The four traffic patterns have the following order of precedence: background (lowest), interactive, streaming, and conversational (highest). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

Drop Precedence	Class			
	Class 1	Class 2	Class 3	Class 4
Low	af11	af21	af31	af41
Medium	af12	af22	af32	af41
High	af13	af23	af33	af43

Precedence (low to high)	DSCP
1	Best Effort (be)
2	Class 1
3	Class 2
4	Class 3
5	Class 4
6	Express Forwarding (ef)

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

Example

The following command configures the DSCP level for the streaming traffic pattern to be ef:**ip gnp-qos-dscp streaming ef**

The following command configures the DSCP levels for the conversational, streaming, interactive and background traffic patterns to be ef, af22, and af41, respectively:**ip gnp-qos-dscp conversational ef streaming ef interactive af22 background af41**

ip qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Wu interface in the downlink direction.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip qos-dscp { qci { 1 { dscp-pt } | 2 { dscp-pt } | 3 { dscp-pt } | 4 { dscp-pt } | 5
 { allocation-retention-priority 1..3 | dscp-pt } | 6 { allocation-retention-priority 1..3
 | dscp-pt } | 7 { allocation-retention-priority 1..3dscp | dscp-pt } | 8 {
allocation-retention-priority 1..3 | dscp-pt } | 9 { dscp-pt } + }
no ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 { allocation-retention-priority 1..3 | dscp-pt
 } | 6 { allocation-retention-priority 1..3 | dscp-pt } | 7 { allocation-retention-priority
 1..3 | dscp-pt } | 8 { allocation-retention-priority 1..3 | dscp-pt } | 9 {+
```

allocation-retention-priority

Specifies the DSCP for interactive class if the allocation priority is present in the QOS profile.

allocation-retention-priority can be the integers 1, 2, or 3.

DSCP values use the following matrix to map based on traffic handling priority and Alloc/Retention priority if the allocation priority is present in the QOS profile.

The following table shows the DSCP value matrix for *allocation-retention-priority*.

Table 5: Default DSCP Value Matrix

	Allocation Priority 1	Allocation Priority 2	Allocation Prior
Traffic Handling Priority			
1	ef	ef	ef
2	af21	af21	af21

	Allocation Priority 1	Allocation Priority 2	Allocation Priority 3
3	af21	af21	af21

qci

Configures the QCI attribute of QoS. Here the *qci_val* is the QCI for which the negotiate limit is being set, it ranges from 1 to 9.

dscp

Default QCI:

- 1: ef
- 2: ef
- 3: af11
- 4: af11
- 5: ef
- 6: ef
- 7: af21
- 8: af21
- 9: be

Specifies the DSCP for the specified traffic pattern. *dscp* can be configured to any one of the following:

• **af11:** Assured Forwarding 11 per-hop-behavior (PHB)	• **af32:** Assured Forwarding 32 PHB
• **af12:** Assured Forwarding 12 PHB	• **af33:** Assured Forwarding 33 PHB
• **af13:** Assured Forwarding 13 PHB	• **af41:** Assured Forwarding 41 PHB
• **af21:** Assured Forwarding 21 PHB	• **af42:** Assured Forwarding 42 PHB
• **af22:** Assured Forwarding 22 PHB	• **af43:** Assured Forwarding 43 PHB
• **af23:** Assured Forwarding 23 PHB	• **be:** Best effort forwarding PHB
• **af31:** Assured Forwarding 31 PHB	• **ef:** Expedited forwarding PHB

+

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

Usage Guidelines

You can assign DSCP to specific traffic patterns to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the outer IP header of every GTP data packet. The diffserv marking of the inner IP header is not modified.

The traffic patterns are defined by QCI (1 to 9). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

Table 6: Class structure for assured forwarding (af) levels

Drop Precedence	Class			
	Class 1	Class 2	Class 3	Class 4
Low	af11	af21	af31	af41
Medium	af12	af22	af32	af41
High	af13	af23	af33	af43

Table 7: DSCP Precedence

Precedence (low to high)	DSCP
0	Best Effort (be)
1	Class 1
2	Class 2
3	Class 3
4	Class 4
5	Express Forwarding (ef)

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

The no ip qos command can be issued to remove a QOS setting and return it to it's default setting.

Example

The following command configures the DSCP level for QCI to be Expedited Forwarding,**ef**:

```
ip qos-dscp qci 1 ef
```

ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected, or for verifying packet routing and labeling within the network.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip source-violation { clear-on-valid-packet | drop-limit num period secs }
default ip source-violation { drop-limit num period secs }
no ip source-violation clear-on-valid-packet
```

clear-on-valid-packet

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

drop-limit *num*

Sets the maximum number of allowed IP source violations within the detection period before dropping a call. If *num* is not specified, the value is set to the default value.

num is an integer from 1 to 1000000. Default: 10

period *secs*

Sets the detection period (in seconds) for IP source violations as an integer from 1 through 1000000. If *secs* is not specified, the value is set to the default value. Default: 120

default ip source-violation { drop-limit *num* period *secs* }

Sets or restores the IP source violation detection defaults, as follows:

- **drop-limit**: Sets or restores the maximum number of IP source violations within the detection period before dropping the call to the default value of 10.
- **period**: Sets or restores the detection period for IP source violations to the default value of 120 seconds.

no ip source-violation clear-on-valid-packet

The drop-limit counters are not reset upon receipt of a properly addressed packet.

Usage Guidelines

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

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

This function operates in the following manner: When a subscriber packet is received with a source IP address violation, the system increments the IP source violation drop-limit counter and starts the timer for the IP source violation period. Every subsequent packet received with a bad source address during the IP source violation period causes the drop-limit counter to increment. For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The detection period timer continues to count throughout this process.

Example

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

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

max-tunnels-per-ue

Specifies the maximum number of IKEv2/IPSec tunnels allowed per UE by the PDG/TTG. This maximum number is specified per PDG service.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-tunnels-per-ue *integer*
default max-tunnels-per-ue

integer

Specifies the maximum number of IKEv2/IPSec tunnels allowed per UE as an integer from 1 to 11. Default: 11

default max-tunnels-per-ue

Sets the maximum number of IKEv2/IPSec tunnels allowed per UE to its default value, which is 11.

Usage Guidelines

Use this command to set the maximum number of IKEv2/IPSec tunnels allowed per UE.

Example

Use the following command to set the maximum number of IKEv2/IPSec tunnels allowed per UE to *2*:

```
max-tunnels-per-ue 2
```

plmn id

Configures location specific mobile network identifiers used to help translate local emergency and service-related numbers. Default is disabled.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

plmn id mcc *mcc_number* **mnc** *mnc_number*
no plmn id mcc *mcc_number* **mnc** *mnc_number*

mcc *mnc_number*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 200 through 999.

mnc *mnc_number*

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

no plmn id mcc *mcc_number* mnc *mnc_number*

Removes a previously configured PLMN identifier for the PDG service.

Usage Guidelines

The PLMN ID is included in the RAI (Routing Area Identity) field of the PDP Create Request messages sent to the GGSN. Multiple PDG services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each PDG service.

Example

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

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

setup-timeout

Specifies the maximum time allowed to set up a session.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDG Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

setup-timeout *integer*
default setup-timeout

setup-timeout integer

Sets the session setup timeout value (in seconds) as an integer from 2 through 300. Default: 60

default setup-timeout

Sets or restores the default session setup timer value to 60 seconds.

Usage Guidelines

The PDG/TTG clears both the user session and tunnels if a call does not initiate successfully before the session setup timer expires.

Example

The following command sets the session setup timeout value to the default value of 60 seconds:

```
default setup-timeout
```

CHAPTER 102

PDSN Service Configuration Mode Commands

The PDSN Service Configuration Mode is used to create and manage PDSN service instances for the current context.

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

a11-signalling-packets

Applies DSCP marking for IP header carrying outgoing A11-signalling packets.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

a11-signalling-packetsip-header-dscp *hexa_number*
[no | default] a11-signalling-packetsip-header-dscp

no

Disables the **a11-signalling-packets ip-header-dscp** option configuration.

default

Sets / Restores default value assigned for specified parameter **a11-signalling-packets ip-header-dscp**.

hexa_number

a Hexa decimal number between 0x0 and 0x3F.

Usage Guidelines

Use this command to configured value of DSCP to be set for all outgoing A11 signaling msg.

By default the CLI is disabled and DSCP is marked as 0 in ip-header.

Example

The following command configures value of DSCP to be set for all outgoing to A11 signaling message *0x3F*:

a11-signalling-packets ip-header-dscp *0x3F*

aaa 3gpp2-service-option

Specifies the value for the 3gpp2-service option.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa 3gpp2-service-option number
no aaa 3gpp2-service-option
default aaa 3gpp2-service-option
```

no

Disables the aaa 3gpp2-service option configuration.

default

Sets / Restores default value assigned for specified parameter **aaa 3gpp2-service-option**.

number

Service option *number* is integer and should be between *0* to *32767*.

Usage Guidelines

Allows the configuration of a default service option value to be sent in accounting when service option values are not received from PCF. The PDSN will default the service option value to the configured value if the value is not specified by the PCF.

Example

The following command sets the service option to be *40*:

```
aaa 3gpp2-service-option 40
```

aaa nas-ip-address

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa nas-ip-address IPv4 address
no aaa nas-ip-address
default aaa nas-ip-address
```

no

Disables the aaa nas-ip-address option configuration.

default

Sets / Restores default value assigned for specified parameter **aaa nas-ip-address** by default this is disabled.

ipv4 address

Specifies the IPv4 addresses to be used.

Usage Guidelines Allows the configuration.

Example

The following command configures *209.165.200.228*:

aaa as-ip-addres *209.165.200.228*

access-flow traffic-validation

If **access-flow traffic-validation** is enabled for the service and the subscriber then the flows are checked against the filter rules. If the packets does not match the filter rules, and N violations occur in K seconds, the rp connection is downgraded to best-effort flow, if it is not already a best-effort flow.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
access-flow traffic-validation [ threshold { interval seconds | violations limit } ]
no access-flow traffic-validation
default access-flow traffic-validation [ threshold { interval | violations } ]
```

no

Disable traffic validation for the service.

default

Traffic validation configuration for the service is set to the default value.

threshold { [violations *limit*] [interval *seconds*] }

violations *limit*: Sets the parameters that determine traffic access violations. This is determined by setting the maximum number of violations within a set time period. must be an integer from *1* through *100000*.

interval *seconds* Sets the time interval, in seconds. must be an integer from *1* through *100000*.

Usage Guidelines Use this command to enable traffic validation for the current PDSN service.

Example

The following command enables traffic validation for the current PDSN service and sets the limit allowed to *100* **violations** within *5* seconds:

```
access-flow traffic-validation threshold violations 100 interval 5
```

access-network

Configures access network parameters.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
access-network { accounting identifier identifier_name | realm realm_name }
no access-network { accounting identifier | realm } }
```

no

Disables the **access-network**.

accounting identifier

Configures accounting for the access-network. This value must be a string from 1 to 128 characters in length.

realm *realm_name*

Configures the realm for the access-network. *realm_name* must be a string from 1 to 128 characters in length.

Usage Guidelines Use this command to configure access-network parameters for accounting and realms.

Example

The following command creates an **access-network realm** named *realm2*.

```
access-networkrealm realm2
```

airlink bad-sequence-number

Configures PDSN behavior for airlink related parameters.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

```
airlink bad-sequence-number { accept | deny [use-deny-code {
poorly-formed-request | unsupported-vendor-id}]}
[ no | default ] airlinkbad-sequence-number
```

no

Disables the deny of bad-sequence number and accept it.

default

It is the default behavior.

accept

Accepts the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.

It is the default behavior.

deny

Rejects the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.

It uses **poorly-formed-request** option by default to deny a request.

use-deny-code { poorly-formed-request | unsupported-vendor-id }

These are optional keywords that used with **deny** sub-command to deny the A11 RRQ messages that have either an unsupported vendor Id or A11 Requests with bad/poor formation.

unsupported-vendor-id denies request on the basis of vendor Id.

poorly-formed-request will deny the A11 request on the basis of request formation or structure. It is the default deny code for **deny** sub-command.

Usage Guidelines

This command is used to configure the airlink parameters for A11 RRQs.

When configured it denies the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.

Example

The following command would configure the system to deny all A11 RRQ messages having unsupported vendor Id or bad structure of message, including those having airlink sequence number less than or equal to a previously received sequence number:

```
airlinkbad-sequence-number deny
```

allow alt-ppp

Allows proprietary modified versions of PPP type sessions to connect this PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
allowalt-ppp
no allow alt-ppp
default allow alt-ppp
```

no

Disables the allowed alternate PPP feature.

default

Sets the specified parameter to default.

Usage Guidelines

This command is used to deviate from standard PPP protocol and use a proprietary modified version of PPP with a pre-defined non-negotiable PPP parameters.

It is a vendor-specific licensed feature command.

Example

```
allow alt-ppp
```

always-on-indication

Enables/disables the inclusion of 3GPP2 Always On Indicators in messages to the PCF.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
always-on-indication
no always-on-indication
```

no

Disables the sending of 3GPP2 Always On Indication messages.

Usage Guidelines This command is available when the 3GPP2 Always-On RP Extensions feature-use license is installed.

When enabled, this command causes the PDSN service to include the Always On Indicators in the Normal Vendor Specific Extension (NVSE) part of an A11 Session Update message to the PCF. The indicator will only be sent for those subscriber sessions in which Always On functionality is enabled as determined after a successful authentication: the 3GPP2-Always-On attribute is set to a value of *1* (Active) for subscribers configured on a AAA server, or the always-on parameter is set for locally configured subscribers.

This functionality is enabled by default.

Example

Use the following command to Enables the inclusion of 3GPP2 Always On Indicators in messages to the PCF.

```
always-on-indication
```

associate

Associates a PDSN-service with a Quality of Service (QoS) policy.

Product PDSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
associate qci-qos-mapping string
no associate qci-qos-mapping
```

no

Disables the configuration to associate PDSN-serivce with qos policy.

qci-qos-mapping *string*

qci-qos-mapping configures QCI to QoS mapping for this PDSN service.

string a string of size 1 to 63.

Usage Guidelines

The following is used for configuration to associate PDSN-serivce with qos policy.

Example

```
associate qci-qos-mapping sample
```

authentication

Configures authentication parameters for specific PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
authentication { [ allow-noauth ] [ chap chap_priority ] [ mschap mschap_priority
 ] [ pap pap_priority  ] } | [  msid-auth  ]
default authentication
```

default

Configures authentication parameters for specific PDSN service.

allow-noauth

Default: Disabled

This option configures the system to provide subscribers with network access even though they have not been authenticated. This command issued by itself would cause the system to not attempt to authenticate subscribers.

When the allow-noauth option is used in conjunction with commands specifying other authentication protocols and priorities to use, then if attempts to use those protocols fail, the system will treat the allow-noauth option as the lowest priority.

If no authentication is allowed, then NAI construct will be implemented in order to provide accounting records for the subscriber.

chap *chap_priority*

Default: 1

This option configures the system to attempt to use the Challenge Handshake Authentication Protocol (CHAP) to authenticate the subscriber.

A *chap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

chap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference. CHAP is enabled by default as the highest preference.

mschap *mschap_priority*

Default: Disabled

This option configures the system to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the subscriber.

A *mschap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

mschap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference.

pap *pap_priority*

Default: 2

This option configures the system to attempt to use the Password Authentication Protocol (PAP) to authenticate the subscriber.

A *pap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

pap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference. PAP is enabled by default as the second highest preference.

msid-auth

Default: Disabled

This option configures the system to attempt to authenticate the subscriber based on their Mobile Station Identity (MSID).

Usage Guidelines

Use to specify how the PDSN service should handle authentication and what protocols to use. The flexibility is given to configure this option to accommodate the fact that not every mobile will implement the same authentication protocols.

The chassis is shipped from the factory with the authentication options set as follows:

- allow-noauth disabled
- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

Important At least one of the keywords must be used to complete the command.

Example

The following command would configure the system to allow no authentication for subscribers and would perform accounting using the default NAI-construct of *username@domain*:

```
authentication allow-noauth
```

The following command would configure the system to attempt subscriber authentication first using CHAP, then MSCHAP, and finally PAP. If the allow-noauth command was also issued, if all attempts to authenticate the subscriber using these protocols fail, then the subscriber would be allowed access:

```
authentication chap 1 mschap 2 pap 3
```

bcmcs

Sets the BCMCS (Broadcast Multicast Service) group username and password for RADIUS access.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
bcmcs { customptt | encrypted grppasswd group_passwd | flow-id value
[flow-id-type { flow-id | program-id } ] | grppasswd group_password |
grpusrnamegroup_name | ptt { destination-context dest_name |
disconnect-dscp-label dscp_label | mtu transmission_unit | rohc-profile-name
rohc_profile_name } }
default bcmcs [ custom ptt | ptt { disconnect-dscp-label | mtu |
rohc-profile-name } ]
no bcmcs { custom ptt | flow-id value [flow-id-type { flow-id | program-id }
 | grppasswd | grpusrname | ptt { destination-context | disconnect-dscp-label
 | mtu | rohc-profile-name } }
```

custom

Customise the BCMCS configuration.

flow-id *value*

Set the BCMCS flow-id. This value must be a hex string between *0x1000* and *0xFFFFFFFF*.

Making this entry opens a new mode: bcmcs-flow-id.

rohc-profile name : Configure ROHC parameters name, name should be string of size *1* to *63*.

grpusrname *group_name*

Sets the BCMCS group name for RADIUS access requests. This value must be a string from *1* to *127* characters in length.

encrypted grppasswd *group_passwd*

Set the BCMCS group password for RADIUS access requests. This value must be a string from *1* to *63* characters in length.

Password can be encrypted or clear.

ptt { destination-context *dest_name* | disconnect-dscp-label *dscp_label*| mtu *transmission_unit* | rohc-profile-name *rohc_profile_name* }

destination-context: Specify the intended destination context name. This value must be string of *1* to *79* characters in length.

disconnect-dscp-label: Configures the DSCP label to be present in the In Call Signalling packet based on which In Call Signalling and Media Flows will be disconnected. This value must be a Hexadecimal number between *0x0* and *0xFF*.

mtu *transmission_unit*: Configures maximum transmission unit, This value must be ranging from *100* to *2000*. Default is *1500*.

rohc_profile_name *rohc_profile_name*: Profile name of the ROHC compressor and decompressor. This value should be a string of *1* to *63*.

Usage Guidelines

Use this command to set the BCMCS group username and password for RADIUS access requests.

Example

```
bcmcsgrpusername group_name
bcmcsgrppasswd group_password
```

bind

Binds the PDSN service to a logical IP interface serving as the R-P interface. Specifies the maximum number of subscribers that can access this service over the interface.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

bind address *address* [**max-subscribers** *count*]
no bind address

no

Removes a previously configured binding.

address

Specifies the IP address (address) of the interface configured as the R-P interface. *address* is specified in dotted decimal notation.

max-subscribers *count*

Default: *500000*

Specifies the maximum number of subscribers that can access this service on this interface.

count can be configured to any integer value between *0* and *2500000*.

Important The maximum number of subscribers supported is dependant on the license key and the number of active PACs/PSCs installed in the system. A fully loaded system with *13* active PACs/PSCs can support *2500000* total subscribers. Refer to the license key command for additional information.

Usage Guidelines

Associate or tie the PDSN service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an R-P interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

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

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

- The total number of interfaces that you will configure for use as R-P interfaces
- The maximum number of subscriber sessions that all of the interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port (10/100Base-Tx or 1000Base-T) to which these interfaces will be bound

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

Example

The following command would bind the logical IP interface with the address of *192.168.3.1* to the PDSN service and specifies that a maximum of *600* simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind  address
```

data-available-indicator

Enables sending Data Available Indicator extension in R-P Registration Reply.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no | default] data-available-indicator

no

Default: Disabled

Disable the sending of the Data Available Indicator extension in R-P Registration Reply.

default

Sets / Restores default value assigned for specified parameter for **data-available-indicator**.

Usage Guidelines

Use this command to enable or disable the sending of the Data Available Indicator extension in R-P Registration Reply

Example

Use the following command to enable sending the Data Available Indicator extension in R-P Registration Reply:

```
data-available-indicator
```

Use the following command to disable sending the Data Available Indicator extension in R-P Registration Reply:

```
no data-available-indicator
```

data-over-signaling

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

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no | default] data-over signaling

default

Sets / Restores default value assigned for specified parameter for **data-over signaling**

no

Default: Enabled

Disable the data-over signaling feature for A10 packets.

Usage Guidelines

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

Important This is a customer-specific command.

Example

```
no data-over-signaling
```

default subscriber

Specifies the name of a subscriber profile configured within the same context as the PDSN service from which to base the handling of all other subscriber sessions handled by the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

default subscriber *profile_name*
no default subscriber

no

Enables/Disables the option **default subscriber** *profile_name*

profile_name

Specifies the name of the configured subscriber profile. *profile_name* can be between *1* and *127* alpha and/or number characters and is case sensitive.

Usage Guidelines

Each subscriber profile specifies "rules" such as permissions, PPP settings, and timeout values.

By default, the PDSN service will use the information configured for the subscriber named default within the same context. This command allows for multiple PDSN services within the same context to apply different "rules" to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.

Use the **no default subscriber** *profile_name* command to delete the configured default subscriber.

Example

To configure the PDSN service to apply the rules configured for a subscriber named *user1* to every other subscriber session it processes, enter the following command:

```
default subscriber user1
```

direct-lte-indicator

Enables sending Direct LTE Indicator VSA in Access Request.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no | default ] direct-lte-indicator
```

default

Sets / Restores default value assigned for specified parameter for **data-over signaling**

no

Default: Enabled

Disables sending Direct LTE Indicator VSA in Access Request.

Usage Guidelines

Use this command to enable or disable sending Direct LTE Indicator VSA in Access Request.

Important This is a customer-specific command.

Example

```
no direct-lte-indicator
```

dormant-transition

Configures the PDSN behavior to terminate A10 session, when the PDSN receives the A11-RRQ (Type 4) before the session for the original MN is established completely.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
[ no | default ] dormant-transition initial-session-setup
```

no

Terminates the A10 session, when PDSN receives the A11-RRQ (Type 4) before the original session established completely.

default

Keeps the A10 session live in case of A11-RRQ (Type 4) is received before the original session is established completely.

Usage Guidelines

When the status of A10 session goes to dormant before the session for the original MN is established completely, the different MN may possibly send the A11-RRQ (Type 4) to the PDSN and PPP renegotiation may start.

This command is used to terminate the A10 session when the PDSN receives the A11-RRQ (Type 4) before the session for original MN is established completely.

Example

Following command is used to release the A10 session in case of receiving A11-RRQ (Type 4) before the original session is established completely:

```
no dormant-transition  initial-session-setup
```

enhanced-pcf-redirection

Enables or disables PDSN support for enhanced PCF redirection.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdsn-service)#`

Syntax Description **`[no] enhanced-pcf-redirection`**

no

Disables PDSN support for enhanced PCF redirection.

enhanced-pcf-redirection

Enables PDSN support for enhanced PCF redirection.

Usage Guidelines Use this command to enable or disable PDSN support for enhanced PCF redirection. By default, this feature is disabled.

Important This is a customer-specific command.

Example

The following command will disable PDSN support for enhanced PCF redirection.

```
no enhanced-pcf-redirection
```

fragment

Enables or disables PPP payload fragmentation.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdsn-service)#`

Syntax Description **`[ no | default ] fragment ppp-data`**

no

Disables the fragmentation of ppp data.

default

Default enables ppp data fragmentation.

Usage Guidelines

This command is to indicate to the RP module to NOT fragment PPP payloads being sent to the PCF, if the total packet size (PPP+GRE+IP) exceeds *1500* bytes.

Disabling fragmentation may cause the **sessmgr** to perform outer IP fragmentation of the outgoing packet, if the resulting packet exceeds the MED MTU.

Example

The following command enables PPP payload fragmentation.

```
fragment ppp-data
```

gre

Configures Generic Routing Encapsulation (GRE) parameters for the A10 protocol within the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
gre { checksum | checksum-verify  | ip-header-dscp value { all-control-packets
 | setup-packets-only } | protocol-type {any | byte-stream | ppp } |
reorder-timeout value | segmentation |sequence-mode { none | reorder } |
sequence-numbers | threegppp2-ext-header qos-marking }
no gre { checksum | checksum-verify | ip-header-dscp | segmentation |
sequence-numbers | threegppp2-ext-headers qos-marking }
default gre { checksum | checksum-verify | ip-header-dscp | protocol-type |
 reorder-timeout | segmentation | sequence-mode | sequence-numbers |
threegppp2-ext-headers qos-marking }
```

no

Disables the specified functionality.

default

Restores the specified parameter to its default setting.

checksum

Default: disabled

Enables the introduction of the checksum field in outgoing GRE packets.

checksum-verify

Default: disabled

Enables verification of the GRE checksum (if present) in incoming GRE packets.

ip-header-dscp *value* { all-control-packets | setup-packets-only }

Default: Disabled

Used to configure the QoS Differentiated Services Code Point (DSCP) marking for GRE packets.

- *value* : Represents the DSCP setting. It represents the first six most-significant bits of the ToS field. It can be configured to any hex value from 0x0 through 0x3F.
- **all-control-packets** : Dictates that the DSCP marking is to be provided in all GRE control packets.
- **setup-packets-only** : Dictates that the DSCP marking is to be provided only in GRE setup packets.

protocol-type { any | byte-stream | ppp }

Specifies the protocol used fro GRE encapsulation that is acceptable to

any: Specifies that the PDSN service will accept GRE packets encapsulated using any protocol.

byte-stream: Specifies that the PDSN service will accept GRE packets only encapsulated using byte stream. Using byte stream encapsulation, PPP packets are framed at different intervals and sent.

ppp: Specifies that the PDSN service will accept GRE packets only encapsulated using the Point-to-Point Protocol (PPP). Using PPP encapsulation, PPP packets are framed at regular intervals and sent.

reorder-timeout

Default: *100*

Configures max number of milliseconds to wait before processing reordered out-of-sequence GRE packets. *milliseconds* must be an integer from *0* through *5000*.

segmentation

Default: disabled

Enables GRE Segmentation for the PDSN service.

sequence-mode { none | reorder }

Default: none

Configures handling of incoming out-of-sequence GRE packets.

none: Specifies that sequence numbers in packets are ignored and all arriving packets are processed in the order they arrive.

reorder: Specifies that out of sequence packets are stored in a sequencing queue until one of the conditions is met:

- The reorder timeout occurs: All queued packets are sent for processing and the accepted sequence number is updated to the highest number in the queue.
- The queue is full (five packets): All packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number in the queue.
- An arriving packet has a sequence number such that the difference between this and the packet at the head of the queue is greater than five. All the packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number that arrived.
- A packet arrives that fills a gap in the sequenced numbers stored in the queue and creates a subset of packets whose sequence numbers are continuous with the current accepted sequence number. This subset of packets in the queue is sent for processing. The reorder timer continues to run and the accepted sequence number is updated to the highest number in the subset delivered.

sequence-numbers

Enables insertion of GRE sequence numbers in data that is about to be transmitted over the A10 interface. Data coming into the system containing sequence numbers but that is out of sequence is not re-sequenced.

threegppp2-ext-headers qos-marking

When threegppp2-ext-headers qos-marking is enabled and the PCF negotiates capability in the A11 RRQ, the PDSN will include the qos optional data attribute in the GRE 3gpp2 extension header.

The **no** keyword, enables qos-marking in the gre header based on the tos value in the header.

Usage Guidelines

The **gre protocol-type** command can be used to prevent the PDSN service from servicing PCFs that use a specific form of encapsulation.

Use the **no gre sequence-numbers** command to disable the inclusion of GRE sequence numbers in the A10 data path.

The chassis is shipped from the factory with the authentication options set as follows:

- **protocol-type any**
- sequence-numbers enabled

Example

Use this command to configure the PDSN service to exclude byte stream encapsulated GRE traffic:

```
gre protocol-type ppp
```

inter-pdsn-handoff mobility-event-indicator

Configures the PDSN to support the Mobility Event Identifier (MEI) during inter-PDSN handoffs. The presence of the Mobility Event Indicator (MEI) and Access Network Identifier (ANID) elements in a A11 handoff request represents an Inter-PDSN handoff.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdsn-service)#`

Syntax Description

```
inter-pdsn-handoff mobility-event-indicator
no inter-pdsn-handoff mobility-event-indicator
default inter-pdsn-handoff mobility-event-indicator
```

no

Disables support for the MEI during inter-PDSN handoffs.

default

Sets / Restores default value assigned for **inter-pdsn-handoff mobility-event-indicator**. By default it is disabled.

Usage Guidelines Use this command to configure support for the MEI during inter-PDSN handoffs.

Example

Use the following command to enable support for the MEI during inter-PDSN handoffs

```
inter-pdsn-handoff  mobility-event-indicator
```

inter-pdsn-handover

Configures Inter-PDSN handoff related parameters.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdsn-service)#`

Syntax Description

```
inter-pdsn-handover use-canid-panid
no inter-pdsn-handover use-canid-panid
default inter-pdsn-handover use-canid-panid
```

no

Disables support for the MEI during inter-PDSN handoffs parameters.

default

Sets / Restores default value assigned for **inter-pdsn-handoff mobility-event-indicator**. By default it is disabled.

Usage Guidelines

Use this command to configure Inter-PDSN handoff related parameters.

Example

Use the following command to econfigure Inter-PDSN handoff related parameters.

```
inter-pdsn-handover use-canid-panid
```

ip header-compression rohc

Enters PDSN Service ROHC Configuration Mode and allows you to configure ROHC parameters that the PDSN conveys to the PCF in the initial A11 RRP message before PPP authentication.

By default, ROHC is disabled for a PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
ipheader-compression rohc
default ipheader-compression rohc
no ipheader-compression rohc
```

default

Sets all PDSN Service ROHC Configuration Mode values back to the defaults and disable ROHC for this PDSN service.

no

Disable IP header compression for this PDSN Service.

Usage Guidelines

Use this command to enter the PDSN Service ROHC Configuration Mode or disable ROHC for the current PDSN service.

Example

The following command disables ROHC for the current PDSN service and sets all of the values for commands in PDSN Service ROHC Configuration Mode back to their default settings:

```
no ip header-compression rohc
```

ip local-port

Configures the local User Datagram Protocol (UDP) port for the R-P interfaces' IP socket.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

ip local-port *number*
default ip local-port

number

Default: *699*

Specifies the UDP port number.

number can be any integer value between *1* and *65535*.

default

Designates UDP port, default value as *699*.

Usage Guidelines

Specify the UDP port that should be used for communications between the Packet Control Function (PCF) and the PDSN.

Important The UDP port setting on the PCF must match the local-port setting for the PDSN service on the system in order for the two devices to communicate.

Example

Use the following command to specify a UDP port of *3950* for the PDSN service to use to communicate with the PCF on the R-P interface:

```
iplocal-port 3950
```

ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product

PDSN

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
ip source-violation { clear-on-valid-packet | drop-limit num | period secs |
 reneg-limit num }
no ip source-violation clear-on-valid-packet
default ip source-violation { drop-limit | period | reneg-limit  }
```

no

Enables/Disables **ip source-violation clear-on-valid-packet**.

default

Configure default settings related to **ip source-violation**.

clear-on-valid-packet

Default: disabled

Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

drop-limit *num*

Default: *10*

Sets the number of allowed source violations within a detection period before forcing a call disconnect. If *num* is not specified, the value is set to the default.

num can be any integer value from *1* to *1000000*.

period *secs*

Default: *120*

The length of time, in seconds, for a source violation detection period to last. drop-limit and reneg-limit counters are decremented each time this value is reached.

The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If *secs* is not specified, the value is set to the default.

secs can be any integer value from *1* to *1000000*.

reneg-limit *num*

Default: *5*

Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If *num* is not specified, the value is set to the default.

num can be any integer value from *1* to *1000000*.

Usage Guidelines

This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDIFs PDSNs a number of times during a handoff scenario.

This function operates in the following manner:

When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.

For example, if reneg-limit is set to 5, then the system allows 5 packets with a bad source address (source violations), but on the 5th packet, it re-negotiates PPP.

If the drop-limit is set to *10*, the above process of receiving *5* source violations and renegotiating PPP occurs only once. After the second *5* source violations, the call is dropped. The period timer continues to count throughout this process.

If the configured source-violation period is exceeded at any time before the call is dropped, the reneg-limit counter is checked. If the reneg-limit counter is greater than zero (0), the reneg-limit is decremented by *1*. If the reneg-limit counter equals zero, the drop-limit is decremented by half.

Example

The following command sets the drop limit to *15* and leaves the other values at their defaults:

```
ip source-violation drop-limit 15
```

lifetime

Specifies the time that an A10 connection can exist before its registration is considered expired.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > **context** *context_name* > **pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

lifetime *time*
no lifetime
default lifetime

no lifetime

Specifies that an A10 connection can exist for an infinite amount of time.

default lifetime

Sets / Restores default value assigned for **lifetime** as 1800.

time

Default: 1800

Specifies the time that an A10 connection can exist before its registration is considered expired.

time is measured in seconds and can be configured to any integer value between *1* and *65534*.

Usage Guidelines

Set a limit to the amount of time that a subscriber session can remain up whether or not the session is active or dormant. If the lifetime timer expires before the subscriber terminates the session, their connection will be terminated automatically.

Use the **no lifetime** command to delete a previously configured lifetime setting. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the **default lifetime** command.

Example

The following command specifies a time of *3600* seconds (1 hour) for subscriber sessions on this PDSN service:

```
lifetime 3600
```

max-retransmissions

Configures the maximum number of times the PDSN service will attempt to communicate with a PCF before it marks it as unreachable.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > **context** *context_name* > **pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

max-retransmissions *count*
default max-retransmissions

default

Sets / Restores default value assigned for **max-retransmissions** as *5*.

count

Specifies the maximum number of times the PDSN service will attempt to communicate with a PCF before it marks it as unreachable.

count can be configured to any integer value between *1* and *1,000,000*.

Usage Guidelines

If the value configured for the max-retransmissions is reached the call will be dropped.

The chassis is shipped from the factory with the Internet maximum number of retransmissions set to *5*.

Example

The following command configures the maximum number of retransmissions for the PDSN service to *3*:

```
max-retransmissions 3
```

mobile-ip foreign-agent context

For Mobile IP support, specifies the context in which the FA service(s) are configured.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

mobile-ip foreign-agent context *context_name* [**fa-service** *name*]
no mobile-ip foreign-agent context

no

Enables/Disables **mobile-ip foreign-agent context**

context_name

Specifies the name of the previously configured context that facilitates the FA service(s).

context_name must be between *1* and *79* alpha or numeric characters and is case sensitive.

fa-service *name*

This optional keyword allows you to link the PDSN service to a particular FA service in the specified context. *name* is the name of the FA service to link to. *name* is a string of size *1* to *63*

Usage Guidelines

FA services on the system can be configured either in the same or different contexts from those facilitating PDSN services. When they are configured in separate contexts, this command configured with a PDSN service instructs the PDSN service to route traffic to the context facilitating the FA service.

Use the **no mobile-ip foreign-agent context** to delete a previously configured destination context.

Example

The following command instructs the PDSN service to use the context named FA-destination for FA functionality:

mobile-ip foreign-agent context *fa-destination*

mobile-ipv6

Configures Mobile IPv6 parameters within specific PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdsn-service)#`

Syntax Description

mobile-ipv6 mobile-access-gateway context *context_name* [**mag-service** *name*]

mobile-access-gateway

Configures Mobile Access Gateway (MAG) parameters within specific PDSN service.

context *context_name*

Designates name of the context in which the MAG service is configured. Must be followed by context name of MAG service.

context_name is a string of size 1 to 79.

mag-service *name*

Designates name of the MAG service in that context. Must be followed by MAG service name.

name is a string of size 1 to 63.

Usage Guidelines This command is used to configure Mobile IPv6 parameters and Mobile Access Gateway (MAG) parameters within specific PDSN service.

Example

The following command configures Mobile IPv6 parameters and Mobile Access Gateway (MAG) parameters within specific PDSN service.

mobile-ipv6 mobile-access-gateway context *pdsn1* **mag-service** *serv1*

msid length

Configures checking the length of the A11 MSID in A11 Session Specific Extn and airlink records.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdsn-service)#`

Syntax Description

msid length { [**min** *min_length*] | **max** *max_length* }
default msid length

default

Specifies the default length of MSID (*10* to *15*) as per standard. By default **msid** is disabled.

min *min_length*

Specifies the minimum length for MSID.

min_length is any Integer value between *10* to *15*, but should be less than *max_length* specified with **max**. Default is *10*.

max *max_length*

Specifies the maximum length for MSID.

max_length is any Integer value between *10* to *15*, but should be more than *min_length* specified with **min**. Default is *15*.

Usage Guidelines MSID length can be configured either in the standard length or different customized length form. This command is used to specify the allowed length of MSID.

Example

The following command specifies an MSID length between *12* and *15*:

```
msid length min 12 max 15
```

nai-construction

Specifies a domain alias that will be used to represent the context which the PDSN service should use for AAA functionality.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
nai-construction domain alias
no nai-construction domain
```

domain *alias*

Alias represents the "domain" name that you would like to associate with the context in which AAA functionality is configured. alias can be between *1* and *79* alpha and/or numeric characters and is case-sensitive.

Usage Guidelines

Enabling NAI will be constructed for the subscriber in the event that their mobile station (MS) does not negotiate CHAP, PAP, or MSCHAP. If this option is selected, no further attempts will be made to authenticate the user. Instead, the constructed NAI will be used for accounting purposes.

The context specified by this command would be used to provide the communication with the RADIUS accounting server.

Use the **no nai-constructed** domain command to deleted a configured alias.

Important This command should only be used if the PDSN service is configured to allow no authentication using the authentication allow-noauth command.

Additionally, the **aaa constructed-nai** command in the Context Configuration mode can be used to configure a password for constructed NAIs.

Example

The following command configured a domain alias of aaa_context for the PDSN service to use when an NAI is constructed for a subscriber session:

```
nai-construction domain aaa_context
```

new-call conflict

Enable or disable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

[no | default] new-call conflict terminate-session-old-pcf

no

Disable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

default

Enable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

Usage Guidelines

This configuration supports to enable or disable to send A11-RUPD to current PCF, when the system receives the A11-RRQ(Type1) from new PCF during the session exists.

If the configuration is **no new-call conflict terminate-session-old-pcf** system will not send registration update to old PCF on receiving a new call (A11-RRQ(Type1)) request for an existing active/dormant session. The default behavior is to send registration updates.

Example

The following command configured a system to send a registration update on receiving an A11-RRQ (Type 1) request for an existing active/dormant session:

```
new-call conflict terminate-session-old-pcf
```

pcf-monitor

Enables the monitoring of all the PCFs that have sessions associated with it. The PDSN stops monitoring a PCF if it is determined to be down. Once a PCF is determined to be down, the PDSN tears down all sessions that correspond to the PCF and generates AAA Accounting Stop messages. All the PCFs that are connected to the PDSN service are monitored.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
pcf-monitor[ interval seconds | max-inactivity-time seconds | num-retry num |
timeout seconds ]
 [ no | default ] pcf-monitor
```

pcf-monitor

Entering the command with no keywords enables the PCF monitoring function with all parameters set to the defaults.

no

Disables the pcf monitoring function.

default

Sets / Restores default value assigned for **pcf-monitor**.

interval *seconds*

Default: 60 seconds

Sets the amount of time to wait between ping request messages.

seconds must be an integer in the range from 1 through 3600.

max-inactivity-time *seconds*

Default: 120 seconds

The maximum amount of time (seconds) with no A10 traffic from a PCF before the ICMP-ping mechanism is triggered.

seconds must be an integer from 1 through 3600.

num-retry *num*

Default: 5

Sets the number of times that the PDSN retries to ping the PCF. When num-retry for a given PCF has been exhausted with no response, sessions that correspond to the non-responsive PCF are terminated and Accounting Stop records for each terminated session are generated.

num must be an integer in the range from 0 through 100.

timeout *seconds*

Default: 3 seconds

The amount of time to wait for a response before retrying.

seconds must be in the range from 1 through 10.

Usage Guidelines

Use this command to enable the PDSN service to monitor the PCFs that have sessions associated with the PDSN service.

Example

The following command enables PCF monitoring with parameters set to the defaults:

```
pcf-monitor
```

The following command enables PCF monitoring and sets the timeout to *10* seconds:

```
pcf-monitor timeout 10
```

The following command disables pcf-monitoring:

```
no pcf-monitor
```

pcf-session-id-change restart-ppp

Manages current session and PPP renegotiation on GRE-key change without any change in PCF/PANID/CANID. This command disables or enables the PPP renegotiation restart on receiving an RP registration request from the current PCF with GRE key (PCF session Id) change. With this command the PDSN aborts and restarts the call causing PPP renegotiation.

This is enabled by default.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
[ no | default ] pcf-session-id-change restart-ppp
```

no

Disables the pcf-session-id-change restart-ppp function.

With this option PDSN does not restart the PPP renegotiation on GRE key change from current PCF in an RP registration request, unless it indicates change in PCF/PANID/CANID.

default

Set the pcf-session-id-change function to the default state on enabled.

Usage Guidelines

GRE key (PCF session ID) is sued to identify the data packet for a session and is negotiated through the A11 signaling messages between PCF and PDSN. By default PDSN aborts and restart the PPP renegotiation on receipt of any RP registration request with change in GRE key or PCF session Id.

With use of no pcf-session-id-change restart-ppp command PDSN is configured to disable the restart of call or PPP renegotiation on receipt of any RP registration request with changed GRE key, unless it has any PCF/ANID/CANID change. PDSN silently switches the GRE key for the session, retaining the existing PPP session.

Example

The following command disables the PPP renegotiation restart action on receipt of any RP RRQ with changed GRE key from same PCF/PANID/CANID.

```
no pcf-session-id-change restart-ppp
```

pdsn type0-tft attempt-inner-match

Configures a type0 traffic flow template (tft) to a type1 traffic flow template.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

[no | default] pdsn type0-tft attempt-inner-match

no

Disables **pdsn type0-tft attempt-inner-match**.

default

Sets / Restores default value assigned for **pdsn type0-tft attempt-inner-match.**

Usage Guidelines

This CLI is used make PDSN match inner IP packets for an AIMS call. When enabled, the PDSN tries to match a type-0 tft to match both outer and inner packet, so that MN can use a Type-0 filter for HoA traffic which are tunneled.

This is disabled by default.

Example

The following command enables type0 tft:

```
pdsn type0-tft attempt-inner-match
```

peer-pcf

Configures settings for any PCF that has a connection with this PDSN.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

peer-pcf { *ip_address* | *ip_address/mask* } **bcmcs-framing** { **hdlc-like** | **segment-based** }

ip_address | *ip_address/mask*

ip_address must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6.

ip_address/mask must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6, followed by the mask.

bcmcs_framing { hdlc-like | segment-based }

Specifies the type of bcmcs_framing to use for this PCF connection.

- hdlc-like: applies HDLC-like framing for all BCMCS flows
- segment-based: applies segment-based framing for all BCMCS flows

Usage Guidelines

Use this command to configure the settings for any PCF that is connected to this PDSN. You can also specify bcmcs framing settings to use for the connection.

Example

The following command configures the peer-pcf for an IP address of *131.2.3.4*:

```
peer-pcf 131.2.3.4
```

pma-capability-indicator

Enables sending PMIP Capability Indicator VSA in Access Request.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
pma-capability-indicator [ 3gpp2 ]
[ no | default ] pma-capability-indicator
```

3gpp2

Use 3GPP2 defined VSA. Default is to use Custom1 VSA.

no

Enables/Disables sending PMIP Capability Indicator VSA in Access Request.

default

Sets / Restores default value assigned for PMIP Capability Indicator.

Usage Guidelines

Use this command to enable sending PMIP Capability Indicator VSA in Access Request.

Example

The following command enables sending PMIP Capability Indicator using 3GPP2 defined VSA in Access Request.

```
pma-capability-indicator 3gpp2
```

policy

Configures PDSN service policies.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

policy msid-match *msid_with_wildcards* **redirect** *address* [**weight** *weight_num*] [*address2* [**weight** *weight_num*]... *address16* [**weight** *weight_num*]] [**weight** *weight_num*]

no policy msid-match *msid_with_wildcards*

policy overload { **redirect** *address* [**weight** *weight_num*] [*address2* [**weight** *weight_num*] ... *address16* [**weight** *weight_num*]] | **reject** [**use-reject-code** { **admin-prohibited** | **insufficient-resources** }] }

no policy overload [**redirect** *address* [*address2* ... *address16*]]

default policy overload

policy pcf-zone-match *zone_number* **redirect** *address* [**weight** *weight_num*] [*address2* [**weight** *weight_num*] ... *address16* [**weight** *weight_num*]] | **restricted** [**redirect** *address* [**weight** *weight_num*] [*address2* [**weight** *weight_num*] ... *address16* [**weight** *weight_num*]]

no policy pcf-zone-match*zone_number*

[**default** | **no**] **policy rrq mei-from-current-pcf suppress-ppp-restart**

policy service-option enforce

[**default** | **no**] **policy service-option**

policy unknown-cvse enforce

[**default** | **no**] **policy unknown-cvse**

no

Enables/Disables the PDSN service policies.

default

Sets / Restores default value assigned for specified PDSN service policies.

policy msid-match *msid_with_wildcards* redirect *address* [weight *weight_num*] [*address2* [weight *weight_num*]... *address16* [weight *weight_num*]] [weight *weight_num*]

Specifies how a PDSN service should handle an incoming call that matches a list of wildcard MSIDs.

msid_with_wildcards: An MSID in which up to 16 digits have been replaced with the wildcard '$'. This defines the list of possible matches for incoming calls.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.

address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

policy overload { redirect *address* [weight *weight_num*] [*address2* [weight *weight_num*] ... *address16* [weight *weight_num*]] | reject [use-reject-code { admin-prohibited | insufficient-resources }] }

Specifies how a PDSN service should handle an overload condition.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.

address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

reject: This option will cause any overload traffic to be rejected. The PDSN will send an A11 Registration Reply Code of 82H (insufficient resources).

use-reject-codeadmin-prohibited: When this keyword is specified and traffic is rejected, the error code admin prohibited is returned instead of the error code insufficient resources. This is the default behavior.

use-reject-codeinsufficient-resources: When this keyword is specified and traffic is rejected, the error code insufficient resources is returned instead of the error code admin prohibited.

policy pcf-zone-match *zone_number* redirect *address* [weight *weight_num*] [*address2* [weight*weight_num*] ... *address16* [weight *weight_num*]] | restricted [redirect *address* [weight *weight_num*] [*address2* [weight *weight_num*] ... *address16* [weight *weight_num*]]]

Specifies how a PDSN service should handle an incoming call that matches a predefined zone number.

zone_number: An integer between 1 and 32 that defines the zone incoming calls must match for redirection.

redirect: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.

address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight *weight_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight_num* must be an integer from 1 through 10.

restricted: This is an optional keyword which means the zone is restricted. Restricted zone is meaningful only if enhanced PCF redirection feature is enabled, otherwise the zone follows the default behavior.

policy rrq mei-from-current-pcf suppress-ppp-restart

rrq configures policy for PPP restart after getting mei in rrq.

mei-from-current-pcf mei is received in rrq from current pcf.

suppress-ppp-restart suppresses ppp restart when mei is received in rrq from current pcf

policy service-option enforce

service-option configures R-P service-option to use for specific PDSN service. Must be followed by valid service-option number, ranging from 0 to 1000.

enforce designates enforcement of R-P service-option number.

policy unknown-cvse enforce

unknown-cvse configures PDSN service unknown cvse policy.

enforce enforces unknown cvse policy where unknown CVSEs in RRQs will cause Deny

Usage Guidelines

Policies can be implemented to dictate PDSN service behavior for various conditions such as overloading.

The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system.

The system automatically invokes the overload policy when an on-line software upgrade is started.

Use the **no policy** { **overload** | **service-option** } command to delete a previously configured policy. If after deleting the policy setting you desire to return the policy parameter to its default setting, use the **default policy** command.

The chassis is shipped from the factory with the policy options set as follows:

- overload disabled
- sequence-numbers enforced enabled

Caution Incorrect configuration of the **policy msid-match** and **policy pcf-zone-match** keywords could result in sessions failing to be established. For example, if PDSN1 is configured to redirect sessions to PDSN2 while PDSN2 is configured to redirect sessions to PDSN1, a loop is created in which all sessions would fail to be connected. In addition, sessions will not be established if the PDSN to which the sessions are being redirected is unavailable.

Example

The following command configures the PDSN service to redirect traffic to two different destinations with weights of *1* and *10* respectively:

```
policy overload redirect 192.168.1.100 weight 1 192.168.1.200 weight 10
```

ppp

Sets PPP tunneling parameters for subscribers in the current PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

ppp { **tunnel-context** *context_name* | **tunnel-type** { **l2tp** | **none** } }
[**no** | **default**] **ppp tunnel-type**

no

Enables/Disables the PPP tunneling parameters for subscribers in the current PDSN service.

default

Sets / Restores default value assigned for PPP tunneling parameters for subscribers in the current PDSN service.

tunnel-context *context_name*

The name of the context that has a LAC service configured to handle all tunnels from this PDSN service.

tunnel-type { l2tp |none }

l2tp: Force all subscriber sessions in this PDSN service to use L2TP tunneling.

none: Do not force L2TP tunneling. This is the default.

Important If the context specified by the **ppp tunnel-context** *context_name* command does not have a LAC service configured and **tunnel-type** is set to **l2tp** or the call is rejected.

Important If the PPP tunnel context has not been set or has been cleared with the **no ppp tunnel-context** command and **tunnel-type** is set to **l2tp**, the context where the current PDSN service resides is used. If that context does not have a LAC service configured the call is rejected.

Usage Guidelines

Use this command to enable or disable forced L2TP tunneling for all subscribers using this PDSN service. Also use this command to define which context defines the L2TP tunneling parameters.

Example

To set the tunnel context to the context named *context1* and enable forced L2TP tunneling, use the following commands;

```
ppp tunnel-context context1
ppp tunnel-type l2tp
```

To enable forced L2TP tunneling with IPSEC security, use the following commands;

```
ppp tunnel-type l2tp-secure
```

To disable forced tunneling, use the following command;

```
ppp tunnel-type none
```

To clear the setting for the tunnel context, use the following command;

```
no ppp tunnel-context
```

qos-profile-id-mapping

Creates the customized QoS profile identifier to QoS mapping for IMS authorization support.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

qos-profile-id-mapping profile-id*id_num* { [**description** *desc*] | [**downlink-bw** *dl_bw*] | [**drop-rate** *drop_percentage*] | [**latency** *latency_duration*] | [**qos-class** { **class-A** | **class-B** | **class-C** | **class-D** | **class-E** | **calss-F** }] | [**uplink-bw***ul_bw*] } +
[**default** | **no**] **qos-profile-id-mappingprofile-id** *id_num*

default

Configures the specified QoS profile ID for QoS mapping with default values in this PDSN service.

no

Removes the configured QoS profile ID mapping in this PDSN service.

profile-id *id_num*

Specifies the profile identifier for QoS parameters to be used as the customized profile ID or modifies the QoS parameters in a profile ID (*id_num*) coming from RAN.

id_num must be an integer between 0 and 65535.

description *desc*

Specifies the user defined description for profile identifier.

desc must be an alpha and/or numeric string between 1 and 32 characters.

downlink-bw *dl_bw*

Default: 32

Specifies the downlink (towards the MN) data traffic bandwidth in kilo-bits per second for this QoS profile.

dl_bw must be an integer value between 0 and 100000.

drop-rate *drop_percentage*

Default: 0

Specifies the permitted packet drop rate in percentage for traffic flow to this QoS profile.

drop_percentage must be an integer value between 0 and 1000.

latency *latency_duration*

Default: 1000

Specifies the permitted latency duration in milli-seconds for this QoS profile.

latency_duration must be an integer value between 0 and 1000.

qos-class {class-A | class-B | class-C | class-D | class-E | class-F }

Default: Class-C

Specifies the type of QoS class associated with this QoS profile

class-A: Specifies the A type of QoS class.

class-B: Specifies the B type of QoS class.

class-C: Specifies the C type of QoS class.

class-D: Specifies the D type of QoS class.

class-E: Specifies the E type of QoS class.

class-F: Specifies the F type of QoS class.

uplink-bw *ul_bw*

Default: 32

Specifies the uplink (from the MN) data traffic bandwidth in kilo-bits per second for this QoS profile.

ul_bw must be an integer value between 0 and 100000.

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines

Use this command to define the values associated with the profile ID on the PDSN. This profile ID is used during the mapping to and from the authorized QoS to the QoS parameters for the A10 link. This mapping is required because the PDSN only knows the profile IDs and not the actual configured values for the profile ID in the RAN. Also this configuration allows the use of custom profile IDs for the subscribers.

If no values are defined with a QoS profile ID, the values from matching QoS profile ID from RAN will be applicable to the subscriber traffic.

Example

The following command sets the downlink bandwidth to *32* kbps, latency duration as *1000* ms, uplink bandwidth to *32* kbps, and QoS class to Class-C for the QoS profile ID *11* in a PDSN service:

```
default qos-profile-id-mapping profile-id 11
```

qos update

Sets QoS update parameters for policy mismatches or wait timeouts.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
qos-update { policy-mismatch | wait-timeout seconds action { disconnect-session
 | downgrade-to-best-effort | drop-packets } }
[ no | default ] qos-update { policy-mismatch | wait-timeout }
```

no

Enables/Disables the **qos-update** [**policy-mismatch** | **wait-timeout**].

default

Sets / Restores default value for **qos-update** [**policy-mismatch** | **wait-timeout**].

policy-mismatch

PDSN raises a TFT violation if there is a QoS policy mismatch.

wait-timeout *seconds* action { disconnect-session | downgrade-to-best-effort | drop-packets }

Sets the wait time for A11 RRQ for QoS changes. *seconds* must be an integer from 1 through 1000.

action: configures the action on the wait-timeout

- **disconnect-session**: Drops the call if the A11 RRQ has not been received for the QoS update. This includes all of the IP flows for the session.
- **downgrade-to-best-effort**: Drops packets if the A11 RRQ has not been received for the QoS update. Sends the forward traffic over best effort (flow FF or FE if available).
- **drop-packets**: Drops packets if the A11 RRQ has not been received for the QoS update.

Usage Guidelines

This command provides a PDSN service level configurable to configure an action, if the PCF ignores the QoS Update request from PDSN. It sets the amount of time to wait and the action to take, if no RRQ is received before the timeout. The action can be to drop packets for the flow, disconnect the session or to downgrade to best effort.

Example

qos-update policy-mismatch

The following command sets **wait-timeout** to *60* seconds and invokes **downgrade-to-best-effort** if the A11 RRQ has not been received for the QoS update:

qos-update wait-timeout *60* **actiondowngrade-to-best-effort**

radius accounting dropped-pkts

This command enables or disables RADIUS accounting related configuration for dropped packets.

Important This command is customer-specific. Contact your Cisco account representative for more information.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > **context** *context_name* > **pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax Description

[no] radius accounting dropped-pkts

no

Enables the RADIUS accounting related configuration for dropped packets.

radius accounting dropped-pkts

Disables the RADIUS accounting related configuration for dropped packets. This is the default behavior.

Usage Guidelines

Use this command to enable or disable the RADIUS accounting related configuration for dropped packets.

By default, the feature is disabled.

Important The configuration will be picked up during **call-setup** and can not be changed dynamically.

Example

The following command enables the RADIUS accounting related configuration for dropped packets for the PDSN service:

```
no radius accounting dropped-pkts
```

registration-accept

Allows the PDSN to accept registration requests when a handoff disconnect is in progress. When the PDSN is tearing down a session and the MN moves over to a new PCF and initiates a new session, the PDSN by default does not accept the handoff until it tears down the old session.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

[no | default] registration-accept handoff session-disconnect-in-progress

no

Disable accepting of registration requests when a handoff disconnect is still in progress.

default

Default is disabled.

Sets / Restores default value assigned for **registration-accept handoff session-disconnect-in-progress**.

Usage Guidelines

Use this command to allow the PDSN service to accept registration requests when a handoff disconnect is still in progress.

Example

```
registration-accept handoffsession-disconnect-in-progress
```

registration-ack-deny terminate-session-on-error

Configures the PDSN service to terminate an A11 session when a Registration ACK received from the PCF has an error status.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdsn-service)#`

Syntax Description **[no | default] registration-ack-deny terminate-session-on-error**

no

Disable terminating A11 sessions on a Registration ACK error from the PCF.

default

Sets / Restores default value assigned to **registration-ack-deny terminate-session-on-error**.

Usage Guidelines Use this command to enable the PDSN service to terminate A11 sessions on a Registration ACK error from the PCF.

Example

Use the following command to enable this functionality in the PDSN:

```
registration-ack-deny terminate-session-on-error
```

registration-deny

Configures parameters related to registration rejection.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdsn-service)#`

Syntax Description

```
registration-deny { handoff { closedrp-rp handoff-in-progress |
connection-setup-record-absent [ use-deny-code { poorly-formed-request |
reason-unspecified } | max-deny-reply-limit num |
mismatched-coa-source-address | new-call { connection-setup-record-absent
 | reverse-tunnel-unavailable } | session-already-active |
session-already-closed | session-already-dormant |
```

```
terminate-session-on-error | use-zero-gre-key}
[ default |no ] registration-deny { handoff { closedrp-rp handoff-in-progress
 | connection-setup-record-absent } | mismatched-coa-source-address |
new-call { connection-setup-record-absent | reverse-tunnel-unavailable } |
 session-already-active | session-already-closed | session-already-dormant
 | terminate-session-on-error | use-zero-gre-key}
```

default

Sets / Restores default value for **registration-deny**.

no

Disables the specified option.

handoff { closedrp-rp handoff-in-progress | connection-setup-record-absent [use-deny-code { poorly-formed-request | reason-unspecified }

This command configures the handoff behavior.

closedrp-rp handoff-in-progress: Configures parameters related to denying handoffs from Closed-RP to RP systems. When enabled the PDSN rejects retransmitted handoff R-P requests when a handoff is already in progress from Closed RP to RP. The deny code used is 'Reason Unspecified'. The default is disabled meaning that the PDSN simply discards such requests.

connection-setup-record-absent [**use-deny-code** { **poorly-formed-request** | **reason-unspecified** }]: When enabled the PDSN denies or discards handoff R-P sessions that do not have an Airlink Connection Setup record in the A11 Registration Request. Default is disabled. Default PDSN behavior is to accept such requests.

[**use-deny-code** { **poorly-formed-request** | **reason-unspecified** }: Sets the specified Registration Deny Code when denying a handoff because of a missing connection setup record.

max-deny-reply-limit *num*

Default: 3

Configures max number of retries of erroneous registration request message from PCF for a session before PDSN terminates the session. *num* can be from 1 to 10.

mismatched-coa-source-address

Default: disabled

Denies RP requests which have a care-of-address field that is different from the request source address.

new-call { connection-setup-record-absent [use-deny-code { poorly-formed-request | reason-unspecified } | reverse-tunnel-unavailable }

connection-setup-record-absent: Configures the PDSN to reject calls that do not have the airlink connection setup record in the RRQ.

use-deny-code { **poorly-formed-request** | **reason-unspecified** } When rejecting calls that do not have the airlink setup record, use the specified deny code.

reverse-tunnel-unavailable: Configures the PDSN to reject calls if the GRE key for a user collides with that of another user.

session-already-active

PDSN denies Registration requests for sessions that are already active with the error code "poorly formed request" .

session-already-closed

PDSN denies RP renew and dereg requests with error code 0x8E for absent R-P sessions.

session-already-dormant

PDSN denies Registration requests for sessions that are already dormant with the error code "poorly formed request" .

terminate-session-on-error

Default: Disabled.

Configures PDSN to terminate session if erroneous registration request message is received for the session.

use-zero-gre-key

Configures the PDSN to set the GRE key to zero (0) when denying a new R-P session.

Usage Guidelines

Use this command to configure parameters relating to the rejection of registration requests.

Example

To reject calls that do not have the airlink setup record in the RRQ, enter the following command:

```
registration-deny new-call connection-setup-record-absent
```

To reject calls if the GRE key collides with that of another user, enter the following command:

```
registration-deny new-call reverse-tunnel-unavailable
```

To set the GRE key to 0 (zero) when a new R-P session is denied, enter the following command:

```
registration-deny new-call use-zero-gre-key
```

registration-discard

Configures the PDSN service to discard any Registration Request message containing multiple information elements of the same type or a different GRE key for existing IMSI session.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

[defualt | no] registration-discard { bad-extension | gre-key-change | handoffconnection-setup-record-absent }

default

Sets/Restores default value assigned for **registration-discard** .

no

Disables the discarding of Registration request messages containing multiple information elements or different GRE keys.

bad-extension

Default: Disabled

Configures the PDSN to discard Registration Request message containing multiple information elements of same type.

gre-key-change

Default: Disabled

Configures PDSN to discard Registration Request message containing different GRE key for existing IMSI session. Default is disable

handoff connection-setup-record-absent

Default: Disabled

When enabled, discards A11 Handoff requests that do not contain the Airlink Setup record.

Usage Guidelines

Use this command to configure the PDSN service to discard and Registration Requests that contain multiple information elements of the same type or discard Registration Requests that contain GRE keys that have different GRE keys for the existing IMSI session.

Example

To configure the PDSN service to discard of Registration Requests that have multiple information elements of the same type, enter the following command:

```
registration-discard bad-extension
```

To configure the PDSN service to discard registration Requests that contain a GRE key that is different than the existing one for the existing IMSI session, enter the following command:

```
registration-discard gre-key-change
```

registration-update

Configures registration update related parameters for the PDSN.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
registration-update { pdsn-code-nvse | wait-timeout secs }
[ default | no ] registration-update { pdsn-code-nvse | wait-timeout }
```

no

If this option is used with the **pdsn-code-nvse** keyword, then pdsn-code-nvse configuration is disabled.

If this option is used with the **wait-timeout** keyword, a separate A11 timer is not used. The PDSN waits for the ppp retransmit-timeout and then sends the A11 Update. If a value is provided, then the "ppp retransmit-timeout" is ignored and a separate A11 timeout is started immediately upon sending the LCP Term-Ack. The A11 Update is then sent when the timer expires.

A value of 0 sends the A11 Update immediately after sending the LCP Term-Ack.

default

Sets/Restores default value assigned for **registration-update** { **pdsn-code-nvse** | **wait-timeout }**

pdsn-code-nvse

Adds the PDSN code NVSE in all A11 registration update messages.

secs

The number of seconds to wait. *secs* must be an integer in the range from 0 through 16.

wait-timeout

After the Mobile Node terminates a PPP session between the PDSN and the Mobile Node, the PDSN service waits for the specified time period to receive an A11 RRQ from the PCF before it sends out a Registration-Update to clear the Session from the PCF.

Usage Guidelines

Use this command to configure registration update related

The **wait-timeout** keyword configures the PDSN to wait the specified amount of time before sending out a Registration-Update to clear the Session from the PCF.

Example

Use the following command to set the registration wait-timeout to *16* seconds:

```
registration-update wait-timeout 16
```

retransmission-timeout

Configures the maximum allowable time for the PDSN service to wait for a response from the PCF before it:

Attempts to communicate with the PCF again (if the system is configured to retry the PCF)

OR

Marks the PCF as unreachable.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
retransmission-timeout time
[default|no] retransmission-timeout
```

no

Enables/Disables the **retransmission-timeout**.

default

Sets / Restores default value assigned for **retransmission-timeout**.

time

Specifies the maximum allowable time for the PDSN service to wait for a response from the PCF before it a) attempts to communicate with the PCF again (if the system is configured to retry the PCF) or b) marks the PCF as unreachable.

time is measured in seconds and can be configured to any integer value between 1 and 1,000,000.

Usage Guidelines

Use the retransmission timeout command in conjunction with the **max-retransmissions** command in order to configure the PDSN services behavior when it does not receive a response from a particular PCF.

Use the **no retransmission-timeout** command to delete a previously configured timeout value. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the **default retransmission-timeout** command.

The chassis is shipped from the factory with the retransmission timeout set to 3 seconds.

Example

The following command configures a retransmission timeout value of *5* seconds:

```
retransmission-timeout 5
```

The following command deletes a previously configured retransmission-timeout setting:

noretransmission-timeout

service-option

If the service option policy is enabled, this command specifies the service options supported by the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pdsn-service)#`

Syntax Description

service-option *number*
no service-option *number*

no

Enables/Disables the **service-option** *number*

default

Sets / Restores default value assigned for **service-option**.

number

Default: 7, 15, 22, 23, 24, 25, 33, 59, 67

Specifies a specific Service Option (SO) number that this PDSN service is allowed to support.

number can be configured to any integer value between 1 and 1000.

Usage Guidelines

Use the service option command in conjunction with the policy service option enforce command to configure specific SO numbers that are supported. If a particular SO number is not configured, then any subscriber session received with that SO number will be rejected and an A11 Registration Reply Code of 86 (poorly formed request) will be sent.

By default, PDSN services are configured to support the following service option numbers:

- 7: PCF specific
- 15: PCF specific
- 22: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS1 reverse)
- 23: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS2 reverse)
- 24: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS1 reverse)

- 25: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS2 reverse)
- 33: 3G High Speed Packet Data
- 59: High Rate Packet Data
- 67: RP A10 connection

Important Option 67 is used for auxiliary connections for Rev-A calls. PPP encapsulation of data packets does not flow over this service option connection. ROHC can be performed without PPP for this service option.

Use the **no service-option** *number* command to delete a previously configured service option. If after deleting the service option setting you desire to return the service option parameter to its default setting, use the **default service-option command**.

Example

The following command enables a service option of *12*:

```
service-option 12
```

The following command disables the default service option *59* :

```
no service-option 59
```

setup-timeout

Specifies the maximum amount of time allowed for session setup.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
[ no ]setup-timeout seconds
default setup-timeout
```

default

Sets/Restores default value assigned for **setup-timeout**.

seconds

Default: 60 seconds

The maximum amount of time, in seconds, to allow for setup of a session. *seconds* must be an integer from 1 through 1000000

Usage Guidelines Use this command to set the maximum amount of time allowed for setting up a session.

Example

Use the following command to set the maximum time allowed for setting up a session to *300* seconds:

```
setup-timeout 300
```

simple-ip allow

Enables or disables Simple-IP sessions from making a connection before authorization takes place.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description `[ no|default ] simple-ip allow`

no

When a session attempts PPP authentication, it is assumed that it is a Simple-IP session and it is disconnected before the user is authenticated (RADIUS or local authentication). Also, if **allow-noauth** is enabled and PPP authentication is not performed, after IPCP the session is disconnected if it is discovered that it is a Simple-IP session.

default

Reset this command to allow Simple-IP sessions to connect.

Usage Guidelines Use this command to prevent Simple-IP sessions from connecting to a PDSN service.

Example

The following command configures the PDSN service so that it will reject any Simple-IP sessions:

```
no simple-ipallow
```

The following command configures the PDSN service to allow Simple-IP sessions:

```
simple-ip allow
```

spi

Configures the security parameter index (SPI) between the PDSN service and the PCF. This command also configures the redirection of call based on PCF zone.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

spi remote-address { *pcf_ip_address* | *ip_addr_mask_combo* } **spi-number** *number* { **encrypted secret** *enc_secret* | **secret** *secret* } [**description** *string*] [**hash-algorithm** { **md5** | **rfc2002-md5** }] [**replay-protection** { **nonce** | **timestamp** }] [**timestamp-tolerance** *tolerance*] [**zone** *zone_id*]
no spi remote-address *pcf_ip_address* **spi-number** *number*

remote-address { *pcf_ip_address* | *ip_addr_mask_combo* }

pcf_ip_address: Specifies the IP address of the PCF. pcf_ip_address is an IP address expressed in IP v4 dotted decimal notation.

ip_addr_mask_combo: Specifies the IP address of the PCF and specifies the IP address network mask bits. *ip_addr_mask_combo* must be specified using the form 'IP Address/Mask Bits' where the IP address must either be an IPv4 address expressed in dotted decimal notation or an IPv6 address expressed in colon notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

spi-number *number*

Specifies the SPI (number) which indicates a security context between the PCF and the PDSN in accordance with IOS 4.1 and RFC 2002.

number can be configured to any integer value between 256 and 4294967295.

encrypted secret *enc_secret* | secret *secret*

Configures the shared-secret between the PDSN service and the PCF. The secret can be either encrypted or non-encrypted.

encrypted secret *enc_secret*: Specifies the encrypted shared key (enc_secret) between the PCF and the PDSN service. enc_secret must be between 1 and 254 alpha and/or numeric characters and is case sensitive.

secret *secret*: Specifies the shared key (secret) between the PCF and the PDSN services. secret must be between 1 and 127 alpha and/or numeric characters and is case sensitive.

The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

description *string*

This is a description for the SPI. *string* must be an alpha and or numeric string of from 1 through 31 characters.

hash-algorithm { md5 | rfc2002-md5 }

Default: md5

Specifies the hash-algorithm used between the PDSN service and the PCF.

md5: Configures the hash-algorithm to implement MD5 per RFC 1321.

rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

replay-protection { nonce | timestamp }

Default: timestamp

Specifies the replay-protection scheme that should be implemented by the PDSN service.

nonce: Configures replay protection to be implemented using NONCE per RFC 2002.

timestamp: Configures replay protection to be implemented using timestamps per RFC 2002.

timestamp-tolerance *tolerance*

Default: 60

Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to 0, then time stamp tolerance checking is disabled at the receiving end.

tolerance is measured in seconds and can be configured to any integer value between 0 and 65535.

zone *zone_id*

Specifies the different PCF zones to configure in PDSN service. Mapping of a zone-number to a set of PDSNs can be done per PDSN service basis.

zone_id must be an integer value between 1 and 32. A maximum of 32 PCF zones can be configured for a PDSN service.

Usage Guidelines

An SPI is a security mechanism configured and shared by the PCF and the PDSN service. Please refer to IOS 4.1 and RFC 2002 for additional information.

Multiple SPIs can be configured if the PDSN service is communicating with multiple PCFs.

Important The SPI configuration on the PCF must match the SPI configuration for the PDSN service on the system in order for the two devices to communicate properly.

Use the **no** version of this command to delete a previously configured SPI.

This command used with **zone** *zone_id* redirects all calls on the basis of PCF zone to the specific PDSN on the basis of parameters configured at policy pcf-zone-match command.

Example

The following command configures the PDSN service to use an SPI of 256 when communicating with a PCF with the IP address 192.168.0.2. The key that would be shared between the PCF and the PDSN service is q397F65.

```
spi remote-address 192.168.0.2 spi-number 256 secret q397F65
```

The following command deletes the configured SPI of *400* for an PCF with an IP address of *172.100.3.200*:

```
no spi remote-address 172.100.3.200 spi-number 400
```

The following command creates the configured SPI of *400* for an PCF with an IP address of *172.100.3.200* and zone id as 11:

```
spi remote-address 172.100.3.200 spi-number 400 zone 11
```

tft-validation wait-timeout

Configures the TFT validation wait timeout value for QoS changes. The QoS update timer triggers automatic QoS updates based on dynamic policies.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

tft-validation wait-timeout *seconds*
[**default** | **no**] **tft-validation wait-timeout**

no

Removes the wait-timeout timer.

default

Sets / Restores default value assigned for **tft-validation wait-timeout**.

Usage Guidelines

Configures the TFT validation wait time value for A11 RRQ for QoS changes. *seconds* must be an integer from 1 through 65535.

Example

Use the following command to set the TFT validation wait-timeout to *5* seconds:

```
tft-validation wait-timeout 5
```

threshold a11-ppp-send-discard

Sets an alarm or alert for the PDSN service based on the number of packets that the PPP protocol processing layer internally discarded on transmit for any reason.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
threshold a11-ppp-send-discard high_thresh [ clear low_thresh ]
no threshold a11-ppp-send-discard
```

no

Deletes the alert or alarm.

high_thresh

Default: *0*

The high threshold number of discarded PPP send packets that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between *0* and *100000*.

clear *low_thresh*

Default:*0*

The low threshold number of discarded PPP send packets that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between *0* and *100000*.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of discarded PPP send packets is equal to or greater than a specified number.

Alerts or alarms are triggered for the number of discarded PPP send packets is based on the following rules:

- **Enter condition:** Actual number of discarded PPP send packets > High Threshold
- **Clear condition:** Actual number of discarded PPP send packets £ Low Threshold

Example

The following command configures a number of discarded PPP send packets threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-ppp-send-discard 1000 clear 500
```

threshold a11-rac-msg-discard

Sets an alarm or alert based on the number of Discarded A11 Registration Acknowledgements for the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

threshold a11-rac-msg-discard *high_thresh* [**clear** *low_thresh*]
no threshold a11-rac-msg-discard

no

Deletes the alert or alarm.

high_thresh

Default: 0

The high threshold number of Discarded A11 Registration Acknowledgements that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear *low_thresh*

Default:*0*

The low threshold number of Discarded A11 Registration Acknowledgements that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between *0* and *100000*.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of Discarded A11 Registration Acknowledgements is equal to or greater than a specified number.

Alerts or alarms are triggered for the number of Discarded A11 Registration Acknowledgements based on the following rules:

- **Enter condition:** Actual number of Discarded A11 Registration Acknowledgements > High Threshold
- **Clear condition:** Actual number of Discarded A11 Registration Acknowledgements £ Low Threshold

Example

The following command configures a number of Discarded A11 Registration Acknowledgements threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-rac-msg-discard 1000 clear 500
```

threshold a11-rrp-failure

Sets an alarm or alert based on the number of A11 Registration Response failures for the PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
threshold a11-rrp-failure high_thresh [ clear low_thresh ]
no threshold a11-rrp-failure
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

The high threshold number of A11 Registration Response failures that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear *low_thresh*

Default:0

The low threshold number of A11 Registration Response failures that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines Use this command to set an alert or an alarm when the number of A11 Registration Response failures is equal to or greater than a specified number.

Alerts or alarms are triggered for the number of A11 Registration Response failures based on the following rules:

- **Enter condition:** Actual number of A11 Registration Response failures > High Threshold
- **Clear condition:** Actual number of A11 Registration Response failures £ Low Threshold

Example

The following command configures a number of A11 Registration Response failures threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-rrp-failure 1000 clear 500
```

threshold a11-rrq-msg-discard

Sets an alarm or alert based on the number of Discarded A11 Registration Requests for the PDSN service.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
threshold a11-rrq-msg-discard high_thresh [ clear low_thresh ]
no threshold a11-rrq-msg-discard
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

The high threshold number of Discarded A11 Registration Requests that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear *low_thresh*

Default:0

The low threshold number of Discarded A11 Registration Requests that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of Discarded A11 Registration Requests is equal to or greater than a specified number.

Alerts or alarms are triggered for the number of Discarded A11 Registration Requests based on the following rules:

- **Enter condition:** Actual number of Discarded A11 Registration Requests > High Threshold
- **Clear condition:** Actual number of Discarded A11 Registration Requests £ Low Threshold

Example

The following command configures a number of Discarded A11 Registration Requests threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold a11-rrq-msg-discard 1000 clear 500
```

threshold init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for the context.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context *context_name* **> pdsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax Description

```
threshold init-rrq-rcvd-rate high_thresh [ clear low_thresh ]
no threshold init-rrq-rcvd-rate
```

no

Deletes the alert or alarm.

high_thresh

Default: 0

The high threshold average number of calls setup per second must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between *0* and *1000000*.

clear *low_thresh*

Default:0

The low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between *0* and *1000000*.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter condition:** Actual number of calls setup per second > High Threshold
- **Clear condition:** Actual number of calls setup per second £ Low Threshold

Example

The following command configures a number of calls setup per second threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold init-rrq-rcvd-rate 1000 clear 500
```

CHAPTER 103

PDSN Service RoHC Configuration Mode Commands

The PDSN Service RoHC Configuration Mode is used to configure RoHC (Robust Header Compression) parameters the PDSN service conveys to the PCF in the initial A11 RRP message before PPP authentication.

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration > PDSN Service ROHC

configure > context *context_name* **> pdsn-service** *service_name* **> ip header-compression rohc**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ip-header-compression-rohc)#
```

Important The commands, keywords and variables in this mode are available dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

cid-mode

Enters the RoHC Profile Compression Options Configuration mode.and configures options that apply during RoHC compression for the current RoHC profile.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > PDSN Service Configuration > PDSN Service ROHC

configure > **context** *context_name* > **pdsn-service** *service_name* > **ip header-compression rohc**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ip-header-compression-rohc)#
```

Syntax Description

```
cid-mode { large | small } max-cid integer
default cid-mode
```

default

Reset all options in the RoHC Profile Compression Configuration mode to their default values.

large

Use large packets with optional information for RoHC

small

This is the default packet size.

Use small RoHC packets.

max-cid *integer*

Default: 15

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.

Usage Guidelines

Use this command to set the RoHC packet size and define the maximum

Example

The following command sets large RoHC packet size and sets the maximum CID to 100:

```
cid-mode large max-cid 100
```

The following command sets the cid-mode to the default settings of small packets and max-cid 0:

```
default cid-mode
```

mrru

Sets the size of the largest reconstructed reception unit, in octets, that the decompressor is expected to reassemble from segments. The size includes the CRC. If MRRU is negotiated to be 0, no segment headers are allowed on the channel.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration > PDSN Service ROHC

configure > **context** *context_name* > **pdsn-service** *service_name* > **ip header-compression rohc**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ip-header-compression-rohc)#
```

Syntax Description

mrru *num_octets*
default mrru

default

reset the value of this command to its default setting

num_octets

Default: 0

This is the number of octets for the maximum size of the largest reconstructed reception unit allowed. *num_octets* must be an integer from 0 through 65535.

Usage Guidelines

Use this command to set the size, in octets, of the largest reconstructed reception unit, in octets, that the decompressor is expected to reassemble from segments.

Example

The following command sets the largest reconstructed reception unit to 1024 octets:

```
mrru 1024
```

The following command resets the mrru size to its default of 0 octets:

```
default mrru
```

profile

Specifies the header compression profiles to use. A header compression profile is a specification of how to compress the headers of a specific kind of packet stream over a specific kind of link. At least one profile must be specified.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PDSN Service Configuration > PDSN Service ROHC

configure > **context** *context_name* > **pdsn-service** *service_name* > **ip header-compression rohc**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ip-header-compression-rohc)#
```

Syntax Description

profile { [esp-ip] [rtp-udp] [udp-ip] [uncompressed-ip] }
default profile

default

Default: esp-ip rtp-udp udp-ip uncompressed-ip

This command sets the RoHC profile configuration back to its default setting.

esp-ip

This enables RoHC Profile 0x0003 which is for ESP/IP compression, compression of the header chain up to and including the first ESP header, but not subsequent subheaders.

rtp-udp

This enables RoHCProfile 0x0001 which is for RTP/UDP/IP compression

udp-ip

This enables RoHC Profile 0x0002 which is for UDP/IP compression, compression of the first 12 octets of the UDP payload is not attempted.

uncompressed-ip

This enables RoHC Profile 0x0000 which is for sending uncompressed IP packets.

Usage Guidelines

Use this command to specify the RoHC header compression profiles to use.

Example

The following command sets the profiles to use as esp-ip and rtp-udp:

```
profile esp-ip rtp-udp
```

CHAPTER 104

Peer List Configuration Mode Commands

Command Modes

The Peer List Configuration Mode is used to add or remove IP address to an SecGW crypto peer list..

Exec > Global Configuration >

configure > crypto peer-list { ipv4 | ipv6 } *peer_list_name*

`[context_name]host_name(config-peer)#`

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

address

Adds or deletes an IPv4 or IPv6 address to a crypto peer list.

Product

SecGW (WSG)

Privilege

Security Administrator

Command Modes

Exec > Global Configuration >

configure > crypto peer-list { ipv4 | ipv6 } *peer_list_name*

`[context_name]host_name(config-peer)#`

Syntax Description

`[ no ] address` *peer_address*

no

Removes the specified IP address from the crypto peer list.

peer_address

Specifies an IP address in either IPv4 dotted-decimal (#.#.#.#/##) or IPv6 colon-separated-hexadecimal (####:####:####:####:####:####:####:####/###) notation with CIDR (required). The only notation allowed will be the one specified when the crypto peer list was created.

Usage Guidelines

Use this command to add or delete an IPv4 or IPv6 address to a crypto peer list.

Repeat this command to add up to 1,000 peer IP addresses to the crypto peer list. The IP addresses in the list can only be entered in either IPv4 or IPv6 notation, depending on the address type specified when the list was created.

The following restrictions apply:

- A maximum of 1,000 peer IP addresses can be added to the peer list via the Peer List Configuration mode address command.
- WSG service address binding is not allowed if a peer list is configured and both address types do not match. An error message is generated if they do not match.
- An IPv4 or IPv6 peer list cannot be modified if peer-list peer_list_name is enabled under the WSG service.

Example

The following command adds IPv4 address 209.165.200.225 to the crypto peer list:

```
address 209.165.200.225
```

CHAPTER 105

Peer Profile Configuration Mode Commands

The Peer Profile Configuration Mode is used to configure the peer profiles for GGSN, P-GW, or S-GW service to allows flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of GGSN, P-GW, or S-GW.

Command Modes

Exec > Global Configuration > Peer Profile Configuration

configure > peer-profile service-type <service-type> {default | name *peer_profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-peer-profile-ggsn/pgw/sgw-access/nw)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

arp-mapping

Configures UMTS ARP to Gx ARP mapping for the specific peer profile.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes Exec > Global Configuration > Peer Profile Configuration

configure > peer-profile service-type <service-type> {default | name *peer_profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-peer-profile-ggsn/pgw/sgw-access/nw)#`

Syntax Description **`[ default ] arp-mapping priority-level high`** *`high_num`* **`medium`** *`med_num`*

default

Sets default values for the peer profile

priority-level high *high_num* medium *high_num*

Configures the high and medium values for peer profile. The *high_num* is an integer and ranges from 1 to 13 while the *high_num* also being an integer, ranges from 2 to 14.

Usage Guidelines Use this command to configure UMTS ARP to Gx ARP mapping for GGSN peer profile configured through this mode.

Example

The following command sets the high priority level 4 and low priority level 9 for UMTS to Gx ARP mapping for a GGSN peer profile:

`arp-mapping priority-level high` *`4`* **`medium`** *`9`*

description

Sets a relevant descriptive string for the specific peer profile. By default it is blank.

Product GGSN

P-GW

SAEGW

S-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Peer Profile Configuration

configure > peer-profile service-type <service-type> {default | name *peer_profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-peer-profile-ggsn/pgw/sgw-access/nw)#`

Syntax Description **`description`** *`desc_string`*
`no description`

no

Removes the set description for GGSN, P-GW, or S-GW service peer profile configured through this mode.

desc_string

Indicates the description for GGSN, P-GW, or S-GW service peer profile configured through this mode; must be an alphanumeric string from 1 through 64 characters.

Usage Guidelines

Use this command to set a relevant description for GGSN, P-GW, or S-GW peer profile configured through this mode.

Example

The following command sets the description *ggsn_gtpc_SGSN_profile1* for a GGSN peer profile:

```
description ggsn_gtpc_SGSN_profile1
```

gtpc

Configure the GTP-C parameters for this peer profile.

Product

GGSN

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Peer Profile Configuration

configure > peer-profile service-type <service-type> {default | name *peer_profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-peer-profile-ggsn/pgw/sgw-access/nw)#
```

Syntax Description

```
gtpc { echo { interval inter_dur | retransmission-timeout echo_retrans_dur }
| max-retransmission retrans_num | retransmission-timeout retrans_dur }
default gtpc { echo [ interval |  retransmission-timeout ] |
max-retransmissions | retransmission-timeout }
no gtpc echo
```

default

Resets the specified parameter to its default value.

no

Disables or removes the configured GTP-C echo settings.

echo interval *inter_dur*

Default: 60

Configures the duration, in seconds, between the sending of echo request messages.

inter_dur must be an integer from 60 through 3600.

echo retransmission-timeout *echo_retrans_dur*

Default: 3

Configures the echo retransmission timeout, in seconds, for the this peer profile.

echo_retrans_dur must be an integer ranging from 1 to 20.

max-retransmissions *retrans_num*

retransmission-timeout *retrans_dur*

Note In 17.3 and later releases, this option has been deprecated. Use **retransmission-timeout-ms** .

retransmission-timeout-ms *retrans_dur*

Usage Guidelines Use this command to configure GTP-C parameters for GGSN, P-GW, or S-GW peer profile.

Example

The following command sets the GTP-C echo parameters to default values:

```
default gtpc echo
```

The following command sets the GTP-C retransmission timeout parameters to 4 seconds:

```
default gtpc retransmission-timeout-ms
```

lawful-intercept

Refer to the *Cisco ASR 5x00 Lawful Intercept Configuration Guide* for a description of this command.

no-qos-negotiation

Configures overriding of No-Qos-Negotiation flag in common flag IE received from peer node.

Product GGSN

P-GW

Privilege Administrator

Command Modes

Exec > Global Configuration > Peer Profile Configuration

configure > peer-profile service-type <service-type> {default | name *peer_profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-peer-profile-ggsn/pgw/sgw-access/nw)#`

Syntax Description

```
no-qos-negotiation { set-flag | unset-flag }
[ no ] no-qos-negotiation
```

no

Disables or removes the configured overriding of No-Qos-Negotiation flag in common flag IE received from peer node.

set-flag

Sets flag value to 1 in common flag IE.

unset-flag

Sets flag value to 0 in common flag IE.

Usage Guidelines

Use this command to configure the overriding of no-qos-negotiation flag value in Common Flags IE received from the peer.

Example

The following command sets the flag value to true, i.e. 1, in Common Flags IE:

```
no-qos-negotiation set-flag
```

upgrade-qos-supported

Configures overriding of upgrade-Qos-supported flag in common flag IE received from peer node.

Product

GGSN

P-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Peer Profile Configuration

configure > peer-profile service-type <service-type> {default | name *peer_profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-peer-profile-ggsn/pgw/sgw-access/nw)#`

Syntax Description

```
upgrade-Qos-supported { set-flag | unset-flag }
[ no ] upgrade-Qos-supported
```

no

Disables or removes the configured overriding of upgrade-Qos-supported flag in common flag IE received from peer node.

set-flag

Sets flag value to 1 in common flag IE.

unset-flag

Sets flag value to 0 in common flag IE.

Usage Guidelines

Use this command to configure the overriding of upgrade-Qos-supported flag value in Common Flags IE received from the peer.

Example

The following command sets the flag value to false, i.e. 0, in Common Flags IE:

```
upgrade-Qos-supported unset-flag
```

CHAPTER 106

Peer-Server Configuration Mode Commands

Command Modes

The Peer-Server configuration mode provides the commands to define and manage the peer server configuration part of the SS7 routing on an SGSN.

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration

configure > ss7-routing-domain *rd_id* **variant** *variant_type* **> peer-server id** *server_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-`*`ss7rd_id`*`-ps-id-peer-`*`server_id`*`)#`

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

mode

Configures the operational mode of the peer-server.

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.

Product

SGSN

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration

configure > ss7-routing-domain *rd_id* **variant** *variant_type* **> peer-server id** *server_id*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-ss7rd_id-ps-id-peer-server_id)#`

Syntax Description

`mode ( loadshare | standby )`

loadshare

Sets the peer-server to load share. This is the default.

standby

Sets the peer-server to be in standby mode.

Usage Guidelines

Configure the operational mode of the peer-server.

Example

Configure the peer-server for standby mode.

`mode standby`

name

Defines the unique identification - the name - of the peer-server in the SS7 routing domain.

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.

Product

SGSN

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration

configure > ss7-routing-domain *rd_id* **variant** *variant_type* **> peer-server id** *server_id*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-ss7rd_id-ps-id-peer-server_id)#`

Syntax Description

name *name*
no name

no

Removes the peer server's name from this configuration instance.

name

name: Must be a string of 1 to 64 alphanumeric characters to define a unique identification for the peer-server within the specific SS7 routing domain. Double quotes must be used to create a name that includes spaces.

Usage Guidelines

Create peer server names that are easy to remember and uniquely identify the PSP.

Example

Use this command to create an easily remembered alphanumeric name for the peer-server:

name *"Berlin West"*

psp

Creates the peer-server-process (PSP) instance and enters the PSP configuration mode. See the PSP Configuration Mode chapter in this guide for information on the configuration commands.

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.

Important This command configures a mandatory parameter in the configuration of the peer server.

Product

SGSN

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration

configure > ss7-routing-domain *rd_id* **variant** *variant_type* **> peer-server id** *server_id*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-ss7rd_id-ps-id-peer-server_id)#`

Syntax Description

[no] psp instance *id*

no

Removes the PSP instance from the peer server configuration.

id

Uniquely identifies the specific peer-server-process configuration.

In releases prior to 15.0, *id* must be an integer from 1 to 4.

In release 15.0, *id* must be an integer from 1 to 12.

In release 21.5, *id* must be an integer from 1 to 32.

Usage Guidelines Use this command to define the peer-server-process (PSP) instance ID number for the SGSN configuration.

Example

Use this command to create instance #3 for the PSP configuration:

```
psp instance 3
```

routing-context

Defines the ID of the routing context for the peer-server to use.

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.

Important This command configures a mandatory parameter in the configuration of the peer server.

Product SGSN

HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration

configure > ss7-routing-domain *rd_id* **variant** *variant_type* **> peer-server id** *server_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-id-peer-server_id)#
```

Syntax Description

```
routing-context id
no routing-context
```

id

id Uniquely identifies a specific routing context for the peer-server-process to use. The Id must be an integer from 1 to 65535.

From release 17.0 onwards, the SGSN supports an integer of 0 to 4294967295 as a valid value for the routing-context ID in M3UA messages.

no

Removes the routing-context definition from the peer server configuration.

Usage Guidelines Use this command to define routing contexts for the peer server.

Example

Define routing-context instance 15:

```
routing-context 15
```

self-point-code

This command defines the point-code to identify the SGSN as a peer server.

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.

Product SGSN

HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration

configure > ss7-routing-domain *rd_id* **variant** *variant_type* **> peer-server id** *server_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-id-peer-server_id)#
```

Syntax Description

```
self-point-code point-code
no self-point-code
```

point-code

Point-code is an SS7-type address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.

- 0.0.1 to 15.31.255 for point-code in the TTC Range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

no

Removes the self-point-code configuration for this linkset in the peer server.

Important Removing the self-point-code will result in the termination of all traffic on this link.

Usage Guidelines

Use this command to define the point-code to identify the SGSN.

Example

Use the following command to remove the self-point-code definition from the peer-server configuration:

```
no self-point-code
```

CHAPTER 107

P-GW Service Configuration Mode Commands

The P-GW (PDN Gateway) Service Configuration Mode is used to create and manage the relationship between specified services used for either GTP or PMIP network traffic.

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

associate

Associates the P-GW service with specific pre-configured services and/or policies configured in the same context.

Product

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Syntax Description

associate { egtp-service *name* **[lma-service** *name* **] | emps-profile** *emps_profile_name* **| gtpc-load-control-profile** *name* **| gtpc-overload-control-profile** *name* **| ggsn-service** *name* **| lma-service** *name* **[egtp-service** *name* **] | peer-map** *map_name* **] | qci-qos-mapping** *name* **}**
no associate { egtp-service | lma-service | emps-profile | peer-map | qci-qos-mapping }

no

Removes the selected association from this service.

egtp-service *name* [lma-service *name*] | lma-service *name* [egtp-service *name*]

egtp-service *name* **[lma-service** *name* **]**: Specifies that the P-GW service is to be associated with an existing eGTP service within this context.

name must be an alphanumeric string of 1 through 63 characters and be an existing eGTP service.

Configure an associated LMA service name to support handoffs between PMIPv6 and GTP. *name* must be an alphanumeric string of 1 through 63 characters and be an existing LMA service.

lma-service *name* **[egtp-service** *name* **]**: Specifies that the P-GW service is to be associated with an existing LMA service within this context.

name must be an alphanumeric string of 1 through 63 characters and be an existing LMA service.

Configure an associated eGTP service name to support handoffs between PMIPv6 and GTP. *name* must be an alphanumeric string of 1 through 63 characters and be an existing eGTP service.

emps-profile*emps_profile_name*

Specifies that an eMPS profile is to be associated with an existing P-GW service in this context.

emps_profile_name must be a string of size 1 to 63 and treated as case insensitive.

gtpc-load-control-profile *name*

Specifies that a GTPC Load Control Profile is to be associated with an existing P-GW service in this context.

name must be an alphanumeric string from 1 to 64 characters in length.

gtpc-overload-control-profile *name*

Specifies that a GTPC Overload Control Profile is to be associated with an existing P-GW service in this context.

name must be an alphanumeric string from 1 to 64 characters in length.

ggsn-service *name*

Specifies that the P-GW service is to be associated with an existing GGSN service within this context.

name must be an alphanumeric string of 1 through 63 characters and be an existing GGSN service.

peer-map *map_name*

Specifies that the P-GW service is to be associated with an existing peer map within this context.

map_name must be an alphanumeric string of 1 through 63 characters and be an existing peer map.

Refer to the *LTE Policy Configuration Mode Commands* chapter for more information on peer map creation.

qci-qos-mapping *name*

Specifies that the P-GW service is to be associated with an existing QCI-QoS mapping configuration within this context.

name must be an alphanumeric string of 1 through 63 characters and be an existing QCI-QoS mapping configuration.

QCI-Qos mapping is typically configured in a AAA context. Refer to the *QCI-QoS Mapping Configuration Mode Commands* chapter for more information.

Important If a GGSN service is associated with a P-GW service, then the GGSN service will use the QCI-QoS mapping tables specified in the **qci-qos-mapping** command and assigned to its associated P-GW service.

Usage Guidelines

Use this command to associate the P-GW service with other pre-configured services and/or policies configured in the same context.

Example

The following command associates this service with an eGTP service called *egtp1*:

```
associate egtp-service egtp1
```

authorize-with-hss

This command enables or disables subscriber session authorization via a Home Subscriber Server (HSS) over an S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Syntax Description

authorize-with-hss [egtp [report-ipv6-addr] [s2b] [s2a [report-ipv6-addr]] [s5-s8] | lma [report-ipv6-addr | s6b-aaa-group *aaa-group-name* **] | report-ipv6-addr | retain-mdn]**
{ default | no } authorize-with-hss

default

Disables the default authorization of subscriber over S6b interface. Resets the command to the default setting of "authorize locally" from an internal APN authorization configuration.

no

Disables the default authorization of subscriber over S6b interface. Resets the command to the default setting of "authorize locally" from an internal APN authorization configuration.

egtp

Enables S6b authorization for eGTP only.

s2a

Enables S6b authorization for eGTP S2a.

s2b

Enables S6b authorization for eGTP S2b.

s5-s8

Enables S6b authorization for eGTP S5S8.

lma

Enables S6b authorization for LMA only.

s6b-aaa-group *aaa-group-name*

AAA group specified for S6b authorization.

aaa-group-name must be an existing AAA group name expressed as an alphanumeric string of 1 through 63 characters.

report-ipv6-addr

Enables the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface.

retain-mdn

Enables MDN/MSISDN value to be retained as negotiated during the call setup (retrieved from S6b interface or Create Session Request). MDN/MSISDN value is retained during the lifetime of call, including handoffs between P-GW and services like eHRPD/trusted/untrusted WiFi. As a result, all Rf records of a session have the same MDN/MSISDN values.

Disabled by default. If disabled, the MDN/MSISDN value received in the CS request is used and the S6b authorized MDN/MSISDN is lost during handoffs. As a result, different values of MDN/MSISDN are sent in the Rf records.

Important This keyword is not applicable to GnGp handoff.

Usage Guidelines Use this command to enable/disable the authorization support for subscriber over S6b interface, which is used between P-GW and the 3GPP AAA to exchange the information related to charging, GGSN discovery, etc.

Example

The following command enables MDN/MSISDN value retention as negotiated during the call setup (retrieved from S6b interface) for the lifetime of call:

```
authorize-with-hss retain-mdn
```

dcnr

Configures the Dual Connectivity with New Radio (DCNR) to support 5G Non Standalone (NSA).

Product P-GW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Syntax Description

`[ no ] dcnr`

no

Disables the DCNR configuration.

Usage Guidelines

Use this command to configure the DCNR for 5G NSA support.

dns-client

Specifies the DNS client context to use for sending DNS queries.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pgw-service)#`

Syntax Description

`dns-client context` *`name`*
`{ default | no } dns-client context`

default

Returns the command to the default setting of targeting the DNS client in the context where the P-GW service resides.

no

Disables DNS queries.

context *name*

Specifies the name of the context where the DNS client is used for the resolution of PCSCF-FQDN received from S6b interface.

name must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to specify the context where the DNS client resides to perform P-CSCF-FQDN resolution from the S6b interface.

Example

The following command identifies the *egress1* context as the context where the DNS client resides:

```
dns-client context egress1
```

egtp

Configures handling of eGTP related procedures.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pgw-service)#`

Syntax Description

egtp { bearer-req reject uli-mismatch apn-ambr-always-include bitrates-rounded-down-kbps | reject-cause | egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi { no-resource [s6b-link-failure] { s6b-retry-code } } | cause-code temp-fail timeout *sec* **retry** *retries* **create-session-rsp | gngp-modify-bearer-rsp-with-apn-ambr | modify-bearer-cmd-negotiate-qos | modify-bearer-rsp { charging-fqdn-or-gw-addr | charging-id | msisdn }| overcharge-protection [drop-all | transmit-all] | s2b-ho-paa-mismatch { allow | reject } [ims-only] | sgw-restoration session-hold timeout** *seconds*| **suppress-ubr no-bitrate-change }**
default egtp { bearer-req reject uli-mismatch | cause-code temp-fail | modify-bearer-cmd-negotiate-qos | modify-bearer-rsp | gngp-modify-bearer-rsp-with-apn-ambr | overcharge-protection | sgw-restoration session-hold | reject-cause | egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi no-resource }
no egtp { bearer-req reject uli-mismatch | apn-ambr-always-include bitrates-rounded-down-kbps | cause-code temp-fail | gngp-modify-bearer-rsp-with-apn-ambr create-session-rsp | modify-bearer-cmd-negotiate-qos | modify-bearer-rsp | overcharge-protection | sgw-restoration session-hold| suppress-ubr no-bitrate-change | reject-cause | egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgino-resource }

default

Resets the command to the default setting.

no

Disables the configuration statement.

bearer-req reject uli-mismatch

Shows the Bearer Request reject options.

Sends Bearer response with CONTEXT_NOT_FOUND (CC 64) cause code if the ULI that is received in Bearer request does not match with the ULI of the existing session.

apn-ambr-always-include

Always includes APN-AMBR IE in Create Session Response.

bitrates-rounded-down-kbps

Bit rate granularity provided by different interfaces was not originally aligned in 3GPP specifications. For example, the PCRF provided bits per second on the Gx and the GTP utilized kilobits per second. Due to the conversion of bps to kbps, there were scenarios where the rounding off could have resulted in the incorrect allocation of MBR/GBR values.

When this keyword is disabled, a bitrate value sent on GTP interface will be rounded up if the conversion from bps (received from Gx) to kbps results in a fractional value. However, the enforcement of bitrate value (AMBR, MBR, GBR) values will remain the same. Once the value (in kbps) that is sent towards the Access side, it needs to be rounded up. Also, **show subscribers pgw-only full all** will show the APN-AMBR in terms of bps.

When enabled, the previous behavior of rounded-down kpbs bitrate (AMBR, MBR, BGR) values being sent towards the Access side is enforced. In addition, **show subscribers pgw-only full all** displays in terms of kpbs.

By default, this command is configured to use rounded-up bitrate values.

reject-cause { no-resource [s6b-link-failure] { s6b-retry-code } }

For S6b interface, it modifies the GTPv2 cause code from 92/0x5C (user authentication failure) to 73/0x49 (no resource available) when S6b server is unreachable due to no-connection or unstable connection and for Diameter server result codes—3002, 3004, 3005 and 5198.

reject-cause: Configures options for handling response with reject-cause.

no-resource: Configures handling for Create Session Response with cause code no-resource.

s6b-link-failure: Responds with no-resource for S6b server unreachability during authentication.

s6b-retry-code : Respond with no-resource for S6b diameter result-code(s) 3002, 3004, 3005, 5198.

cause-code temp-fail timeout *sec* retry *retries*

Enables eGTP Cause Code Handling when the P-GW receives a temporary failure response from peer (cause code 110). By default, this option is disabled.

When enabled, all transactions that were moved to pending queue because of temporary cause failure would be re-attempted after the temporary failure timer expires. After timer expiry, the P-GW informs PCRF about the transient failure. PCRF sends new Re-Auth-Request (RAR) and Create Bearer Request (CBR)/Modify Bearer Request (MBR)/Update Bearer Request (UBR) would succeed.

timeout *sec*: Specifies the time to wait (in seconds) before re-attempting the CBR/MBR/UBR.

sec must be an integer from 1 to 100.

retry *retries*: Specifies the maximum number of retries. The P-GW discards CBR/MBR/UBR after the maximum number of retries are exceeded.

retries must be an integer from 1 to 4.

create-session-rsp

Provides an option to include APN-AMBR in the Create Session Response.

gngp-modify-bearer-rsp-with-apn-ambr

Sends Modify Bearer Response with APN-AMBR only for GnGp Handoff. By default, this option is disabled.

modify-bearer-cmd-negotiate-qos

This configuration only impacts the P-GW QoS negotiation behavior when PCRF is unreachable or disabled, or event trigger is not registered while handling Modify Bearer Command. By default, this configuration is disabled.

When enabled, P-GW will always enforce previous QoS values, which is already applied. When disabled, the P-GW will always accept new QoS values (APN-AMBR/Def-EPS-Bearer-QoS) received in Modify Bearer Command.

modify-bearer-rsp { charging-fqdn-or-gw-addr | charging-id | msisdn }

Configures parameters in Modify Bearer Response messages from P-GW service. All parameters will be disabled by default.

- **charging-fqdn-or-gw-addr**: Sends Modify Bearer Response with Charging FQDN or Charging Gateway address whichever is present.
- **charging-id**: Sends Modify Bearer Response with Charging-ID.
- **msisdn**: Sends Modify Bearer Response with MSISDN.

overcharge-protection [drop-all | transmit-all]

Configures overcharging protection by temporarily not charging during loss of radio coverage. By default, this configuration is disabled.

drop-all: Configures overcharging protection to drop all packets received in LORC.

transmit-all: Configures overcharging protection to send all packets received in LORC mode to S-GW.

s2b-ho-paa-mismatch { allow | reject } [ims-only]

This command configures the behavior of an S2B handover at P-GW when there is a PAA mismatch for a given APN with a different PAA for the same APN.

- **allow**: Accepts a new call after clearing the existing LTE/S2B session when the P-GW receives a S2B handover request
- **reject**: Rejects a new call after clearing the existing LTE/S2B session when the P-GW receives a S2B handover request with a different PAA for the same APN.
- **ims-only**: Enable this behavior for an ims-only APN. By default, its applicable to all APNs when enabled.

sgw-restoration session-hold timeout *seconds*

Enables S-GW Restoration functionality and configure session hold timeout on a P-GW service. By default, S-GW Restoration is disabled.

seconds must be an integer from 1 to 3600.

Default: 0 (disabled).

On S-GW failure indication, P-GW shall check if S-GW Restoration feature is enabled or not. If enabled, P-GW shall maintain all the affected sessions for session-hold timeout. After session-hold timeout, P-GW shall clear all the sessions which are not recovered yet.

suppress-ubr no-bitrate-change

Enables the P-GW to suppress the Update Bearer Request (UBR) message UBR if the bit rate is the same after the round-off.

As the bit rate is expressed in bps on Gx and kbps on GTP, the P-GW does a round-off to convert a Gx request into a GTP request. When the P-GW receives a RAR from the PCRF with minimal bit rate changes (in bps), a UBR is sent, even if the same QoS (in kbps) is already set for the bearer. The UBR suppression feature enables the P-GW to suppress such a UBR where there is no update for any of the bearer parameters.

When the UBR has multiple bearer contexts, the bearer context for which the bit rate change is less than 1 kbps after round-off is suppressed. If other parameters, such as QCI, ARP, and TFT, that might trigger an UBR are changed and there is no change in bit rates after round-off, then UBR is not suppressed. Suppression of UBR is applicable for UBR triggered by CCA-I, RAR, and Modify Bearer Command.

Default: disabled. This means that the UBReq should be triggered even if the Gx and GTP bit-rates in kbps are same after round-off.

If the **no** option is used, it will disable this feature. That is, the UBReq should be triggered even if the Gx and GTP bit-rates in kbps are same after round-off.

There is no separate **default** keyword for this feature. Use the **no** option to revert to the default behavior.

Important The UBR Suppression Feature is a licensed-controlled feature. Contact your Cisco account or service representative for detailed licensing requirements.

egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi

Configure this parameter to ignore SAI/RAI/CGI in the Change Notification Request message under 4G CALL FLOW (EUTRAN RAT type) for P-GW services.

Usage Guidelines

Use this command to configure the behavior of the P-GW/SAEGW for eGTP procedures.

Example

The following command sets the temporary failure timer to *30* seconds and *2* retries:

```
egtp cause-code temp-fail timeout 30 retry 2
```

The following command configures the P-GW to accept new QoS values from the modify bearer command while the PCRF is not reachable:

```
egtp modify-bearer-cmd-negotiate-qos
```

The following command enables S-GW restoration functionality and configures session hold timeout on a P-GW service:

```
sgw-restoration session-hold timeout seconds
```

fqdn

Configures a Fully Qualified Domain Name for this P-GW service used in messages between the P-GW and a 3GPP AAA server over the S6b interface.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Syntax Description

fqdn host *domain_name* **realm** *realm_name*
{ default | no } fqdn

default

Returns the command to the default setting of "null".

no

Removes the configured FQDN from this service configuration.

host *domain_name*

Specifies the domain name of the P-GW service.

domain_name must be an alphanumeric string of 1 through 255 characters.

realm *realm_name*

Specifies the realm name of the P-GW service.

realm_name must be an alphanumeric string of 1 through 255 characters.

Usage Guidelines

Use this command to identify the P-GW service using an FQDN required when sending messages over the S6b interface to a 3GPP AAA server.

Important In order to properly interact with other nodes in the network, the FQDN should be less than or equal to 96 alphanumeric characters.

Topology Matching (eHRPD only)

You may specify which P-GW you wish an HSGW interface to connect with by enabling topology matching within the FQDNs for both the HSGW service and P-GW service. Topology matching selects geographically closer nodes and reduces backhaul traffic for a specified interface.

The following optional keywords enable or disable topology matching when added to the beginning of an FQDN:

- **topon.***interface_name*.

  Beginning an FQDN with **topon** initiates topology matching with available HSGWs in the network. Once this feature is enabled, the rest of the FQDN is processed from right to left until a matching regional designator is found on a corresponding HSGW FQDN.

- **topoff.***interface_name*.

  By default, topology matching is disabled. If you enable topology matching for any interfaces within a node, however, all interfaces not using this feature should be designated with **topoff**.

Example

The following command configures the FQDN for this P-GW service as *123abc.all.com* with a realm name of *all.com*:

```
fqdn host 123abc.all.com realm all.com
```

The following command configures this P-GW service with an FQDN that enables topology matching:

```
fqdn host topon.interface_name.pgw01.bos.ma.node.epc
.mnc<value>.mcc<value>.3gppnetwork.org realm
node.epc.mnc.mcc.3gppnetwork.org
```

Important The associated HSGW service must have a corresponding FQDN similar to the following:

```
topon.interface_name.hsgw01.bos.ma.node.epc.mncvalue.mccvalue.3gppnetwork.org
```

gtpc handle-collision upc nrupc

This command helps in enabling or disabling collision handling between SGSN initiated UPC and NRUPC request.

Product P-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration >P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Syntax Description `[ no | default ] gtpc handle-collision upc nrupc`

no

Disables collision handling between SGSN initiated UPC and NRUPC request.

default

Sets default collision handling behavior between SGSN initiated UPC and NRUPC request. By default, collision handling is enabled.

handle-collision upc nrupc

Enables/Disables collision handling between SGSN initiated UPC and network requested UPC. By default, collision handling is enabled.

Usage Guidelines This command is used to enable or disable collision handling between SGSN initiated UPC and NRUPC request.

Example

The following example disables collision handling between SGSN initiated UPC and NRUPC request.

```
no gtpc handle-collision upc nrupc
```

gx-li

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail

Maps Gx cause code (5xxx) to access side GTP cause code Auth-failure(92) in Create Session Response message.

Product

P-GW

SAEGW

Privilege

P-GW

SAEGW

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > **context** *context_name* > **pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Syntax Description `[ default | no ] map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail`

default

Maps Gx cause code (5xxx) to access side GTP cause code No-Resource(73) in Create Session Response message.

no

Maps Gx cause code (5xxx) to access side GTP cause code No-Resource(73) in Create Session Response message.

Usage Guidelines

When Create Session Request message arrives at P-GW, CCR-I is sent to PCRF and PCRF rejects calls with 5xxx cause code in CCA-I. In this case, Create Session Response is sent with failure indicated by GTP cause code. Use this command to control which GTP cause code is sent, "No Resources Available" or "User Authentication Failed", in Create Session Response message for this scenario. By default, "No Resources Available" is sent for this case; however, enabling this command sends "User Authentication Failed" cause code in Create Session Response.

Example

The following command maps Gx cause code (5xxx) to access side GTP cause code Auth-failure(92) in Create Session Response message:

```
map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail
```

message-timestamp-drift

Allows drift time configuration to take care of NTP drift issues.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Syntax Description

message-timestamp-drift *time_in_seconds*
{ default | no } message-timestamp-drift

default

Sets drift time to 180 seconds.

If P-GW detects drift less than 180 seconds, it will check for condition "MWT + ReceivedTimeStamp (time from MME) > CurrentTimeStampAtPGW", and based on that P-GW will reject the call. If this condition is not met, it will transparently forward MWT and timestamp to AAA/Gx/Gy interfaces.

no

Disables message timestamp drift. MWT and received timestamp will not be passed on to all AAA/Gx/Gy interfaces.

message-timestamp-drift *time_in_seconds*

Configures the drift time from the message timestamp, in seconds, up to which P-GW will consider processing the message timestamp and max-wait-time (MWT) IEs.

If the create-time from MME is off from the currenttime by configured-drift-duration, then this could lead to a high NTP drift and session uniqueness falls back to using currenttime toward Diameter servers.

If the timestamp received in CSReq is significantly off (more than configured drift), then P-GW will not take action based on MWT and received timestamp and will transparently pass it to all AAA/Gx/Gy interfaces.

When received drift is less than configured limit, P-GW will reject the call if "MWT + ReceivedTimeStamp > CurrentTimeStampAtPGW" condition is met. Otherwise, P-GW will forward the timestamp and MWT to AAA/Gx/Gy interfaces.

time_in_seconds must be an integer from 0 to 1000.

Default: 180

Usage Guidelines

When the MME is reselected by the UE or when the MME reselects a different P-GW during timeout scenarios, it is possible that the old PDN connection request is still being processed in the network and the session created by the new PDN connection request is overwritten by the stale procedure.

IEs TimeStamp and MWT (MaxWaitTime) have been added in CSReq and forwarded on S6b/Gx/Gy interfaces in order to maintain session uniqueness at P-GW.

Important Drift time configuration under P-GW service shall be used by the associated LMA service.

Example Scenario

In the following scenario, stale session won't be present on P-GW.

The P-GW is still processing the session creation but the S-GW times out due to timer configurations and notifies the MME with Create Session Failure (Cause #100: Remote Peer Not Responding). MME reselects an alternate P-GW in this case, but the original P-GW still continues to process the session. In certain scenarios, the original P-GW can overwrite the Gx session on the PCRF that is created by the newly selected P-GW. In this case, the new P-GW session is the valid session and original P-GW session is invalid as far as the UE, MME, and S-GW are concerned. The same can occur with the AAA session as well based on timing. This results in PCRF having invalid session information and the user plane works fine anchored on the second P-GW, but the Rx and Gx signaling fails as this terminates via original P-GW.

This results in VoLTE calls failing after SIP signaling between UE and P-CSCF.

To solve the problem, TimeStamp and MWT IE have been incorporated to be transmitted from MME and shared across the network nodes.

Example

The following command sets drift time to 200 seconds.

```
message-timestamp-drift 200
```

newcall

Configures the P-GW to accept or reject requests for a static IP address if the address is already in use by another session.

Product

P-GW

SAEGW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Syntax Description

```
newcall { duplicate-subscriber-requested-address  |
duplicate-subscriber-requested-v6-address } { accept | reject }
no newcall { duplicate-subscriber-requested-address  |
duplicate-subscriber-requested-v6-address }
```

no

Returns the command to the default setting of "reject".

duplicate-subscriber-requested-address

Configures how duplicate sessions with same IPv4 address request are handled.

duplicate-subscriber-requested-v6-address

Configures how duplicate sessions with same IPv6 address request are handled.

accept | reject

Default: **reject**

accept: Specifies that the old session with the requested address will be ended to accept the new session with the same address.

reject: Specifies that the new session requesting the same address will be rejected.

Usage Guidelines

Use this command to configure the behavior of the P-GW service when receiving requests for static IP or IPv6 address already in use by other sessions.

Important This command is only applicable to sessions using services supporting duplicate address abort. These services include HA, GGSN, and P-GW.

Example

The following command allows for the acceptance of requests for static IP addresses already in use by other sessions:

```
newcall duplicate-subscriber-requested-address accept
```

pcscf-restoration

Configures the mechanism to support P-CSCF restoration when a failure is detected. The P-CSCF restoration procedures were standardized to minimize the time a UE is unreachable for terminating calls after a P-CSCF failure.

Product

P-GW

SAEGW

Privilege

Administrator, Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > **context** *context_name* > **pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Syntax Description

```
pcscf-restoration { hss-solution | custom-hss-solution }
[ no ] pcscf-restoration emergency-pdn
[ no ] pcscf-restoration s6b-reauth
default pcscf-restoration
```

hss-solution

Enables the Release 12-based HSS solution for P-CSCF restoration.

Important This keyword must be configured on a separate command line from **emergency-pdn**.

custom-hss-solution

Enables private extension-based HSS solution for P-CSCF restoration.

This is the default setting.

Important This keyword must be configured on a separate command line from **emergency-pdn**.

emergency-pdn

Enables P-CSCF Restoration for Emergency PDNs.

By default, this functionality is disabled.

Important This keyword is license dependent. For more information, contact your Cisco account representative.

s6b-reauth

Enables Re-Auth after S6b triggered P-CSCF Restoration of WLAN. Only applicable for S2a and S2b. By default, Re-Auth will be performed for P-CSCF restoration extension on S6b.

By default, this functionality is disabled.

Important This keyword is license dependent. For more information, contact your Cisco account representative.

default

Returns P-CSCF Restoration to the following:

- **custom-hss-solution**: Enables private extension-based HSS solution for P-CSCF restoration.
- **emergency-pdn**: P-CSCF Restoration is disabled for Emergency PDNs and Private Extn mechanism will be used for P-CSCF Restoration.
- **s6b-reauth**: Re-Auth will be performed for P-CSCF restoration extension on S6b.

no

Disables P-CSCF Restoration for the following:

- **emergency-pdn**: Disables P-CSCF restoration for Emergency PDNs.
- **s6b-reauth**: Disables Re-Auth after P-CSCF restoration extension on S6b.

Usage Guidelines

Use this command to enable/disable the standards-based mechanism for P-CSCF failure detection. This command enables operators to ensure a failed P-CSCF address is not provided to the IMS client. Prior to StarOS release18.2, P-CSCF restoration was supported by using the Private Extn IE. In StarOS releases 18.2 and later, the failure detection mechanism can be configured as standards-based. By default this feature is disabled; therefore, the Private Extn mechanism will be used for P-CSCF restoration.

In compliance with 3GPP standard Release 13, extended P-CSCF Restoration procedures were added in StarOS release 21.0. For more information on this functionality, refer to the *HSS and PCRF Based P-CSCF Restoration Support* chapter in the *P-GW Administration Guide* or *SAEGW Administration Guide*.

Example

This example configures P-CSCF restoration to **custom-hss-solution**:

```
pcscf-restoration custom-hss-solution
```

plmn id

Configures Public Land Mobile Network (PLMN) identifiers used to determine if a mobile station is visiting, roaming, or belongs to a network. Up to 512 PLMN IDs can be configured for each P-GW service.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Syntax Description

plmn id mcc *mcc_value* **[mnc** *mnc_value* **] [primary]**
no plmn id mcc *mcc_value* **[mnc** *mnc_value* **]**

no

Removes a previously configured PLMN identifier for the P-GW service.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN identifier.

mcc_value is the PLMN MCC identifier and must be an integer from 100 through 999.

mnc *mnc_value*

Specifies the mobile network code (MNC) portion of the PLMN identifier.

mnc_value is the PLMN MNC identifier and can be configured to a 2- or 3-digit integer from 00 through 999.

primary

When multiple PLMN IDs are configured, the **primary** keyword can be used to designate one of the PLMN IDs to be used for the AAA attribute.

Usage Guidelines

The PLMN identifier is used to aid the P-GW service in the determination of whether or not a mobile station is visiting, roaming, or home. Multiple P-GW services can be configured with the same PLMN identifier. Up to 512 PLMN IDs can be configured for each P-GW Service.

Important The number of supported PLMN IDs was increased from 5 to 512 in StarOS Release 17.1. In addition, the MNC portion of the PLMN ID became optional.

If the MNC portion of a PLMN ID is not specified, home PLMN qualification will be done based solely on the MCC value and the MNC portion will be ignored for these particular MCCs.

Example

The following command configures the PLMN identifier with an MCC of *462* and MNC of *02*:

```
plmn id mcc 462 mnc 02
```

reporting-action

Configures reporting of events.

Product P-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *pgw_service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-pgw-service)#
```

Syntax Description **`[ no ] reporting-action event-record`**

no

Disables RTT record generation for this P-GW service.

event-record

Configures event records.

Syntax Description Use this command to configure the reporting of events for the P-GW service.

Example

The following command configures the reporting of event records:

```
reporting-action event-record
```

session-delete-delay

Configures a delay in terminating a session.

Product P-GW

SAEGW

Privilege Administrator

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pgw-service)#`

Syntax Description

`session-delete-delay timeout [ msec ]`
`{ default | no } session-delete-delay timeout`

default

Resets the command to the default setting of 10000 milliseconds.

no

Disables the feature.

timeout *msec*

Default: 10000

Specifies the time to retain the session (in milliseconds) before terminating it.

msec must be an integer from 1000 to 60000.

Usage Guidelines

Use this command to set a delay to provide session continuity in break-before-make scenarios.

Example

The following command sets the session delete delay to the default setting of 10,000 milliseconds:

```
session-delete-delay timeout
```

setup-timeout

Configures the maximum amount of time the P-GW service takes for creating a session.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context *context_name* **> pgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pgw-service)#`

Syntax Description

`setup-timeout` *`setup_time`*
`default setup-timeout`

default

Configures the default guard timer value for session creation.

Important This keyword is introduced in Release 18.0 as part of *Configurable Guard Timer on Create Session Request Processing* feature. Prior to Release 18.0, on receiving a Create Session Request, the P-GW service started with a hardcoded setup timer value of 60 seconds.

setup-time

Default: 60

Specifies the maximum amount of time taken by P-GW for service creation.

setup_time is measured in seconds and can be configured to an integer from 1 through 120.

Important This variable is introduced in Release 18.0 as part of *Configurable Guard Timer on Create Session Request Processing* feature. The guard session setup timeout value has been made configurable from 1 to 120 seconds. If a Create Session Request is received and setup timeout is configured, the timer starts with the configured value. If the setup timeout is not configured, the timer starts with the default value of 60 seconds.

Usage Guidelines

Use this command to limit the amount of time allowed for creating a session. If a "Create Session Request" is received and the setup-timeout is configured, the timer starts with the configured value. If the setup timeout is not configured, the timer starts with the default value of 60 seconds.

Example

The following command allows a maximum of *120* seconds for creating a session:

```
setup-timeout 120
```

CHAPTER 108

Policy Control Configuration Mode Commands

Policy Control Configuration mode is used to configure the Diameter dictionary, origin host, host table entry and host selection algorithm for IMS Authorization service.

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

apn-name-to-be-included

This command configures the APN name to be included in CCR Gx messages.

Product

GGSN

IPSG

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name* > **policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
apn-name-to-be-included { gn | virtual }
default apn-name-to-be-included
```

gn | virtual

Specifies which APN name must be sent in the Gx messages.

gn: Specifies to send the real APN name.

virtual: Specifies to send the virtual APN name if present, else to send the real APN name.

default

Applies the default setting for this command.

Default: **gn**

Usage Guidelines

This feature is developed to implement a single global APN for the Enterprise services with the ability to have separate virtual APNs per single Enterprise, group of Enterprises sharing the same service group or per department.

To implement this feature, a configurable option is introduced per interface Rf, Gx, Gy and per APN. That is, a service specific CLI "**apn-name-to-be-included**" is configured for interfaces Rf, Gx, Gy separately. It can take values 'gn' or 'virtual'. Based on the value configured for this command, the Called-Station-Id AVP is populated.

This command is used to configure the APN name to be included in the CCR Gx messages to the PCRF — the real APN name or the virtual APN name.

The name of the virtual APN and the IP pool are signaled during the UE attach to the Enterprise PDN from the 3GPP AAA server over S6b interface with a new vendor-specific AVP "Virtual-APN-Name". The RADIUS Start, Gy CCR to OFCS and Rf ACR to OCS messages contain the Virtual APN name instead of the Enterprise APN.

This feature provides customers the desired granularity per enterprise and per department. This also allows bundling of number of small enterprises under the umbrella of single APN and logically separating them by virtual APN.

Example

The following command configures sending the real APN name in Gx messages:

```
apn-name-to-be-included gn
```

arp-priority-level

This command enables mapping of the ARP priority-level value received from PCRF to inter-user-priority value and be sent in A11 session update.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
arp-priority-level map-to inter-user-priority
{ default | no } arp-priority-level map-to
```

default

Configures the default setting for this command.

Default: arp-priority-level to inter-user-priority mapping not applicable

no

Disables arp-priority-level to inter-user-priority mapping.

Usage Guidelines

Important This command is for a customer-specific implementation to support IP-CAN policy control via Gx interface in PDSN, wherein the PCRF informs the subscriber's subscription level (such as gold, silver, bronze) to PDSN/PCEF via Priority-Level AVP, then PDSN maps the subscriber's subscription level to inter-user-priority and transmits it to PCF via A11 session update message. For more information on the use of this command contact your Cisco account representative.

associate

This command associates/disassociates a failure handling templateor a local policy template with the IMS authorization service.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name* > **policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

associate { **failure-handling-template** *template_name* **| local-policy-service** *service_name* **[dual-mode] }**
no associate { **failure-handling-template | local-policy-service }**

no

Disassociates a failure handling templateor local policy template with the IMS authorization service.

failure-handling-template *template_name*

Associates a previously created failure handling template with the IMS authorization service. *template_name* specifies the name for a pre-configured failure handling template. *template_name* must be an alphanumeric string of 1 through 63 characters.

For more information on failure handling templates, refer to the **failure-handling-template** command in the *Global Configuration Mode Commands* chapter.

local-policy-service *service_name* [dual-mode]

Associates a previously created local policy service with the IMS authorization service. *service_name* specifies the name for a pre-configured local policy service. *service_name* must be an alphanumeric string of 1 through 63 characters.

dual-mode: This keyword enables both PCRF and local-policy to work together. When this CLI command is enabled, for a few set of events, PCRF will be contacted and for a few local-policy will be contacted.

This keyword is configured to provide load balancing support for PCRF, and failure-handling support when PCRF is down or any failure is detected.

By default, the **dual-mode** keyword will not enabled and only on PCRF failure the local-policy will be contacted.

For more information on local policy service configuration, refer to the **local-policy-service** command in the *Global Configuration Mode Commands* chapter.

Usage Guidelines

Use this command to associate a configured failure handling template or local policy service with the IMS authorization service.

The failure handling template defines the action to be taken when the Diameter application encounters a failure supposing a result-code failure, tx-expiry or response-timeout. The application will take the action given by the template. For more information on failure handling template, refer to the *Failure Handling Template Configuration Mode Commands* chapter.

Important Only one failure handling template can be associated with the IMS authorization service. The failure handling template should be configured prior to issuing this command.

If the association is not made to the template then failure handling behavior configured in the application with the **failure-handling** command will take effect.

To support fallback to local policy in case of failure at PCRF for CCFH continue, the local policy service should be associated with an IMS authorization service. In case of any failures, the local policy template associated with the ims-auth service will be chosen for fallback.

Example

The following command associates a pre-configured failure handling template called *fht1* to the IMS authorization service:

```
associate failure-handling-template fht1
```

cc-profile

This command configures the value of the **Offline** AVP sent to the PCRF based on the Charging Characteristics (CC) profile received from the SGSN.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

cc-profile *cc_profile_number* **[to** *cc_profile_number_range_end* **] map-to offline-avp { 0 | 1 }**
{ default | no } cc-profile

default

Configures the default setting for this command.

Default: Deletes all previously configured mappings.

no

Deletes all previously configured mappings.

cc_profile_number

Specifies the CC profile number to map.

For example, 1 for Hot Billing.

cc_profile_number must be an integer from 0 through 15.

cc_profile_number_range_end

Specifies, for a range of CC profile numbers to map, the end number. That is, from *cc_profile_number* through *cc_profile_number_range_end*.

cc_profile_number_range_end must be an integer from 1 through 15.

map-to offline-avp { 0 | 1 }

Specifies to map the CC profile number(s) to the **Offline** AVP value sent to the PCRF.

- **0**: Corresponds to the value DISABLE_OFFLINE (0).
- **1**: Corresponds to the value ENABLE_OFFLINE (1).

Usage Guidelines

Use this command to configure the CC Profile to **Offline** AVP value mapping. The **Offline** AVP's value (DISABLE_OFFLINE (0), ENABLE_OFFLINE (1)) is derived based on the CC profile received from the SGSN as specified by this mapping.

The following example shows how this command can be configured multiple times:

```
cc-profile 1 to 2 map-to offline-avp 1
cc-profile 4 map-to offline-avp 0
cc-profile 8 map-to offline-avp 1
```

On configuring the above set of commands, the Offline AVP value is sent as 1 (Offline enabled) for the CC profiles 1 (Hot Billing), 2 (Flat Rate), and 8 (Post-Paid). And, as 0 (Offline disabled) for the CC profile 4 (Pre-paid).

When configuring this command, overlapping of CC profile numbers is not permitted. In the following example, after configuring the first command, which specifies to send the **Offline** AVP's value as 1 (Offline enabled) for the CC profiles 1 through 15, the second command, which specifies to map CC profile 7, is not permitted:

```
cc-profile 1 to 15 map-to offline-avp 1
cc-profile 7 map-to offline-avp 0
```

Example

The following command specifies to send **Offline** AVP value as 1 (Offline enabled) for the CC profile 1 (Hot Billing):

```
cc-profile 1 map-to offline-avp 1
```

The following command specifies to delete all previously configured mappings:

```
no cc-profile
```

custom-reauth-trigger

This command enables custom reauthorization event triggers.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
custom-reauth-trigger { apn-ambr-mod-failure | default-bearer-qos-change
 | default-bearer-qos-mod-failure | qos-change |
resource-modification-request | ue-ip-addr-allocate | ue-ip-addr-release
 | none | { preservation-changed | reactivation-changed } + }
default custom-reauth-trigger
```

default

Configures the default setting for this command. The default setting is to enable all the event triggers.

none

Disables all custom event triggers.

apn-ambr-mod-failure

Enables APN AMBR Modification Failure event trigger.

default-bearer-qos-change

Enables Default EPS bearer QoS change event trigger.

default-bearer-qos-mod-failure

Enables Default EPS Bearer QOS Modification Failure event trigger.

qos-change

Enables QoS change trigger.

resource-modification-request

Enables Resource modification trigger.

ue-ip-addr-allocate

Enables UE IP address allocate trigger.

ue-ip-addr-release

Enables UE IP address release trigger.

preservation-changed

Enables preservation-changed event trigger.

Important This keyword is for use with a customer-specific implementation, and will be available only if a valid license is installed.

reactivation-changed

Enables reactivation-changed event trigger.

Important This keyword is for use with a customer-specific implementation, and will be available only if a valid license is installed.

Usage Guidelines

Use this command to enable/disable custom reauth event triggers.

It is recommended that the preservation-changed and reactivation-changed triggers both be enabled. As, when the bearer goes into preservation mode with the preservation-changed trigger, the reactivation-changed trigger must also be enabled for the bearer to get reactivated subsequently.

In 16.0 and later releases, this CLI command overwrites the previously configured triggers with the new event triggers. For example, if the following triggers are configured – QoS change, UE IP address allocation, UE IP address release, preservation-changed, reactivation-changed, then the APN-AMBR modification failure and Resource modification request triggers should be configured. This operation will overwrite all previously configured triggers and will configure only new APN-AMBR modification failure and Resource modification request triggers. By default, these event triggers are enabled.

Example

The following command disables all custom event triggers:

```
custom-reauth-trigger none
```

diameter 3gpp-r9-flow-direction

This command controls PCEF from sending Flow-Description, TFT-Filter, andPacket-Filter-Content AVPs in Rel. 9 format.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
[ no ] diameter 3gpp-r9-flow-direction
```

3gpp-r9-flow-direction

Encodes Flow-Direction, Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs based on 3GPP Rel. 9 specification.

no

Encodes Flow-Direction, Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in Rel. 8 format. This is the default configuration.

Usage Guidelines

Use this command to enable Rel.9 changes for Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs sent by PCEF in CCR-U. This CLI command works in conjunction with **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }**. When **diameter 3gpp-r9-flow-direction** is configured and negotiated supported feature is 3gpp-r9 or above, PCEF will send Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in 3GPP Rel. 9 format.

Per the 3GPP Rel. 8 standards, the IPFilterRule in Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs is sent as "permit in" for UPLINK and "permit out" for DOWNLINK direction. From 3GPP Rel. 9 onwards, the Flow-Description AVP within the Flow-Information AVP will have only "permit out" and the traffic flow direction is indicated through Flow-Direction AVP. In 3GPP Rel. 9 format, both UPLINK and DOWNLINK are always sent as "permit out" and hence the usage of "permit in" is deprecated.

Backward compatibility is maintained, i.e. both Rel. 8 (permit in/out) and Rel. 9 (permit out with flow-direction) formats are accepted by PCEF.

This CLI command must be used only after the PCRF is upgraded to Rel. 9. For more information on this feature, see the *3GPP Rel.9 Compliance for IPFilterRule* section in the *Gx Interface Support* chapter in the administration guide for the product you are deploying.

Example

The following command enables Rel.9 changes for Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs:

```
diameter 3gpp-r9-flow-direction
```

diameter clear-session

This command enables the system to clear the subscriber sessions which are affected by session ID mapping mismatch.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter clear-session sessid-mismatch
[ no ] diameter clear-session
```

sessid-mismatch

Clears the session with mismatched session ID. This CLI configuration is optional.

no

This keyword does not delete the subscriber sessions. This is the default configuration.

Usage Guidelines

Use this command to clear the subscriber sessions that are impacted due to the mismatch in the Diameter proxy-session manager mapping.

In the event of rapid back-to-back ICSR switchovers or extensive multiple process failures, the Diameter proxy-Session manager mapping information is not preserved across ICSR pairs. This mismatch in the Diameter proxy-Session ID results in rejection of RAR with 5002 - DIAMETER_UNKNOWN_SESSION_ID cause code. This behavior impacts the VoLTE call setup procedure. This CLI configuration is provided to control the behavior and delete the mismatched subscriber sessions.

When session manager sends an RAA with 5002 DIAMETER_UNKNOWN_SESSION_ID cause code, the dpca-rar-dp-mismatch bulk statistic counter in IMSA schema is incremented to indicate the session ID/Diamproxy grouping mismatch and also initiate the session termination. A Delete Bearer Request is sent to S-GW with a Reactivation Requested as the cause code while suppressing the CCR-T from being sent to PCRF. With this approach, the subscriber reattaches immediately without impacting the subsequent VoLTE calls, encountering only one failure instead of manual intervention.

Example

The following command enables the system to delete the mismatched subscriber sessions:

```
diameter clear-session sessid-mismatch
```

diameter dictionary

This command specifies the Diameter Policy Control Application dictionary to be used by the IMS Authorization Service for the policy control application.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter dictionary { Standard | dpca-custom1 | dpca-custom10 |
dpca-custom11 | dpca-custom12 | dpca-custom13 | dpca-custom14 |
```

```
dpca-custom15 | dpca-custom16 | dpca-custom17 | dpca-custom18 |
dpca-custom19 | dpca-custom2 | dpca-custom20 | dpca-custom21 |
dpca-custom22 | dpca-custom23 | dpca-custom24 | dpca-custom25 |
dpca-custom26 | dpca-custom27 | dpca-custom28 | dpca-custom29 |
dpca-custom3 | dpca-custom30 | dpca-custom4 | dpca-custom5 | dpca-custom6
 | dpca-custom7 | dpca-custom8 | dpca-custom9 | dynamic-load |
gx-wimax-standard | gxa-3gpp2-standard | gxc-standard | pdsn-ty |
r8-gx-standard | std-pdsn-ty | ty-plus | ty-standard }
default diameter dictionary
```

dpca-custom1

Custom-defined Diameter dictionary for the Gx interface.

dpca-custom2

Custom-defined Diameter dictionary for Rel. 7 Gx interface.

dpca-custom3

Custom-defined Diameter dictionary for the Gx interface in conjunction with IP Services Gateway (IPSG).

dpca-custom4

Standard Diameter dictionary for 3GPP Rel. 7 Gx interface.

dpca-custom5

Custom-defined Diameter dictionary for Rel. 7 Gx interface.

dpca-custom6 ... dpca-custom30

Custom-defined Diameter dictionaries.

dynamic-load

Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters.

For more information on dynamic loading of Diameter dictionaries, see the **diameter dynamic-dictionary** in the *Global Configuration Mode Commands* chapter of this guide.

gx-wimax-standard

Gx WiMAX standard dictionary.

gxa-3gpp2-standard

Gxa 3GPP2 standard dictionary.

gxc-standard

Gxc standard dictionary.

pdsn-ty

This keyword is restricted.

r8-gx-standard

R8 Gx standard dictionary.

Standard

Standard Diameter dictionary for the 3GPP Rel. 6 Gx interface.

Default: Enabled for Gx support in 3GPP networks.

std-pdsn-ty

This keyword is restricted.

ty-plus

This keyword is restricted.

ty-standard

This keyword is restricted.

default

Sets the default Diameter dictionary.

Default: **Standard**

Usage Guidelines

Use this command to specify the Diameter dictionary for IMS Authorization Service.

Example

The following command sets the **Standard** dictionary for Diameter Policy Control functions in 3GPP network:

```
diameter dictionary Standard
```

diameter encode-event-avps

This command enables encoding of all the event-related information AVPs in CCR-U messages.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
[ default ] diameter encode-event-avps { always | local-fallback }
```

default

Applies the default setting for this command.

Default: Sends AVPs relevant to the Event-Trigger subscribed by the PCRF.

always

This keyword option always sends the event-related AVPs in all CCR messages.

local-fallback

This keyword option sends the event-related AVPs in CCR-U messages in the event of local fallback scenario.

Usage Guidelines

Use this command to facilitate sending of all the event-related information AVPs in CCR-U messages.

In releases prior to 14.0, per the 3GPP standards for Gx, AVPs relevant to the Event-Trigger subscribed by the PCRF were always sent in the CCR messages. This release onwards, sending of event-related AVPs for all update (both access side and internal) and terminate requests is CLI controlled.

Note that the QoS-Info AVP will be encoded in all CCR-U messages if the CLI command "**diameter encode-event-avps always**" is enabled. This implementation impacts only the dpca-custom15 dictionary.

Example

The following command enables to always send the event-related AVPs in all CCR messages:

```
diameter encode-event-avps always
```

diameter encode-supported-features

This command enables/disables encoding and sending of Supported-Features AVP.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter encode-supported-features { adc-rules | cno-uli |
conditional-apn-policy-info | conditional-policy-info |
conditional-policy-info-default-qos | extended-bw-newradio |
mission-critical-qcis | multiple-pra | netloc | netloc-ran-nas-cause |
pcscf-restoration-ind | pending-transactions | session-recovery |
session-sync | sgw-restoration | sponsored-connectivity | trusted-wlan |
 netloc-trusted-wlan | netloc-untrusted-wlan | virtual-apn }
{ default | no } diameter encode-supported-features
```

adc-rules

This keyword enables configuration of Application Detection and Control (ADC) rules over Gx interface. For ADC 6th bit of supported feature will be set. By default, this supported feature will be disabled.

Important ADC Rule support is a licensed-controlled feature. Contact your Cisco account representative for detailed information on specific licensing requirements.

This keyword "**adc-rules**" will be available only when the feature-specific license is configured.

In release 18, the gateway node will use ADC functionality over Gx as defined in the Release 11 specification of 3GPP standard. ADC extension over Gx provides the functionality to notify PCRF about the start and stop of a specific protocol or a group of protocols, and provide the possibility to PCRF that with the knowledge of this information, change the QoS of the user when the usage of application is started and until it is finished.

The provision of ADC information is done through the ADC rule, the action initiated by PCRF is done through the PCC rule.

ADC rules are certain extensions to dynamic and predefined PCC rules in order to support specification, detection and reporting of an application flow. These rules are installed (modified/removed) by PCRF via CCA-I/CCA-U/RAR events. ADC rules can be either dynamic PCC or predefined PCC rules, and the existing attributes of dynamic and predefined rules will be applicable.

Dynamic PCC rule contains either traffic flow filters or Application ID. When Application ID is present, the rule is treated as ADC rule. Application ID is the name of the ruledef which is pre-defined in the boxer configuration. This ruledef contains application filters that define the application supported by P2P protocols.

PCEF will process and install ADC rules that are received from PCRF interface, and will detect the specified applications and report detection of application traffic to the PCRF. PCRF in turn controls the reporting of application traffic.

PCEF monitors the specified applications that are enabled by PCRF and generates Start/Stop events along with the Application ID. Such application detection is performed independent of the bearer on which the ADC PCC rule is bound to. For instance, if ADC rule is installed on a dedicated bearer whereas the ADC traffic is received on default bearer, application detection unit still reports the start event to PCRF.

cno-uli

This keyword enables the Presence Reporting Area (PRA) feature. Configuring cno-uli keyword enables feature bit in supported feature AVP and helps in negotiating with PCRF.

The Presence Reporting Area is an area defined within the 3GPP packet domain for the purpose of reporting of UE presence within that area. This is required for policy control and in charging scenarios.

During an IP-CAN session, the PCRF determines whether the reports for change of the UE presence in the PRA are required for an IP-CAN session. This determination is made based on the subscriber's profile configuration and the supported AVP features.

conditional-apn-policy-info

This keyword enables the Conditional APN Policy Information feature. This feature bit support is added to enable this feature for negotiation with PCRF. By default, this supported feature is disabled.

Use all three keywords—conditional-apn-policy-info, conditional-policy-info, conditional-policy-info-default-qos—to enable conditional Policy information feature on the P-GW. Using the no form of the command for all the three keywords, disables this feature.

Using only one of the keywords enables the feature bit in supported feature AVP.

Using no form of this command with only one of the keywords disables a specific feature bit in negotiation of this feature.

Important This keyword is customer-specific. For more information, contact your Cisco account representative.

conditional-policy-info

This keyword enables the Conditional Policy Information feature. This feature bit support is added to enable this feature for negotiation with PCRF. By default, this supported feature is disabled.

Use all three keywords—conditional-apn-policy-info, conditional-policy-info, conditional-policy-info-default-qos—to enable conditional Policy information feature on the P-GW. Using the no form of the command for all the three keywords, disables this feature.

Using only one of the keywords enables the feature bit in supported feature AVP.

Using no form of this command with only one of the keywords disables a specific feature bit in negotiation of this feature.

Important This keyword is customer-specific. For more information, contact your Cisco account representative.

conditional-policy-info-default-qos

This keyword enables the Conditional Policy Information Default QoS feature. This feature bit support is added to enable this feature for negotiation with PCRF. By default, this supported feature is disabled.

Use all three keywords—conditional-apn-policy-info, conditional-policy-info, conditional-policy-info-default-qos—to enable conditional Policy information feature on the P-GW. Using the no form of the command for all the three keywords, disables this feature.

Using only one of the keywords enables the feature bit in supported feature AVP.

Using no form of this command with only one of the keywords disables a specific feature bit in negotiation of this feature.

Important This keyword is customer-specific. For more information, contact your Cisco account representative.

extended-bw-newradio

This keyword enables Extended Bandwidth with New-Radio feature.

mission-critical-qcis

This keyword enables Mission Critical (MC)-Push to Talk (PTT) (MC-PTT) QCI feature. By default, this feature will not be enabled.

Important This keyword can be enabled only if the Wireless Priority Feature Set (WPS) license is configured. For licensing information, contact your Cisco account or support representative.

To support the MC-PTT services, a new set of standardized QoS Class Identifiers (QCIs) (65, 66, 69, 70) have been introduced. These are 65-66 (GBR) and 69-70 (non-GBR) network-initiated QCIs defined in 3GPP TS 23.203 v13.6.0 and 3GPP TS 23.401 v13.5.0 specifications. These QCIs are used for Premium Mobile Broadband (PMB)/Public Safety solutions.

In releases prior to 21, the gateway accepted only standard QCIs (1-9) and operator defined QCIs (128-254). If the PCRF sends QCIs with values between 10 and 127, then the gateway rejected the request. The MC QCI support was not negotiated with PCRF. In 21 and later releases, PCRF accepts the new standardized QCI values 69 and 70 for Default Bearer creation and 65, 66, 69 and 70 for Dedicated Bearer creation.

When **mission-critical-qcis** option is enabled, the gateway allows configuring MC QCIs as a supported feature and then negotiates the MC-PTT QCI feature with PCRF through Supported-Features AVP.

The gateway rejects the session create request with MC-PTT QCIs when the WPS license is not enabled and Diameter is not configured to negotiate MC-PTT QCI feature, which is part of Supported Feature bit.

To disable the negotiation of this feature, the existing **no diameter encode-supported-features** command needs to be configured. On executing this command, none of the configured supported features will be negotiated with the PCRF.

For more information on this feature, see the *Gx Interface Support* chapter in the administration guide of the product you are deploying.

multiple-pra

Enables the Multiple Presence Reporting Area Information Reporting.

netloc

Enables the NetLoc feature. The NetLoc feature indicates the support for reporting of the Access Network Information.

Important Network Provided Location Information (NPLI) feature is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

A new feature "netloc" (feature bit 10) has been added as part of the Supported-Features AVP to implement the Network provided Location Info (NPLI) feature for IMS. NPLI is used to support variety of applications like emergency call, Lawful intercept, charging, etc.

Important This feature works only if PCRF too supports netloc.

The netloc feature bit will be sent to PCRF on demand via CCR-I message. A new event trigger "ACCESS_NETWORK_INFO_REPORT (45)" and a new Diameter AVP "Required-Access-Info" have been added to support the NPLI enhancement.

The gateway node provides the required access network information (e.g. user location and/or user time zone information) to the PCRF within the 3GPP-User-Location-Info AVP, User-Location-Info-Time AVP (if available), and/or 3GPP-MS-TimeZone AVP as requested by the PCRF. The gateway also provides the ACCESS_NETWORK_INFO_REPORT event trigger within Event-Trigger AVP.

netloc-ran-nas-cause

Enables the Netloc-RAN-NAS-Cause feature. By default, this supported feature will be disabled.

This feature is used to send detailed RAN and/or NAS release cause code information from the access network to PCRF. This feature is added to be in compliance with Release 12 specification of 3GPP TS 29.212. It requires that the NetLoc feature is also supported.

A new feature "netloc-ran-nas-cause" (feature bit 22) has been added as part of the Supported-Features AVP to support the 3GPP RAN/NAS Release Cause Code Information Element (IE) on Gx interface. Starting from Release 21.2, this feature is supported on S5/S8, and S2b interfaces.

Important This feature can be enabled only when the NetLoc feature license is installed. However, from StarOS Release 21.1, you can enable the RAN/NAS feature without configuring the NetLoc feature. It is not mandatory to configure the "netloc" keyword to configure the "netloc-ran-nas-code" keyword.

If the supported features "netloc-ran-nas-code" and "netloc" are enabled, then netloc-ran-nas-cause code will be sent to PCRF via CCR-T message. A new Diameter AVP "RAN-NAS-Release-Cause" has been added to support this feature. This AVP will be included in the Charging-Rule-Report AVP and in CCR-T for bearer and session deletion events respectively.

pcscf-restoration-ind

Enables the P-CSCF Restoration Indication feature. By default, this feature is disabled.

Important This keyword is license dependent. For more information, contact your Cisco account representative.

This keyword, when enabled, allows the negotiation of P-CSCF Restoration feature support with PCRF. A new Diameter AVP "**PCSCF-Restoration-Indication**" is introduced to indicate to PCEF that a P-CSCF Restoration is requested. This is achieved by setting AVP value to 0.

For more information on this feature, see the *Gx Interface Support* chapter in the administration guide of the product you are deploying.

pending-transactions

Configures the Pending Transactions feature as part of supported features. This keyword addition is to handle race conditions on Gx i.e. process the Diameter messages in the order they are received.

Gx-based applications are vulnerable to certain race conditions (e.g. concurrent RAR/CCR). Enhancements are done on the Diameter protocol to deterministically handle the race conditions on Gx.

In a scenario wherein RAR is received while waiting for CCA-U, Gx application rejects RAR with Experimental-Result-Code AVP set to DIAMETER_PENDING_TRANSACTION. This should be done only if PCRF supports this functionality otherwise Gx client should continue with the current implementation.

If race conditions are not processed properly, it can lead to unpredictable behavior from each node, resulting in subscriber disconnection. With this feature, the outcome in such situation is deterministic and operator has the ability to influence the node behavior aligned with their policy.

Important Currently only one pending transaction is supported. So, all other transactions (like handoffs, etc) while one is pending will be rejected.

In 17.0 and later releases, in order to comply with 4G Network Upgrade 3GPP Standard, the following changes are implemented:

- Support for Negotiation of PT in initial session establishment.
- Support for receiving/sending 4144 with 3GPP Vendor ID in CCA/RAA.
- Retry of CCR-U when 4144 is received from PCRF.
- No Support for 4198 with Proprietary Vendor ID.
- Recovery of negotiated Supported features.

session-recovery

Enables the Session Recovery feature. This functionality helps ensure that the PCRF and P-GW can be in sync on session information and recover any lost Gx sessions. By default, session recovery and session sync features are not enabled.

Gx sessions typically tend to be long-lived. In case of session loss in PCRF (e.g. due to software failure), or a message loss in PCRF (e.g. Gx:RAA is dropped due to overload control), there is no existing mechanism to allow the PCRF and P-GW to sync-up on session state like Rules Status, APN-AMBR, QoS, Event Triggers, etc. In this release, the Gx interface between P-GW and PCRF has been enhanced to allow the PCRF and P-GW to sync-up. This is currently not part of 3GPP 29.212.

Important In this release, the Session Recovery and Sync will be supported only for the IMS APN.

This keyword is used to achieve the session recovery. When this feature is enabled, P-GW and PCRF will exchange session information and P-GW provides the complete subscriber session information to enable PCRF to build the session state.

session-sync

Enables the Session Synchronization feature. This functionality helps ensure that the PCRF and P-GW can be in sync on session information and recover any lost Gx sessions. By default, Session Recovery and Session Sync features will not be enabled.

Gx sessions typically tend to be long-lived. In case of session loss in PCRF (e.g. due to software failure), or a message loss in PCRF (e.g. Gx:RAA is dropped due to overload control), there is no existing mechanism to allow the PCRF and P-GW to sync-up on session state like Rules Status, APN-AMBR, QoS, Event Triggers, etc. The Gx interface between P-GW and PCRF is enhanced to allow the PCRF and P-GW to sync-up. This is currently not part of 3GPP 29.212.

Important In this release, the Session Recovery and Sync will be supported only for the IMS APN.

This keyword is used to achieve the session sync-up. When this feature is enabled, P-GW and PCRF will exchange session information and P-GW provides the complete subscriber session information to enable PCRF to build the session state.

sgw-restoration

This keyword enables configuration of S-GW Restoration feature.

P-GW is configured to support S-GW Restoration feature. P-GW sends S-GW Restoration feature in Supported-Features AVP through the CCR-I message during session creation. If P-GW receives S-GW Restoration feature in Supported-Features AVP in CCA-I message, then P-GW enables S-GW Restoration feature.

If P-GW and PCRF support S-GW Restoration feature, then the P-GW accepts CCA and RAR during S-GW restoration. Only Rule removal or RAR with session release cause is processed. Any rule install or modify is dropped. P-GW triggers CCR-U with PCC rule failure report and AN_GW_STATUS AVP to inform PCRF that S-GW is down. After receiving the SGW_Restoration indication, PCRF does not initiate any rule install or modification towards the P-GW. The P-GW informs the PCRF when the S-GW has recovered using the Event-Trigger AVP set to AN_GW_CHANGE and including the AN-GW-Address AVP related to the restored or new S-GW. If S-GW restoration is reported to PCRF, then the P-GW sends CCR-U with AN_GW_CHANGE trigger.

If S-GW Restoration feature is not negotiated through the Supported-Features AVP, then P-GW falls back to the old behavior as follows:

- Drops all internal updates towards PCRF
- Rejects CCA and RAR during S-GW Restoration
- Does not include AN_GW_STATUS as AN_GW_FAILED (0) AVP in CCR-U
- Sends an RAA command with the Experimental-Result-Code set to UNABLE_TO_COMPLY (5012) upon receiving RAR command

After configuring the S-GW Restoration feature on Gx interface, the failure is sent to PCRF with Rule-Failure-Code as AN_GW_FAILED in both failure and restoration scenarios.

sponsored-connectivity

Enables the Sponsored (data) Connectivity feature.

With sponsored data connectivity, the sponsor has a business relationship with the operator and the sponsor reimburses the operator for the user's data connectivity in order to allow the user access to an associated Application Service Provider's (ASP) services. Alternatively, the user pays for the connectivity with a transaction which is separate from the subscriber's charging. It is assumed the user already has a subscription with the operator.

The purpose of this feature is to identify the data consumption for a certain set of flows differently and charge it to sponsor. To support this, a new reporting level "SPONSORED_CONNECTIVITY_LEVEL" is added for reporting at Sponsor Connection level and two new AVPs "Sponsor-Identity" and "Application-Service-Provider-Identity" have been introduced at the rule level.

This CLI command "**diameter encode-supported-features**" has been added in Policy Control Configuration mode to send Supported-Features AVP with Sponsor Identity.

Sponsored Connectivity feature will be supported only when both P-GW and PCRF support 3GPP Rel. 10. P-GW advertises release as a part of supported features in CCR-I to PCRF. If P-GW supports Release 10 and also Sponsored Connectivity but PCRF does not support it (as a part of supported features in CCA-I), this feature is turned off.

This feature implementation impacts only the Gx dictionary "dpca-custom15".

trusted-wlan

Enables the Trusted WLAN feature.

netloc-trusted-wlan

Enables the NetLoc trusted WLAN feature over Gx interface.

This command takes effect when Gx is enabled on S2b call. By default, the feature is disabled and TWAN information will not be sent over Gx.

netloc-untrusted-wlan

Enables the NetLoc untrusted WLAN feature over Gx interface.

This command takes effect when Gx is enabled on S2b call. By default, the feature is disabled and UWAN information will not be sent over Gx.

virtual-apn

This keyword enables configuration of Gx-based Virtual APN (VAPN) feature. For VAPN 4th bit of supported feature will be set. By default, this supported feature will be disabled.

Important Gx-based VAPN is a licensed-controlled feature. Contact your Cisco account representative for detailed information on specific licensing requirements.

This keyword "**virtual-apn**" will be available only when the feature-specific license is configured.

In releases prior to 19, VAPN selection was possible through RADIUS or local configuration. In Release 19, ASR5K uses PCRF and Gx interface for Virtual APN selection to achieve signaling reduction.

This keyword enables Gx based Virtual APN Selection feature for a given IMS authorization service. When this configuration is enabled at P-GW/GGSN, then P-GW/GGSN advertises this feature to PCRF through the Supported-Features AVP in CCR-I. When the VAPN is selected, then the PCRF rejects the CCR-I message

with the Experimental-Result-Code AVP set to 5999 (DIAMETER_GX_APN_CHANGE), and sends a new APN through the Called-Station-Id AVP in CCA-I message. The existing call is then disconnected and established with the new virtual APN. Note that the Experimental Result Code 5999 will have the Cisco Vendor ID.

Important Enabling this feature might have CPU impact (depending on the number of calls using this feature).

Limitations:

- Virtual APN supported feature negotiation, Experimental Result Code (5999), Called-Station-Id AVP should be received to establish the call with new virtual APN. When any one of conditions is not met then the call will be terminated.
- Failure-handling will not be taken into account for 5999 result-code when received in the CCA-I message.
- When the Experimental Result Code 5999 is received in the CCA-U then failure-handling action will be taken.
- If the Called-Station-Id AVP is received in CCA-U or CCA-T, then the AVP will be ignored.
- If virtual-apn is received in local-policy initiated initial message then the call will be terminated.
- When PCRF repeatedly sends the same virtual-apn, then the call will be terminated.

default | no

This keyword removes the previously configured supported features.

Usage Guidelines This command is used to enable encoding and sending of Supported-Features AVP.

diameter host-select reselect

This command controls pacing of the reselection or switching of the PCRF after a change occurs in the table configuration for an IMS Authorization Service.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name* > **policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter host-select reselect subscriber-limit subs_limit time-interval
duration
{ default | no } diameter host-select reselect
```

subscriber-limit *subs_limit*

Specifies the limit of subscribers to switch or reselect the PCRF for subscribers not more than *subs_limit* in time duration of *duration* second(s).

subs_limit must be an integer from 1 through 10000000.

time-interval *duration*

Specifies the time duration, in seconds, to reselect PCRF for subscribers not more than *subs_limit* in time duration of *duration* second(s).

duration must be an integer from 1 through 3600.

default

Applies the default setting for this command.

Sets the PCRF reselection or switching to default state.

no

Removes the configured PCRF reselection method and disables the reselection or switching of PCRF.

Usage Guidelines

Use this command to specify the pacing of reselection or switching of the PCRF in an IMS authorization service..

In case IMS authorization session have been opened on certain PCRF on the basis of the current selection table, and the current active table configuration is changed, the IMSA starts selection procedure for the PCRF. Existing sessions on current PCRF from earlier table is required to close and reopened on the selected PCRF from the new table. This reselection periodicity is controlled by this command and it indicates the number of subscriber sessions *subs_limit* to be reselected or moved in *duration* seconds.

For example, if this command is configured with *100* subscribers and *2* seconds, then the system reselects the PCRF for no more than *100* subscribers per *2* seconds.

Example

The following command sets the system to reselect the new PCRF for no more than *1000* subscriber in *15* seconds:

```
diameter host-select reselect subscriber-limit 1000 time-interval 15
```

diameter host-select row-precedence

This command adds/appends rows with precedence to a Diameter host table or MSISDN prefix range table.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name* > **policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter host-select row-precedence precedence_value table { { { 1 | 2 } host
 host_name [ realm realm_id ] [ secondary host host_name [ realm realm_id ] ] }
| { prefix-table { 1 | 2 } msisdn-prefix-from msisdn_prefix_from
msisdn-prefix-to msisdn_prefix_to host host_name [ realm realm_id ] [ secondary
 host sec_host_name [ realm sec_realm_id ] algorithm { active-standby |
round-robin } ] } } [ -noconfirm ]
no diameter host-select row-precedence precedence_value table { { 1 | 2 } |
 prefix-table { 1 | 2 } }
```

diameter host-select row-precedence *precedence_value* table { 1 | 2 } host *host_name* [realm *realm_id*] [secondary host *sec_host_name* [realm *sec_realm_id*]]

This command adds/appends a row in the specified Diameter host table.

In 8.0, a maximum of 16 rows can be added to a table. In 8.1 and later releases, a maximum of 128 rows can be added per table.

row-precedence *precedence_value*: Specifies precedence of the row in the Diameter host table.

Important In 8.1 and later releases, *precedence_value* must be an integer from 1 through 128. In 8.0 and previous releases, *precedence_value* must be an integer from 1 through 100.

table { 1 | 2 }: Specifies the Diameter host table to add/append the primary and secondary Diameter host addresses.

host *host_name*: Specifies the primary host name. *host_name* must be an alphanumeric string of 1 through 127 characters in length.

realm *realm_id*: Specifies the primary realm ID. *realm_id* must be an alphanumeric string of 1 through 127 characters in length.

secondary host *sec_host_name* **[realm** *sec_realm_id* **]**: Specifies the secondary host name and realm ID:

host *sec_host_name*: Specifies the secondary host name. *host_name* must be an alphanumeric string of 1 through 127 characters in length.

realm *sec_realm_id*: Specifies the secondary realm ID. *realm_name* must be an alphanumeric string of 1 through 127 characters in length.

no diameter host-select row-precedence *precedence_value* table prefix-table { 1 | 2 } }

Removes the row with the specified precedence from the specified MSISDN prefix range table.

diameter host-select row-precedence *precedence_value* table prefix-table { 1 | 2 } msisdn-prefix-from *msisdn_prefix_from* msisdn-prefix-to *msisdn_prefix_to* host *host_name* [realm *realm_id*] [secondary host *sec_host_name* [realm *sec_realm_id*] algorithm { active-standby | round-robin }] [-noconfirm]

Use this command to configure the MSISDN prefix range based PCRF selection mechanism for Rel. 7 Gx interface support, wherein the PCEF is required to discover and select an appropriate PCRF to establish control relationship at primary PDP context activation.

This command adds a row in the specified MSISDN prefix range table. A maximum of 128 rows can be added per prefix range table.

row-precedence *precedence_value*: Specifies precedence of the row in the table.

Important In 8.1 and later releases, *precedence_value* must be an integer from 1 through 128. In 8.0 and previous releases, *precedence_value* must be an integer from 1 through 100.

prefix-table { 1 | 2 }: Specifies the MSISDN prefix range table to add the primary and/or secondary Diameter host addresses.

msisdn-prefix-from *msisdn_prefix_from*: For a range of MSISDNs, specifies the starting MSISDN.

msisdn-prefix-to *msisdn_prefix_to*: For a range of MSISDNs, specifies the ending MSISDN.

Important To enable the Gx interface to connect to a specific PCRF for a range of MSISDNs/subscribers configure *msisdn_prefix_from* and *msisdn_prefix_to* with the starting and ending MSISDNs respectively. The MSISDN ranges must not overlap between rows. To enable the Gx interface to connect to a specific PCRF for a specific MSISDN/subscriber, configure both *msisdn_prefix_from* and *msisdn_prefix_to* with the same MSISDN.

host *host_name*: Specifies the primary host name. *host_name* must be an alphanumeric string of 1 through 127 characters in length.

realm *realm_id*: Specifies the primary realm ID. *realm_id* must be an alphanumeric string of 1 through 127 characters in length.

secondary host *sec_host_name* **[realm** *sec_realm_id* **]**: Specifies the secondary host name and realm ID: **host** *sec_host_name*: Specifies the secondary host name. *sec_host_name* must be an alphanumeric string of 1 through 127 characters in length.

realm *sec_realm_id*: Specifies the secondary realm ID. *sec_realm_id* must be an alphanumeric string of 1 through 127 characters in length.

algorithm { active-standby | round-robin }: Specifies the algorithm for selection between primary and secondary servers in the MSISDN prefix range table.

Default: **active-standby**

active-standby: Specifies selection of servers in the Active-Standby fashion.

round-robin: Specifies selection of servers in the Round-Robin fashion.

Important The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.

[-noconfirm]

Specifies that the command is to execute without any additional prompt and confirmation from the user.

no diameter host-select row-precedence *precedence_value* table { 1 | 2 }

Removes the row with the specified precedence from the specified Diameter host table.

Usage Guidelines

Use this command to add, update, or delete rows specified with a precedence from a Diameter host table or MSISDN prefix range table.

In the Rel. 7 Gx implementation, when the Gateway interworks with multiple PCRFs, the Gateway can configure the primary and secondary server based on the MSISDN-prefix range in the MSISDN prefix range table. Using this command, you can add a new prefix row into the MSISDN prefix table.

If a row with the precedence that you add already exists in a table, the existing prefix row is removed and the new row is inserted with the same precedence.

Example

The following command adds a row with precedence *12* in table **2** with primary host name as *star_ims1* and secondary host name as *star_ims2* to Diameter host table.

```
diameter host-select row-precedence 12 table 2 host star_ims1 secondary host
 star_ims2
```

diameter host-select table

This command selects the Diameter host table or the MSISDN prefix range table, and the algorithm to select rows from the Diameter host table.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter host-select table { { 1 | 2 } algorithm { ip-address-modulus [
prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin } | prefix-table
 { 1 | 2 } }
{ default | no } diameter host-select table
```

diameter host-select table { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus | round-robin }

table { 1 | 2 }: Specifies the Diameter host table to obtain the primary and secondary host names for PCRF.

algorithm { ip-address-modulus [prefer-ipv4 | prefer-ipv6] | msisdn-modulus | round-robin }: Specifies the algorithm to select row from the Diameter host table.

Default: **round-robin**

- **ip-address-modulus [prefer-ipv4 | prefer-ipv6]**: This algorithm divides the IP address, in binary, of the subscriber by the number of rows in the table, and the remainder is used as an index into the specified table to select the row.
- prefer-ipv4: Specifies that IPv4 addresses are to be used, if an IPv4v6 call is received, for selecting the rows in the host table.
- prefer-ipv6: Specifies that IPv6 addresses are to be used, if an IPv4v6 call is received, for selecting the rows in the host table.
- **msisdn-modulus**: This algorithm divides the MSISDN value in binary without the leading "+" of the subscriber by the number of rows in the table, and the remainder is used as an index in the specific table to select the row.
- **round-robin**: This algorithm rotates all rows in the active table for selection of the row in round-robin fashion. If no algorithm is specified this is the default behavior.

Important The Round Robin algorithm is effective only over a large number of selections, and not at a granular level.

diameter host-select table prefix-table { 1 | 2 }

Specifies the MSISDN Prefix Range table to be used in case of MSISDN prefix range based PCRF discovery mechanism.

default

Applies the default setting for this command.

no

Removes previous configuration.

When no table is selected, the system will not communicate with any PCRF for new sessions.

Usage Guidelines

Use this command to configure the Diameter host table and row selection methods to select host name or realm for PCRF.

When this command is used to change which table the system should be using, user must re-determine which E-PDF the system should be using for each subscriber. If a different E-PDF results from the configuration change in the table, the system will wait for all of the IMS sessions for the subscriber to be no longer active and then the system either closes/opens Gx sessions with the old/new PDFs respectively, or the system deactivates the PDP contexts of the subscriber.

Here is an example of how row selection is configured for three hosts that the system will use for load-balancing. Operator can configure six rows in a table, as follows.

Modulo 6	Primary Host	Secondary Host
0	1	2
1	1	3
2	2	1
3	2	3
4	3	1
5	3	2

In the above table, the three hosts are named 1, 2, and 3. When all hosts are working, the load will be distributed among all the three hosts. If host 1 fails, then the load will be distributed between the remaining two hosts. In this scenario, the modulo 6 results of 2 and 4 will return rows that have primary hosts but no working back-up host.

In the Rel. 7 Gx implementation, the GGSN/PCEF is required to discover and select an appropriate PCRF to establish control relationship at primary PDP context activation. The ip-address-modulus, msisdn-modulus, and round-robin algorithms are supported by the GGSN/PCEF for PCRF discovery. In addition, the active/standby and round-robin algorithms are used for selection between primary and secondary servers based on the MSISDN Prefix Range Table.

Example

The following command specifies **table 1** with **round-robin** algorithm to select the rows with host name for E-PDF in Diameter host table.

```
diameter host-select table 1 algorithm round-robin
```

diameter host-select-template

This command specifies the Diameter host server template to be associated with this IMS Authorization service. The service uses the specified template (and associated host-select table) to select a Diameter peer server. It then uses the returned host name(s) to contact the PCRF and establish the call.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

diameter host-select-template *tmplt_name*
no diameter host-select-template

no

Removes the binding of the Diameter host select template with the IMS Authorization service.

tmplt_name

Specifies the name of an existing Diameter host server template (configured in Global Configuration mode) to bind with the IMS Authorization service. It is an alphanumeric string of 1 through 255 characters.

Usage Guidelines

Use this command to bind a configured Diameter host select template to the IMS Authorization service for DPCA. This IMS authorization service searches the associated host select table to select a Diameter peer server. For additional information refer to the *Diameter Host Select Configuration Mode Commands* chapter and the description of the **diameter-host-template** command in the *Global Configuration Mode Commands* chapter.

Important Prior to issuing this command, the Diameter host select template should be configured using the **diameter-host-template** command in the Global Configuration mode.

Important If no association is made to the template then the **diameter peer-select** command configured at the application level will be used for peer selection.

Example

The following command binds a configured Diameter host select template named *diamtemplate* to the IMS authorization service:

```
diameter host-select-template diamtemplate
```

diameter map

This command enables selecting the value to which the USAGE_REPORT and APN_AMBR_MOD_FAILURE Event-Trigger should be mapped to.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter map usage-report { 29 | [ 26 | 33 ] [ 26 | 33 ] }
default diameter map usage-report
```

usage-report { 29 | [26 | 33] [26 | 33] }

Maps the USAGE_REPORT of Event-Trigger AVP to one or a combination of these values.

- 26 – Event-Trigger 26 will mapped to USAGE_REPORT. Note this will not affect any other Event-Trigger.
- 29 – Event-Trigger 29 will mapped to USAGE_REPORT, and 33 to APN_AMBR_MOD_FAILURE.
- 33 – Event-Trigger 33 will mapped to USAGE_REPORT, and 29 to APN_AMBR_MOD_FAILURE.

default

The default behavior is to configure the Event-Trigger USAGE_REPORT to be mapped to 26.

Usage Guidelines

The Event-Trigger AVP's USAGE_REPORT has been given different values in the 3GPP TS 29.212 standard spec. As a result of that, the releases of TS 29.212 are not backward compatible. To address this, this CLI command has been introduced in Policy Control configuration mode to map the USAGE_REPORT to either 26/29/33 or a combination of these values in order to be flexible enough to interoperate with various operators.

- TS 29.212 v9.5.0 - USAGE_REPORT (26)
- TS 29.212 v9.6.0 - USAGE_REPORT (29)
- TS 29.212 v9.7.0 - USAGE_REPORT (33)

If this CLI command **diameter map usage-report 29** is configured in the chassis and PCRF sends 29 event-trigger then on volume threshold breach CCR-U with volume-report and event-trigger 29 will be sent to the PCRF. Same is the case with the values 26 and 33.

In 17.1 and later releases, to be able to gracefully handle the change when moving between 3GPP releases supporting the different values for the Usage Report, the existing CLI command **diameter map usage-report** is modified to support configuration of multiple values of usage report mapping. While migrating from older versions to current version, all of the sessions created before the migration will continue to use 26 as usage report event trigger value. The new session will use usage-report value based on PCRF value or default value.

In releases prior to 17.1, when **diameter map usage-report** is mapped to 26, then APN AMBR modification failure event trigger is not supported. In 17.1 and later releases, APN AMBR modification failure event trigger is supported for all usage report trigger values (26, 33, 29).

Example

The following command maps the Event-Trigger USAGE_REPORT to 29 and APN_AMBR_MOD_FAILURE to 33:

```
diameter map usage-report 29
```

diameter origin endpoint

This command binds the origin endpoint configured in Context Configuration mode to the IMS Authorization service for Diameter Policy Control Application (DPCA).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

diameter origin endpoint *endpoint_name*
no diameter origin

endpoint *endpoint_name*

endpoint_name is the Diameter endpoint configured in Context Configuration Mode to bind with IMS authorization service, and must be an alpha/numeric string of 1 through 63 characters in length.

no

Removes the binding of Diameter origin endpoint with IMS Authorization service.

Usage Guidelines

Use this command to bind a configured Diameter origin endpoint to the IMS Authorization service for DPCA. This IMS authorization service searches all system contexts until it finds one with a matching Diameter origin endpoint name specified.

Example

The following command binds a configured endpoint named test to the IMS authorization service:

```
diameter origin endpoint test
```

diameter request-timeout

This command configures the request-timeout setting for Diameter-IMSA Gx interface.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter request-timeout timeoutdeciseconds msg-type { any | ccr-initial
| ccr-terminate | ccr-update }
default diameter request-timeout
```

timeout

Specifies the timeout duration (in deciseconds). The value must be an integer from 1 through 3000.

Default: 10 seconds

deciseconds msg-type { any | ccr-initial | ccr-terminate | ccr-update }

Specifies independent timers (in deciseconds) for all message types like CCR-I, CCR-U and CCR-T. The default time will be 100 deciseconds (10 seconds).

This keyword option provides additional flexibility for operator to configure independent timers with reduced granularity.

This feature implementation ensures that the timer configuration is backward compatible. If the CLI command is configured without "**desiseconds**" and "**msg-type**", the configured time will be taken as seconds and while displaying the CLI it will be converted to deciseconds and msg-type will be "**any**".

default

Applies the default setting for this command.

Usage Guidelines

Use this command to configure the request-timeout setting for Diameter-IMSA Gx interface. At the request-timeout value, DPCA will apply failure-handling to the subscriber. Action will be taken based on the failure-handling configuration (terminate/retry-terminate/continue).

Example

The following command configures the Diameter request-timeout setting to *20* seconds:

```
diameter request-timeout 20
```

diameter session-prioritization

This command enables prioritization of Gx messages based on eMPS state of the session. From Release 21.4, it also supports DRMP AVP with value 0 to be sent in Credit Control Request (Initial, Update and Terminate) messages over the Gx interface for P-GW eMPS sessions and for eMPS upgrade and downgrade transactions. Also the help string for “session prioritization” keyword is updated accordingly.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

`[ no ] diameter session-prioritization`

no

Disables the command and has the following implications:

- Disables prioritization of Gx messages for eMPS sessions and eMPS upgrade and downgrade.
- Disables encoding of DRMP AVP (value 0) in Credit Control Request (Initial, Update, and Terminate) messages for eMPS sessions and eMPS upgrade and downgrade.

By default, the CLI is disabled and Gx messages will not be prioritized based on eMPS value.

Usage Guidelines

Use this command to facilitate prioritization of Gx messages based on eMPS state of the session. From Release 21.4, it also supports DRMP AVP with value 0 to be sent in Credit Control Request (Initial, Update and Terminate) messages over the Gx interface for P-GW eMPS sessions and for eMPS upgrade and downgrade transactions. The help string is also changed for the existing command.

The Gx DRMP AVP is encoded when the **diameter session-prioritization** CLI is enabled in IMS Authorization Policy Control mode for policy control application. The following table summarizes the DRMP AVP values that are sent based on the different configurations and scenarios.

session prioritization CLI	eMPS Status of Session	Scenario	DRMP Encoding/Value
Off	Any	CCR Messages	Not Encoded
Any	Any	RAA response to RAR with DRMP X	Encoded/X
Off	eMPS	CCR Messages	Not Encoded
On	Yes	CCR Messages	Not Encoded
On	eMPS	CCR Messages	Encoded/0
On	Non-eMPS	CCR-U generated on eMPS state change from disabled to enabled.	Encoded/0

session prioritization CLI	eMPS Status of Session	Scenario	DRMP Encoding/Value
On	eMPS	CCR-U generated on eMPS state change from enabled to disabled.	Encoded/0
On	Non-eMPS	eMPS Upgrade failed and CCR-U follows	Encoded/0

This CLI takes affect when Gx, along with eMPS profile, is enabled in the configuration.

Example

The following command enables to prioritize Gx messages for sessions marked with eMPS:

```
diameter session-prioritization
```

diameter sgsn-change-reporting

This command enables reporting of SGSN_CHANGE event trigger and SGSN-Address AVP for 2G and 3G calls on GnGp P-GW.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter sgsn-change-reporting
no diameter sgsn-change-reporting
```

sgsn-change-reporting

This keyword specifies to detect SGSN change and send SGSN-Address AVP and SGSN_CHANGE event trigger for a subscriber in 2G/3G on Gx interface during GnGp scenario.

no

This variant specifies to send AN-GW-Address AVP during the call setup, when SGSN change happens, or during the handoff from 4G to 3G. This is the default setting.

Usage Guidelines

The current implementation does not send SGSN_CHANGE event trigger and SGSN- Address AVP. Instead it sends AN-GW-Address AVP and AN_GW_CHANGE event trigger for GnGp case. This behavior is not compliant to 3GPP standard TS 29.212 specification. Hence, in release 18, this CLI command "**diameter sgsn-change-reporting**" has been introduced to control this behavior.

This release provides, the GnGp P-GW users, the flexibility to configure detection of SGSN_CHANGE event trigger and to send SGSN-Address AVP for a subscriber in 2G/3G on Gx interface, so that PCRF can use this information to apply appropriate policies.

In releases prior to 18, AN-GW-Address AVP was sent in CCR-I message on GnGp scenario. AN_GW_CHANGE event trigger and AN-GW-Address AVP were sent when the inter-sgsn handoff or 4G to 2G/3G GnGp handoff happens.

When this CLI command is configured, SGSN-Address AVP will be sent in the CCR-I message for 2G/3G GnGp P-GW subscribers. SGSN_CHANGE event trigger and SGSN-Address AVP will be sent when the inter-sgsn handoff or 4G to 2G/3G GnGp handoff happens.

Important This feature is applicable only for SGSN IPv4 address. For SGSN IPv6 address, the SGSN-Address AVP will not be sent.

By default, AN-GW-Address AVP will be sent during the call setup, when SGSN change happens, or during the handoff from 4G to 3G.

Example

The following command configures to detect SGSN change and send SGSN-Address AVP in CCR-I :

```
diameter sgsn-change-reporting
```

diameter update-dictionary-avps

This command enables dictionary control of the AVPs that need to be added based on the version of the specification to which the PCEF is compliant with.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
diameter update-dictionary avps { 3gpp-r8 | 3gpp-r9 | 3gpp-r10 }
{ default | no } diameter update-dictionary avps
```

default | no

Configures this command with the default setting.

The default behavior is that R9 support will not be indicated as part of Supported-Features AVP in a R7/R8 dictionary and R8 support will not be indicated as part of Supported-Features AVP in a R7 dictionary.

3gpp-r8

Specifies to select the 3GPP Rel. 8 AVPs for encoding.

3gpp-r9

Specifies to select the 3GPP Rel. 9 AVPs for encoding.

3gpp-r10

Specifies to select the 3GPP Rel. 10 AVPs for encoding.

Usage Guidelines

Important This command is applicable only to Diameter dictionaries that support standard based volume reporting over Gx feature.

Use this command to encode the AVPs in the dictionary based on the release version of the specification to which the PCEF is compliant with.

Release 12.0 onwards, if a 3GPP Rel. 7 based dictionary is already configured with **diameter dictionary dpca-custom4** command, and then if the **diameter update-dictionary-avps 3gpp-r9** command is applied, the Supported-Features AVP with feature bit 1 being set will be sent in the CCR-I to indicate that 3GPP Rel. 9 AVPs are also supported.

Both **default** and **no** command have the same behavior, as if the CLI command is not configured. Hence, in the output of **show configuration verbose** command, the **default** and **no** command is shown as **no diameter update-dictionary-avps**.

This CLI command when configured results in behavioral changes as indicated in the following table.

Possible Upgrade Scenarios	Behavior
3GPP Rel. 7 based dictionary upgraded to 3GPP Rel. 9 For example: **diameter dictionary dpca-custom4** **diameter update-dictionary-avps 3gpp-r9**	In the CCR-I, Supported-Features AVP will be encoded with value 2 for the Feature-List AVP. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 2 The Feature-List AVP value suggest that it is 3GPP Rel. 9 compliant. But, it is not fully complaint to 3GPP Rel. 9. In the current release, for this upgrade scenario (3GPP Rel. 7 to 3GPP Rel. 9), only volume reporting related AVPs mentioned in the 3GPP Rel. 9 will be supported.

Possible Upgrade Scenarios	Behavior
3GPP Rel. 7 based dictionary upgraded to 3GPP Rel. 8 For example: **diameter dictionary dpca-custom4** **diameter update-dictionary-avps 3gpp-r8**	In the CCR-I, Supported-Features AVP will be encoded with value 1 for the Feature-List AVP. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 1 The Feature-List AVP value suggest that it is 3GPP Rel. 8 compliant. But, it is not fully complaint to 3GPP Rel. 8. In the current release, for this upgrade scenario (3GPP Rel. 7 to 3GPP Rel. 8), none of the features mentioned in 3GPP Rel. 8 will be supported.
3GPP Rel. 8 based dictionary upgraded to 3GPP Rel. 9 For example: **diameter dictionary r8-gx-standard** **diameter update-dictionary-avps 3gpp-r9**	In the CCR-I, value for the Feature-List AVP in the Supported-Features AVP will be 2. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 2 The Feature-List AVP value suggest that it is 3GPP Rel. 9 compliant. But, it is not fully complaint to 3GPP Rel. 9. Currently for this upgrade scenario (3GPP Rel. 8 to 3GPP Rel. 9), only volume reporting related AVPs mentioned in 3GPP Rel. 9 will be supported.
3GPP Rel. 9 based dictionary upgraded to 3GPP Rel. 10 For example: **diameter dictionary r8-gx-standard** **diameter update-dictionary-avps 3gpp-r10**	In the CCR-I, value for the Feature-List AVP in the Supported-Features AVP will be 8. [V] [M] Supported-Features: [M] Vendor-Id: 10415 [V] [M] Feature-List-ID: 1 [V] [M] Feature-List: 8 The Feature-List AVP value suggest that it is 3GPP Rel. 10 compliant. But, it is not fully complaint to 3GPP Rel. 10.

In 14.1 and later releases, Supported-Features AVP is extended to support 3GPP Rel. 10 in EPS 3.0 in addition to 3GPP Rel. 8 and Rel. 9. If the **diameter update-dictionary-avps 3gpp-r10** command is applied, the Supported-Features AVP with feature bit 1 being set will be sent in the CCR-I / CCA to indicate that 3GPP Rel. 10 AVPs are also supported. The 'M' bit setting for the Feature-List AVP and Feature-List-ID AVP must be the same as defined in 3GPP TS 29.229 and must not be affected by the 'M' bit setting of the Supported-Features AVP.

Example

The following command enables encoding of AVPs in the dictionary based on 3GPP Rel. 9:

```
diameter update-dictionary-avps 3gpp-r9
```

encode-cc-in-r8-gx-dict

This command enables r8-gx-standard dictionary configuration to send 3GPP-Charging-Characteristics AVP in CCR message.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the preceeding command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
encode-cc-in-r8-gx-dict
{ default | no } encode-cc-in-r8-gx-dict
```

encode-cc-in-r8-gx-dict

Specifies to perform r8-gx-standard dictionary configuration by sending 3GPP-Charging-Characteristics AVP in CCR message.

default | no

Default/no behavior is to avoid r8-gx-standard dictionary configuration impacting other users. By default, this feature is disabled.

Usage Guidelines

Use this command to enable the inclusion of 3GPP-Charging-Characteristics AVP in CCR-I messages when using the r8-gx-standard dictionary.

Example

This command enables r8-gx-standard dictionary configuration to send 3GPP-Charging-Characteristics AVP in CCR message.

```
encode-cc-in-r8-gx-dict
```

endpoint-peer-select

This command enables Diabase to select the Diameter peers in all failure scenarios.

Product

GGSN

PGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
endpoint-peer-select [ on-host-select-failure | on-inactive-host ]
{ default | no } endpoint-peer-select
```

on-host-select-failure

Specifies to perform server selection at Diabase when the hosts could not be selected by IMS Authorization application.

on-inactive-host

Specifies to perform server selection at diabase when the hosts selected by application are inactive.

default | no

Default/no behavior is to terminate the call when the hosts could not be selected by application or when the hosts selected by application are inactive.

Usage Guidelines

Use this command to perform server selection at Diabase when the hosts could not be selected by application or when the hosts selected by the IMS Authorization application is inactive. For example, host table is not configured in IMSA service, host table is configured but not activated, none of the rows in prefix table match the subscriber, host template is not associated with IMSA service, host template could not select the hosts.

This CLI command is added in policy control configuration mode to maintain backward compatibility with the old behavior of terminating the call when server selection fails at application.

Example

The following command enables Diabase to select peers when the hosts selected by application are inactive.

```
endpoint-peer-select on-inactive-host
```

event-report-indication

This command enables event report indication.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
event-report-indication { all | pgw-trace-control | qos-change | rai-change
 | rat-change | sgsn-change | ue-timezone-change | user-loc-change } [
pgw-trace-control ] [ qos-change ] [ rai-change ] [ rat-change ] [
sgsn-change ] [ ue-timezone-change ] [ user-loc-change ]
{ default | no } event-report-indication
```

all | pgw-trace-control | qos-change | rai-change | rat-change | sgsn-change | ue-timezone-change | user-loc-change

Specifies which types of changes will trigger an event report from the PCRF.

- **all**: all triggers
- **pgw-trace-control**: P-GW trace control change trigger
- **qos-change**: QoS change trigger
- **rai-change**: RAI change trigger
- **rat-change**: RAT change trigger
- **sgsn-change**: SGSN change trigger
- **ue-timezone-change**: UE time zone change trigger
- **user-loc-change**: User location change trigger

default | no

Disables event report indication.

Usage Guidelines

Use this command to determine what type of event changes are reported from the PCRF.

Example

The following command enables event report indication for all triggers.

```
event-report-indication all
```

event-update

This command configures sending usage monitoring information in event updates either for all event triggers or for a specific event trigger.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
event-update send-usage-report [ reset-usage ] [ events { an-gw-change |
 apn-ambr-mod-failure | bearer-loss | bearer-rcvry |
charging-correlation-exchange | default-bearer-qos-change |
default-bearer-qos-mod-failure | ip-can-change | out-of-credit |
pgw-trace-control | plmn-change | qos-change | qos-excess-change |
rai-change | rat-change | reallocation-of-credit |
resource-modification-request | revalidation-timeout | sgsn-change |
successful-resource-alloc | tft-change | ue-ip-addr-allocate |
ue-ip-addr-release | ue-timezone-change| user-loc-change }+ ]
{ default | no } event-update
```

default

Configures the default setting for this command.

Default: Usage report is not sent in event update.

no

Disables sending usage report in event update.

reset-usage

Resets the usage at PCEF after reporting in event update.

events { an-gw-change | apn-ambr-mod-failure | bearer-loss | bearer-rcvry | charging-correlation-exchange | default-bearer-qos-change | default-bearer-qos-mod-failure | | ip-can-change | out-of-credit | pgw-trace-control | plmn-change | qos-change | qos-excess-change | rai-change | rat-change | reallocation-of-credit | resource-modification-request | revalidation-timeout | sgsn-change |

successful-resource-alloc | tft-change | ue-ip-addr-allocate | ue-ip-addr-release | ue-timezone-change| user-loc-change }+

Sends the custom usage report based on the following event triggers:

- an-gw-change — AN GW change event trigger
- apn-ambr-mod-failure — APN AMBR Modification Failure event trigger
- bearer-loss — Loss of bearer trigger
- bearer-rcvry — Recovery of bearer trigger
- charging-correlation-exchange — Charging Correlation Exchange trigger
- default-bearer-qos-change — Default EPS bearer QoS change event trigger
- default-bearer-qos-mod-failure — Default EPS Bearer QOS Modification Failure event trigger
- ip-can-change — IP-CAN Change trigger
- out-of-credit — Out of credit trigger
- pgw-trace-control — P-GW Trace Control
- plmn-change — PLMN change trigger
- qos-change — QoS change trigger
- qos-excess-change — Qos Change Exceeding Authorization trigger
- rai-change — RAI Change trigger
- rat-change — RAT change trigger
- reallocation-of-credit — Reallocation of credit trigger
- resource-modification-request — Resource modification trigger
- revalidation-timeout — Revalidation timeout trigger
- sgsn-change — SGSN change trigger
- successful-resource-alloc — Successful Resource Allocation event trigger
- tft-change — TFT change trigger
- ue-ip-addr-allocate — UE IP address allocate trigger
- ue-ip-addr-release — UE IP address release trigger
- ue-timezone-change — UE Time Zone Change event trigger
- user-loc-change — User Location Change trigger

Usage Guidelines

Use this command to send volume usage information when an event change is reported to the PCRF in a CCR-U message.

To send customized usage information based on specific event triggers, the event should be accordingly configured with the **event-update send-usage-report events** command. For example, if the usage report is

required whenever RAT change occurs, this can be accomplished using the **event-update send-usage-report events rat-change** command.

Example

The following command specifies to send volume usage report in event updates to the PCRF for all event triggers:

```
event-update send-usage-report reset-usage
```

The following command specifies to send volume usage report in event updates to the PCRF for RAT change scenarios:

```
event-update send-usage-report reset-usage events rat-change
```

The following command specifies to send volume usage report in event updates to the PCRF if either RAT change or QOS change occurs:

```
event-update send-usage-report reset-usage events rat-change qos-change
```

failure-handling

This command configures Diameter failure handling behavior.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

In Release 8.0:

```
failure-handling { continue | retry-and-terminate | terminate |
diameter-result-code { any-error | result_code } ccfh { continue |
retry-and-terminate | terminate } [ cc-request-type { initial-request |
terminate-request | update-request } ] }
no failure-handling diameter-result-code { any-error | integer result_code
 } [ cc-request-type { initial-request | terminate-request | update-request
 } ]
```

In 8.1 and later releases:

```
failure-handling cc-request-type { any-request | initial-request |
terminate-request | update-request } { diameter-result-code { any-error
| result_code [ to end_result_code ] } } { continue [ retry-server-on-event |
send-ccrt-on-call-termination ] | retry-and-terminate | terminate }
no failure-handling cc-request-type { any-request | initial-request |
terminate-request | update-request } [ diameter-result-code { any-error
```

```
| result_code [ to end_result_code] } ] [ continue {
send-ccrt-on-call-termination } ]
```

no

Disables previous failure-handling configuration.

retry-and-terminate

Specifies that in the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.

terminate

Specifies that in the event of a failure the user session be terminated.

diameter-result-code { any-error | *result_code* [to *end_result_code*] }

Specifies failure handling behavior for any/specific result-code(s) to identify the type of failure and failure handling action for specific credit control request type.

any-error: Specifies failure handling behavior for those result-codes for which failure-handling behavior has not been specified.

result_code: Specifies a Diameter failure result code. *result_code* is the code returned for a failure handling action and must be an integer from 3000 through 4999.

to *end_result_code*: Use to specify a range of Diameter failure result codes. *end_result_code* must be an integer from 3000 through 4999, and must be greater than *result_code*.

continue [retry-server-on-event | send-ccrt-on-call-termination] | retry-and-terminate | terminate

As in 8.1 and later releases:

Specifies the credit control failure handling action.

- **continue**: In the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.
  - **retry-server-on-event**: This optional keyword enables reconnecting with PCRF server on update and termination requests or re-authorization from server, for failure-handling CONTINUE sessions.

Important This keyword is valid only for **update-request** though it is allowed to configure for all the requests. The **failure-handling** command configuration will throw an error/warning message if it is configured for any request other than the update request.

Important Failure handling action "**continue retry-server-on-event**" will be taken only if failure happens to CCR-U message, not for CCR-I messages.

send-ccrt-on-call-termination: This optional keyword enables to send CCR-T on call termination if the failure action is **continue**.

Important This keyword is valid only for **update-request** though it is allowed to configure for all the requests. The **show configuration errors** command will throw an error/warning message if it is configured for any request other than the update request.

- **retry-and-terminate**: In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.
- **terminate**: In the event of a failure the user session is terminated.

ccfh { continue | retry-and-terminate | terminate }

As in 8.0 release:

Specifies the credit control failure handling (CCFH) action with or without credit control request type.

- **continue**: In the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.
- **retry-and-terminate**: In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.
- **terminate**: In the event of a failure the user session is terminated.

cc-request-type

As in 8.0 release:

This optional keyword defines the type of credit control request with failure result code and credit control failure handling action for a session.

- **any-request**: Specifies the request type as any request for a new session.
- **initial-request**: Specifies the request type as initial request for a new session.
- **terminate-request**: Specifies the request type as terminate request for a session.
- **update-request**: Specifies the request type as update request for an active session.

Usage Guidelines

Use this command to configure the Diameter Policy Control Application (DPCA) failure handling behavior.

When an unknown rulebase comes in CCA, changing of rulebase and failure handling is managed in the following manner:

- If the new and existing rulebases have the same CCA policy, then switch to the new rulebase is successful.
- If the new rulebase is valid and has CCA-enabled, in CCA-Initial/Update request, switch to the new rulebase is successful.

- If the new rulebase is valid and does NOT have CCA enabled, whereas the existing rulebase has credit enabled, or vice versa, in CCA-Initial/Update request:
  - CCFH-Continue: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-RETRY and TERMINATE: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-TERMINATE: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
- If the new rulebase is invalid, in CCA-Initial/Update request:
  - CCFH-Continue: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  - CCFH-RETRY and TERMINATE: Terminates on successful CCA-T, or terminates after successful/failed retry to secondary.
  - CCFH-TERMINATE: Terminates on successful/failed CCR-T to Primary.

The default failure handling behavior is:

failure-handling diameter-result-code any-error ccfh terminate

In StarOS release 14.1 and earlier, when an IP CAN session is up, if any CCR-U message delivery fails due to timeout or TCP link failure, the failure-handling action "**continue**" will be taken for the session and there will not be any further interaction with PCRF and RAR from PCRF is also not accepted (result code 5002 is sent in RAA). If the CCR-U that is triggered for reporting Usage-Monitoring-Information AVP fails, then the usage information is lost.

In 15.0 and later releases, after the IP-CAN session is up, if CCR-U message delivery fails due to timeout or TCP link failure, the failure-handling action "**continue retry-server-on-event**" will be taken at PCEF. Any request coming from session manager will be forwarded to PCRF, and if message delivery again fails session manager will be notified with status "SN_STATUS_NO_ACTIONS_TAKEN".

If CCR-U for reporting Usage-Monitoring-Information fails, then the unreported usage information is given back to ECS and the usage information is stored at ECS. Usage will be reported in CCR-T or in the next CCR-U (if CLI "**event-update send-usage-report**" is configured). Also, RAR message from PCRF will be processed and responded with result-code success in RAA.

Important Unreported usage will be lost, if CCR-U message delivery fails for last rule removal or usage reporting for monitoring stop indication from PCRF. Also, note that preserving unreported usage monitoring information is currently not supported for dpca-custom9 dictionary.

Example

The following command sets the DPCA failure handling to **retry-and-terminate** and return a result code of *3456* for credit control request type **initial-request**:

As in 8.0 release:

failure-handling diameter-result-code *3456* **ccfh retry-and-terminate cc-request-type initial-request**

As in 8.1 and later releases:

failure-handling cc-request-type initial-request diameter-result-code *3456* **retry-and-terminate**

li-secret

Refer to the *Cisco ASR 5000 Lawful Intercept Configuration Guide* for a description of this command.

max-outstanding-ccr-u

This command enables or disables the gateway to send multiple back-to-back CCR-Us to PCRF.

Product

GGSN

HA

PDSN

P-GW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context *context_name* **> ims-auth-service** *service_name* **> policy-control**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-imsa-dpca)#`

Syntax Description

[default] max-outstanding-ccr-u *value*

default

This keyword sets the default value as 1 for the maximum number of outstanding CCR-U messages to be sent to PCRF.

value

This keyword configures a value for the maximum number of outstanding CCR-U messages to be sent to PCRF.

value must be an integer value from 1 through 12.

Usage Guidelines

This command enables the gateway to send multiple outstanding CCR-Us per session to PCRF.

In releases prior to 17.0, ASR5K node supports only one pending CCR-U message per session over Gx interface. Any request to trigger CCR-U (for access side updates/internal updates) were ignored/dropped, when there was already an outstanding message pending at the node. PCEF and PCRF were out of synch if CCR-U for critical update (like RAT change/ULI change) was dropped.

In 17.1 and later releases, this CLI command "**max-outstanding-ccr-u**" under IMS Authorization Service configuration mode allows multiple CCR-Us towards PCRF. That is, this CLI will allow the user to configure a value of up to 12 as the maximum number of CCR-U messages per session.

The CLI-based implementation allows sending request messages as and when they are triggered and processing the response when they are received. The gateway does re-ordering if the response messages are received out of sequence.

Example

The following command configures the maximum number of outstanding CCR-U messages as 2.

```
max-outstanding-ccr-u 2
```

subscription-id service-type

This command enables required subscription-id types for various services. The Subscription-ID AVP will be encoded based on the configured subscription-ID type.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > **context** *context_name* > **ims-auth-service** *service_name* > **policy-control**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Syntax Description

```
subscription-id service-type { closed_rp | ggsn | ha | ipsg | l2tplns |
mipv6ha | pdsn | pgw | samog-epdg } { e164 | imsi | nai } +
{ default | no } subscription-id service-type { closed_rp | ggsn | ha |
ipsg | l2tplns | mipv6ha | pdsn | pgw | samog-epdg }
```

default | no

Configures this command with the default setting.

The default behavior is that Subscription-ID AVP will be encoded based on service-type and Diameter dictionary.

{ closed_rp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw | samog-epdg }{ e164 | imsi | nai }

Controls the encoding of Subscription-ID AVP based on the following service-types associated with services such as GGSN, HA, IPSG, PDSN, SaMOG, ePDG,etc.

- E164
- IMSI
- NAI

In Release 21, **samog-epdg** service type is added to allow encoding of Subscription-ID with a combination of MSISDN, NAI or IMSI in CCR for SaMOG (S2a) or ePDG (S2b) service for WLAN access types (trusted and untrusted 3GPP access types). This keyword is supported to send the Subscription-ID AVP with MSISDN in CCR-I or CCR-U towards PCRF. For more information on the functionality, see the *Gx Interface Support* chapter in the administration guide of the product you are deploying.

+

Indicates that more than one of the keywords can be entered in a single command.

Usage Guidelines

In releases prior to 15.0, Subscription-ID AVP is encoded based on service-type and Diameter dictionary.

In 15.0 and later releases, when IMS Authorization service encodes the Subscription-ID AVP, IMSA will first check whether or not this CLI command **subscription-id service-type** is configured. If the CLI is configured for the current service, then IMSA will encode the Subscription-ID AVP based on the configured subscription-ID type. This CLI command takes more precedence than the default behavior.

If the CLI configuration does not encode any Subscription-ID AVP, then IMSA will encode this AVP based on the default behavior. For example, in GGSN/IPSG service, NAI support is not available. If this CLI command is configured for GGSN/IPSG service with NAI type, then based on CLI IMSA cannot encode any Subscription-ID AVP. By this time default behavior (old behavior based on service-type and dictionary) will add the subscription-ID.

Example

The following command enables encoding of the Subscription-ID AVP based on IMSI parameter for GGSN service:

```
subscription-id service-type ggsn imsi
```

CHAPTER 109

Plugin Configuration Mode Commands

You enter this mode using the **plugin** command in the Global Configuration mode.

Command Modes

This chapter describes the commands available in the Plugin Configuration Mode. This mode is associated with the Dynamic Software Upgrade (DSU) process described in the *System Administration Guide*.

Exec > Global Configuration > Plugin Configuration

configure > plugin *plugin_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-plugin-plugin_name)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

attribute

This command is not supported in this release.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Plugin Configuration

configure > plugin *plugin_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-plugin-plugin_name)#
```

Syntax Description **attribute** *attribute_name attribute_value*

Usage Guidelines The command is not supported in this release.

module priority

Configures the priority in the Version Priority List (VPL) for a specified version of a plugin module.

Product ADC

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Plugin Configuration

configure > plugin *plugin_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-plugin-plugin_name)#
```

Syntax Description **module priority** *number* **version** *plugin_version* **attribute** *attribute_name attribute_value*
no module priority *number*

no

Removes the configured priority in the module priority list.

priority *number*

Specifies the priority of the plugin module as an integer from 1 through 100. Priority "1" has the highest priority.

version *plugin_version*

Specifies the version number of the plugin module. The version number is derived from the filename of the downloaded plugin.

attribute *attribute_name attribute_value*

Specifies an attribute value pair.

attribute_name specifies the name of an attribute value pair as an alphanumeric string from 1 through 255 characters.

attribute_value specifies the value of an attribute value pair as an alphanumeric string from 1 through 255 characters.

Usage Guidelines Assign a priority number to a specific version of patch for the corresponding plugin. The priority number in the module priority list determines which version will be loaded when the **update module** command is used.

The **show plugin** command displays the VPL configuration status of this plugin module.

Example

The following command sets the priority of p2p plugin module version *1.17.4340* to *2* where the filename was **libp2p-1.2.0.so.tgz**:

```
module priority 2 version 1.2.0
```

CHAPTER 110

PVC Configuration Mode Commands

Command Modes

The Permanent Virtual Connection (PVC) configuration mode commands bind IP interfaces or SS7-Frame Relay links a PVC as well as configure PVC operational parameters for a specific port.

Exec > Global Configuration > ATM Port Configuration > PVC Configuration

configure > port atm *slot_number/port_number* **> pvc vpi** *vpi_number* **vci** *vci_number*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-port-`*`slot_number/port_number`*`-pvc-`*`pvc_number/vci_number`*`)#`

Important The commands or keywords/variables that are available are dependent on platform type, version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

bind

This command binds an IP interface or an SS7 link to the PVC.

Important Prior to attempting the binding, the interface and context or the SS7 routing information and link must have been configured.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ATM Port Configuration > PVC Configuration

configure > port atm *slot_number/port_number* **> pvc vpi** *vpi_number* **vci** *vci_number*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-port-slot_number/port_number-pvc-pvc_number/vci_number)#`

Syntax Description

`[ no ] bind { interface` *`interface_name context_name`* **`| link ss7-routing-domain`** *`rd_id`* **`linkset-id`** *`id`* **`link-id`** *`id`* **`}`**

no

Removes the binding from the configuration.

interface_name

Defines the name of the virtual interface to be bound to the PVC. *interface_name:* Must be a unique string consisting of 1 to 79 alphanumeric characters.

context_name

Specifies the name of the context to be bound to the virtual interface. *context_name:* Must be a unique string consisting of 1 to 79 alphanumeric characters.

ss7-routing-domain *rd_id*

Identifies a specific SS7 routing domain. *rd_id* must be an integer from 1 to 12

linkset-id *id*

Identifies a specific linkset within the routing domain. *id*: must be an integer from 1 to 33

link-id *id*

Identifies a specific link within the linkset. *id*: must be an integer value 1 - 16

Usage Guidelines

Use this command to bind the PVC to an interface or a specific link.

Example

Use a command similar to the following to bind a PVC to a link ID #2:

`bind ss7-routing-domain` *`1`* **`linkset-id`** *`23`* **`link-id`** *`2`*

encapsulation aal5

Specify the data encapsulation type for the ATM adaptation layer 5 (AAL5) frames for the PVC.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ATM Port Configuration > PVC Configuration

configure > port atm *slot_number/port_number* **> pvc vpi** *vpi_number* **vci** *vci_number*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-port-slot_number/port_number-pvc-pvc_number/vci_number)#`

Syntax Description

`encapsulation aal5 { llc-snap | vc-mux }`

llc-snap

Frames protocol is identified in the AAL5 using logical link control (LLC) encapsulation.

vc-mux

Frames are not encapsulated and use virtual circuit multiplexing (VC-MUX) to identify the protocols used for the AAL5 frames.

Usage Guidelines

Use this command to identify the protocol type for the circuit.

Example

`encapsulation aal5 vc-mux`

shaping

Specify the type of traffic shaping (rates) for this PVC.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ATM Port Configuration > PVC Configuration

configure > port atm *slot_number/port_number* **> pvc vpi** *vpi_number* **vci** *vci_number*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-port-slot_number/port_number-pvc-pvc_number/vci_number)#`

Syntax Description

`shaping { cbr pcr` *`prc_num`* **`| ubr pcr`** *`prc_num`* **`| ubr+ pcr`** *`prc_num`* **`mrc`** *`mrc_num`* **`| vbr pcr`** *`prc_num`* **`scr`** *`src_num`* **`mbs`** *`mbs_num`* **`}`**

cbr

Constant bit rate

pcr - peak cell rate = cells per second

prc_num: Must be an integer from 75 to 1412830

ubr

Unspecified Bit Rate

pcr - peak cell rate = cells per second

prc_num: Must be an integer from 75 to 1412830

ubr+

Unspecified Bit Rate with Minimum Cell Rate.

The PCR and MCR values should be set to maintain the following relationship: PCR >= (MCR + minRate), where the current recomment minRate is 75.

pcr - peak cell rate = cells per second

prc_num: Must be an integer from 75 to 1412830

mcr - minimum cell rate

mrc_num: Must be an integer from 75 to 1412830

vbr

Variable Bit Rate, NRT (not real time) type.

The PCR and MCR values should be set to maintain the following relationship: PCR >= (MCR + minRate), where the current recomment minRate is 75.

pcr - peak cell rate = cells per second

prc_num must be an integer from 75 to 1412830

scr - sustained cell rate

src_num must be an integer from 75 to 1412830

mbs - maximum burst size

mbs_num must be an integer from 75 to 1412830

Usage Guidelines Use this command to configure the shaping for egress traffic on this PVC.

Example

```
shaping cbr pcr 56000
```

shutdown

Disables/enables traffic over the current VLAN.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ATM Port Configuration > PVC Configuration

configure > **port atm** *slot_number/port_number* > **pvc vpi** *vpi_number* **vci** *vci_number*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-port-`*`slot_number/port_number`*`-pvc-`*`pvc_number/vci_number`*`)#`

Syntax Description

shutdown
no shutdown

no

Enables the VLAN. When omitted the VLAN is non-functional.

Usage Guidelines

Enables/ Disables specified VLAN.

This command is necessary to bring a VLAN into service by enabling it via the **no** keyword.

Example

To disable a VLAN from sending or receiving network traffic use the following command:

shutdown

To enable a VLAN use the following command:

no shutdown

CHAPTER 111

PVC Interface Configuration Mode Commands

Command Modes

The PVC (permanent virtual connection) Interface configuration mode is used to create and manage the IP parameters for PVC interface(s) associated with an OLC (ATM-type) for a specific context.

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

description

Defines descriptive text to provide useful information about the current interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Syntax Description

description *text*
no description

no

Erases the port's description from the configuration file.

text

text: Must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

Usage Guidelines

Set the description to provide helpful information, for example the port's primary function, services, end users. Define any information, the only limit is the number of characters, 79.

Example

description *"PVC12 connects server 1 to home office."*

ip

The commands in this section are used to configure the IP parameters for the PVC interface.

Important Before configuring the OSPF parameters in this section, you need to enable OSPF using the router command and OSPF configuration sub-mode commands accessed in the Context configuration mode and documented in the Context Configuration Mode chapter of this Command Line Interface Reference.

ip access-group

This command identities the access control list (ACL to be associated with this PVC interface in this context.

Important Prior to using this command, the access list must be created for this context with the **ip access-list** command in the Context configuration mode and then the ACL must be configured using the commands described in CLI chapter ACL Configuration Mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-if-pvc)#`

Syntax Description

```
ip access-group name { in | out }
no ip access-group name { in | out }
```

no

Indicates the specified access group to be removed from the access list.

name

Specifies the access control list (ACL) rule to be added or removed from the group.

name: Must be a string of 1 to 79 alphanumeric characters with no spaces.

Important Up to 8 ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128 rule limit for the interface.

in | out

in: Specifies list is for in-bound access control.

out: Specifies the list is for out-bound access control.

Important Even though "in" or "out" can be specified, context-level ACL rules are automatically applied to both directions.

Usage Guidelines

Use this command to add IP access lists configured for the same context to an IP access-group. The list can be configured to apply to all inbound and/or outbound traffic.

Example

The following adds ACL access-list-1 to the IP access-group associated with this PVC for this context.

```
ip access-group access-list-1 in
```

ip address

Defines the primary IP address and the network mask to be associated with this PVC interface for this context. This command can also be used to configure the secondary IP address.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Syntax Description

```
ip address ip_address ip_mask [ secondary ]
no ip address ip_address
```

no

Removes the IP address information for this PVC from the configuration. It is not necessary to include the subnet mask with the command.

The command must first be issued with the secondary IP address if one exists and then re-issued with the primary IP address.

address *ip_address ip_mask*

Configures the IP address and the network mask for this PVC interface. The first time this command is entered, it automatically defines the primary IP address for this interface.

ip_address and *ip_mask* must be specified using the standard IPv4 or IPv6 dotted decimal notation.

secondary

secondary: Including this keyword indicates the IP address and subnet mask being defined are to be used as the secondary IP address for this PVC interface. This is referred to as multi-homing of the interface.

Usage Guidelines

Configures or deletes the IPv4 or IPv6 addresses and subnet mask to be associated with this PVC.

Example

The following configures the secondary IP address to associate with the interface.

```
ip address 131.2.3.4 255.255.255.224  secondary
```

The following set of commands removes the primary IP address from the PVC interface configuration for this context.

```
no ip address secondary address
no ip address primary address
```

ip mtu

Configures the maximum transmission unit (MTU) to be supported on this interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Syntax Description

ip mtu *value*
no ip mtu

no

Disables and/or restores the option to the system default.

mtu *value*

Configures the maximum transmission unit in octets.

value: Enter an integer between 576 and 1600. Default is 1500.

Usage Guidelines

Change the maximum transmission unit size to 1300.

Example

ip mtu *1300*

ip ospf authentication-key

This command configures the password or key to be used for OSPF (Open Shortest Path First) authentication with neighboring routers.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Syntax Description

```
ip ospf authentication-key [ encrypted ] password auth_key
no ip ospf authentication-key
```

no

Deletes the authentication key.

encrypted

Enter this keyword if you are pasting a previously encrypted authentication key into the **password** *auth_key* for this command.

password*auth_key*

auth_key is a string variable, from 1 through 16 alphanumeric characters, that denotes the authentication key (password). This variable is entered in clear text format.

Usage Guidelines

Use this command to set the authentication key used when authenticating with neighboring routers.

Example

To set the authentication key to 123abc, use the following command;

```
ip ospf authentication-key password 123abc
```

Use the following command to delete the authentication key;

```
no ip ospf authentication-key
```

ip ospf authentication-type

This command configures the OSPF authentication method to be used with OSPF neighbors over the logical interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Syntax Description

```
ip ospf authentication-type { message-digest | null | text }
no ip ospf authentication-type { message-digest | null | text }
```

no

Disable this function.

message-digest

Set the OSPF authentication type to use the message digest (MD) authentication method.

null

Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.

text

Set the OSPF authentication type to use the clear text authentication method.

Usage Guidelines

Use this command to set the type of authentication to use when authenticating with neighboring routers.

Example

To set the authentication type to use clear text, enter the following command;

```
ip ospf authentication-type text
```

ip ospf cost

This command configures the cost associated with sending a packet over this logical interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Syntax Description

ip ospf cost *value*
no ip ospf cost

no

Disable this function.

value

Default: 10

The cost to assign to OSPF packets. This must be an integer from 1 through 65535.

Usage Guidelines

Use this command to set the cost associated with routes from the interface.

Example

Use the following command to set the cost to 20;

```
ip ospf cost 20
```

Use the following command to disable the cost setting;

```
no ip ospf cost
```

ip ospf dead-interval

This command configures the dead-interval and the delay time in seconds, for OSPF communications.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Syntax Description

```
ip ospf dead-interval value
no ip ospf dead-interval
```

no

Deletes the value set and returns the value to its default.

value

The interval, in seconds, that the router should wait. During this interval, if no packets are received then the system considers the neighboring router to be off-line. This interval is typically 4 times the duration of the hello-interval.

value must be an integer from 1 through 65535. Default: 40

Usage Guidelines

Use this command to set the dead-intervals or delays for OSPF communications.

Example

To set the dead-interval to 100, use the following command;

```
ip ospf dead-interval 100
```

To delete the setting for the dead-interval and reset the dead-interval value to its default of 40, use the following command'

```
no ip ospf dead-interval
```

ip ospf hello-interval

This command configures the delay time in seconds, for OSPF hello interval.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Syntax Description

ip ospf hello-interval *value*
no ip ospf hello-interval

no

Deletes the value set and returns the value to its default.

value

The interval, in seconds, between sending hello packets. This value is typically set to be 1/4 of the value of the **dead-interval**.

value must be an integer from 1 through 65535. Default: 10

Usage Guidelines

Use this command to set the delays for the hello-interval.

Example

To set the hello-interval to 25, use the following command;

ip ospf hello-interval *25*

To delete the setting for the hello-interval and reset the hello-interval value to its default of 10, use the following command'

no ip ospf hello-interval

ip ospf message-digest-key

This command enables the use of MD5-based OSPF authentication.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Syntax Description

ip ospf message-digest-key *key_id* **md5 [encrypted] password** *authentication_key*
no ip ospfmessage-digest-key *key_id*

no

Deletes the key.

message-digest-key key_id

Specifies the key identifier number. key_id must be an integer from 1 through 255.

encrypted

Use this if you are pasting a previously encrypted authentication key into the CLI command.

password *authentication_key*

The password to use for authentication. *authentication_key* is a string variable, from 1 through 16 alphanumeric characters, that denotes the authentication password. This variable is entered in clear text format.

Usage Guidelines

Use this command to create an authentication key that uses MD5-based OSPF authentication.

Example

To create a key with the ID of 25 and a password of 123abc, use the following command;

ip ospf message-digest-key *25* **md5 password** *123abc*

To delete the same key, enter the following command;

no ip ospf message-digest-key *25*

ip ospf network

Configures the OSPF network type.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Syntax Description

```
ip ospf network { broadcast | non-broadcast | point-to-multipoint |
point-to-point }
no ip ospf network
```

no

Disable this function.

broadcast

Sets the network type to broadcast.

non-broadcast

Sets the network type to non-broadcast multi access (NBMA).

point-to-multipoint

Sets the network type to point-to-multipoint.

point-to-point

Sets the network type to point-to-point.

Usage Guidelines

Use this command to specify the OSPF network type.

Example

To set the OSPF network type to broadcast, enter the following command;

```
ip ospf network broadcast
```

To disable the OSPF network type, enter the following command;

```
no ip ospf network
```

ip ospf priority

This command designates the OSPF router priority.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

Syntax Description

ip ospf priority *value*
no ip ospf priority *value*

no

Disable this function.

value

The priority value to assign. This must be an integer from 0 through 255.

Usage Guidelines

Use this command to set the OSPF router priority.

Example

To set the priority to 25, enter the following command:

ip ospf priority *25*

To disable the priority, enter the following command:

no ip ospf priority

ip ospf retransmit-interval

This command configures the retransmit-interval and the delay time in seconds, for OSPF communications.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-if-pvc)#`

Syntax Description

ip ospf dead-interval *value*
no ip ospf dead-interval

no

Deletes the value set and returns the value to its default.

value

The interval, in seconds, between LSA (Link State Advertisement) retransmissions.

value must be an integer from 1 through 65535. Default: 5

Usage Guidelines

Use this command to set the retransmit-intervals or delays for OSPF communications.

Example

To set the dead-interval to 25, use the following command;

ip ospf retransmit-interval *25*

ip ospf transmit-delay

This command configures the transmit-delay the OSPF communications parameters.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context *context_name* **> interface** *interface_name* **point-to-point**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-if-pvc)#`

Syntax Description

ip ospf transmit-delay *value*
no ip ospf transmit-delay

no

Deletes the value set and returns the value to its default.

transmit-delay *value*

The interval, in seconds, that the router should wait before transmitting a packet.

value must be an integer from 1 through 65535. Default: 1

Usage Guidelines

Use this command to set the transmit-delay.

Example

To set the transmit delay to 5 seconds, use the following command;

ip ospf transmit-delay *5*

To delete the setting for the transmit-delay or reset the transmit-delay value to its default of 1, use the following command'

no ip ospf transmit-delay

CHAPTER 112

QCI - QoS Mapping Configuration Mode Commands

The QoS Class Index (QCI) to QoS Mapping Configuration Mode is used to map QoS Class Indexes to enforceable QoS parameters. Mapping can occur between the RAN and the Serving Gateway (S-GW), the Mobility Management Entity (MME), and/or the PDN Gateway (P-GW) in an LTE network or between the RAN and the eHRPD Serving Gateway (HSGW) in an eHRPD network.

Command Modes

Exec > Global Configuration > QCI-QoS Mapping Configuration

configure > qci-qos-mapping *name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-qci-qos-mapping)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

operator-defined-qci

Creates and maps non-standard QCI values to enforceable QoS parameters.

Product

P-GW

SAEGW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > QCI-QoS Mapping Configuration

configure > qci-qos-mapping *name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-qci-qos-mapping)#
```

Syntax Description

operator-defined-qci *num* **{ gbr | non-gbr } [{ downlink | uplkink } [encaps-header { copy-inner | copy-outer | dscp-marking** *dscp-marking-value* **} [internal-qos priority** *priority* **] | internal-qos priority** *priority* **| user-datagram dscp-marking** *dscp-marking-value* **[encaps-header { copy-inner | copy-outer | dscp-marking** *dscp-marking-value* **} [internal-qos priority** *priority* **]] | pre-rel8-qos-mapping** *num* **]**
no operator-defined-qci *num*

no

Disables the selected non-standard QCI value.

num

Specifies the non-standard, operator-defined QCI value to be enabled. *num* must be an integer from 128 through 254.

Important Standards-based QCI values 1 through 9 are configured through the **qci** command.

gbr

Specifies that this QCI type is Guaranteed Bit Rate (GBR).

non-gbr

Specifies that this QCI type is non-Guaranteed Bit Rate (non-GBR).

downlink

Configures parameters for downlink traffic.

uplink

Configures parameters for uplink traffic.

encaps-header { copy-inner | copy-outer | dscp-marking *dscp-marking-value* }

Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.

- **copy-inner**: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.

- **copy-outer** used to copy the DSCP value coming in the data packet from S1u interface to the data packet sent on the S5 interface and vice-versa.
- **dscp-marking** *dscp-marking-value*: Specifies that the DSCP marking is to be defined by this keyword.

  dscp-marking-value is expressed as a hexadecimal number from 0x00 through 0x3F.

internal-qos priority *priority*

Sets the internal QoS. These get resolved in L2 values.

priority is an integer value from 0 through 7.

user-datagram dscp-marking *dscp-marking-value*

Specifies that the IP DSCP marking is to be defined by this keyword.

dscp-marking-value is expressed as a hexadecimal number from 0x00 through 0x3F.

pre-rel8-qos-mapping *num*

Maps non-standard QCI to a standard QCI that has the characteristics (TC, THP, SI, TD, SSD) similar to desired pre-rel8 standard QoS values during 3G call or GnGp handover.

num must be an integer from:

- 1 through 4 for GBR
- 5 through 9 for non-GBR

Important If the wrong value is chosen, one of the following configuration errors will appear: "Failure: Only QCI range 1 - 4 are allowed for GBR QCI" or "Failure: Only QCI range 5 - 9 are allowed for Non-GBR QCI".

QCI values 1 through 9 are defined in *3GPP Specification TS 23.203 "Policy and charging control architecture"*.

Usage Guidelines

Use this command to create and map non-standard QCI values to enforceable QoS parameters in P-GW so that calls can be accepted when non-standard QCI values are received from UE or PCRF.

Important Use of non-standard QCIs require that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

3G GGSN Call

If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI under P-GW which is associated with a GGSN, then the 3G call would be rejected.

GnGp Handoff

1. If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI for default bearer, then the handoff would be rejected.
2. If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI for dedicated bearer, then only that bearer would be rejected during handoff.

3. In the following scenario:
   - default bearer with standard QCI or non-standard QCI (with **pre-rel8-qos-mapping** configured)
   - more than one dedicated bearer (some with standard QCI, some with non-standard QCI with **pre-rel8-qos-mapping** configured, and some with non-standard QCI with no mapping)

   During LTE-to-GnGp handoff:
   - UPC Request for all the dedicated bearers with non-standard QCI with no mapping would be rejected
   - handoff will be successful for the remaining bearers

Example

The following command creates an operator-defined GBR QCI value of *129* and maps it to a pre-rel8 standard QoS value of *2*:

```
operator-defined-qci 129 gbr pre-rel8-qos-mapping 2
```

qci

Creates and maps standard QCI values to enforceable QoS parameters.

Product

HSGW

P-GW

SAEGW

S-GW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > QCI-QoS Mapping Configuration

configure > qci-qos-mapping *name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-qci-qos-mapping)#
```

Syntax Description

Syntax for StarOS releases 16 and forward

qci *num* **[arp-priority-level** *arp_value* **] [downlink [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]] [uplink [downlink] [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]]**

qci *num* **[delay-class** *delay-class-value* **precedence-class** *precedence-class-value* **reliability-class** *reliability-class-value* **[downlink [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]] [uplink [**

downlink] [encaps-header { copy-inner | dscp-marking *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]]]**

qci *num* **[downlink [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]]**

qci *num* **[gbr [delay-class** *delay-class-value* **precedence-class** *precedence-class-value* **reliability-class** *reliability-class-value* **] [downlink [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]] [max-packet-delay** *max-packet-delay-value* **max-error-rate** *max-error-rate* **] [traffic-policing interval** *value* **] [uplink [downlink] [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]]]**

qci *num* **[max-packet-delay** *max-packet-delay-value* **max-error-rate** *max-error-rate* **[downlink [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]] [uplink [downlink] [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]]]**

qci *num* **[non-gbr [delay-class** *delay-class-value* **precedence-class** *precedence-class-value* **reliability-class** *reliability-class-value* **] [downlink [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]] [max-packet-delay** *max-packet-delay-value* **max-error-rate** *max-error-rate* **] [traffic-policing interval** *value* **] [uplink [downlink] [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]]]**

qci *num* **[pre-rel8-qos-mapping** *num* **]**

qci *num* **[traffic-policing interval** *interval* **[delay-class** *delay-class-value* **precedence-class** *precedence-class-value* **reliability-class** *reliability-class-value* **] [downlink [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]] [max-packet-delay** *max-packet-delay-value* **max-error-rate** *max-error-rate* **] [uplink [downlink] [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]]]**

qci *num* **[uplink [downlink] [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **}] [internal-qos priority** *priority* **] [user-datagram dscp-marking** *dscp-marking-value* **]]**

[default | no] qci *num* **[arp-priority-level** *arp_value* **]**

Important The optional keywords associated with each of the initial optional keywords are abbreviated in the syntax examples above for clarity. Refer to the definitions below for the full keyword paths and associated descriptions for each keyword string in this command.

default

Resets the default values for the select QCI value.

no

Disables the selected QCI value.

num

Specifies the QCI value to be enabled; must be an integer between 1-9, or 128-254, or 65, 66, 69, 70, 80, 82, 83.

QCI values 1 through 9 are defined in *3GPP Specification TS 23.203 "Policy and charging control architecture"*.

In release 21 and forward, QCI options 65 and 66 are available for guaranteed bit rate (GBR) network initiated QCI values only.

In release 21 and forward, QCI options 69 and 70 are available for non-GBR network initiated QCI values only.

arp-priority-level *arp_value*

Specifies the address retention priority (ARP) priority level.

arp_value must be an integer from 1 through 15.

delay-class *delay-class-value* precedenced-class *precedence-class-value* reliability-class *reliability-class-value*

delay-class: Specifies the pre-release 8 value for configuring packet delay.

delay-class-value must be an integer from 1 through 9.

precedence-class: Specifies the pre-release 8 value for configuring packet precedence.

precedence-class-value must be an integer from 1 through 32.

reliability-class: Specifies the pre-release 8 value for configuring packet reliability.

reliability-class-value must be an integer from 1 through 32.

downlink

Configures parameters for downlink traffic.

encaps-header { copy-inner | dscp-marking *dscp-marking-value* }

encaps-header: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.

- **copy-inner**: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.
- **dscp-marking** *dscp-marking-value*: Specifies that the DSCP marking is to be defined by this keyword.

  dscp-marking-value is expressed as a hexadecimal number from 0x00 through 0x3F.

gbr

Specifies that this QCI type is Guaranteed Bit Rate (GBR).

internal-qos priority *priority*

Sets the internal QoS. These get resolved in L2 values.

priority is an integer value from 0 through 7.

max-packet-delay *max-packet-delay-value* max-error-rate *max-error-rate*

max-packet-delay *num*: Specifies the maximum packet delay (in milliseconds) that can be applied to the data with the QCI.

max-packet-delay-value must be an integer from 10 through 1000.

max-error-rate *num*: Specifies the maximum error loss rate of non-congestion related packet loss.

max-error-rate must be an integer from 1 through 6, specifying 10-1 through 10-6.

Important Defaults for standards-based QCI values are defined in *3GPP Specification TS 23.203 "Policy and charging control architecture"*.

non-gbr

Specifies that this QCI type is non-Guaranteed Bit Rate (non-GBR).

pre-rel8-qos-mapping

Specifies the standard QCI to be mapped. Must be an integer from 1 to 9. Values 1 through 4 correspond to GBR QCIs and values 5 through 9 corresponds to non-GBR QCIs.

traffic-policing interval *interval*

Specifies the traffic policing interval associated with the this QCI.

interval must be an integer from 1 through 100.

uplink

Configures parameters for uplink traffic.

user-datagram dscp-marking *dscp-marking-value*

user-datagram dscp-marking: Specifies that the IP DSCP marking is to be defined by this keyword.

dscp-marking-value is expressed as a hexadecimal number from 0x00 through 0x3F.

Syntax Description

Syntax for StarOS releases 15 and earlier

```
qci num [ delay-class num precedence-class num reliability-class num [
downlink | uplink ] ]

qci num [ downlink [ 802.1p-value priority | encaps-header { copy-inner [
802.1p-value priority ] | dscp-marking hex [ 802.1p-value priority ] } |
user-datagram dscp-marking hex [ 802.1p-value priority ] | encaps-header {
copy-inner [ 802.1p-value priority ] | dscp-marking hex | copy-outer [
802.1p-value priority ] } ] ]

qci num [ gbr [ delay-class | downlink | max-packet-delay | traffic-policing
 | uplink ] ]

qci num [ max-packet-delay num max-error-rate num [ downlink | uplink ] ]

qci num [ non-gbr [ delay-class | downlink | max-packet-delay |
traffic-policing | uplink ] ]

qci num  [ traffic-policing interval interval [ delay-class | downlink |
max-packet-delay | uplink ] ]

qci num [ uplink [ 802.1p-value priority | encaps-header { copy-inner [
802.1p-value priority ] | dscp-marking hex | copy-outer[ 802.1p-value priority
 ] } | mpls-exp-value value [ downlink { 802.1p-value priority | encaps-header
 { copy-inner [ 802.1p-value priority ] | dscp-marking  hex| copy-outer }
| user-datagram dscp-marking hex [ 802.1p-value priority | encaps-header {
 copy-inner [ 802.1p-value priority ] | dscp-marking hex [ 802.1p-value
priority ] } ] ] ]| user-datagram dscp-marking hex [ 802.1p-value priority ]
 | encaps-header { copy-inner [ 802.1p-value priority ] | dscp-marking |
copy-outer hex [ 802.1p-value priority ] } ] ]

[ default | no ] qci num
```

Important The optional keywords associated with each of the initial optional keywords are abbreviated in the syntax examples above for clarity. Refer to the definitions below for the full keyword paths and associated descriptions for each keyword string in this command.

default

Resets the default values for the select standards-based QCI value.

no

Disables the selected standards-based QCI value.

num

Specifies the standards-based QCI value to be enabled.

num must be an integer from 1 through 256.

Important Only standards-based QCI values of 1 through 9 are supported.

QCI values 1 through 9 are defined in *3GPP Specification TS 23.203 "Policy and charging control architecture"*.

delay-class *num* precedence-class *num* reliability-class *num*

delay-class *num*: Specifies the pre-release 8 value for configuring packet delay.

num must be an integer from 1 through 32.

precedence-class *num*: Specifies the pre-release 8 value for configuring packet precedence.

num must be an integer from 1 through 32.

reliability-class *num*: Specifies the pre-release 8 value for configuring packet reliability.

num must be an integer from 1 through 32.

downlink [802.1p-value *priority* | encaps-header { copy-inner [802.1p-value *priority*] | dscp-marking *hex* [802.1p-value *priority*] } | user-datagram dscp-marking *hex* [802.1p-value *priority*] | encaps-header { copy-inner [802.1p-value *priority*] | dscp-marking *hex* | copy-outer[802.1p-value *priority*] }]]

Configures parameters for downlink traffic.

802.1p-value *priority*: Maps the qci value to the priority value set in the Ethernet frame header.

priority is an integer value from 0 through 7.

encaps-header: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.

user-datagram dscp-marking *hex*: Specifies that the IP DSCP marking is to be defined by this keyword.

hex is expressed as a hexadecimal number from 0x00 through 0x3F.

{ copy-inner | dscp-marking *hex* **| copy-outer }**

- **copy-inner**: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.
- **dscp-marking** *hex*: Specifies that the DSCP marking is to be defined by this keyword.

  hex ia expressed as a hexadecimal number from 0x00 through 0x3F.
- **copy-outer** used to copy the DSCP value coming in the data packet from S1u interface to the data packet sent on the S5 interface and vice-versa.

gbr

Specifies that this QCI type is Guaranteed Bit Rate (GBR).

max-packet-delay *num* max-error-rate *num*

max-packet-delay *num*: Specifies the maximum packet delay (in milliseconds) that can be applied to the data with the QCI.

num must be an integer from 10 through 1000.

max-error-rate *num*: Specifies the maximum error loss rate of non-congestion related packet loss.

num must be an integer from 1 through 6, specifying 10-1 through 10-6.

Important Defaults for standards-based QCI values are defined in *3GPP Specification TS 23.203 "Policy and charging control architecture"*.

non-gbr

Specifies that this QCI type is non-Guaranteed Bit Rate (non-GBR).

traffic-policing interval *interval*

Specifies the traffic policing interval associated with the this QCI.

interval must be an integer from 1 through 100.

uplink [802.1p-value *priority* | encaps-header { copy-inner [802.1p-value *priority*] | dscp-marking *hex* [802.1p-value *priority*] } | mpls-exp-value *value* [downlink { 802.1p-value *priority* | encaps-header { copy-inner [802.1p-value *priority*] | dscp-marking *hex* } | user-datagram dscp-marking *hex* [802.1p-value *priority* | encaps-header { copy-inner [802.1p-value *priority*] | dscp-marking *hex*| copy-outer [802.1p-value *priority*] }]]] | user-datagram dscp-marking *hex* [802.1p-value *priority*] | encaps-header { copy-inner [802.1p-value *priority*] | dscp-marking *hex* [802.1p-value *priority*] }]]

Configures parameters for uplink traffic.

802.1p-value *priority*: Maps the qci value to the priority value set in the Ethernet frame header.

priority is an integer value from 0 through 7.

encaps-header: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.

mpls-exp-value *value*: Sets EXP bits for MPLS for mobile to egress side traffic.

value is an integer value from 0 through 7.

user-datagram dscp-marking *hex*: Specifies that the IP DSCP marking is to be defined by this keyword.

hex is expressed as a hexadecimal number from 0x00 through 0x3F.

{ copy-inner | dscp-marking *hex*| **copy-outer }**

- **copy-inner**: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.
- **dscp-marking** *hex*: Specifies that the DSCP marking is to be defined by this keyword.

  hex is expressed as a hexadecimal number from 0x00 through 0x3F.
- **copy-outer** used to copy the DSCP value coming in the data packet from S1u interface to the data packet sent on the S5 interface and vice-versa.

Usage Guidelines

Use this command to create and map QCI values to enforceable QoS parameters.

Important Non-standard QCI values are only supported with the license-enabled **operator-defined-qci** command.

Example

The following command creates a QCI value of *8* and defines the uplink encapsulation header as using the DSCP marking from the encapsulated UDP header:

```
qci 8 uplink encaps-header copy-inner
```

CHAPTER 113

QCI - RAN ID Mapping Configuration Mode Commands

The QoS Class Index (QCI) Mapping Configuration Mode is used to map RAN profile IDs to QoS Class Indexes via the HRPD Serving Gateway (HSGW) in an eHRPD network.

Command Modes

Exec > Global Configuration > QCI - RAN ID Mapping Configuration

configure > profile-id-qci-mapping-table *name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-profile-id-qci-mapping-table)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

profile-id

Maps a QCI ID to a RAN profile ID and modifies data flow bit rate ranges.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > QCI - RAN ID Mapping Configuration

configure > profile-id-qci-mapping-table *name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-profile-id-qci-mapping-table)#
```

Syntax Description

profile-id *id* **qci** *num* **[uplink { gbr** *rate* **[mbr** *rate* **] | mbr** *rate* **[gbr** *rate* **] } downlink { gbr** *rate* **[mbr** *rate* **] | mbr** *rate* **[gbr** *rate* **]]**
no profile-id *id*

no

Removes the specified profile ID entry from this map.

id

Specifies the profile ID to which a QCI ID will be mapped. *id* must be an integer value from 1 to 65535.

qci *num*

Specifies the QCI number to which the profile ID will be mapped. *num* must be an integer value from 1 to 255.

uplink

Specifies that the guaranteed bit rate (GBR) and/or maximum bite rate (MBR) setting that follow this keyword will be applied to the uplink data flow.

downlink

Specifies that the guaranteed bit rate (GBR) and/or maximum bite rate (MBR) settings that follow this keyword will be applied to the downlink data flow.

gbr *rate*

Specifies the guaranteed bit rate for the uplink or downlink data flow. *rate* must be an integer value from 0 to 4294967295.

mbr *rate*

Specifies the maximum bit rate for the uplink or downlink data flow. *rate* must be an integer value from 0 to 4294967295.

Usage Guidelines

Use this command to map a QCI ID to a RAN profile ID and, optionally, modify data flow bit rate ranges.

Example

The following command maps a QCI ID (*1*) to a profile ID (*10*) and sets the uplink guaranteed bite rate to *10000* and the downlink guaranteed bit rate to *20000*:

```
profile-id 10 qci 1 uplink gbr 10000 downlink gbr 20000
```

CHAPTER 114

QoS L2 Mapping Configuration Mode Commands

The QoS Mapping Mode is used to map internal QoS priority with Class of Service (CoS) values.

Command Modes

Exec > Global Configuration > QoS L2 Mapping Configuration

configure > qos-l2-mapping

Enter the above command sequence results in the following prompt:

```
[local] host_name (config-qos-l2-mapping)#
```

The commands or keywords/variables that are available are dependent on platform type, product version and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

internal-priority

Maps internal QoS priority with Class of Service (COS) values

Product

ePDG

HSGW

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Qos L2 Mapping Configuration

configure > **qos l2-mapping-table { name** *map_table_name* **| system-default }**

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-qos-l2-mapping)#
```

Syntax Description

internal-priority cos *class_of_service_value* **color** *color_value* **[802.1p-value** *802.1p_value* **] [mpls-tc** *mpls_tc_value* **]**
default internal-priority cos *cos_value* **color** *color_value*

default

Restores default value assigned for specified parameter.

cos *class_of_service_value*

Maps to the internal QoS priority/COS.

class_of_service_value must be a Hexadecimal number between 0x0 and 0x7.

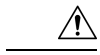
color *color_value*

Controls drop precedence of service to map to.

color_value must be a Hexadecimal number between 0x0 and 0x3.

802.1p-value *802.1p_value*

Map to a 802.1p value. This also includes both P-bits and DEI/CFI. DEI is the lsb bit.



Caution Setting an odd value (DEI/CFI to 1) makes some switches drop packets.

802.1p_value must be a Hexadecimal number between 0x0 and 0xF.

mpls-tc *mpls_tc_value*

Map to an MPLS traffic class.

mpls_tc_value must be a Hexadecimal number between 0x0 and 0x7.

Usage Guidelines

This command is used to map internal QoS priority with COS values.

Important The **internal-priority** CLI command also offers the ability to configure both 802.1p priority and setting of DEI/CFI bit. This flexibility installation will treat the bit as DEI (drop eligibility indicator). However, for installations that treat the bit as CFI (canonical format indicator), this should be set to 0. Otherwise, the packet will be dropped.

Example

This command is used to map internal QoS priority with COS values:

```
internal-priority cos 0x2 color 0x1
```

CHAPTER 115

QoS Profile Configuration Mode Commands

Command Modes

The QoS Profile Configuration mode is used to create and configure a QoS Profile.

Exec > Global Configuration > Quality of Service Profile Configuration

configure > quality-of-service-profile

Entering the above command sequence results in the following prompt:

```
[local]host_name(qos-of-service-profile)#
```

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

Important For information on common commands available in this configuration mode, refer to the Common Commands, on page 1 chapter.

apn-ambr

Configures the APN-AMBR (aggregate maximum bit rate) that will be stored in the Home Subscriber Server (HSS).

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Quality of Service Profile Configuration

configure > quality-of-service-profile

Entering the above command sequence results in the following prompt:

```
[local]host_name(qos-of-service-profile)#
```

Syntax Description

apn-ambr max-ul *mbr-up* **max-dl** *mbr-dwn* **{ pgw-upgrade | prefer-as-cap } { local | minimum | rej-if-exceed }**
remove apn-ambr

remove

Removes the APN-AMBR changes from the configuration for this APN profile.

max-ul *mbr-up* max-dl *mbr-dwn*

Defines the maximum bit rates for uplink (subscriber to network) and downlink (network to subscriber) traffic.

mbr-up is an integer from 0 through 1410065408.

mbr-dwn is an integer from 0 through 1410065408.

prefer-as-cap

This keyword configures the capping that is applied on the subscription value received from the HSS or the value received from the peer-node (MME/S4-SGSN) during inbound relocation. One of the following actions must be configured under **prefer-as-cap** -- Note that the resulting value is used for the QoS parameter and sent in the Create Session Request or the Modify Bearer Command (in case of HSS-initiated QoS/APN-AMBR modification) message:

- **local** - The configured local value will be used.
- **minimum** - The minimum (lowest) value of the configured local value or the HSS-provided value will be used.
- **reject-if-exceed** - The request/procedure is rejected if the HSS-provided value exceeds the configured local value.

pgw-upgrade

MME only.

This keyword configures the QoS capping to be applied on the values received from the PGW during Attach / PDN-connectivity / Bearer-creation / Bearer-modification procedures. One of the following actions must be configured under **pgw-upgrade** -- Note that the resulting value is used for the QoS parameter and sent to the UE:

- **local** - The configured local value will be used.
- **minimum** - The minimum (lowest) value of the configured local value or the PGW-provided value will be used.
- **reject-if-exceed** - The request/procedure is rejected if the PGW-provided value exceeds the configured local value.

Usage Guidelines

Use this command to define the MBR that will be enforced by the P-GW for both uplink and downlink traffic shaping.

For the MME, use the **apn-ambr** command to set local values QoS capping type to be applied for the APN-AMBR received from HSS/PGW/peer-node. One or both **prefer-as-cap** and/or **pgw-upgrade** must be configured to override the default behavior, which is to accept the received value from the HSS/peer-node/PGW.

Example

A command similar to the following sets the APN-AMBR maximum uplink and maximum downlink bit rates for the QoS profile:

```
qos apn-ambr max-ul 24234222 max-dl 23423423
```

A command similar to the following sets the **prefer-as-cap minimum**capping action to be taken when the SGSN or MME receives outside of APN-AMBR maximum uplink and maximum downlink bit rates :

```
qos apn-ambr max-ul 24234222 max-dl 23423423 prefer-as-cap minimum
```

associate

This command associates a specific bearer control profile with this QoS profile.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Quality of Service Profile Configuration

configure > quality-of-service-profile

Entering the above command sequence results in the following prompt:

```
[local]host_name(qos-of-service-profile)#
```

Syntax Description

associate bearer-control-profile *bc_profile_name* **qci** *qci_value* **[to** *end_qci_value* **]**
remove associate bearer-control-profile *bc_profile_name*

remove

Add this command prefix to the command to delete the association between the QoS profile and the identified bearer-control-profile.

bc_profile_name

Identifies the name of the bearer control profile being associated with the QoS profile. Enter 1 to 64 alphanumeric characters.

qci *qci_value* [to *end_qci_value*]

qci - Identifies either a specific QoS class identifier (QCI) or a range of QCI:

- *qci_value* - Enter an integer from 1 through 9 to identify a specific QCI. You can enter the new standardized QCI values 65, 66, 67, 69 and 70.
- **to** *end_qci_value* - Type "to" and then enter an integer from 2 through 9 that is greater than the QCI value entered for the beginning of the range. You can enter the new standardized QCI values 65, 66, 67, 69 and 70.

Usage Guidelines

Use the **associate** command in Quality of Service Profile configuration mode to associate the bearer control profile with the QoS profile and map a specific QCI or a range of QCI to the bearer control profile being associated with the QoS profile.

A specific QCI cannot be associated to more than one bearer control profile. The QCI of the bearer is used to identify the applicable bearer control profile.

- For dedicated bearers, the QCI of bearer is initially determined by the QCI value received from PGW during dedicated bearer activation or the value received from peer MME/S4-SGSN.
- For default bearers, the QCI of bearer is initially determined by the subscription from HSS or the value received from peer MME/S4-SGSN during inbound relocation.

Example

The following sample command associates the *BCprof1* bearer control profile with the QoS profile and maps QCI *7* to this bearer control profile:

```
associate bearer-control-profile BCprof1 qci 7
```

class

Configures local values for the traffic class (TC) parameters for the quality of service (QoS) configured for this QoS profile.

Important To enable any of the values/features configured with this command, the **prefer-as-cap** configuration (also in the QoS profile configuration mode) must be set to either **local** or **both-hlr-and-local**.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Quality of Service Profile Configuration

configure > quality-of-service-profile

Entering the above command sequence results in the following prompt:

```
[local]host_name(qos-of-service-profile)#
```

Syntax Description

```
class { background | conversational | interactive | streaming } [
qualif_option ]
remove class { background | conversational | interactive | streaming } [
 qualif_option ]
```

remove

Removes previously defined values for the specified option or for an entire class if a qualifying option is not included in the command.

background

Selects the background traffic class. This 'best-effort' class manages traffic that is handled as a background function, like email, where time to delivery is not a key factor. The selection of background traffic class can be refined with the addition of one of the following qualifying options:

- **all-values**
- **arp**
- **evolved-arp**
- **mbr-down**
- **mbr-map-down**
- **mbr-map-up**
- **mbr-up**
- **residual-bit-error-rate**
- **sdu**

All qualifying options are explained below.

conversational

Selects the 'real-time' conversational traffic class of service, which has the most stringent time requirements of the four classes and is typically reserved for voice traffic. The section of the conversational traffic class can be refined with the addition of one of the following qualifying options:

- **all-values**
- **arp**
- **evolved-arp**
- **gbr-down**
- **gbr-up**
- **mbr-down**
- **mbr-map-down**
- **mbr-map-up**
- **mbr-up**
- **min-transfer-delay**
- **residual-bit-error-rate**
- **sdu**

All qualifying options are explained below.

interactive

Selects interactive traffic class of service. This class is characterized by a request/response pattern (someone sends data and then waits for a response) which requires the preservation of the data but delivers on a 'best-effort' model. The section of the interactive traffic class can be refined with the addition of one of the following qualifying options:

- **all-values**

- **arp**
- **evolved-arp**
- **mbr-down**
- **mbr-map-down**
- **mbr-map-up**
- **mbr-up**
- **residual-bit-error-rate**
- **sdu**
- **thp**

All qualifying options are explained below.

streaming

Selects the streaming traffic class of service, which handles one-way, real-time data transmission - such as streaming video or audio. The section of the interactive traffic class can be refined with the addition of one of the following qualifying options:

- **all-values**
- **arp**
- **evolved-arp**
- **gbr-down**
- **gbr-up**
- **mbr-down**
- **mbr-map-down**
- **mbr-map-up**
- **mbr-up**
- **min-transfer-delay**
- **residual-bit-error-rate**
- **sdu**

All qualifying options are explained below.

qualif_option

Qualifying options are the QoS parameters and they include:

- **all-values** - This option will change the configuration to predefined values for *all* the relevant QoS parameters for the class. This keyword is not used if other options are to be defined. The predefined values are:

Table 8: Predefined QoS Parameters

QoS Parameter	Predefined Value
Traffic Class	**Background**
SDU delivery order	No
Delivery of Erroneous SDUs	No
Max Bit Rate Uplink	64 kbps

QoS Parameter	Predefined Value
Max Bit Rate Downlink	64 kbps
Allocation/Retention Priority	3
SDU Max Size	1500 octets
SDU Error Ratio	3 (1 * 10 ^ -3)
Residual Bit Error Rate	4 (4 * 10 ^ -3)
Traffic Class	**Conversational**
SDU delivery order	No
Delivery of Erroneous SDUs	No
Max Bit Rate Uplink	16 kbps
Max Bit Rate Downlink	16 kbps
Allocation/Retention Priority	3
Guaranteed Bit Rate Uplink	16 kbps
Guaranteed Bit Rate downlink	16 kbps
SDU Max Size	1500 octets
Minimum Transfer Delay	100 milliseconds
SDU Error Ratio	1 (1 * 10 ^ -2)
Residual Bit Error Rate	1 (5 * 10 ^ -2)
Traffic Class	**Interactive**
SDU delivery order	No
Delivery of Erroneous SDUs	No
Max Bit Rate Uplink	64 kbps
Max Bit Rate Downlink	64 kbps
Traffic Handling Priority	3
SDU Max Size	1500 octets
SDU Error Ratio	3 (1 * 10 ^ -3)
Residual Bit Error Rate	4 (4 * 10 ^ -3)
Traffic Class	**Streaming**
SDU delivery order	No
Delivery of Erroneous SDUs	No
Max Bit Rate Uplink	16 kbps
Max Bit Rate Downlink	16 kbps

QoS Parameter	Predefined Value
Allocation/Retention Priority	3
Guaranteed Bit Rate Uplink	16 kbps
Guaranteed Bit Rate downlink	16 kbps
SDU Max Size	1500 octets
Minimum Transfer Delay	300 milliseconds
SDU Error Ratio	7 (1 * 10 ^ -3)
Residual Bit Error Rate	1 (5 * 10 ^ -2)

- **arp** - Sets the allocation/retention priority. Enter an integer from 1 to 3.
- **evolved-arp** - This keyword is used to configure the E-ARP values. The values for pre-emption capability, pre-emption vulnerability and priority value can be configured using this option.
  - **preemption-capability**: The value of **preemption-capability** is configured as either "0" or "1".
  - **preemption-vulnerability**: The value of **preemption-vulnerability** is configured as either "0" or "1".
  - **priority-level**: The **priority-level** can be configured as an integer value in the range "1" up to "15".
- **gbr-down** - Guaranteed Kbps rate for the downlink direction. Enter an integer from the range 1 to 256000.
- **gbr-up** - Guaranteed Kbps rate for the uplink direction. Enter an integer from 1 to 256000.
- **mbr-down** - Maximum Kbps rate for the downlink direction. Enter an integer from the range 1 to 256000.
- **mbr-map-down from** *from_kbps* **to** *to_kbps* - Map received HLR MBR (**from** value) to a locally configured downlink MBR value (**to** value):
  - *from_kbps* - Enter an integer from 1 to 25600.
  - *to_kbps* - Enter an integer from 1 to 25600.
- **mbr-map-up from** *from_kbps* **to** *to_kbps* - Map received HLR MBR (**from** value) to a locally configured uplink MBR value (**to** value):
  - *from_kbps* - Enter an integer from 1 to 25600.
  - *to_kbps* - Enter an integer from 1 to 25600.
- **mbr-up** - Maximum Kbps rate for the uplink direction. Enter an integer from 1 to 256000.
- **min-transfer-delay** - Minimum transfer delay in milliseconds. Enter an integer from 80 to 4000.
- **residual-bit-error-rate** -
  - Background TC residual-bit-error-rate range is from 4*10^-4 to 6*10^-8. Enter on of the following integers, where:
    - **4**: represents 4*10^-3
    - **7**: represents 10^-5
    - **9**: represents 6*10^-8
  - Conversational TC residual-bit-error-rate range is from 5*10^-2 to 10^-6. Enter one of the following integers, where:

- **1**: represents 5*10^-2
- **2**: represents 10^-2
- **3**: represents 5*10^-3
- **5**: represents 10^-3
- **6**: represents 10^-4
- **7**: represents 10^-5
- **8**: represents 10^-6

- Interactive TC residual-bit-error-rate range is from 4*10^-4 to 6*10^-8. Enter one of the following integers, where:
  - **4**: represents 4*10^-3
  - **7**: represents 10^-5
  - **9**: represents 6*10^-8

- Streaming TC residual-bit-error-rate range is from 5*10^-2 to 10^-6. Enter one of the following integers, where:
  - **1**: represents 5*10-2
  - **2**: represents 10^-2
  - **3**: represents 5*10^-3
  - **5**: represents 10^-3
  - **6**: represents 10^-4
  - **7**: represents 10^-5
  - **8**: represents 10^-6

- **sdu** - Signalling data unit keyword, must include one of the following options:
  - **delivery-order**- Enter one of the two following options:
    - **no**- Without delivery order
    - **yes**- With delivery order
  - **erroneous**- Enter one of the two following options:
    - **no**- Erroneous SDUs will not be delivered
    - **no-detect**- Erroneous SDUs are not detected ('-')
    - **yes**- Erroneous SDUs will be delivered
  - **error-ratio**- The SDU error-ratio range is from 10^-3 to 10^-6. Enter an integer from 1 to 6, where:
    - **3**- Represents 10^-3
    - **4**- Represents 10^-4
    - **6**- Represents 10^-6
  - **max-size**- Defines the maximum number of octets (size) of the SDU. Enter an integer from 10 to 1502.
- **thp** - Sets the traffic handling priority. Enter an integer from 1 to 3.

Usage Guidelines

This command defines the qualifying options (parameters) for each QoS traffic class defined for this QoS profile.

Repeat the command as often as needed with different options to define all required QoS criteria. For example, to configure the maximum bit rate (MBR) for the downlink and uplink directions for a traffic class, this command must be used twice, specifying **mbr-down** once and **mbr-up** once.

Advantage for local mapping of MBR: some HLRs cannot be configured with high MBR values. Using the **mbr-map-up** and the **mbr-map-down** parameters allows the SGSN to be configured to treat a specific HLR value as meaning the desired high MBR value. In a case where the HLR does not support HSPA+ bit rates, but the handsets and network do, this feature allows the operator to overcome limitations on the HLR and provide HSPA+ bit rates by overwriting the provisioned HLR-QoS MBR values with SGSN-configured values. When MBR mapping is configured, if QoS is preferred as the HLR value, then the subscription QoS MBR received from the HLR is compared with the "from" value in the table. If it matches, then it is converted to the value specified by the "to" value in the table. QoS negotiation happens based on the converted value.

Advantage for QoS capping with THP and ARP: Controlling THP and ARP via Operator Policy: This functionality can differentiate home vs. roaming subscribers, and prevent visiting subscribers from receiving a high-tiered service. For example, a service provider could offer service differentiation using Ultra/Super/Standard service levels based upon QoS; this could justify charging a corporate customer more to use the Internet APN than would be charged to a consumer. This could be accomplished by controlling the traffic handling priority (THP) over the air interface, i.e. THP 1 = Ultra, THP 2 = Super and THP 3 = Standard.

Example

Use the following command to configure the entire conversational traffic class with predefined QoS options:

```
class conversational all-values
```

Now change the background class ARP from 3 to 2:

```
class background arp 2
```

Invalidate the THP parameter, by removing all value from the parameter, for the interactive class:

```
remove class interactive thp
```

description

Defines a descriptive string relevant to the specific QoS profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Quality of Service Profile Configuration

configure > quality-of-service-profile

Entering the above command sequence results in the following prompt:

```
[local]host_name(qos-of-service-profile)#
```

Syntax Description

description *description*
remove description

remove

Removes the configured description from this QoS profile.

description

Specifies a description for this QoS profile as an alphanumeric string of 1 through 100 characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotation marks (").

Usage Guidelines

Define information that identifies this particular QoS profile.

Example

Indicate that QoS profile *qosprof1* is to be used for customers in India and that the profile was created on April 10th of 2014:

```
description "qosprof1 defines QoS for customers in India (4/10/14)."
```

epc-qos-params-in-gtpv1

This command enables or disables the SGSN to send EPC QoS parameters to the GGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Quality of Service Profile Configuration

configure > quality-of-service-profile

Entering the above command sequence results in the following prompt:

```
[local]host_name(qos-of-service-profile)#
```

Syntax Description

```
epc-qos-params-in-gtpv1 { eps-subscription | gprs-subscription }
remove epc-qos-params-in-gtpv1
```

remove

Removes previous configuration changes and resets the default.

eps-subscription

If the keyword **eps-subscription** is configured, the EPC QoS parameters from EPS subscription are sent to the GGSN. (Note: This option is not supported in this release).

gprs-subscription

If the keyword **gprs-subscription** is configured, E-ARP and APN-AMBR from the GPRS subscription are sent. The UE-AMBR value is read from the user (local capping).

Usage Guidelines This command is disabled by default. On enabling this command E-ARP and APN-AMBR parameters are included in the GTPV1 SM messages towards the GGSN.

Example

The following command enables the SGSN to send EPC QoS parameters to the GGSN. The E-ARP and APN-AMBR values are picked from the GPRS subscription and the UE-AMBR value is read from the user (local capping).

```
epc-qos-params-in-gtpv1 gprs-subscription
```

operator-defined-qci

This command enables Operator Specific QCI in MME. If this command is enabled, MME accepts the QCI range 128 - 254 from HSS and P-GW.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Quality of Service Profile Configuration

configure > quality-of-service-profile

Entering the above command sequence results in the following prompt:

```
[local]host_name(qos-of-service-profile)#
```

Syntax Description **`[ remove ] operator-defined-qci`**

remove

Removes the operator defined QCI configuration from the QoS profile.

Usage Guidelines The non-standard QCIs provides Operator Specific QoS for M2M and other mission critical communications.

In order to use operator specific QCIs, the QoS parameters need to be configured using the **pre-rel8-qos-mapping** command. On configuring this command, the operator defined QCI values are mapped to the PreRelease8QoS parameters during to UTRAN/GERAN.

Example

The following command enables Operator Defined QCI :

```
operator-defined-qci
```

prefer-as-cap

This command instructs the SGSN to choose the QoS configuration as the "qos parameters" for session establishment.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Quality of Service Profile Configuration

configure > quality-of-service-profile

Entering the above command sequence results in the following prompt:

```
[local]host_name(qos-of-service-profile)#
```

Syntax Description **prefer-as-cap [both-subscription-and-local | subscription | local]**

both-subscription-and-local

This keyword instructs the SGSN to use, as the capping value during session establishment, the lower of either the locally configured QoS bit rate or the subscription received from HLR/HSS.

subscription

Instructs the SGSN to take QoS parameters from the subscription received from HLR (or HSS) and use the same as the capping value for session establishment.

Default for SGSN.

local

Instructs the SGSN to take QoS parameters from the local configuration and use it for session establishment.

Usage Guidelines Use this command to instruct the SGSN to choose the QoS configuration for sessionestablishment.

Example

The following command instructs the SGSN to cap the bit rate with the lower rate of the two configurations, subscription or local:

prefer-as-cap both-subscription-and-local

prefer-tc

Use this command to instruct which traffic class to use. This command overrides the traffic class received from subscription.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Quality of Service Profile Configuration

configure > quality-of-service-profile

Entering the above command sequence results in the following prompt:

```
[local]host_name(qos-of-service-profile)#
```

Syntax Description

prefer-tc [background | conversational | streaming | interactive] remove prefer-tc

remove

Removes previous configuration changes and resets the default.

background

Use this keyword to use the **background** traffic class.

conversational

Use this keyword to use the **conversational** traffic class.

streaming

Use this keyword to use the **streaming** traffic class.

interactive

Use this keyword to use the **interactive** traffic class.

Usage Guidelines

Use this command to instruct which traffic class to use. This command is applicable only if following is configured, or the configuration will be ignored during call processing:

- The **prefer-as-cap** is set to **local** or **both-subscription-and-local**.
- The Traffic class configured in **prefer-tc** should be configured. For example, if **prefer-tc** is configured as background then background class under QoS should also be configured.

Example

The following command is used to choose the background traffic class as the preferred traffic class:

prefer-tc background

qci-when-missing-in-subscription

This command is used to assign a default QCI value when a QCI value is not received from the subscription.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Quality of Service Profile Configuration

configure > quality-of-service-profile

Entering the above command sequence results in the following prompt:

```
[local]host_name(qos-of-service-profile)#
```

Syntax Description **`[ remove ] qci-when-missing-in-subscription`***`qci_value`*

remove

Removes the default QCI value configuration from the QoS profile.

qci_value

The *qci_value* variable in this configuration is considered as a default QCI value. The QCI value accepted is either a Standard QCI value or Operator Specific value. The Standard QCI values range from 1 to 9. The Operator Specific values range from 128 to 254. The configuration does not accept any other value apart from the ones mentioned above.

Usage Guidelines Use this command to configure a default QCI to avoid rejection during handovers to UTRAN/GERAN by MME when a QCI value is not received from the Subscription.

Example

The following command configures a default value QCI of value 5:

```
qci-when-missing-in-subscription 5
```

qci-reject

Use this command to identify a specific QCI or a range of QCI for which the MME must reject bearer establishment or modification.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Quality of Service Profile Configuration

configure > quality-of-service-profile

Entering the above command sequence results in the following prompt:

```
[local]host_name(qos-of-service-profile)#
```

Syntax Description

```
qci-reject { default-bearer | dedicated-bearer } qci_value [ to  end_qci_value ]
remove qci-reject
```

remove qci-reject

Deletes this configuration from the QoS profile configuration.

dedicated-bearer

Identifies either a specific QoS class identifier (QCI) or a range of QCI for the dedicated-bearer.

default-bearer

Identifies either a specific QoS class identifier (QCI) or a range of QCI for the default-bearer.

qci_value

Identifies a specific QCI value.

- For dedicated-bearers, enter an integer from 1 through 9. You can enter the new standardized QCI values 65, 66, 67, 69 and 70.
- For default-bearers, enter an integer from 5 through 9. You can enter the new standardized QCI values 69 and 70.

to *end_qci_value*

Type "to" and then enter an integer for the QCI value to end the range.

- For dedicated-bearers, enter an integer from 2 through 9 that is greater than the QCI value entered for the beginning of the range. You can enter the new standardized QCI values 65, 66, 67, 69 and 70.
- For default-bearers, enter an integer from 6 through 9 that is greater than the QCI value entered for the beginning of the range. You can enter the new standardized QCI values 69 and 70.

Usage Guidelines

The MME can reject default-bearers and dedicated-bearers based on QCI received from the subscription or the peer-MME/S4-SGSN during inbound relocation or the Create Session Response/Update Bearer Request/Create Bearer Request procedure.

Example

The following is a sample command that illustrates the configuration for the MME to reject bearer establishment for the dedicated-bearer channel if QCI 7 is received from the P-GW:

```
 qci-reject
dedicated-bearer 7
```