Ultra Cloud Core 5G Session Management Function, Release 2020.02 - CLI Command Reference

First Published: 2020-04-30

Last Modified: 2020-05-29

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

This preface describes the *5G Session Management Function Guide*, how it is organized and its document conventions.

This guide describes the Cisco Session Management Function (SMF) and includes infrastructure and interfaces, feature descriptions, specification compliance, session flows, configuration instructions, and CLI commands for monitoring and troubleshooting the system.

• Conventions Used, on page xxxiii

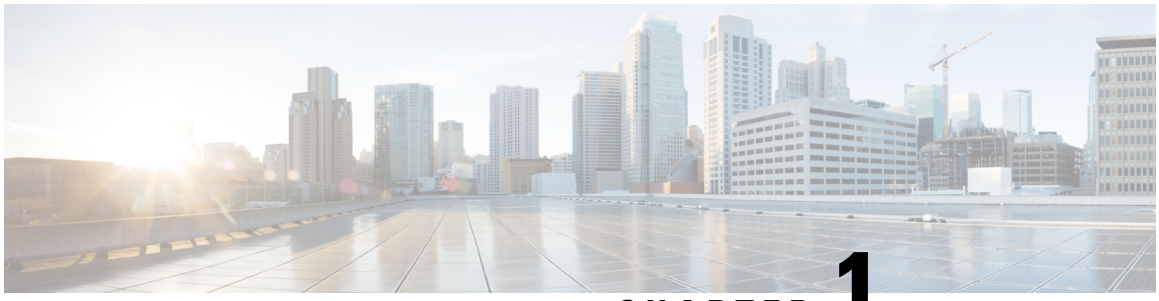
Conventions Used

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.

Typeface Conventions	Description
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.
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**



CHAPTER 1

SMF Executive Commands

aaa

Configures AAA based user management parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec

Syntax Description

aaa { authentication { users *list_of_local_users* **admin change-password old-password** *user_password* **new-password** *user_password* **confirm-password** *user_password* **} }**

users *list_of_local_users*

Specify the user name.

Must be a string.

old-password *user_password*

Specifies the current password of the user.

Must be a string.

new-password *user_password*

Specifies a new password of the user.

Must be a string.

confirm-password *user_password*

Enter the new password once again to change the password.

Must be a string.

Usage Guidelines

Use this command to configure the AAA based user management parameters.

cd

Configures the change directory command.

Privilege

Security Administrator, Administrator

Command Modes Exec

Syntax Description **cd** *directory*.**ssh**

directory

Specify the directory path.

Must be an alphanumeric string.

Usage Guidelines Use this command to configure the change directory command.

cdl clear

Configures the Cisco Common Data Layer (CDL) parameters to delete the database sessions.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **cdl clear sessions [db-name** *db_name* **| filter { condition { ends-with | match | starts-with } key** *key_value* **} | map-id** *map_id* **]**

db-name *db_name*

Specifies the database name to be queried for deleting the data.

Must be a string of 1 to 16 characters.

key *key_value*

Specifies the query value.

Must be a string of 0 to 512 characters.

map-id *map_id*

Specifies the map ID to delete the data for a map.

Must be an integer in the range of 0-1024.

filter condition { ends-with | match | starts-with }

Specify the query expression to filter the results of query.

Usage Guidelines Use this command to delete the CDL database sessions.

cdl show sessions

Configures the CDL parameters to display the session details.

Privilege

Security Administrator, Administrator

Command Modes

Exec

Syntax Description

cdl show sessions count { detailed { db-name *db_name* **| filter { condition { ends-with | match | starts-with } | key** *key_value* **} | limit** *limit* **| map-id** *map_id* **} | summary { db-name** *db_name* **| filter { condition { ends-with | match | starts-with } | key** *key_value* **} | limit** *limit* **| map-id** *map_id* **}**

count

Display the session count information.

detailed

Display the session details with data.

summary

Display the session details without data.

db-name *db_name*

Specifies the database name to be queried for displaying the session details.

Must be a string of 1 to 16 characters.

key *key_value*

Specifies the query value.

Must be a string of 0 to 512 characters.

map-id *map_id*

Specifies the map ID to display the data for a map.

Must be an integer in the range of 0-1024.

limit *limit*

Specifies the maximum number of records to display.

Must be an integer in the range of 1 to 500 characters.

filter condition { ends-with | match | starts-with }

Specify the query expression to filter the results of query.

Usage Guidelines

Use this command to display the session details.

cdl show status

Configures the CDL parameters to display the status of the database.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`cdl status db-name`** *`db_name`*

db-name *db_name*

Specifies the database name for displaying the corresponding status.

Must be a string of 1 to 16 characters.

Usage Guidelines Use this command to display the status of the queried database.

clear ipam

Clears the IPAM operational data.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`clear ipam`**

Usage Guidelines Use this command to clear the IPAM operational data.

clear subscriber

Clears the subscriber data.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`clear subscriber`**

Usage Guidelines Use this command to clear the subscriber data.

commit

Configures the commit parameters.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`commit [ abort { persist-id`** *`persist_id`* **`} | confirm { persist-id`** *`persist_id`* **`} | persist-id`** *`persist_id`* **`]`**

abort persist-id *persist_id*

Specify to abort commit. Specify the persistence ID for the commit operation.

Must be an integer.

confirm persist-id *persist_id*

Specify to confirm commit. Specify the persistence ID for the commit operation.

Must be an integer.

persist-id *persist_id*

Specify the persistence ID for the commit operation.

Must be an integer.

Usage Guidelines Use this command to configure the commit parameters.

compare

Compares the running configuration to another configuration or a file.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **compare file { *filename*[.kube | .ssh/] | *configuration* }**

***filename*[.kube | .ssh/]**

Specify the file name or the directory path of the file to be compared.

Must be a string.

configuration

Specify the desired configuration to be compared against.

Must be a string.

Usage Guidelines Use this command to compare the files.

config

Manipulates the software configuration information.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `config [ exclusive | no-confirm | shared | terminal ]`

exclusive

Specify to enter the exclusive configuration mode.

no-confirm

Specify to apply the command without asking for confirmation.

shared

Specify to enter the shared configuration mode.

terminal

Specify to enter the terminal configuration mode.

Usage Guidelines Use this command to manipulate the software configuration information.

describe

Displays the command information.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `describe command`

command

Specify the command name to display detailed information about the command.

The command must be one of the following:

- **aaa**
- **cd**
- **cdl**
- **commit**
- **compare**
- **config**
- **describe**
- **dump**
- **exit**
- **help**

- **history**
- **id**
- **idle-timeout**
- **ignore-leading-space**
- **job**
- **leaf-prompting**
- **license**
- **logout**
- **monitor**
- **no**
- **paginate**
- **quit**
- **rcm**
- **screen-length**
- **screen-width**
- **send**
- **show**
- **show-defaults**
- **smiuser**
- **system**
- **terminal**
- **timestamp**
- **who**

Usage Guidelines Use this command to display the command specific information.

dump

Removes the transaction history.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `dump transactionhistory`

Usage Guidelines Use this command to remove the transaction history.

exit

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

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **exit**

Usage Guidelines Use this command to exit the current configuration mode and return to the previous configuration mode. When used in the Exec mode, exits the management session.

help

Displays help information for a specified command.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **help** *command*

command

Specify the command name to display the corresponding help information.

The command must be one of the following:

- **aaa**
- **cd**
- **cdl**
- **commit**
- **compare**
- **config**
- **describe**
- **dump**
- **exit**
- **help**
- **history**
- **id**

- **idle-timeout**
- **ignore-leading-space**
- **job**
- **leaf-prompting**
- **license**
- **logout**
- **monitor**
- **no**
- **paginate**
- **quit**
- **rcm**
- **screen-length**
- **screen-width**
- **send**
- **show**
- **show-defaults**
- **smiuser**
- **system**
- **terminal**
- **timestamp**
- **who**

Usage Guidelines Use this command to view help information for a specified command.

history

Configures the command history cache size.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **history** *history_size*

history_size

Specify the command history cache size.

Must be an integer in the range of 0-1000.

Usage Guidelines Use this command to configure the command history cache size.

id

Displays user ID information.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `id`

Usage Guidelines Use this command to view the user ID information.

idle-timeout

Configures the maximum duration a command can remain idle in seconds after which the system automatically terminates the connection.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `idle-timeout` *duration*

duration

Specify the idle timeout duration in seconds.

Must be an integer in the range of 1-8192.

Usage Guidelines Use this command to configure the maximum duration a command can remain idle.

ignore-leading-space

Configures whether to ignore or consider the leading whitespace at the beginning of a command.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `ignore-leading-space { false | true }`

{ false | true }

Specify false to ignore the leading whitespace, and true to consider it.

Must be either "false" or "true".

Usage Guidelines Use this command to configure whether to ignore or consider leading whitespace at the beginning of a command.

job

Suspends the jobs that are running in the background.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`job stop`** *`job_id`*

job_id

Specify the job ID for suspending the corresponding job.

Must be an integer.

Usage Guidelines Use this command to suspend the jobs that are running in the background.

leaf-prompting

Enables or disables automatic querying for leaf values.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`leaf-prompting { false | true }`**

{ false | true }

Specify false to disable leaf prompting, and true to enable.

Must be either "false" or "true".

Usage Guidelines Use this command to automatically query for leaf values.

license smart deregister

Configures the license parameters for the VNF deregistration.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `license smart deregister`

deregister

Specify to deregister the VNF for smart licensing.

Usage Guidelines Use this command to configure the license parameters for the VNF deregistration.

license smart register

Configures the license parameters for the VNF registration.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `license smart register force idtoken token_id`

register

Specify to register the VNF for Smart Licensing.

force

Specify to enable the force registration of the agent.

idtoken *token_id*

Specify the ID token to register the agent with.

Must be an integer.

Usage Guidelines Use this command to configure the license parameters for the VNF registration.

license smart renew

Configures the license parameters for the VNF renewal.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `license smart renew { ID | auth }`

renew

Renew the smart agent IDs and authentication.

ID

Specify to renew the smart agent license registration information.

auth

Initiate the manual update of the license usage information with Cisco.

Usage Guidelines Use this command to configure the license parameters for the VNF renewal.

logout

Logout a specific session or a specific user from all sessions.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **logout [session** *session_id* **| user** *user_name* **]**

session *session_id*

Specify the session ID from the possible completion options.

Must be a string.

user *user_name*

Specify the user name or the user process from the possible completion options.

Must be a string.

Usage Guidelines Use this command to log out a specific session or a specific user from all sessions.

monitor protocol

Configures the SMF to monitor the protocol.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **monitor protocol interface** *interface_name* **[capture-duration** *duration* **]**

interface *interface_name*

Specify the name of interface on which PCAP is captured.

Must be a string.

capture-duration *duration*

Specify the duration, in seconds, during which PCAP is captured. The default value is 300 seconds.

Must be an integer.

Usage Guidelines Use this command to monitor the protocol.

monitor subscriber

Configures the SMF to monitor the subscribers.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description

```
monitor subscriber supi supi [ capture-duration duration ] | subscriber-dump
 filename file_name | subscriber-list
```

supi *supi*

Specify the subscriber identifier.

Must be a string.

capture-duration *duration*

Specify the duration, in seconds, during which PCAP is captured. The default value is 300 seconds.

Must be an integer.

filename *file_name*

Specify the path of the file name to be dumped.

Must be a string.

Usage Guidelines Use this command to monitor the subscribers.

no

Restores the command history cache size to its default setting. See the history command.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description

```
no history
```

Usage Guidelines Use this command to configure the command history cache size to its default setting. For more details, see the history command.

paginate

Configures whether or not to paginate CLI command output.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `paginate { false | true }`

{ false | true }

Specify false to disable paginating CLI command output, and true to enable.

Must be either "false" or "true".

Usage Guidelines Use this command to paginate the command output.

quit

Exits the management session.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `quit`

Usage Guidelines Use this command to exit the management session.

rcm switchover

Configures Redundancy and Configuration Manager (RCM) switchover operation.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `rcm switchover source` *`ip_address`* `destination` *`ip_address`*

source *ip_address*

Specify the source IP address.

Must be an IP address.

destination *ip_address*

Specify the destination IP address.

Must be an IP address.

Usage Guidelines Use this command to configure RCM switchover operation.

screen-length

Configures the number of rows of text that the terminal screen displays.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`screen-length`** *`number_of_rows`*

number_of_rows

Specify the number of rows that the terminal screen displays.

Must be an integer.

Usage Guidelines Use this command to set the number of rows that the terminal screen displays.

screen-width

Configures the number of columns that the terminal screen displays.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`screen-width`** *`number_of_columns`*

number_of_columns

Specify the number of columns that the terminal screen displays.

Must be an integer.

Usage Guidelines Use this command to set the number of columns that the terminal screen displays.

send

Sends messages to the terminal of a specific user or all users.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **send** *user message*

user

Specify the user to whom the message must be sent.

Must be a string. Select from the possible completion options.

message

Specify the message that must be sent.

Must be a string.

Usage Guidelines Use this command to send messages to the terminal of a specific user or to all users.

show

Displays the system information.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **show** *system_component*

system_component

Specify the component to view the information.

Must be a string. Select from the possible completion options.

Usage Guidelines Use this command to view the system information.

show-defaults

Displays the default configuration.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **show-defaults { false | true }**

{ false | true }

Specify whether to display or hide the default values. To display, select true. Otherwise, select false.

Must be either "false" or "true".

Usage Guidelines Use this command to view the default configuration.

smiuser

Configures the Subscriber Microservices Infrastructure (SMI) user account parameters.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **smiuser { add-group groupname** *group_name* **| add-user { username** *username* **| password** *password* **} | change-password { username** *username* **| current_password** *current_password* **| new_password** *new_password* **| confirm_password** *new_password* **| password_expire_days** *expire_days* **} | change-self-password { current_password** *current_password* **| new_password** *new_password* **| confirm_password** *new_password* **| password_expire_days** *expire_days* **} | delete-group groupname** *group_name* **| delete-user username** *username* **| unassign-user-group { groupname** *groupname_pam* **| username** *username_pam* **} | update-password-length length** *password_length* **}**

username *username*

Specify the username.

Must be a string.

password *password*

Specify the user password.

Must be a string.

confirm_password *new_password*

Confirm the new password.

Must be a string.

current_password *current_password*

Specify the current password.

Must be a string.

new_password *new_password*

Specify the new password.

Must be a string.

password_expire_days *expire_days*

Specify the number of days before the password expires.

Must be an integer.

groupname *group_name*

Specify the group name.

Must be a string.

groupname *groupname_pam*

Specify the group name in PAM.

Must be a string.

username *username_pam*

Specify the user name in PAM.

Must be a string.

length *password_length*

Specify the minimum password length.

Must be an integer.

Usage Guidelines Use this command to configure the smiuser parameters.

system

Configures the NF's system operations.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **system { ops-center stop | synch { start | stop } | upgrade | uuid-override new-uuid** *uuid_value* **}**

ops-center stop

Stop the synching of configuration.

synch { start | stop }

Starts or stops the synching of configuration,

upgrade

Initiates the upgrade of a product.

uuid-override new-uuid *uuid_value*

Change the Universally Unique Identifier (UUID) to a new value.

Must be a string.

Usage Guidelines Use this command to display the NF's system operations.

terminal

Configures the type of terminal.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`terminal`** *`terminal_type`*

terminal_type

Specify the terminal type.

Must be one of the following:

- ansi
- generic
- linux
- vt100
- xterm

Usage Guidelines Use this command to configure the terminal type.

timestamp

Configures the timestamp parameters.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`timestamp { disable | enable }`**

{ disable | enable }

Enable or disable the timestamp display.

Usage Guidelines Use this command to configure the timestamp.

who

Displays information on currently logged on users.

Privilege

Security Administrator, Administrator

Command Modes

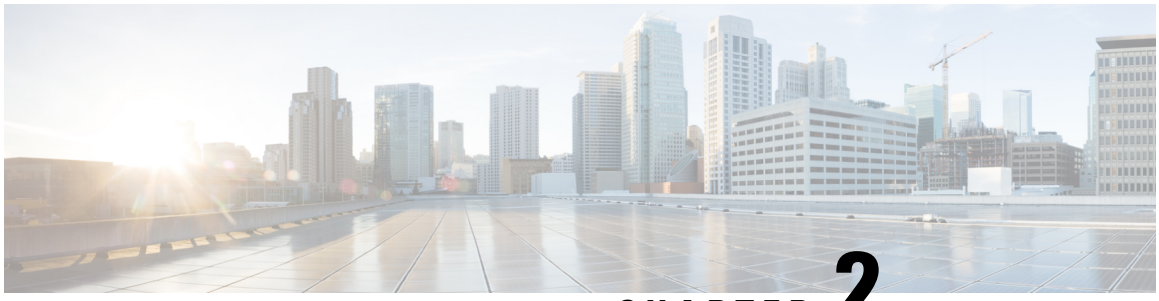
Exec

Syntax Description

who

Usage Guidelines

Use this command to view information on currently logged on users. The command output displays the Session, User, Context, From (IP address), Protocol, Date, and Mode information.



CHAPTER 2

SMF Active Charging Service CLI Commands

apn-profile

Configures Access Point Name (APN) profile.

Privilege

Security Administrator, Administrator

Syntax Description

apn-profile *apn_profile_name*

apn_profile_name

Specify the APN profile name.

Must be a string.

Usage Guidelines

Use this command to create an instance of an APN profile and configure it. An APN profile is a template which groups a set of APN-specific commands that may be applicable to one or more APNs.

Example

```
apn-profile apnprof27
```

apn-profile accounting mode

Configures type of accounting to be performed for this subscriber template.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > APN Profile

Syntax Description

mode *accounting_mode*

accounting_mode

Specify the accounting mode.

Must be one of the following:

- none: No accounting.
- gtpp: GTPP accounting.

Default Value: "gtpp".

Usage Guidelines

Use this command to configure the type of accounting to be performed for this subscriber template.

apn-profile timeout bearer-inactivity

Configures checks for low activity in a bearer.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > APN Profile

Syntax Description **bearer-inactivity exclude-default-bearer**

exclude-default-bearer

Specify to exclude bearer inactivity handling for default/primary bearer.

Usage Guidelines Use this command to configure checks for low activity in a bearer.

apn-profile timeout bearer-inactivity gbr

Configures checks for low activity in a GBR bearer.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > APN Profile

Syntax Description **timeout bearer-inactivity gbr timer** *bearer_inactivity_timer*

timer *bearer_inactivity_timer*

Specify the bearer inactivity timer in seconds. Must be an integer in the range of 300-2592000.

Must be an integer.

Usage Guidelines Use this command to configure checks for low activity in a GBR bearer.

apn-profile timeout bearer-inactivity gbr volume-threshold

Configures threshold value of the data traffic in a bearer.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > APN Profile

Syntax Description **volume-threshold [total** *total_data_traffic* **| downlink** *downlink_data_traffic* **| uplink** *uplink_data_traffic* **]**

total *total_data_traffic*

Specify the uplink and downlink data traffic in a bearer, in bytes.

Must be an integer.

downlink *downlink_data_traffic*

Specify the downlink data traffic in a bearer, in bytes.

Must be an integer.

uplink *uplink_data_traffic*

Specify the uplink data traffic in a bearer, in bytes.

Must be an integer.

Usage Guidelines Use this command to configure the threshold value of the data traffic in a bearer.

call-control-profile

Configures call-control profile.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **call-control-profile** *cc_profile_name*

cc_profile_name

Specify the call-control profile name.

Must be a string.

Usage Guidelines Use this command to create and configure an instance of a call-control profile. A call-control profile is a template which groups a set of call-handling instructions that may be applicable to one or more incoming calls.

call-control-profile accounting mode

Configures the name of the accounting context or mode of accounting for this operator policy.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile

Syntax Description **mode** *accounting_mode*

accounting_mode

Specify the accounting mode.

Must be one of the following:

- none: No accounting.
- gtpp: GTPP accounting.
- radius-diameter: RADIUS or Diameter accounting.

Usage Guidelines Use this command to designate the name of the accounting context or mode of accounting for this operator policy.

content-filtering category database directory

Configures Content Filtering directory parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`directory path`** *`cf_directory_path`*

path *cf_directory_path*

Specify the Content Filtering directory path.

Must be a string.

Usage Guidelines Use this command to configure Content Filtering directory parameters.

context

Creates and configures a context.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`context`** *`context_name`*

context_name

Specify the context name.

Must be a string.

Usage Guidelines Use this command to create and configure a context. If the named context does not exist, it is created. Enters the Context Configuration mode.

context aaa group

Configures handling of AAA within context.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group

Syntax Description **group** *aaa_group_name*

aaa_group_name

Specify the AAA group name.

Must be a string.

Usage Guidelines Use this command to configure the handling of AAA within context.

context aaa group diameter authentication dictionary

Configures Diameter authentication dictionary.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group

Syntax Description **dictionary** *dictionary_name*

dictionary_name

Specify the Diameter authentication dictionary name.

Must be one of the following:

- aaa-custom1
- aaa-custom10
- aaa-custom11
- aaa-custom12
- aaa-custom13
- aaa-custom14
- aaa-custom15
- aaa-custom16
- aaa-custom17
- aaa-custom18
- aaa-custom19
- aaa-custom2
- aaa-custom20
- aaa-custom21

- aaa-custom22
- aaa-custom23
- aaa-custom24
- aaa-custom25
- aaa-custom26
- aaa-custom27
- aaa-custom28
- aaa-custom29
- aaa-custom3
- aaa-custom30
- aaa-custom4
- aaa-custom5
- aaa-custom6
- aaa-custom7
- aaa-custom8
- aaa-custom9
- dynamic-load
- nasreq

Usage Guidelines Use this command to configure the Diameter authentication dictionary.

context aaa group diameter authentication endpoint

Configures Diameter endpoint parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **endpoint** *endpoint_name*

endpoint_name

Specify the Diameter endpoint name.

Must be a string.

Usage Guidelines Use this command to configure the Diameter endpoint parameters.

context aaa group diameter authentication server

Configures Diameter host name.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description

server *host_name* **[priority** *priority* **]**

host_name

Specify the Diameter server host name.

Must be a string.

priority *priority*

Specify the priority.

Must be an integer in the range of 1-1000.

Usage Guidelines

Use this command to configure the Diameter host name.

context aaa group radius accounting interim

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

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description

interim [interval *duration* **]**

interval *duration*

Specify the periodic interval at which to send an interim accounting record in seconds.

Must be an integer in the range of 50-40000000.

Usage Guidelines

Use this command to configure when the system should send an interim accounting record to the server.

context aaa group radius accounting interim volume

Configures the uplink/downlink volume octet counts for the generation of RADIUS interims. This command is applicable for GGSN only.

Privilege

Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **volume [downlink** *downlink_volume* **| uplink** *uplink_volume* **| total** *total_volume* **]**

downlink *downlink_volume*

Specify the downlink volume limit for RADIUS interim generation in bytes.

Must be an integer in the range of 100000-4000000000.

uplink *uplink_volume*

Specify the uplink volume limit for RADIUS interim generation in bytes.

Must be an integer in the range of 100000-4000000000.

total *total_volume*

Specify the total volume limit for RADIUS interim generation in bytes.

Must be an integer in the range of 100000-4000000000.

Usage Guidelines Use this command to configure the uplink/downlink volume octet counts for the generation of RADIUS interims. This command is applicable for GGSN only.

context aaa group radius algorithm

Configures the algorithm for selecting among various defined RADIUS servers.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **algorithm** *algorithm*

algorithm

Specify the algorithm.

Must be one of the following:

- round-robin
- first-server

Usage Guidelines Use this command to configure the algorithm for selecting among various defined RADIUS servers.

context aaa group radius attribute nas-ip-address address

Configures the system's NAS-IP-Address attribute.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **address { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **}**

ipv4-address *ipv4_address*

Specify the IPv4 address.

Must be an IPv4 address.

ipv6-address *ipv6_address*

Specify the IPv6 address.

Must be an IPv6 address.

Usage Guidelines Use this command to configure the system's NAS-IP-Address attribute.

context aaa group radius dictionary

Configures dictionary used by RADIUS for specific context.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **dictionary** *radius_dictionary_name*

dictionary *radius_dictionary_name*

Specify the RADIUS dictionary name.

Must be one of the following:

- standard: Contains all standard RADIUS attributes, as defined in RFC-2865, RFC-2866, and RFC-2869.
- starent: Contains master set of all attributes found in all other non-custom dictionaries supported. Starent VSAs use a two-byte VSA Type.
- 3gpp: Contains standard dictionary plus all attributes specified in 3GPP 32.015.
- 3gpp2: Contains standard dictionary plus all attributes specified in IS-835-B, plus some attributes specified in IS-835-C.
- custom1: Custom-defined dictionary.
- custom10: Custom-defined dictionary.
- custom11: Custom-defined dictionary.
- custom12: Custom-defined dictionary.
- custom14: Custom-defined dictionary.
- custom15: Custom-defined dictionary.

- custom16: Custom-defined dictionary.
- custom17: Custom-defined dictionary.
- custom18: Custom-defined dictionary.
- custom19: Custom-defined dictionary.
- custom2: Custom-defined dictionary.
- custom20: Custom-defined dictionary.
- custom21: Custom-defined dictionary.
- custom22: Custom-defined dictionary.
- custom23: Custom-defined dictionary.
- custom24: Custom-defined dictionary.
- custom25: Custom-defined dictionary.
- custom26: Custom-defined dictionary.
- custom27: Custom-defined dictionary.
- custom28: Custom-defined dictionary.
- custom29: Custom-defined dictionary.
- custom3: Custom-defined dictionary.
- custom30: Custom-defined dictionary.
- custom31: Custom-defined dictionary.
- custom32: Custom-defined dictionary.
- custom33: Custom-defined dictionary.
- custom34: Custom-defined dictionary.
- custom35: Custom-defined dictionary.
- custom36: Custom-defined dictionary.
- custom37: Custom-defined dictionary.
- custom38: Custom-defined dictionary.
- custom39: Custom-defined dictionary.
- custom4: Custom-defined dictionary.
- custom40: Custom-defined dictionary.
- custom41: Custom-defined dictionary.
- custom42: Custom-defined dictionary.
- custom43: Custom-defined dictionary.
- custom44: Custom-defined dictionary.

- custom45: Custom-defined dictionary.
- custom46: Custom-defined dictionary.
- custom47: Custom-defined dictionary.
- custom48: Custom-defined dictionary.
- custom49: Custom-defined dictionary.
- custom5: Custom-defined dictionary.
- custom50: Custom-defined dictionary.
- custom51: Custom-defined dictionary.
- custom52: Custom-defined dictionary.
- custom53: Custom-defined dictionary.
- custom54: Custom-defined dictionary.
- custom55: Custom-defined dictionary.
- custom56: Custom-defined dictionary.
- custom57: Custom-defined dictionary.
- custom58: Custom-defined dictionary.
- custom59: Custom-defined dictionary.
- custom6: Custom-defined dictionary.
- custom60: Custom-defined dictionary.
- custom61: Custom-defined dictionary.
- custom62: Custom-defined dictionary.
- custom63: Custom-defined dictionary.
- custom64: Custom-defined dictionary.
- custom65: Custom-defined dictionary.
- custom66: Custom-defined dictionary.
- custom67: Custom-defined dictionary.
- custom68: Custom-defined dictionary.
- custom69: Custom-defined dictionary.

Usage Guidelines Use this command to configure the dictionary used by RADIUS for specific context.

context aaa group radius mediation-device

Configures mediation-device specific AAA transactions.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration > Redundancy Group Configuration > Host Configuration

Syntax Description **`radius mediation-device`**

Usage Guidelines Use this command to configure the mediation-device specific AAA transactions.

context aaa group radius server

Configures RADIUS server that the system communicates with for specific context.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **`server { `** *`ipv4_address`* **`| `** *`ipv6_address`* **`}`**

{ ipv4_address | ipv6_address }

Specify the RADIUS server IP address.

Must be an IPv4 address.

-Or-

Must be an IPv6 address.

Usage Guidelines Use this command to configure the RADIUS server parameters.

context aaa group radius server encrypted key

Configures use of encrypted key.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **`key`** *`encrypted_key`* **`[ port`** *`port_number`* **`]`**

key *encrypted_key*

Specify the encrypted key that is exchanged between server and client. Must be followed by shared secret.

Must be a string.

port *port_number*

Specify the UDP port that the RADIUS server is using.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure the use of encrypted key.

context aaa group radius server key

Configures the key that is exchanged between server and client.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **key** *key*

key

Specify the key that is exchanged between server and client. Must be followed by shared secret.

Must be a string.

Usage Guidelines Use this command to configure the key that is exchanged between server and client. Must be followed by shared secret.

context aaa group redundancy-group

Configures the redundancy group parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **redundancy-group** *group_name*

group_name

Specify the redundancy group name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group parameters.

context aaa group redundancy-group host

Configures redundancy group host parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **host** *host_name*

host_name

Specify the host name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group host parameters.

context aaa group redundancy-group host diameter authentication dictionary

Configures Diameter authentication dictionary.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group

Syntax Description **dictionary** *dictionary_name*

dictionary_name

Specify the Diameter authentication dictionary name.

Must be one of the following:

- aaa-custom1
- aaa-custom10
- aaa-custom11
- aaa-custom12
- aaa-custom13
- aaa-custom14
- aaa-custom15
- aaa-custom16
- aaa-custom17
- aaa-custom18
- aaa-custom19
- aaa-custom2
- aaa-custom20
- aaa-custom21
- aaa-custom22
- aaa-custom23

- aaa-custom24
- aaa-custom25
- aaa-custom26
- aaa-custom27
- aaa-custom28
- aaa-custom29
- aaa-custom3
- aaa-custom30
- aaa-custom4
- aaa-custom5
- aaa-custom6
- aaa-custom7
- aaa-custom8
- aaa-custom9
- dynamic-load
- nasreq

Usage Guidelines Use this command to configure the Diameter authentication dictionary.

context aaa group redundancy-group host diameter authentication endpoint

Configures Diameter endpoint parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **endpoint** *endpoint_name*

endpoint_name

Specify the Diameter endpoint name.

Must be a string.

Usage Guidelines Use this command to configure the Diameter endpoint parameters.

context aaa group redundancy-group host diameter authentication server

Configures Diameter host name.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description

server *host_name* **[priority** *priority* **]**

host_name

Specify the Diameter server host name.

Must be a string.

priority *priority*

Specify the priority.

Must be an integer in the range of 1-1000.

Usage Guidelines

Use this command to configure the Diameter host name.

context aaa group redundancy-group host radius accounting interim

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

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description

interim [interval *duration* **]**

interval *duration*

Specify the periodic interval at which to send an interim accounting record in seconds.

Must be an integer in the range of 50-40000000.

Usage Guidelines

Use this command to configure when the system should send an interim accounting record to the server.

context aaa group redundancy-group host radius accounting interim volume

Configures the uplink/downlink volume octet counts for the generation of RADIUS interims. This command is applicable for GGSN only.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description

`volume [ downlink` *`downlink_volume`* **`| uplink`** *`uplink_volume`* **`| total`** *`total_volume`* **`]`**

downlink *downlink_volume*

Specify the downlink volume limit for RADIUS interim generation in bytes.

Must be an integer in the range of 100000-4000000000.

uplink *uplink_volume*

Specify the uplink volume limit for RADIUS interim generation in bytes.

Must be an integer in the range of 100000-4000000000.

total *total_volume*

Specify the total volume limit for RADIUS interim generation in bytes.

Must be an integer in the range of 100000-4000000000.

Usage Guidelines

Use this command to configure the uplink/downlink volume octet counts for the generation of RADIUS interims. This command is applicable for GGSN only.

context aaa group redundancy-group host radius algorithm

Configures the algorithm for selecting among various defined RADIUS servers.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description

`algorithm` *`algorithm`*

algorithm

Specify the algorithm.

Must be one of the following:

- round-robin

- first-server

Usage Guidelines Use this command to configure the algorithm for selecting among various defined RADIUS servers.

context aaa group redundancy-group host radius attribute nas-ip-address address

Configures the system's NAS-IP-Address attribute.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **address { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **}**

ipv4-address *ipv4_address*

Specify the IPv4 address.

Must be an IPv4 address.

ipv6-address *ipv6_address*

Specify the IPv6 address.

Must be an IPv6 address.

Usage Guidelines Use this command to configure the system's NAS-IP-Address attribute.

context aaa group redundancy-group host radius dictionary

Configures dictionary used by RADIUS for specific context.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **dictionary** *radius_dictionary_name*

dictionary *radius_dictionary_name*

Specify the RADIUS dictionary name.

Must be one of the following:

- standard: Contains all standard RADIUS attributes, as defined in RFC-2865, RFC-2866, and RFC-2869.
- starent: Contains master set of all attributes found in all other non-custom dictionaries supported. Starent VSAs use a two-byte VSA Type.

- 3gpp: Contains standard dictionary plus all attributes specified in 3GPP 32.015.
- 3gpp2: Contains standard dictionary plus all attributes specified in IS-835-B, plus some attributes specified in IS-835-C.
- custom1: Custom-defined dictionary.
- custom10: Custom-defined dictionary.
- custom11: Custom-defined dictionary.
- custom12: Custom-defined dictionary.
- custom14: Custom-defined dictionary.
- custom15: Custom-defined dictionary.
- custom16: Custom-defined dictionary.
- custom17: Custom-defined dictionary.
- custom18: Custom-defined dictionary.
- custom19: Custom-defined dictionary.
- custom2: Custom-defined dictionary.
- custom20: Custom-defined dictionary.
- custom21: Custom-defined dictionary.
- custom22: Custom-defined dictionary.
- custom23: Custom-defined dictionary.
- custom24: Custom-defined dictionary.
- custom25: Custom-defined dictionary.
- custom26: Custom-defined dictionary.
- custom27: Custom-defined dictionary.
- custom28: Custom-defined dictionary.
- custom29: Custom-defined dictionary.
- custom3: Custom-defined dictionary.
- custom30: Custom-defined dictionary.
- custom31: Custom-defined dictionary.
- custom32: Custom-defined dictionary.
- custom33: Custom-defined dictionary.
- custom34: Custom-defined dictionary.
- custom35: Custom-defined dictionary.
- custom36: Custom-defined dictionary.

- custom37: Custom-defined dictionary.
- custom38: Custom-defined dictionary.
- custom39: Custom-defined dictionary.
- custom4: Custom-defined dictionary.
- custom40: Custom-defined dictionary.
- custom41: Custom-defined dictionary.
- custom42: Custom-defined dictionary.
- custom43: Custom-defined dictionary.
- custom44: Custom-defined dictionary.
- custom45: Custom-defined dictionary.
- custom46: Custom-defined dictionary.
- custom47: Custom-defined dictionary.
- custom48: Custom-defined dictionary.
- custom49: Custom-defined dictionary.
- custom5: Custom-defined dictionary.
- custom50: Custom-defined dictionary.
- custom51: Custom-defined dictionary.
- custom52: Custom-defined dictionary.
- custom53: Custom-defined dictionary.
- custom54: Custom-defined dictionary.
- custom55: Custom-defined dictionary.
- custom56: Custom-defined dictionary.
- custom57: Custom-defined dictionary.
- custom58: Custom-defined dictionary.
- custom59: Custom-defined dictionary.
- custom6: Custom-defined dictionary.
- custom60: Custom-defined dictionary.
- custom61: Custom-defined dictionary.
- custom62: Custom-defined dictionary.
- custom63: Custom-defined dictionary.
- custom64: Custom-defined dictionary.
- custom65: Custom-defined dictionary.

- custom66: Custom-defined dictionary.
- custom67: Custom-defined dictionary.
- custom68: Custom-defined dictionary.
- custom69: Custom-defined dictionary.

Usage Guidelines Use this command to configure the dictionary used by RADIUS for specific context.

context aaa group redundancy-group host radius mediation-device

Configures mediation-device specific AAA transactions.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration > Redundancy Group Configuration > Host Configuration

Syntax Description **`radius mediation-device`**

Usage Guidelines Use this command to configure the mediation-device specific AAA transactions.

context aaa group redundancy-group host radius server

Configures RADIUS server that the system communicates with for specific context.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description **`server { ipv4_address | ipv6_address }`**

{ ipv4_address | ipv6_address }

Specify the RADIUS server IP address.

Must be an IPv4 address.

-Or-

Must be an IPv6 address.

Usage Guidelines Use this command to configure the RADIUS server parameters.

context aaa group redundancy-group host radius server encrypted key

Configures use of encrypted key.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description

key *encrypted_key* **[port** *port_number* **]**

key *encrypted_key*

Specify the encrypted key that is exchanged between server and client. Must be followed by shared secret.

Must be a string.

port *port_number*

Specify the UDP port that the RADIUS server is using.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to configure the use of encrypted key.

context aaa group redundancy-group host radius server key

Configures the key that is exchanged between server and client.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Group Configuration

Syntax Description

key *key*

key

Specify the key that is exchanged between server and client. Must be followed by shared secret.

Must be a string.

Usage Guidelines

Use this command to configure the key that is exchanged between server and client. Must be followed by shared secret.

context apn

Configures Access Point Name (APN) templates.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **apn** *apn_name*

apn_name

Specify the APN name.

Must be a string.

Usage Guidelines Use this command to create and configure an APN.

Example

The following command creates an APN template named isp1:

```
apn isp1
```

context apn active-charging

Enables a configured ACS rulebase.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **active-charging rulebase** *rulebase_name*

rulebase *rulebase_name*

Specify the rulebase name.

Must be a string.

Usage Guidelines Use this command to enable a configured ACS rulebase.

context apn authorize-with-hss

Configures s6b authentication.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **authorize-with-hss [report-ipv6** *ipv6_address* **]**

Usage Guidelines Use this command to configure s6b authentication. Enables IPv6 reporting through AAR towards s6b interface.

context apn authorize-with-hss egtp

Enables s6b authorization for all the interfaces of EGTP along with GN-GP Handover except 3G initial attach.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration > Redundancy Group Configuration

Syntax Description **`authorize-with-hss egtp [ report-ipv6 ]`**

Usage Guidelines Use this command to enable s6b authorization for all the interfaces of EGTP along with GN-GP Handover except 3G initial attach.

context apn authorize-with-hss egtp gn-gp-enabled

Enables s6b authorization for 3G initial attach and GNGP handover.

Privilege Security Administrator, Administrator

Syntax Description **`gn-gp-enabled report-ipv6`** *`ipv6_address`*

Usage Guidelines Use this command to enable s6b authorization for 3G initial attach and GNGP handover.

context apn authorize-with-hss egtp s2b

Enables s6b authorization for egtp-s2b.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`authorize-with-hss egtp s2b report-ipv6-addr`**

Usage Guidelines Use this command to enable s6b authorization for egtp-s2b.

context apn authorize-with-hss egtp s2b gn-gp-enabled

Enables s6b authorization for 3G initial attach and GNGP handover.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **`gn-gp-enabled report-ipv6`** *`ipv6_address`*

Usage Guidelines Use this command to enable s6b authorization for 3G initial attach and GNGP handover.

context apn authorize-with-hss egtp s2b s5-s8

Enables s6b authorization for egtp-s5s8.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **authorize-with-hss egtp s2b s5-s8 [** *gn_gp_option* **| report-ipv6-addr]**

Usage Guidelines Use this command to enable s6b authorization for egtp-s5s8.

context apn authorize-with-hss egtp s5-s8

Enables s6b authorization for egtp-s5s8.

Privilege Security Administrator, Administrator

Syntax Description **s5-s8**

Usage Guidelines Use this command to enable s6b authorization for egtp-s5s8.

context apn authorize-with-hss egtp s5-s8 s2b

Enables s6b authorization for egtp-s2b.

Command Modes Exec > Global Configuration > Context Configuration

Privilege Security Administrator, Administrator

Syntax Description **s2b**

Usage Guidelines Use this command to enable s6b authorization for egtp-s2b.

context apn authorize-with-hss lma

Enables IPv6 reporting through AAR towards s6b.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **lma [report-ipv6** *ipv6_address* **| s6b-aaa-group** *group_name* **]**

s6b-aaa-group *group_name*

Specify the AAA group name for s6b authorization.

Must be a string.

Usage Guidelines Use this command to enable IPv6 reporting through AAR towards s6b.

context apn cc-profile

Configures the subscriber charging characteristics profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`cc-profile`** *`index`* **`{ credit-control-group`** *`cc_group_name`* **`| prepaid-prohibited }`**

index

Specify the charging characterstics profile index.

Must be an integer.

-Or-

Must be one of the following:

- any

credit-control-group *cc_group_name*

Specify the credit control group name.

Must be a string.

prepaid-prohibited

Specify to disable prepaid for the configured profile index.

Usage Guidelines Use this command to configure the subscriber charging characteristics profile parameters.

context apn content-filtering category

Configures Content Filtering category.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`category policy-id`** *`policy_id`*

policy-id *policy_id*

Specify the Content Filtering policy ID.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Use this command to configure Content Filtering category.

context apn data-tunnel

Configures the data tunnel MTU parameter.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`data-tunnel mtu`** *`max_transmission_unit`*

mtu *max_transmission_unit*

Specify the data tunnel MTU value, in octets.

Must be an integer.

Usage Guidelines Use this command to configure the data tunnel MTU parameter.

context apn gtpp group

Enables and configures the GTPP group to be used by this APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`gtpp group`** *`gtpp_group_name`*

group *gtpp_group_name*

Specify the GTPP group name.

Must be a string.

Usage Guidelines Use this command to enable and configure the GTPP group to be used by this APN.

context apn ip

Configures IP-related parameters.

Privilege Security Administrator, Administrator

Syntax Description **ip context-name** *context_name*

context-name *context_name*

Specify name of the destination context to use for subscribers accessing this APN.

Must be a string.

Usage Guidelines Use this command to configure IP-related parameters.

context apn ip access-group

Configures the access group to be used by this APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **ip access-group** *access_group_name* **[in | out]**

access_group_name

Specify the access group name.

Must be a string.

in

Specify the access group as inbound.

out

Specify the access group as outbound.

Usage Guidelines Use this command to specify the access group to be used by this APN.

You can configure a maximum of eight elements with this command.

context apn ip source-violation

Enables packet source validation.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **source-violation [ignore]**

ignore

Specify to disable source address checking for this APN.

Usage Guidelines Use this command to enable packet source validation.

context apn ppp

Configures PPP parameters for specified APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **ppp mtu** *max_transmission_unit*

mtu *max_transmission_unit*

Specify the maximum transmission unit. Default: 1500.

Must be an integer.

Usage Guidelines Use this command to configure the PPP parameters for specified APN.

context apn redundancy-group

Configures redundancy group parameters.

Privilege Security Administrator, Administrator

Syntax Description **redundancy-group** *group_name*

group_name

Specify the redundancy group name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group parameters.

context apn redundancy-group active-charging

Enables a configured ACS rulebase.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **active-charging rulebase** *rulebase_name*

rulebase *rulebase_name*

Specify the rulebase name.

Must be a string.

Usage Guidelines Use this command to enable a configured ACS rulebase.

context apn redundancy-group authorize-with-hss

Configures s6b authentication.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`authorize-with-hss [ report-ipv6`** *`ipv6_address`* **`]`**

Usage Guidelines Use this command to configure s6b authentication. Enables IPv6 reporting through AAR towards s6b interface.

context apn redundancy-group authorize-with-hss egtp

Enables s6b authorization for all the interfaces of EGTP along with GN-GP Handover except 3G initial attach.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration > Redundancy Group Configuration

Syntax Description **`authorize-with-hss egtp [ report-ipv6 ]`**

Usage Guidelines Use this command to enable s6b authorization for all the interfaces of EGTP along with GN-GP Handover except 3G initial attach.

context apn redundancy-group authorize-with-hss egtp gn-gp-enabled

Enables s6b authorization for 3G initial attach and GNGP handover.

Privilege Security Administrator, Administrator

Syntax Description **`gn-gp-enabled report-ipv6`** *`ipv6_address`*

Usage Guidelines Use this command to enable s6b authorization for 3G initial attach and GNGP handover.

context apn redundancy-group authorize-with-hss egtp s2b

Enables s6b authorization for egtp-s2b.

Privilege	Security Administrator, Administrator
Command Modes	Exec > Global Configuration > Context Configuration
Syntax Description	**authorize-with-hss egtp s2b report-ipv6-addr**
Usage Guidelines	Use this command to enable s6b authorization for egtp-s2b.

context apn redundancy-group authorize-with-hss egtp s2b gn-gp-enabled

Enables s6b authorization for 3G initial attach and GNGP handover.

Privilege	Security Administrator, Administrator
Command Modes	Exec > Global Configuration > Context Configuration > APN Configuration
Syntax Description	**gn-gp-enabled report-ipv6** *ipv6_address*
Usage Guidelines	Use this command to enable s6b authorization for 3G initial attach and GNGP handover.

context apn redundancy-group authorize-with-hss egtp s2b s5-s8

Enables s6b authorization for egtp-s5s8.

Privilege	Security Administrator, Administrator
Command Modes	Exec > Global Configuration > Context Configuration > APN Configuration
Syntax Description	**authorize-with-hss egtp s2b s5-s8 [** *gn_gp_option* **| report-ipv6-addr]**
Usage Guidelines	Use this command to enable s6b authorization for egtp-s5s8.

context apn redundancy-group authorize-with-hss egtp s5-s8

Enables s6b authorization for egtp-s5s8.

Privilege	Security Administrator, Administrator
Syntax Description	**s5-s8**
Usage Guidelines	Use this command to enable s6b authorization for egtp-s5s8.

context apn redundancy-group authorize-with-hss egtp s5-s8 s2b

Enables s6b authorization for egtp-s2b.

Command Modes Exec > Global Configuration > Context Configuration

Privilege Security Administrator, Administrator

Syntax Description **`s2b`**

Usage Guidelines Use this command to enable s6b authorization for egtp-s2b.

context apn redundancy-group authorize-with-hss lma

Enables IPv6 reporting through AAR towards s6b.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`lma [ report-ipv6`** *`ipv6_address`* **`| s6b-aaa-group`** *`group_name`* **`]`**

s6b-aaa-group *group_name*

Specify the AAA group name for s6b authorization.

Must be a string.

Usage Guidelines Use this command to enable IPv6 reporting through AAR towards s6b.

context apn redundancy-group cc-profile

Configures the subscriber charging characteristics profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`cc-profile`** *`index`* **`{ credit-control-group`** *`cc_group_name`* **`| prepaid-prohibited }`**

index

Specify the charging characterstics profile index.

Must be an integer.

-Or-

Must be one of the following:

- any

credit-control-group *cc_group_name*

Specify the credit control group name.

Must be a string.

prepaid-prohibited

Specify to disable prepaid for the configured profile index.

Usage Guidelines Use this command to configure the subscriber charging characteristics profile parameters.

context apn redundancy-group content-filtering category

Configures Content Filtering category.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`category policy-id`** *`policy_id`*

policy-id *policy_id*

Specify the Content Filtering policy ID.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Use this command to configure Content Filtering category.

context apn redundancy-group data-tunnel

Configures the data tunnel MTU parameter.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`data-tunnel mtu`** *`max_transmission_unit`*

mtu *max_transmission_unit*

Specify the data tunnel MTU value, in octets.

Must be an integer.

Usage Guidelines Use this command to configure the data tunnel MTU parameter.

context apn redundancy-group gtpp group

Enables and configures the GTPP group to be used by this APN.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

Syntax Description

gtpp group *gtpp_group_name*

group *gtpp_group_name*

Specify the GTPP group name.

Must be a string.

Usage Guidelines

Use this command to enable and configure the GTPP group to be used by this APN.

context apn redundancy-group ip

Configures IP-related parameters.

Privilege

Security Administrator, Administrator

Syntax Description

ip context-name *context_name*

context-name *context_name*

Specify name of the destination context to use for subscribers accessing this APN.

Must be a string.

Usage Guidelines

Use this command to configure IP-related parameters.

context apn redundancy-group ip access-group

Configures the access group to be used by this APN.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description

ip access-group *access_group_name* **[in | out]**

access_group_name

Specify the access group name.

Must be a string.

in

Specify the access group as inbound.

out

Specify the access group as outbound.

Usage Guidelines Use this command to specify the access group to be used by this APN.

You can configure a maximum of eight elements with this command.

context apn redundancy-group ip source-violation

Enables packet source validation.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`source-violation [ ignore ]`**

ignore

Specify to disable source address checking for this APN.

Usage Guidelines Use this command to enable packet source validation.

context apn redundancy-group ppp

Configures PPP parameters for specified APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **`ppp mtu`** *`max_transmission_unit`*

mtu *max_transmission_unit*

Specify the maximum transmission unit. Default: 1500.

Must be an integer.

Usage Guidelines Use this command to configure the PPP parameters for specified APN.

context apn redundancy-group timeout

Configures session timeout parameters for the current APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`timeout idle`** *`idle_timeout`*

idle *idle_timeout*

Specify the session idle timeout period for the current APN.

Must be an integer in the range of 0-4294967295.

Usage Guidelines Use this command to configure the session timeout parameters for the current APN.

context apn timeout

Configures session timeout parameters for the current APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`timeout idle`** *`idle_timeout`*

idle *idle_timeout*

Specify the session idle timeout period for the current APN.

Must be an integer in the range of 0-4294967295.

Usage Guidelines Use this command to configure the session timeout parameters for the current APN.

context gtpp group

Configures GTPP group related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`gtpp`** *`gtpp_group_name`*

gtpp_group_name

Specify the GTPP group name.

Must be a string.

Usage Guidelines Use this command to configure GTPP group related parameters.

context gtpp group gtpp

Disables GTPP trigger conditions that cause either partial CDR record closure or opening of a new CDR record container. GTPP Triggers are specified in 3GPP TS 32.251 v6.6.0. All GTPP trigger changes take effect immediately, except volume-limit.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

gtpp trigger { time-limit | volume-limit }

Usage Guidelines

Use this command to disable or enable GTTP triggers that can cause partial CDR record closure or cause a new CDR to be created.

Example

The following command disables partial record closure when a configured time limit is reached:

```
gtpp trigger time-limit
```

context gtpp group gtpp egcdr

Configures the eG-CDR and P-CDR (P-GW CDR) parameters and triggers.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

gtpp egcdr { service-data-flow threshold { interval *duration* **| volume { downlink** *bytes* **| uplink** *bytes* **| total** *bytes* **} } | service-idle-timeout { 0 |** *service_idle_timeout* **} }**

Usage Guidelines

Use this command to configure individual triggers for eG-CDR/P-CDR generation. Use the service-data-flow threshold option to configure the thresholds for closing a service data flow container within an eG-CDR (eG-CDRs for GGSN and P-CDRs for P-GW) during flow-based charging (FBC). A service data flow container has statistics regarding an individual content ID.

context gtpp group gtpp egcdr final-record closing-cause

Configures closing cause for final EGCDR.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description `gtpp egcdr final-record closing-cause { same-in-all-partials | unique }`

unique

Specify unique closing cause for final EGCDR.

same-in-all-partials

Specify same closing cause for multiple final EGCDR(s).

Usage Guidelines Use this command to configure closing cause for final EGCDR.

context gtpp group gtpp egcdr losdv-max-containers

Configures maximum number of LoSDV containers in one EGCDR.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description `losdv-max-containers` *max_containers*

max_containers

Specify the number of LOSDV containers.

Must be an integer in the range of 1-255.

Usage Guidelines Use this command to configure the maximum number of LoSDV containers in one EGCDR.

context gtpp group gtpp egcdr service-data-flow threshold

Configures service data flow related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description `threshold interval` *duration*

interval *duration*

Specify the time interval, in seconds, to close the eG-CDR/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging. By default, this option is disabled.

Must be an integer in the range of 60-40000000.

Usage Guidelines Use this command to assign volume or interval values to the interim GCDRs.

context gtpp group gtpp egcdr service-data-flow threshold volume

Configures the uplink/downlink volume octet counts for the generation of interim GCDRs.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

`volume { downlink` *`bytes`* **`| uplink`** *`bytes`* **`| total`** *`bytes`* **`}`**

downlink *bytes*

Specify the limit for the number of downlink octets after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

uplink *bytes*

Specify the limit for the number of uplink octets after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

total *bytes*

Specify the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

Usage Guidelines

Use this command to configure the uplink/downlink volume octet counts for the generation of interim GCDRs.

context gtpp group gtpp egcdr service-idle-timeout

Enables configuration for service idle out closure of LOSDV container.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

`gtpp egcdr service-idle-timeout { zero |` *`service_idle_timeout`* **`}`**

service_idle_timeout

Specify time limit in seconds for service-idle-timeout.

Must be an integer in the range of 10-86400.

zero

Specify no service-idle-timeout trigger.

Must be one of the following:

- 0

Usage Guidelines Use this command to enable configuration for service idle out closure.

context gtpp group gtpp storage-server ip-address

Configures IP address of the external GTPP storage server for storing CDRs.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **gtpp storage-server { { *ipv4_address* | *ipv6_address* } | port *port_number* }**

{ *ipv4_address* | *ipv6_address* }

Specify the IP address.

Must be IPv4 CIDR notation ##.##.##.##/x or in IPv6 CIDR notation ####:####:####:####:####:####:####:####/###.

-Or-

Must be an IP address.

port *port_number*

Specify the UDP port number that the GTPP Backup server is using.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure the IP address of the external GTPP storage server for storing CDRs.

context gtpp group gtpp storage-server local

Configures storage-server local-mode configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **local aaamgr-wait-time** *aaamgr_wait_time*

aaamgr-wait-time *aaamgr_wait_time*

Specify the time in seconds that AAAmgr has to wait trying to accumlate 255 CDRs.

Must be an integer in the range of 1-300.

Default Value: 300.

Usage Guidelines Use this command to configure the storage-server local-mode configuration.

context gtpp group gtpp storage-server local file

Configures GTPP file related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`file compression {`** *`file_compression`* **`| format`** *`file_format`* **`}`**

compression *file_compression*

Specify the GTPP file compression related configurations. By default, GZIP file compression is disabled.

Must be one of the following:

- gzip
- none

Default Value: "none".

format *file_format*

Specify the file format to be used for local storage.

Must be one of the following:

- custom1
- custom2
- custom3
- custom4
- custom5
- custom6
- custom7
- custom8

Default Value: "custom1".

Usage Guidelines Use this command to configure the GTPP file related parameters.

context gtpp group gtpp storage-server local file name

Configures file name related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **name { format** *file_name_format* **| prefix** *file_name_prefix* **}**

format *file_name_format*

Specify the file name format to be used.

Must be a string.

prefix *file_name_prefix*

Specify the file name prefix to be used.

Must be a string.

Usage Guidelines Use this command to configure the file name related parameters.

context gtpp group gtpp trigger

Configures triggers for CDR.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **trigger { time-limit | volume-limit }**

time-limit

When this trigger is disabled, no partial record closure occurs when the configured time limit is reached. Default: Enabled.

volume-limit

When this trigger is disabled no partial record closure occurs when volume limit is reached. Default: Enabled.

Usage Guidelines Use this command to configure triggers for CDR.

context gtpp group gtpp trigger egcdr

Enables or disables and configures eGCDR-related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **egcdr max-losdv**

max-losdv

Enable trigger for eGCDR release at MAX LoSDV containers.

Usage Guidelines Use this command to enable or disable and configure eGCDR-related parameters.

context gtpp group redundancy-group

Configures redundancy group parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **redundancy-group** *group_name*

group_name

Specify the redundancy group name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group parameters.

context gtpp group redundancy-group host

Configures redundancy group host parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **host** *host_name*

host_name

Specify the host name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group host parameters.

context gtpp group redundancy-group host gtpp

Disables GTPP trigger conditions that cause either partial CDR record closure or opening of a new CDR record container. GTPP Triggers are specified in 3GPP TS 32.251 v6.6.0. All GTPP trigger changes take effect immediately, except volume-limit.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **gtpp trigger { time-limit | volume-limit }**

Usage Guidelines Use this command to disable or enable GTTP triggers that can cause partial CDR record closure or cause a new CDR to be created.

Example

The following command disables partial record closure when a configured time limit is reached:

```
gtpp trigger time-limit
```

context gtpp group redundancy-group host gtpp egcdr

Configures the eG-CDR and P-CDR (P-GW CDR) parameters and triggers.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **gtpp egcdr { service-data-flow threshold { interval** *duration* **| volume { downlink** *bytes* **| uplink** *bytes* **| total** *bytes* **} } | service-idle-timeout { 0 |** *service_idle_timeout* **} }**

Usage Guidelines Use this command to configure individual triggers for eG-CDR/P-CDR generation. Use the service-data-flow threshold option to configure the thresholds for closing a service data flow container within an eG-CDR (eG-CDRs for GGSN and P-CDRs for P-GW) during flow-based charging (FBC). A service data flow container has statistics regarding an individual content ID.

context gtpp group redundancy-group host gtpp egcdr final-record closing-cause

Configures closing cause for final EGCDR.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **gtpp egcdr final-record closing-cause { same-in-all-partials | unique }**

unique

Specify unique closing cause for final EGCDR.

same-in-all-partials

Specify same closing cause for multiple final EGCDR(s).

Usage Guidelines Use this command to configure closing cause for final EGCDR.

context gtpp group redundancy-group host gtpp egcdr losdv-max-containers

Configures maximum number of LoSDV containers in one EGCDR.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`losdv-max-containers`** *`max_containers`*

max_containers

Specify the number of LOSDV containers.

Must be an integer in the range of 1-255.

Usage Guidelines Use this command to configure the maximum number of LoSDV containers in one EGCDR.

context gtpp group redundancy-group host gtpp egcdr service-data-flow threshold

Configures service data flow related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`threshold interval`** *`duration`*

interval *duration*

Specify the time interval, in seconds, to close the eG-CDR/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging. By default, this option is disabled.

Must be an integer in the range of 60-40000000.

Usage Guidelines Use this command to assign volume or interval values to the interim GCDRs.

context gtpp group redundancy-group host gtpp egcdr service-data-flow threshold volume

Configures the uplink/downlink volume octet counts for the generation of interim GCDRs.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`volume { downlink`** *`bytes`* **`| uplink`** *`bytes`* **`| total`** *`bytes`* **`}`**

downlink *bytes*

Specify the limit for the number of downlink octets after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

uplink *bytes*

Specify the limit for the number of uplink octets after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

total *bytes*

Specify the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

Usage Guidelines Use this command to configure the uplink/downlink volume octet counts for the generation of interim GCDRs.

context gtpp group redundancy-group host gtpp egcdr service-idle-timeout

Enables configuration for service idle out closure of LOSDV container.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`gtpp egcdr service-idle-timeout { zero |`** *`service_idle_timeout`* **`}`**

service_idle_timeout

Specify time limit in seconds for service-idle-timeout.

Must be an integer in the range of 10-86400.

zero

Specify no service-idle-timeout trigger.

Must be one of the following:

- 0

Usage Guidelines Use this command to enable configuration for service idle out closure.

context gtpp group redundancy-group host gtpp storage-server ip-address

Configures IP address of the external GTPP storage server for storing CDRs.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

gtpp storage-server { { *ipv4_address* | *ipv6_address* } | port *port_number* }

{ *ipv4_address* | *ipv6_address* }

Specify the IP address.

Must be IPv4 CIDR notation ##.##.##.##/x or in IPv6 CIDR notation ####:####:####:####:####:####:####:####/###.

-Or-

Must be an IP address.

port *port_number*

Specify the UDP port number that the GTPP Backup server is using.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to configure the IP address of the external GTPP storage server for storing CDRs.

context gtpp group redundancy-group host gtpp storage-server local

Configures storage-server local-mode configuration.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

local aaamgr-wait-time *aaamgr_wait_time*

aaamgr-wait-time *aaamgr_wait_time*

Specify the time in seconds that AAAmgr has to wait trying to accumlate 255 CDRs.

Must be an integer in the range of 1-300.

Default Value: 300.

Usage Guidelines

Use this command to configure the storage-server local-mode configuration.

context gtpp group redundancy-group host gtpp storage-server local file

Configures GTPP file related parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

`file compression {` *`file_compression`* **`|`** **`format`** *`file_format`* **`}`**

compression *file_compression*

Specify the GTPP file compression related configurations. By default, GZIP file compression is disabled.

Must be one of the following:

- gzip
- none

Default Value: "none".

format *file_format*

Specify the file format to be used for local storage.

Must be one of the following:

- custom1
- custom2
- custom3
- custom4
- custom5
- custom6
- custom7
- custom8

Default Value: "custom1".

Usage Guidelines

Use this command to configure the GTPP file related parameters.

context gtpp group redundancy-group host gtpp storage-server local file name

Configures file name related parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

`name { format` *`file_name_format`* **`| prefix`** *`file_name_prefix`* **`}`**

format *file_name_format*

Specify the file name format to be used.

Must be a string.

prefix *file_name_prefix*

Specify the file name prefix to be used.

Must be a string.

Usage Guidelines

Use this command to configure the file name related parameters.

context gtpp group redundancy-group host gtpp trigger

Configures triggers for CDR.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

`trigger { time-limit | volume-limit }`

time-limit

When this trigger is disabled, no partial record closure occurs when the configured time limit is reached. Default: Enabled.

volume-limit

When this trigger is disabled no partial record closure occurs when volume limit is reached. Default: Enabled.

Usage Guidelines

Use this command to configure triggers for CDR.

context gtpp group redundancy-group host gtpp trigger egcdr

Enables or disables and configures eGCDR-related parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

egcdr max-losdv

max-losdv

Enable trigger for eGCDR release at MAX LoSDV containers.

Usage Guidelines

Use this command to enable or disable and configure eGCDR-related parameters.

context gtpu-service

Creates specified user plane service name to allow configuration of user plane service.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

gtpu-service *gtpu_service_name*

gtpu_service_name

Specify the GTPU service name.

Must be a string.

Usage Guidelines

Use this command to create specified user plane service name to allow configuration of user plane service.

context gtpu-service bind

Binds the service to an IP address.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > GTPU Service Configuration

Syntax Description

bind { ipv4-address *ipv4_address* **| ipv6-address** *ipv6_address* **} [bearer-type** *bearer_type* **]**

ipv4-address *ipv4_address*

Specify the GTPU address of the GTPU service.

Must be an IP address.

ipv4-address *ipv6_address*

Specify the GTPU address of the GTPU service.

Must be an IPv6 address.

bearer-type *bearer_type*

Specify the media type supported for the GTPU endpoint.

Must be one of the following:

- all
- ims-media
- non-ims-media

Usage Guidelines Use this command to bind the service to an IP address.

context gtpu-service echo-interval

Configures the echo interval.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > GTPU Service Configuration

Syntax Description **`echo-interval`** *`echo_interval`*

echo_interval

Specify the echo interval.

Must be an integer in the range of 60-3600.

Usage Guidelines Use this command to configure the echo interval.

context gtpu-service echo-interval dynamic

Enables the dynamic echo timer for GTPU Service.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > GTPU Service Configuration

Syntax Description **`dynamic [ smooth-factor`** *`smooth_factor`* **`]`**

dynamic

Specify the enable dynamic echo timer for GTPU service.

smooth-factor *smooth_factor*

Specify the smooth-factor used in the dynamic echo timer for GTPU service.

Must be an integer in the range of 1-5.

Usage Guidelines Use this command to enable the dynamic echo timer for GTPU service.

context gtpu-service redundancy-group

Configures redundancy group parameters.

Privilege Security Administrator, Administrator

Syntax Description **redundancy-group** *redundancy_group_name*

redundancy_group_name

Specify the redundancy group name.

Must be a string.

Usage Guidelines Use this command to configure redundancy group parameters.

context gtpu-service redundancy-group host

Configures redundancy group host parameters.

Privilege Security Administrator, Administrator

Syntax Description **host** *host_name*

host_name

Specify the redundancy group host name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group host parameters.

context gtpu-service redundancy-group host bind

Binds the service to an IP address.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > GTPU Service Configuration

Syntax Description **bind { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **} [bearer-type** *bearer_type* **]**

ipv4-address *ipv4_address*

Specify the GTPU address of the GTPU service.

Must be an IP address.

ipv4-address *ipv6_address*

Specify the GTPU address of the GTPU service.

Must be an IPv6 address.

bearer-type *bearer_type*

Specify the media type supported for the GTPU endpoint.

Must be one of the following:

- all
- ims-media
- non-ims-media

Usage Guidelines Use this command to bind the service to an IP address.

context gtpu-service redundancy-group host echo-interval

Configures the echo interval.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > GTPU Service Configuration

Syntax Description **echo-interval** *echo_interval*

echo_interval

Specify the echo interval.

Must be an integer in the range of 60-3600.

Usage Guidelines Use this command to configure the echo interval.

context gtpu-service redundancy-group host echo-interval dynamic

Enables the dynamic echo timer for GTPU Service.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > GTPU Service Configuration

Syntax Description

dynamic [smooth-factor *smooth_factor* **]**

dynamic

Specify the enable dynamic echo timer for GTPU service.

smooth-factor ***smooth_factor***

Specify the smooth-factor used in the dynamic echo timer for GTPU service.

Must be an integer in the range of 1-5.

Usage Guidelines

Use this command to enable the dynamic echo timer for GTPU service.

context interface-loopback

Configures loopback interface parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

interface-loopback *interface_name*

interface_name

Specify the interface name.

Must be a string.

Usage Guidelines

Use this command to configure loopback interface parameters.

context interface-loopback redundancy-group

Configures redundancy group parameters.

Privilege

Security Administrator, Administrator

Syntax Description **redundancy-group** *group_name*

group_name

Specify the redundancy group name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group parameters.

context interface-loopback redundancy-group host

Configures redundancy group host parameter.

Privilege Security Administrator, Administrator

Syntax Description **host** *host_name*

host_name

Specify the redundancy group host name.

Must be a string.

ipv4-address ***ipv4_address***

Specify the IPv4 address.

Must be IPv4 CIDR notation ##.##.##.##/x.

ipv6-address ***ipv6_address***

Specify the IPv6 address.

Must be IPv6 CIDR notation ####:####:####:####:####:####:####:####/###.

Usage Guidelines Use this command to configure the redundancy group host parameter.

context lawful-intercept

Configures Lawful Intercept.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **lawful-intercept**

Usage Guidelines Use this command to configure Lawful Intercept. Changes to the Lawful Intercept Configuration mode.

context lawful-intercept dictionary

Configures the dictionary to use for Lawful Intercept.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

Syntax Description

dictionary *dictionary_name*

dictionary_name

Specify the Lawful Intercept dictionary name.

Must be one of the following:

- custom1
- custom2
- custom3
- custom4
- custom5
- custom6
- custom7
- custom8
- custom9
- custom10
- standard

Usage Guidelines

Use this command to configure the dictionary to use for Lawful Intercept.

context lawful-intercept redundancy-group

Configures Lawful Intercept redundancy group parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

Syntax Description

redundancy-group *group_name*

group_name

Specify the redundancy group name.

Must be a string.

Usage Guidelines Use this command to configure Lawful Intercept redundancy group parameters.

context lawful-intercept redundancy-group host

Configures Lawful Intercept redundancy group hosts parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`host`** *`host_name`*

host_name

Specify the host name.

Must be a string.

Usage Guidelines Use this command to configure Lawful Intercept redundancy group hosts parameters.

context lawful-intercept redundancy-group host dictionary

Configures the dictionary to use for Lawful Intercept.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`dictionary`** *`dictionary_name`*

dictionary_name

Specify the Lawful Intercept dictionary name.

Must be one of the following:

- custom1
- custom2
- custom3
- custom4
- custom5
- custom6
- custom7
- custom8

- custom9
- custom10
- standard

Usage Guidelines Use this command to configure the dictionary to use for Lawful Intercept.

context lawful-intercept redundancy-group host src-ip-addr

Configures the source IP address used by Lawful Intercept.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`src-ip-addr { ipv4_address | ipv6_address }`**

{ ipv4_address | ipv6_address }

Specify the IP address.

Must be an IPv4 address.

Usage Guidelines Use this command to configure the source IP address used by Lawful Intercept.

context lawful-intercept src-ip-addr

Configures the source IP address used by Lawful Intercept.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`src-ip-addr { ipv4_address | ipv6_address }`**

{ ipv4_address | ipv6_address }

Specify the IP address.

Must be an IPv4 address.

Usage Guidelines Use this command to configure the source IP address used by Lawful Intercept.

context sx-service

Configures SX service parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **sx-service** *sx_service_name*

sx_service_name

Specify the SX service name.

Must be a string.

Usage Guidelines Use this command to configure SX service parameters.

context sx-service bind

Designates an IPv4 address of the Sx service.

Privilege Security Administrator, Administrator

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

Syntax Description **bind { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **}**

ipv4-address *ipv4_address*

Specify the IPv4 address.

Must be an IPv4 address.

ipv6-address *ipv6_address*

Specify the IPv6 address.

Must be an IPv6 address.

Usage Guidelines Use this command to designate an IPv4 address of the Sx service.

context sx-service instance-type

Configures the instance type that this service is going to be used for.

Privilege Security Administrator, Administrator

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

Syntax Description **instance-type { controlplane** *cp_instance* **| userplane** *up_instance* **}**

controlplane *cp_instance*

Specify the SX service control plane instance.

userplane *up_instance*

Specify the SX service user plane instance.

Usage Guidelines Use this command to configure the instance type that this service is going to be used for.

context sx-service redundancy-group

Configures redundancy group parameters.

Privilege Security Administrator, Administrator

Syntax Description **redundancy-group** *group_name*

group_name

Specify the redundancy group name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group parameters.

context sx-service redundancy-group host

Configures redundancy group host parameters.

Privilege Security Administrator, Administrator

Syntax Description **host** *host_name*

host_name

Specify the host name.

Must be a string.

Usage Guidelines Use this command to configure redundancy group host parameters.

context sx-service redundancy-group host bind

Designates an IPv4 address of the Sx service.

Privilege Security Administrator, Administrator

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

Syntax Description **bind { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **}**

ipv4-address *ipv4_address*

Specify the IPv4 address.

Must be an IPv4 address.

ipv6-address *ipv6_address*

Specify the IPv6 address.

Must be an IPv6 address.

Usage Guidelines Use this command to designate an IPv4 address of the Sx service.

context sx-service redundancy-group host instance-type

Configures the instance type that this service is going to be used for.

Privilege Security Administrator, Administrator

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

Syntax Description **`instance-type { controlplane`** *`cp_instance`* **`| userplane`** *`up_instance`* **`}`**

controlplane *cp_instance*

Specify the SX service control plane instance.

userplane *up_instance*

Specify the SX service user plane instance.

Usage Guidelines Use this command to configure the instance type that this service is going to be used for.

context sx-service redundancy-group host sx-protocol association

Configures SX Association parameters.

Privilege Security Administrator, Administrator

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

Syntax Description **`association reattempt-timeout`** *`reattempt_timeout`*

reattempt-timeout *reattempt_timeout*

Specify the Association Reattempt timeout for SX Service in seconds.

Must be an integer in the range of 30-300.

Usage Guidelines Use this command to configure SX Association parameters.

context sx-service redundancy-group host sx-protocol heart-beat interval

Configures SX heartbeat interval.

Privilege Security Administrator, Administrator

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

Syntax Description **`interval`** *`heartbeat_interval`*

interval *heartbeat_interval*

Specify the SX heartbeat interval.

Must be an integer in the range of 1-3600.

Usage Guidelines Use this command to configure the SX heartbeat Interval.

context sx-service redundancy-group host sx-protocol heart-beat max-retransmissions

Configures maximum number of retries for SX heartbeat request.

Privilege Security Administrator, Administrator

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

Syntax Description **`max-retransmissions`** *`max_retransmissions`*

max-retransmissions *max_retransmissions*

Specify the maximum number of retries for SX heartbeat requests.

Must be an integer in the range of 1-15.

Default Value: 4.

Usage Guidelines Use this command to configure maximum number of retries for SX heartbeat request.

context sx-service redundancy-group host sx-protocol heart-beat retransmission-timeout

Configures the heartbeat retransmission timeout for SX Service.

Privilege Security Administrator, Administrator

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

Syntax Description **`retransmission-timeout`** *`retransmission_timeout`*

retransmission_timeout

Specify the heartbeat retransmission timeout for SX service.

Must be an integer in the range of 1-20.

Default Value: 5.

Usage Guidelines Use this command to configure the heartbeat retransmission timeout for SX service.

context sx-service sx-protocol association

Configures SX Association parameters.

Privilege Security Administrator, Administrator

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

Syntax Description **`association reattempt-timeout`** *`reattempt_timeout`*

reattempt-timeout *reattempt_timeout*

Specify the Association Reattempt timeout for SX Service in seconds.

Must be an integer in the range of 30-300.

Usage Guidelines Use this command to configure SX Association parameters.

context sx-service sx-protocol heart-beat interval

Configures SX heartbeat interval.

Privilege Security Administrator, Administrator

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

Syntax Description **`interval`** *`heartbeat_interval`*

interval *heartbeat_interval*

Specify the SX heartbeat interval.

Must be an integer in the range of 1-3600.

Usage Guidelines Use this command to configure the SX heartbeat Interval.

contextsx-servicesx-protocolheart-beatmax-retransmissions

Configures maximum number of retries for SX heartbeat request.

Privilege Security Administrator, Administrator

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

Syntax Description **max-retransmissions** *max_retransmissions*

max-retransmissions *max_retransmissions*

Specify the maximum number of retries for SX heartbeat requests.

Must be an integer in the range of 1-15.

Default Value: 4.

Usage Guidelines Use this command to configure maximum number of retries for SX heartbeat request.

context sx-service sx-protocol heart-beat retransmission-timeout

Configures the heartbeat retransmission timeout for SX Service.

Privilege Security Administrator, Administrator

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

Syntax Description **retransmission-timeout** *retransmission_timeout*

retransmission_timeout

Specify the heartbeat retransmission timeout for SX service.

Must be an integer in the range of 1-20.

Default Value: 5.

Usage Guidelines Use this command to configure the heartbeat retransmission timeout for SX service.

context user-plane-service

Creates and configures user plane service.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description `user-plane-service up_service_name`

up_service_name

Specify the user plane service name.

Must be a string.

Usage Guidelines Use this command to create and configure a user plane service.

context user-plane-service associate control-plane-group

Associates control plane Group to which user plane service will perform Sx-Association.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description `control-plane-group cp_group_name`

cp_group_name

Specify the control plane group name.

Must be a string.

Usage Guidelines Use this command to associate control plane group to which user plane service will perform Sx-Association.

context user-plane-service associate fast-path service

Configures fast path related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description `fast-path service`

Usage Guidelines Use this command to configure fast path related parameters.

context user-plane-service associate gtpu-service

Configures the GTPU service for this user plane service.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **gtpu-service** *gtpu_service_name*

gtpu_service_name

Specify the GTPU service name.

Must be a string.

Usage Guidelines Use this command to configure the GTPU service for this user plane service.

context user-plane-service associate gtpu-service cp-tunnel

Configures the interface type as cp-tunnel (tunnel towards control plane function).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **cp-tunnel**

Usage Guidelines Use this command to configure the interface type as cp-tunnel (tunnel towards control plane function).

contextuser-plane-serviceassociategtpu-servicepgw-ingress

Configures the interface type as PGW ingress.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **pgw-ingress**

Usage Guidelines Use this command to configure the interface type as PGW ingress.

context user-plane-service associate gtpu-service sgw-egress

Configures the interface type as SGW egress.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **sgw-egress**

Usage Guidelines Use this command to configure the interface type as SGW egress.

contextuser-plane-serviceassociategtpu-servicesgw-ingress

Configures the interface type as SGW ingress.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **`sgw-ingress`**

Usage Guidelines Use this command to configure the interface type as SGW ingress.

context user-plane-service associate gtpu-service upf-ingress

Configures the interface type as UPF ingress.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **`upf-ingress`**

Usage Guidelines Use this command to configure the interface type as UPF ingress.

context user-plane-service associate sx-service

Configures the Sx service for this user plane service.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **`sx-service`** *`sx_service_name`*

sx_service_name

Specify the Sx service name.

Must be a string.

Usage Guidelines Use this command to configure the Sx service for this user plane service.

context user-plane-service redundancy-group

Configures redundancy group parameters.

Privilege Security Administrator, Administrator

Syntax Description **redundancy-group** *redundancy_group_name*

redundancy_group_name

Specify the redundancy group name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group parameters.

context user-plane-service redundancy-group host

Configures redundancy group host parameters.

Privilege Security Administrator, Administrator

Syntax Description **host** *host_name*

host_name

Specify the host name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group host parameters.

context user-plane-service redundancy-group host associate control-plane-group

Associates control plane Group to which user plane service will perform Sx-Association.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **control-plane-group** *cp_group_name*

cp_group_name

Specify the control plane group name.

Must be a string.

Usage Guidelines Use this command to associate control plane group to which user plane service will perform Sx-Association.

context user-plane-service redundancy-group host associate fast-path service

Configures fast path related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **`fast-path service`**

Usage Guidelines Use this command to configure fast path related parameters.

context user-plane-service redundancy-group host associate gtpu-service

Configures the GTPU service for this user plane service.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **`gtpu-service`** *`gtpu_service_name`*

gtpu_service_name

Specify the GTPU service name.

Must be a string.

Usage Guidelines Use this command to configure the GTPU service for this user plane service.

context user-plane-service redundancy-group host associate gtpu-service cp-tunnel

Configures the interface type as cp-tunnel (tunnel towards control plane function).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **`cp-tunnel`**

Usage Guidelines Use this command to configure the interface type as cp-tunnel (tunnel towards control plane function).

context user-plane-service redundancy-group host associate gtpu-service pgw-ingress

Configures the interface type as PGW ingress.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description `pgw-ingress`

Usage Guidelines Use this command to configure the interface type as PGW ingress.

context user-plane-service redundancy-group host associate gtpu-service sgw-egress

Configures the interface type as SGW egress.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description `sgw-egress`

Usage Guidelines Use this command to configure the interface type as SGW egress.

context user-plane-service redundancy-group host associate gtpu-service sgw-ingress

Configures the interface type as SGW ingress.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description `sgw-ingress`

Usage Guidelines Use this command to configure the interface type as SGW ingress.

context user-plane-service redundancy-group host associate gtpu-service upf-ingress

Configures the interface type as UPF ingress.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **upf-ingress**

Usage Guidelines Use this command to configure the interface type as UPF ingress.

context user-plane-service redundancy-group host associate sx-service

Configures the Sx service for this user plane service.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > User Plane Service Configuration

Syntax Description **sx-service** *sx_service_name*

sx_service_name

Specify the Sx service name.

Must be a string.

Usage Guidelines Use this command to configure the Sx service for this user plane service.

control-plane-group

Configures control plane group on user plane.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **control-plane-group** *cp_group_name*

cp_group_name

Specify the control plane group name.

Must be a string.

Usage Guidelines Use this command to configure control plane group on user plane.

control-plane-group peer-node-id ipv4-address

Configures IPv4 address.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Control Plane Group Configuration

Syntax Description **peer-node-id** *ipv4_address* **[interface** *interface* **]**

ipv4_address

Specify the IPv4 address.

Must be an IPv4 address.

interface *interface_type*

Specify the interface type for peer node.

Must be one of the following:

- n4

Usage Guidelines Use this command to configure IPv4 address.

control-plane-group peer-node-id ipv6-address

Configures IPv6 address.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Control Plane Group Configuration

Syntax Description **peer-node-id** *ipv6_address* **[interface** *interface* **]**

ipv6_address

Specify the IPv6 address.

Must be an IPv6 address.

interface *interface_type*

Specify the interface type for peer node.

Must be one of the following:

- n4

Usage Guidelines Use this command to configure the IPv6 address.

control-plane-group redundancy-group

Configures redundancy group parameters.

Privilege Security Administrator, Administrator

Syntax Description **redundancy-group** *redundancy_group_name*

redundancy_group_name

Specify the redundancy group name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group parameters.

control-plane-group redundancy-group host

Configures redundancy group host parameters.

Privilege Security Administrator, Administrator

Syntax Description **host** *redundancy_group_host_name*

redundancy_group_host_name

Specify the redundancy group host name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group host parameters.

control-plane-group redundancy-group host peer-node-id ipv4-address

Configures IPv4 address.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Control Plane Group Configuration

Syntax Description **peer-node-id** *ipv4_address* **[interface** *interface* **]**

ipv4_address

Specify the IPv4 address.

Must be an IPv4 address.

interface *interface_type*

Specify the interface type for peer node.

Must be one of the following:

- n4

Usage Guidelines Use this command to configure IPv4 address.

control-plane-group redundancy-group host peer-node-id ipv6-address

Configures IPv6 address.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Control Plane Group Configuration

Syntax Description **peer-node-id** *ipv6_address* **[interface** *interface* **]**

ipv6_address

Specify the IPv6 address.

Must be an IPv6 address.

interface *interface_type*

Specify the interface type for peer node.

Must be one of the following:

- n4

Usage Guidelines Use this command to configure the IPv6 address.

control-plane-group redundancy-group host sx-association initiated-by-cp

Configures the Sx Association Setup Request be initiated by control plane.

Privilege Security Administrator, Administrator

Syntax Description `sx-association initiated-by-cp`

Usage Guidelines Use this command to specify Sx Association Setup Request will be initiated by control plane.

control-plane-group redundancy-group host sx-association initiated-by-up

Configures the Sx Association Setup Request be initiated by user plane.

Privilege Security Administrator, Administrator

Syntax Description `sx-association initiated-by-up`

Usage Guidelines Use this command to specify Sx Association Setup Request will be initiated by user plane. This is the default setting.

control-plane-group sx-association initiated-by-cp

Configures the Sx Association Setup Request be initiated by control plane.

Privilege Security Administrator, Administrator

Syntax Description `sx-association initiated-by-cp`

Usage Guidelines Use this command to specify Sx Association Setup Request will be initiated by control plane.

control-plane-group sx-association initiated-by-up

Configures the Sx Association Setup Request be initiated by user plane.

Privilege Security Administrator, Administrator

Syntax Description `sx-association initiated-by-up`

Usage Guidelines Use this command to specify Sx Association Setup Request will be initiated by user plane. This is the default setting.

interface

Configures interface parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **interface** *interface_name*

interface_name

Specify the interface name.

Must be a string.

loopback

Specfiy to enable loopback.

ipaddress ***ip_address***

Specify the IP address.

Must be IPv4 CIDR notation ##.##.##.##/x or in IPv6 CIDR notation ####:####:####:####:####:####:####:####/###.

-Or-

Must be an IP address.

Usage Guidelines Use this command to configure interface parameters.

rcm switchover

Configures RCM switchover operation.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **rcm switchover source** *ip_address* **[destination** *ip_address* **]**

source ***ip_address***

Specify the source IP address.

Must be an IP address.

destination ***ip_address***

Specify the destination IP address.

Must be an IP address.

Usage Guidelines Use this command to configure RCM switchover operation.

url-blacklisting database directory

Configures URL Blacklisting database directory parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

`url-blacklisting directory path` *`directory_path`*

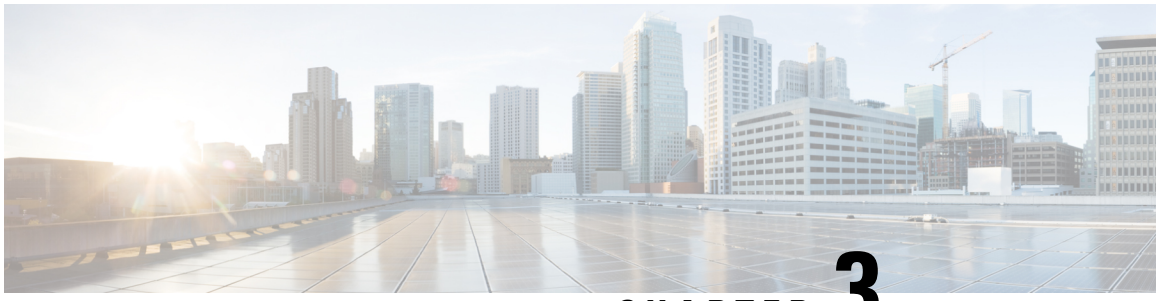
path *directory_path*

Specify the URL Blacklisting directory path.

Must be a string.

Usage Guidelines

Use this command to configure URL Blacklisting database directory parameters.



CHAPTER 3

SMF IPAM CLI Commands

ipam address-pool

Configures IPAM address pools.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > IPAM Configuration

Syntax Description

`address-pool` *`pool_name`* **`[ static | offline | vrf-name`** *`vrf_name`* **`]`**

pool_name

Specify the address pool's name.

Must be a string.

static

Specify the pool as a static pool.

offline

Specify the pool as an offline pool.

vrf-name *vrf_name*

Specify the VRF name.

Must be a string.

Usage Guidelines Use this command to configure IPAM address pools.

ipam address-pool ipv4 address-range

Configures IPv4 address ranges.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IPAM Configuration > Address Pool Configuration

Syntax Description **`address-range`** *`start_ipv4_address end_ipv4_address`* **`[ offline ]`**

start_ipv4_address

Specify the start address of the IPv4 address range.

Must be an IPv4 address.

end_ipv4_address

Specify the end address of the IPv4 address range.

Must be an IPv4 address.

offline

Specify the IPv4 address range as offline.

Usage Guidelines Use this command to configure IPv4 address ranges.

ipam address-pool ipv4 split-size

Configures chunk split size.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IPAM Configuration

Syntax Description **`split-size [ per-cache`** *`number_of_addresses`* **`] [ per-dp`** *`number_of_addresses`* **`]`**

per-cache *number_of_addresses*

Specify the number of addresses per chunk for IPAM cache allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

per-dp *number_of_addresses*

Specify the number of addresses per chunk for data-plane allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

no-split

Specify not to split the address range into smaller chunks.

Usage Guidelines Use this command to configure chunk split sizes.

ipam address-pool ipv4 threshold

Configures pool thresholds.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IPAM Configuration

Syntax Description **`threshold upper-threshold`** *`upper_threshold`*

upper-threshold *upper_threshold*

Specify the upper threshold value in percentage.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure pool thresholds.

ipam address-pool ipv6 address-ranges address-range

Configures IPv6 address ranges.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IPAM Configuration > Address Pool Configuration > Address Ranges Configuration

Syntax Description **`address-range`** *`start_ipv6_address end_ipv6_address`* **`[ offline ]`**

start_ipv6_address

Specify the start address of the IPv6 address range.

Must be an IPv6 address.

end_ipv6_address

Specify the end address of the IPv6 address range.

Must be an IPv6 address.

offline

Specify the IPv6 address range as offline.

Usage Guidelines Use this command to configure IPv6 address ranges.

ipam address-pool ipv6 address-ranges split-size

Configures chunk split size.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IPAM Configuration

Syntax Description **`split-size [ per-cache`** *`number_of_addresses`* **`] [ per-dp`** *`number_of_addresses`* **`]`**

per-cache *number_of_addresses*

Specify the number of addresses per chunk for IPAM cache allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

per-dp *number_of_addresses*

Specify the number of addresses per chunk for data-plane allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

no-split

Specify not to split the address range into smaller chunks.

Usage Guidelines Use this command to configure chunk split sizes.

ipam address-pool ipv6 address-ranges threshold

Configures pool thresholds.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IPAM Configuration

Syntax Description **`threshold upper-threshold`** *`upper_threshold`*

upper-threshold *upper_threshold*

Specify the upper threshold value in percentage.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure pool thresholds.

ipam address-pool ipv6 prefix-ranges prefix-range

Configures IPv6 prefix ranges.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IPAM Configuration > Address Pool Configuration > Prefix Ranges Configuration

Syntax Description **`prefix-range`** *`prefix_value`* **`length`** *`prefix_length`* **`[ offline ]`**

prefix-range *prefix_value*

Specify the IPv6 prefix range.

Must be an IPv6 address.

length *prefix_length*

Specify the prefix length.

Must be an integer in the range of 1-63.

offline

Specify the IPv6 prefix range as offline.

Usage Guidelines Use this command to configure IPv6 prefix ranges.

ipam address-pool ipv6 prefix-ranges split-size

Configures chunk split size.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IPAM Configuration

Syntax Description **`split-size [ per-cache`** *`number_of_addresses`* **`] [ per-dp`** *`number_of_addresses`* **`]`**

per-cache *number_of_addresses*

Specify the number of addresses per chunk for IPAM cache allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

per-dp *number_of_addresses*

Specify the number of addresses per chunk for data-plane allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

no-split

Specify not to split the address range into smaller chunks.

Usage Guidelines Use this command to configure chunk split sizes.

ipam address-pool ipv6 prefix-ranges threshold

Configures pool thresholds.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IPAM Configuration

Syntax Description **`threshold upper-threshold`** *`upper_threshold`*

upper-threshold *upper_threshold*

Specify the upper threshold value in percentage.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure pool thresholds.

ipam dp

Displays IPAM data-plane allocations.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`show ipam dp`**

dp-name

Displays name of the data plane.

Must be a string.

ipv4-total

Displays the IPv4 total addresses.

Must be an integer.

ipv4-used

Displays the IPv4 used addresses.

Must be an integer.

ipv4-threshold

Displays the IPv4 usage threshold.

Must be an integer.

ipv6-addr-total

Displays the IPv6 total addresses.

Must be an integer.

ipv6-addr-used

Displays the IPv6 used addresses.

Must be an integer.

ipv6-addr-threshold

Displays the IPv6 address usage threshold.

Must be an integer.

ipv6-pfx-total

Displays the IPv6 total prefixes.

Must be an integer.

ipv6-pfx-used

Displays IPv6 used prefixes.

Must be an integer.

ipv6-pfx-threshold

Displays IPv6 prefix usage threshold.

Must be an integer.

Usage Guidelines Use this command to view IPAM data-plane allocations.

ipam pool

Displays pool allocation information.

Privilege Security Administrator, Administrator

Command Modes

Exec

Syntax Description

`show ipam pool`

pool-name

Displays the pool name.

Must be a string.

ipv4-total

Displays the IPv4 total addresses.

Must be an integer.

ipv4-used

Displays the IPv4 used addresses.

Must be an integer.

ipv4-threshold

Displays the IPv4 usage threshold.

Must be an integer.

ipv6-addr-total

Displays total IPv6 addresses.

Must be an integer.

ipv6-addr-used

Displays used IPv6 addresses.

Must be an integer.

ipv6-addr-threshold

Displays IPv6 address usage threshold.

Must be an integer.

ipv6-pfx-total

Displays total IPv6 prefixes.

Must be an integer.

ipv6-pfx-used

Displays used IPv6 prefixes.

Must be an integer.

ipv6-pfx-threshold

Displays IPv6 prefix usage threshold.

Must be an integer.

Usage Guidelines Use this command to view pool allocation information.

ipam source

Configures pool-datastore source selection.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `ipam source local`

local

Specify to use local address pool datastore.

Usage Guidelines Use this command to configure pool-datastore source selection.";

ipam source external ipam

Configures external IPAM server for pool information.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **ipam source external ipam [host** *ip_address* **| port** *port_number* **| vendor** *vendor_id* **]**

host *ip_address*

Specify the IPAM server's IP address.

Must be an IP address.

port *port_number*

Specify the IPAM server's port number.

Must be an integer in the range of 1-65535.

vendor *vendor_id*

Specify the IPAM server's vendor ID. Default: cisco.

Must be a vendor ID.

Usage Guidelines Use this command to configure external IPAM server for pool information.

ipam threshold

Configures global thresholds.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > IPAM Configuration

Syntax Description **threshold [[ipv4-addr** *ipv4_address_threshold* **] | [ipv6-addr** *ipv6_address_threshold* **] | [ipv6-prefix** *ipv6_prefix_threshold* **]]**

ipv4-addr *ipv4_address_threshold*

Specify the IPv4 address threshold in percentage.

Must be an integer in the range of 1-100.

ipv6-addr *ipv6_address_threshold*

Specify the IPv6 address threshold in percentage.

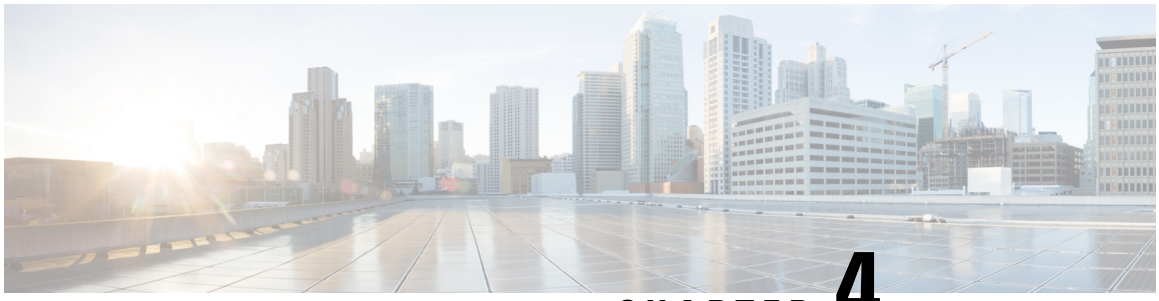
Must be an integer in the range of 1-100.

ipv6-prefix *ipv6_prefix_threshold*

Specify the IPv6 prefix threshold in percentage.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure global thresholds.



CHAPTER 4

SMF Mobile CLI Commands

active-charging service

Configures Active Charging Service parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

`active-charging service` *`service_name`*

service_name

Specify the service name.

Must be a string.

accelerate-flow

Specify accelerated flow packet processing.

Usage Guidelines

Use this command to configure the Active Charging Service parameters.

You can configure a maximum of one element with this command.

active-charging service bandwidth-policy

Configures bandwidth policy parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration

Syntax Description

`bandwidth-policy` *`bandwidth_policy_name`*

bandwidth_policy_name

Specify the active charging bandwidth policy name.

Must be a string.

Usage Guidelines

Use this command to configure bandwidth policy parameters. Enters the Bandwidth Policy Configuration mode.

active-charging service bandwidth-policy flow limit-for-bandwidth id

Configures bandwidth policy parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Bandwidth Policy Configuration

Syntax Description

`flow limit-for-bandwidth id` *`id`* **`group-id`** *`group_id`*

id *id*

Specify the bandwidth ID.

Must be an integer in the range of 1-65535.

group-id *group_id*

Specify the bandwidth policy group ID.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to configure the bandwidth policy parameters.

active-charging service bandwidth-policy group-id

Configures bandwidth policy group ID.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Bandwidth Policy Configuration

Syntax Description

`group-id` *`group_id`*

group_id

Specify the bandwidth policy group ID.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to configure the bandwidth policy group ID.

active-charging service bandwidth-policy group-id direction downlink

Configures bandwidth control in downlink direction.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Bandwidth Policy Configuration

Syntax Description **`group-id`** *`group_id`* **`direction downlink`**

Usage Guidelines Use this command to configure bandwidth control in downlink direction.

active-charging service bandwidth-policy group-id direction downlink grpPeakBwp

Configures peak bandwidth parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`grpPeakBwp`**

peak-options *peak_options*

Specify the peak data rate option.

Must be one of the following:

- peak-data-rate
- peak-data-rate-kbps

peak-value *peak_value*

Specify the bandwidth in bits per second.

Must be an integer in the range of 1-4294967295.

peak-burst-size *peak_burst_size*

Specify the burst size in bytes.

Must be an integer in the range of 1-4294967295.

violate-action *violate_action*

Specify the action to be taken if Peak Data Rate is surpassed.

Must be one of the following:

- discard
- lower-ip-precedence

committed-options *committed_option*

Specify the committed option.

Must be one of the following:

- committed-data-rate
- committed-data-rate-kbps

committed-value *committed_value*

Specify the bandwidth in bits per second.

Must be an integer in the range of 1-4294967295.

committed-burst-size *committed_burst_size*

Specify the committed burst size in bytes.

Must be an integer in the range of 1-4294967295.

exceed-action *exceed_action*

Specify the action to be taken if committed data rate is surpassed.

Must be one of the following:

- discard
- lower-ip-precedence

Usage Guidelines Use this command to configure the peak bandwidth parameters.

active-charging service bandwidth-policy group-id direction uplink

Configures bandwidth control in uplink direction.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Bandwidth Policy Configuration

Syntax Description **`group-id`** *`group_id`* **`direction uplink`**

Usage Guidelines Use this command to configure bandwidth control in uplink direction.

active-charging service bandwidth-policy group-id direction uplink grpPeakBwp

Configures peak bandwidth parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

`grpPeakBwp`

peak-options *peak_options*

Specify the peak data rate option.

Must be one of the following:

- peak-data-rate
- peak-data-rate-kbps

peak-value *peak_value*

Specify the bandwidth in bits per second.

Must be an integer in the range of 1-4294967295.

peak-burst-size *peak_burst_size*

Specify the burst size in bytes.

Must be an integer in the range of 1-4294967295.

violate-action *violate_action*

Specify the action to be taken if Peak Data Rate is surpassed.

Must be one of the following:

- discard
- lower-ip-precedence

committed-options *committed_option*

Specify the committed option.

Must be one of the following:

- committed-data-rate
- committed-data-rate-kbps

committed-value *committed_value*

Specify the bandwidth in bits per second.

Must be an integer in the range of 1-4294967295.

committed-burst-size *committed_burst_size*

Specify the committed burst size in bytes.

Must be an integer in the range of 1-4294967295.

exceed-action *exceed_action*

Specify the action to be taken if committed data rate is surpassed.

Must be one of the following:

- discard
- lower-ip-precedence

Usage Guidelines Use this command to configure the peak bandwidth parameters.

active-charging service buffering-limit

Configures flow/session-based packet buffering.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **`buffering-limit { [ flow-max-packets`** *`flow_max_packets`* **`] [ subscriber-max-packets`** *`subscriber_max_packets`* **`] }`**

flow-max-packets *flow_max_packets*

Specify the maximum number of packets to be buffered per flow.

Must be an integer in the range of 1-255.

subscriber-max-packets *subscriber_max_packets*

Specify the maximum number of packets to be buffered per subscriber.

Must be an integer in the range of 1-255.

Usage Guidelines Use this command to configure flow/session-based packet buffering configuration.

active-charging service charging-action

Configures ACS charging actions.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration

Syntax Description

charging-action *charging_action_name* **[content-id** *content_id* **| nexthop-forwarding-address {** *ipv4_address* **|** *ipv6_address* **} | qos-class-identifier** *qos_class_id* **| service-identifier** *service_id* **| tft-notify-ue]**

charging_action_name

Specify the charging action name.

Must be a string.

content-id *content_id*

Specify the content ID to use in the generated billing records, as well as the AVP used by the Credit Control Application, such as the "Rating-Group" AVP for use by the Diameter Credit Control Application (DCCA). This identifier assists the carrier's billing post processing and is also used by the credit-control system to use independent quotas for different value of content-id.

Must be an integer in the range of 1-2147483647.

nexthop-forwarding-address { *ipv4_address* | *ipv6_address* }

Specify the nexthop forwarding address for this charging action. When an uplink packet matches a rule and a charging action is applied to it this nexthop forwarding address is used.

Must be an IP address.

qos-class-identifier *qos_class_id*

Specify the QoS Class Identifier (QCI).

Must be an integer in the range of 1-9.

service-identifier *service_id*

Specify the service identifier to use in the generated billing records, as well as the AVP used by the Credit Control Application, such as the "Service-Identifier" AVP for use by DCCA. This is a more general classifier than content-id.

Must be an integer in the range of 1-2147483647.

tft-notify-ue

Specify whether or not TFT updates are sent to UE. Use this command to suppress the selected TFT updates from being sent to the UE. This helps to identify if the appropriate TFT defined in the charging action needs to be sent to the UE or not.

Usage Guidelines

Use this command to create and configure an ACS charging action. A charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (for example, an EDR) to dropping the IP packet, etc. The charging action will also determine the metering principle whether to count retransmitted packets and which protocol field to use for billing (L3/L4/L7 etc).

Example

The following command creates a charging action named action123 and changes to the ACS Charging Action Configuration Mode:

```
charging-action action123
```

active-charging service charging-action allocation-retention-priority

Configures the Allocation Retention Priority (ARP).

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description

`allocation-retention-priority` *`priority`* **`[ pci`** *`pci_value`* **`| pvi`** *`pvi_value`* **`]`**

priority

Specify the priority.

Must be an integer in the range of 1-15.

pci *pci_value*

Specify the Pre-emption Capability Indicator (PCI).

Must be one of the following:

- NOT_PREEMPT
- MAY_PREEMPT

pvi *pvi_value*

Specify the Pre-emption Vulnerability Indicator (PVI).

Must be one of the following:

- NOT_PREEMPTABLE
- PREEMPTABLE

Usage Guidelines

This command configures the ARP, which indicates the priority of allocation and retention of the service data flow. The ARP resolves conflicts in demand for network resources. At the time of resource crunch, this parameter prioritizes allocation of resources during bearer establishment and modification. In a congestion situation, a lower ARP flow may be dropped to free up capacity. Once a service flow is successfully established, this parameter plays no role in quality of service (QoS) experienced by the flow.

Example

The following command sets the ARP to 10:

```
allocation-retention-priority 10
```

active-charging service charging-action billing-action

Configures the billing action for packets that match specific ruledefs.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description

`billing-action egcdr`

egcdr

Specify to enable eG-CDR billing.

Usage Guidelines

Use this command to enable eG-CDR type of billing for content matching this charging action.

active-charging service charging-action cca

Configures the credit control behavior.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description

`cca charging credit [ rating-group` *`coupon_id`* **`] [ preemptively-request ]`**

Usage Guidelines

Use this command to configure RADIUS/Diameter Prepaid Credit Control Charging behavior.

active-charging service charging-action cca charging credit

Configures credit control charging credit behavior.

Privilege

Security Administrator, Administrator

Syntax Description

`credit rating-group` *`coupon_id`* **`preemptively-request`**

rating-group *coupon_id*

Specify the coupon ID used in prepaid charging as rating-group which maps to the coupon ID for prepaid customer. This option also assigns different content-types for the same charging action depending upon whether or not prepaid is enabled. This rating-group overrides the content ID, if present in the same

charging-action for the prepaid customer in Diameter Credit Control Application (DCCA). But, only the content IDs will be used in eG-CDRs irrespective of the presence of rating-group in that charging action.

Must be an integer in the range of 0-65535.

preemptively-request

Specify preemptively requested charging credit behavior.

Usage Guidelines Use this command to configure credit control charging credit behavior.

active-charging service charging-action flow action

Configures to take the redirect-url or terminate-flow action on packets that match ruledefs.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `action { redirect-url | terminate-flow }`

redirect-url

Specify to redirect URL.

Must be a string.

terminate-flow

Specify to terminate flow.

Usage Guidelines Use this command to specify the action to take on packets, for example to terminate.

Example

The following command sets the flow action to terminate:

```
flow action terminate-flow
```

active-charging service charging-action flow action discard

Configures discard action on packets that match ruledefs.

Privilege Security Administrator, Administrator

Syntax Description `action discard { downlink | uplink }`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure discard action on packets that match ruledefs.

active-charging service charging-action flow action readdress

Configures the readdress server for this charging action.

Privilege Security Administrator, Administrator

Syntax Description **`readdress server {`** *`ipv4_address`* **`|`** *`ipv6_address`* **`}`**

server { *ipv4_address* | *ipv6_address* }

Specify the readdress server IP address.

Must be an IP address.

Usage Guidelines Use this command to configure the readdress server for this charging action.

active-charging service charging-action flow limit-for-bandwidth

For Session Control functionality, this command allows you to enable or disable bandwidth limiting.

Privilege Security Administrator, Administrator

Syntax Description **`flow limit-for-bandwidth direction id`** *`bw_limit_id`*

id *bw_limit_id*

Specify the bandwidth limiting identifier.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to limit the bandwidth a subscriber uses in the uplink and downlink directions under Session Control.

active-charging service charging-action flow limit-for-bandwidth direction downlink

Configures bandwidth control in downlink direction.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `direction downlink`

Usage Guidelines Use this command to configure bandwidth control in downlink direction.

active-charging service charging-action flow limit-for-bandwidth direction downlink peak-data-rate

Configures the peak data rate in bits per second.

Privilege Security Administrator, Administrator

Syntax Description **`peak-data-rate`** *`peak_data_rate`*

peak_data_rate

Specify the peak data rate in bits per second.

Must be an integer in the range of 1-4294967295.

peak-burst-size *peak_burst_size*

Specify the peak burst size in bytes.

Must be an integer in the range of 1-4294967295.

violate-action { discard | lower-ip-precedence }

Specify the action to be taken if Peak Data Rate is surpassed.

Must be one of the following:

- discard: Discards the packet.
- lower-ip-precedence: Indicates lower the IP precedence of the packet.

committed-data-rate *committed_data_rate*

Specify the Committed Data Rate in bits per second. This can also be used to specify GBR for Bearer Binding (without the exceed-action).

Must be an integer in the range of 1-4294967295.

Default Value: 144000.

committed-burst-size *committed_burst_size*

Specify the committed burst size in bytes.

Must be an integer in the range of 1-4294967295.

Default Value: 3000.

exceed-action { discard | lower-ip-precedence }

Specify the action to be taken if Committed Data Rate is surpassed.

Must be one of the following:

- discard: Specify to discard the packet.
- lower-ip-precedence: Specify to lower IP precedence of the packet.

Usage Guidelines Use this command to configure the peak data rate in bits per second.

active-charging service charging-action flow limit-for-bandwidth direction uplink

Configures bandwidth control in uplink direction.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description **`direction uplink`**

Usage Guidelines Use this command to configure bandwidth control in uplink direction.

active-charging service charging-action flow limit-for-bandwidth direction uplink peak-data-rate

Configures the peak data rate in bits per second.

Privilege Security Administrator, Administrator

Syntax Description **`peak-data-rate`** *`peak_data_rate`*

peak_data_rate

Specify the peak data rate in bits per second.

Must be an integer in the range of 1-4294967295.

peak-burst-size *peak_burst_size*

Specify the peak burst size in bytes.

Must be an integer in the range of 1-4294967295.

violate-action { discard | lower-ip-precedence }

Specify the action to be taken if Peak Data Rate is surpassed.

Must be one of the following:

- discard: Discards the packet.
- lower-ip-precedence: Indicates lower the IP precedence of the packet.

committed-data-rate *committed_data_rate*

Specify the Committed Data Rate in bits per second. This can also be used to specify GBR for Bearer Binding (without the exceed-action).

Must be an integer in the range of 1-4294967295.

Default Value: 144000.

committed-burst-size *committed_burst_size*

Specify the committed burst size in bytes.

Must be an integer in the range of 1-4294967295.

Default Value: 3000.

exceed-action { discard | lower-ip-precedence }

Specify the action to be taken if Committed Data Rate is surpassed.

Must be one of the following:

- discard: Specify to discard the packet.
- lower-ip-precedence: Specify to lower IP precedence of the packet.

Usage Guidelines Use this command to configure the peak data rate in bits per second.

active-charging service charging-action tft packet-filter

Configures the packet filter to use in TFTs sent to the MS.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description **`tft packet-filter`** *`packet_filter_name`*

packet_filter_name

Specify the packet filter name.

Must be a string.

Usage Guidelines Use this command to configure the packet filter to be sent to the MS. Up to eight packet filters can be specified in a charging action.

You can configure a maximum of eight elements with this command.

Example

The following command configures the packet filter filter23 to be sent to the MS:

```
tft packet-filter filter23
```

active-charging service charging-action tos af11

Configures using Assured Forwarding 11 Per Hop Behavior (PHB).

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description

`tos af11 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines

Use this command to configure using Assured Forwarding 11 Per Hop Behavior (PHB).

active-charging service charging-action tos af12

Configures using Assured Forwarding 12 Per Hop Behavior (PHB).

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description

`tos af12 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines

Use this command to configure using Assured Forwarding 12 Per Hop Behavior (PHB).

active-charging service charging-action tos af13

Configures using Assured Forwarding 13 Per Hop Behavior (PHB).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos af13 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 13 Per Hop Behavior (PHB).

active-charging service charging-action tos af21

Configures using Assured Forwarding 21 Per Hop Behavior (PHB).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos af21 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 21 Per Hop Behavior (PHB).

active-charging service charging-action tos af22

Configures using Assured Forwarding 22 Per Hop Behavior (PHB).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos af22 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 22 Per Hop Behavior (PHB).

active-charging service charging-action tos af23

Configures using Assured Forwarding 23 Per Hop Behavior (PHB).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos af23 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 23 Per Hop Behavior (PHB).

active-charging service charging-action tos af31

Configures using Assured Forwarding 31 Per Hop Behavior (PHB).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos af31 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 31 Per Hop Behavior (PHB).

active-charging service charging-action tos af32

Configures using Assured Forwarding 32 Per Hop Behavior (PHB).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos af32 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 32 Per Hop Behavior (PHB).

active-charging service charging-action tos af33

Configures using Assured Forwarding 33 Per Hop Behavior (PHB).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos af33 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 33 Per Hop Behavior (PHB).

active-charging service charging-action tos af41

Configures using Assured Forwarding 41 Per Hop Behavior (PHB).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos af41 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 41 Per Hop Behavior (PHB).

active-charging service charging-action tos af42

Configures using Assured Forwarding 42 Per Hop Behavior (PHB).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos af42 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 42 Per Hop Behavior (PHB).

active-charging service charging-action tos af43

Configures using Assured Forwarding 43 Per Hop Behavior (PHB).

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos af43 [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 43 Per Hop Behavior (PHB).

active-charging service charging-action tos be

Configures using Best Effort Forwarding PHB.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos be [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Best Effort Forwarding Per Hop Behavior (PHB).

active-charging service charging-action tos ef

Configures using Expedited Forwarding PHB.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description `tos ef [ downlink | uplink ]`

uplink

Specify only uplink packets.

downlink

Specify only downlink packets.

Usage Guidelines Use this command to configure using Expedited Forwarding Per Hop Behavior (PHB).

active-charging service charging-action tos lower-bits

Configures the least-significant 6 bits in the ToS byte with the specified numeric value.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description

tos lower-bits *value*

value

Specify the value.

Must be an integer in the range of 0-63.

uplink

Specify the ToS only for uplink packets.

downlink

Specify the ToS only for downlink packets.

Usage Guidelines

Use this command to configure the least-significant 6 bits in the ToS byte with the specified numeric value.

active-charging service charging-action xheader-insert xheader-format

Configures the extension-header (x-header) format whose fields have to be inserted in HTTP request packets and HTTP response packets.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Charging Action Configuration

Syntax Description

xheader-insert xheader-format *xheader_format_name* **[encryption { rc4md5 | aes-256-gcm-sha384 [salt] }**

xheader_format_name

Specify the Xheader format name.

Must be a string.

Usage Guidelines

Use this command to enable x-header mode, and specify the x-header format name whose fields are to be inserted in HTTP GET and POST request packets and HTTP response packets.

Example

The following command enables x-header mode, and specifies the x-header format name as test12 for Request message:

```
xheader-insert xheader-format test12
```

active-charging service charging-action xheader-insert xheader-format encryption aes-256-gcm-sha384 encrypted

Configures encryption of x-header fields.

Privilege

Security Administrator, Administrator

Syntax Description

encrypted key *encrypted_key*

key

Specify the key to encrypt xheader fields.

encrypted_key

Specify the key that will be used for encryption of xheader fields.

Must be a string.

Usage Guidelines

Use this command to configure use of aes-256-gcm-sha384 to encrypt the x-header fields with AES-256-GCM algorithm and SHA384 to hash key in 384 bits.

active-charging service charging-action xheader-insert xheader-format encryption aes-256-gcm-sha384 key

Configures key to encrypt xheader fields.

Privilege

Security Administrator, Administrator

Syntax Description

key *encryption_key*

encryption_key

Specify the key to use for encryption of xheader fields.

Must be a string.

Usage Guidelines

Use this command to configure key to encrypt xheader fields.

active-charging service charging-action xheader-insert xheader-format encryption aes-256-gcm-sha384 salt encrypted

Configures encryption of x-header fields.

Privilege

Security Administrator, Administrator

Syntax Description

encrypted key *encrypted_key*

key

Specify the key to encrypt xheader fields.

encrypted_key

Specify the key that will be used for encryption of xheader fields.

Must be a string.

Usage Guidelines

Use this command to configure use of aes-256-gcm-sha384 to encrypt the x-header fields with AES-256-GCM algorithm and SHA384 to hash key in 384 bits.

active-charging service charging-action xheader-insert xheader-format encryption aes-256-gcm-sha384 salt key

Configures key to encrypt xheader fields.

Privilege

Security Administrator, Administrator

Syntax Description

key *encryption_key*

encryption_key

Specify the key to use for encryption of xheader fields.

Must be a string.

Usage Guidelines

Use this command to configure key to encrypt xheader fields.

active-charging service charging-action xheader-insert xheader-format encryption rc4md5 encrypted

Configures encryption of x-header fields.

Privilege

Security Administrator, Administrator

Syntax Description **`encrypted key`** *`encrypted_key`*

key

Specify the key to encrypt xheader fields.

encrypted_key

Specify the key that will be used for encryption of xheader fields.

Must be a string.

Usage Guidelines Use this command to configure use of aes-256-gcm-sha384 to encrypt the x-header fields with AES-256-GCM algorithm and SHA384 to hash key in 384 bits.

active-charging service charging-action xheader-insert xheader-format encryption rc4md5 key

Configures key to encrypt xheader fields.

Privilege Security Administrator, Administrator

Syntax Description **`key`** *`encryption_key`*

encryption_key

Specify the key to use for encryption of xheader fields.

Must be a string.

Usage Guidelines Use this command to configure key to encrypt xheader fields.

active-charging service content-filtering category policy-id

Configures Content filtering policy ID.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Content Filtering Category Policy ID Configuration

Syntax Description **`content-filtering category policy-id`** *`policy_id`*

policy_id

Specify the policy ID.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Use this command to configure the Content Filtering policy ID.

active-charging service content-filtering category policy-id analyze priority

Assigns priority to a Content Filtering Category in a Content Filtering Policy.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Content Filtering Category Policy ID Configuration

Syntax Description

`analyze priority` *`priority`*

priority

Specify the priority.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to assign priority to a Content Filtering Category in a Content Filtering Policy.

active-charging service content-filtering category policy-id analyze priority all

Configures all content to be rated.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Content Filtering Category Policy ID Configuration

Syntax Description

`all`

action

Specify the action.

allow

Specify the allow action.

content-insert

Specify the content insert action.

Must be a string.

Usage Guidelines

Use this command to configure the all content to be rated.

active-charging service content-filtering category policy-id analyze priority category

Configures category of the content to be rated.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Content Filtering Category Policy ID Configuration

Syntax Description

category *category_name*

category_name

Specify the category name.

Must be one of the following:

- ABOR
- ADULT
- ADVERT
- ANON
- ART
- AUTO
- BACKUP
- BLACK
- BLOG
- BUSI
- CAR
- CDN
- CHAT
- CMC
- CRIME
- CULT
- DRUG
- DYNAM
- EDU
- ENERGY

- ENT
- FIN
- FORUM
- GAMB
- GAME
- GLAM
- GOVERN
- HACK
- HATE
- HEALTH
- HOBBY
- HOSTS
- KIDS
- LEGAL
- LIFES
- MAIL
- MIL
- NEWS
- OCCULT
- PEER
- PERS
- PHOTO
- PLAG
- POLTIC
- PORN
- PORTAL
- PROXY
- REF
- REL
- SCI
- SEARCH
- SHOP

- SPORT
- STREAM
- SUIC
- SXED
- TECH
- TRAVE
- UNKNOW
- VIOL
- VOIP
- WEAP
- WHITE

action

Specify the action.

allow

Specify the allow action.

content-insert

Specify the content insert action.

Must be a string.

Usage Guidelines Use this command to configure the category of the content to be rated.

active-charging service content-filtering category policy-id analyze priority x-category

Unclassified category to be rated.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Content Filtering Category Policy ID Configuration

Syntax Description **`x-category`** *`xcategory_name`*

xcategory_name

Specify the x-category name.

Must be a string.

action

Specify the action.

allow

Specify the allow action.

content-insert

Specify the content insert action.

Must be a string.

Usage Guidelines Use this command to configures the unclassified category to be rated.

active-charging service credit-control group

Configures prepaid services for Diameter/RADIUS applications.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **`credit-control group`** *`cc_group_name`*

cc_group_name

Specify the credit control group name.

Must be a string.

Usage Guidelines Use this command to enable/disable Prepaid Credit Control Configuration for RADIUS/Diameter charging mode, and specify the credit control group.

active-charging service credit-control group associate

Associates failure handling template name.

Privilege Security Administrator, Administrator

Syntax Description **`associate failure-handling-template`** *`template_name`*

failure-handling-template *template_name*

Specify the failure-handling template name.

Must be a string.

Usage Guidelines Use this command to associate failure handling template name.

active-charging service credit-control group diameter

This command enables to accept/ignore service ID in the Service-Identifier AVP defined in the Diameter dictionaries.

Privilege

Security Administrator, Administrator

Syntax Description

`diameter ignore-service-id { false | true }`

ignore-service-id { false | true }

Disables usage of Service ID.

Must be either "false" or "true".

Default Value: false.

Usage Guidelines

Use this command to ignore/accept service ID value in the Service-Identifier AVP in the Diameter dictionaries.

Example

The following command specifies to ignore service ID in the Diameter dictionaries:

```
diameter ignore-service-id
```

active-charging service credit-control group diameter origin

Configures the Diameter Credit Control Origin endpoint name.

Privilege

Security Administrator, Administrator

Syntax Description

`origin` *`origin_endpoint_name`*

origin_endpoint_name

Specify the Diameter Credit Control Origin endpoint name.

Must be a string.

Usage Guidelines

Use this command to configure the Diameter Credit Control Origin endpoint name.

active-charging service credit-control group diameter service-context-id

Configures the value to be sent in the Service-Context-Id AVP, which defines the context in which DCCA is used.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`service-context-id`** *`service_context_id`*

service_context_id

Specify the value to be sent in the Service-Context-Id AVP.

Must be a string.

Usage Guidelines Use this command to specify the value to be sent in the Service-Context-Id AVP, which defines the context in which DCCA is used.

active-charging service credit-control group diameter session

Configures Diameter Credit Control Session Failover.

Privilege Security Administrator, Administrator

Syntax Description **`session failover`**

failover

Specify Diameter Credit Control Session Failover.

Usage Guidelines Use this command to configure Diameter Credit Control Session Failover.

active-charging service credit-control group failure-handling

Configures Diameter Credit Control Failure Handling action.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Credit Control Group Configuration

Syntax Description **`failure-handling`**

Usage Guidelines Use this command to configure Diameter Credit Control Failure Handling action.

active-charging service credit-control group failure-handling initial-request continue

Configures failure handling action to continue.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Credit Control Group Configuration

Syntax Description **continue** *continue_option*

continue_option

Specify the continue option.

Must be one of the following:

- go-offline-after-tx-expiry
- retry-after-tx-expiry

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to continue.

active-charging service credit-control group failure-handling initial-request retry-and-terminate

Configures Diameter Credit Control Failure Handling action to retry, and in case of failure, to terminate.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Credit Control Group Configuration

Syntax Description **retry-and-terminate** *retry_and_terminate_option*

retry_and_terminate_option

Specify the retry-and-terminate option.

Must be one of the following:

- retry-after-tx-expiry

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to retry, and in case of failure, to terminate.

active-charging service credit-control group failure-handling initial-request terminate

Configures Diameter Credit Control Failure Handling action as terminate.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Credit Control Group Configuration

Syntax Description **terminate**

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to terminate.

active-charging service credit-control group failure-handling terminate-request continue

Configures failure handling action to continue.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Credit Control Group Configuration

Syntax Description **continue** *continue_option*

continue_option

Specify the continue option.

Must be one of the following:

- go-offline-after-tx-expiry
- retry-after-tx-expiry

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to continue.

active-charging service credit-control group failure-handling terminate-request retry-and-terminate

Configures Diameter Credit Control Failure Handling action to retry, and in case of failure, to terminate.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Credit Control Group Configuration

Syntax Description **retry-and-terminate** *retry_and_terminate_option*

retry_and_terminate_option

Specify the retry-and-terminate option.

Must be one of the following:

- retry-after-tx-expiry

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to retry, and in case of failure, to terminate.

active-charging service credit-control group failure-handling terminate-request terminate

Configures Diameter Credit Control Failure Handling action as terminate.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Credit Control Group Configuration

Syntax Description **`terminate`**

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to terminate.

active-charging service credit-control group failure-handling update-request continue

Configures failure handling action to continue.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Credit Control Group Configuration

Syntax Description **`continue`** *`continue_option`*

continue_option

Specify the continue option.

Must be one of the following:

- go-offline-after-tx-expiry
- retry-after-tx-expiry

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to continue.

active-charging service credit-control group failure-handling update-request retry-and-terminate

Configures Diameter Credit Control Failure Handling action to retry, and in case of failure, to terminate.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Credit Control Group Configuration

Syntax Description **`retry-and-terminate`** *`retry_and_terminate_option`*

retry_and_terminate_option

Specify the retry-and-terminate option.

Must be one of the following:

- retry-after-tx-expiry

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to retry, and in case of failure, to terminate.

active-charging service credit-control group failure-handling update-request terminate

Configures Diameter Credit Control Failure Handling action as terminate.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Credit Control Group Configuration

Syntax Description **`terminate`**

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to terminate.

active-charging service credit-control group pending-traffic-treatment

Controls the pass/drop treatment of traffic while waiting for definitive credit information from the server.

Privilege Security Administrator, Administrator

Syntax Description **`pending-traffic-treatment { { { forced-reauth | trigger | validity-expired } drop | pass } | { noquota { buffer | drop | limited-pass`** *`volume`* **`| pass } } | { quota-exhausted { buffer | drop | pass } } }`**

Usage Guidelines Use this command to set the Diameter credit control pending traffic treatment while waiting for definitive credit information from the server.

Example

The following command sets the Diameter credit control pending traffic treatment to drop any traffic when there is no quota present:

```
pending-traffic-treatment noquota drop
```

active-charging service credit-control group pending-traffic-treatment forced-reauth

Configures the Diameter Credit Control pending traffic treatment to forced reauthorization.

Privilege

Security Administrator, Administrator

Syntax Description

`forced-reauth`

drop

Specify to drop.

pass

Specify to pass.

Usage Guidelines

Use this command to configure the Diameter Credit Control pending traffic treatment to forced reauthorization.

active-charging service credit-control group pending-traffic-treatment noquota

Configures the Diameter Credit Control pending traffic treatment.

Privilege

Security Administrator, Administrator

Syntax Description

`noquota`

buffer

Specify to tentatively count/time traffic, and then buffer traffic pending arrival of quota. Buffered traffic will be forwarded and fully charged against the quota when the quota is eventually obtained and the traffic is passed.

drop

Specify to drop any traffic when there is no quota present.

pass

Specify to pass all traffic more or less regardless of quota state.

Usage Guidelines Use this command to configure the Credit Control pending traffic treatment.

active-charging service credit-control group pending-traffic-treatment noquota limited-pass

Enables limited access for subscribers when the OCS is unreachable.

Privilege Security Administrator, Administrator

Syntax Description **`limited-pass`** *`volume`*

volume

Specify limited volume access to subscriber in case OCS is unreachable.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Use this command to enable limited access for subscribers when the OCS is unreachable.

active-charging service credit-control group pending-traffic-treatment quota-exhausted

Configures Diameter Credit Control pending traffic treatment to quota exhausted.

Privilege Security Administrator, Administrator

Syntax Description **`quota-exhausted`**

buffer

Specify to tentatively count/time traffic, and then buffer traffic pending arrival of quota. Buffered traffic will be forwarded and fully charged against the quota when the quota is eventually obtained and the traffic is passed.

drop

Drops any traffic when there is no quota present.

pass

Passes all traffic more or less regardless of quota state.

Usage Guidelines Use this command to configure the Diameter Credit Control pending traffic treatment to quota exhausted.

active-charging service credit-control group pending-traffic-treatment trigger

Configures the Diameter Credit Control pending traffic treatment to trigger.

Privilege

Security Administrator, Administrator

Syntax Description

`trigger`

drop

Specify to drop.

pass

Specify to pass.

Usage Guidelines

Use this command to configure the Diameter Credit Control pending traffic treatment to trigger.

active-charging service credit-control group pending-traffic-treatment validity-expired

Configures the Diameter Credit Control pending traffic treatment to trigger.

Privilege

Security Administrator, Administrator

Syntax Description

`validity-expired`

drop

Specify to drop.

pass

Specify to pass.

Usage Guidelines

Use this command to configure the Diameter Credit Control pending traffic treatment to trigger.

active-charging service credit-control group quota

This command sets various time-based quotas in the prepaid credit control service.

Privilege

Security Administrator, Administrator

Syntax Description

`quota holding-time` *`holding_time`*

Usage Guidelines Use this command to configure the prepaid credit control quotas.

Example

The following command sets the prepaid credit control request holding time to 30000 seconds:

```
quota holding-time 30000
```

active-charging service credit-control group quota holding-time

Specify the Credit Control Quota Holding Time (QHT).

Privilege Security Administrator, Administrator

Syntax Description **`holding-time`** *`holding_time`*

holding_time

Specify the holding time in seconds.

Must be an integer in the range of 1-4000000000.

Usage Guidelines Use this command to configure the Credit Control Quota Holding Time.

active-charging service credit-control group quota request-trigger

Configures Credit Control include/exclude packet causing threshold.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`request-trigger [ exclude-packet-causing-trigger | include-packet-causing-trigger ]`**

exclude-packet-causing-trigger

Specify to exclude packet causing trigger.

include-packet-causing-trigger

Specify to include packet causing trigger.

Usage Guidelines Use this command to configure the Credit Control include/exclude packet causing threshold.

active-charging service credit-control group timestamp-rounding

Configures the rounding mechanism for quota consumption.

Privilege

Security Administrator, Administrator

Syntax Description

`timestamp-rounding`

types *rounding_mechanism*

Specify the rounding mechanism for quota consumption.

Must be one of the following:

- ceiling
- floor
- roundoff

Usage Guidelines

Use this command to configure the rounding mechanism for quota consumption.

active-charging service credit-control group usage-reporting

Configures the ACS Credit Control usage reporting type.

Privilege

Security Administrator, Administrator

Syntax Description

`usage-reporting quotas-to-report based-on-grant { report-only-granted-volume }`

Usage Guidelines

Use this command to configure reporting usage only for granted quota. On issuing this command, the Used-Service-Unit AVP will report quotas based on grant i.e, only the quotas present in the Granted-Service-Unit AVP. With this command only the units for which the quota was granted by the DCCA server will be reported irrespective of the reporting reason.

Example

The following command configures to report usage based only on granted quota:

```
usage-reporting quotas-to-report based-on-grant
```

active-charging service credit-control group usage-reporting quotas-to-report

Configfures the quota types to be reported.

Privilege

Security Administrator, Administrator

Syntax Description

`quotas-to-report`

active-charging service credit-control group usage-reporting quotas-to-report based-on-grant

Configures to report usage only for granted quota.

Privilege

Security Administrator, Administrator

Syntax Description

`based-on-grant`

report-only-granted-volume

Suppresses the input and output octets. If the Granted-Service-Unit (GSU) AVP comes with CC-Total-Octets, then the device will send total, input and output octets in Used-Service-Unit (USU) AVP. If it comes with Total-Octets, the device will send only Total-Octets in USU.

active-charging service edr-format

Enables Event Data Record.

Privilege

Security Administrator, Administrator

Syntax Description

`edr-format`

edr_format_name

Specify the EDR format's name.

Must be a string.

Usage Guidelines

Use this command to enable Event Data Record.

active-charging service edr-format attribute bandwidth-policy

Configures the CSV position priority of the bandwidth-policy attribute in an EDR or UDR record. Contains the ACS Bandwidth Policy.

Privilege Security Administrator, Administrator

Syntax Description **attribute bandwidth-policy priority** *priority*

Usage Guidelines Active Charging Service bandwidth policy.

active-charging service edr-format attribute radius-called-station-id

Configures the CSV position priority of the radius-called-station-id attribute in an EDR or UDR record. Contains the Called Station ID of the flow.

Privilege Security Administrator, Administrator

Syntax Description **attribute radius-called-station-id priority** *priority*

Usage Guidelines Called station ID of the flow.

active-charging service edr-format attribute radius-calling-station-id

Configures the CSV position priority of the radius-calling-station-id attribute in an EDR or UDR record. Contains the Calling Station ID of the mobile handling the flow.

Privilege Security Administrator, Administrator

Syntax Description **attribute radius-calling-station-id priority** *priority*

Usage Guidelines Calling Station ID of the mobile handling the flow.

active-charging service edr-format attribute radius-fa-nas-identifier

Configures the CSV position priority of the radius-fa-nas-identifier attribute in an EDR or UDR record. Contains the RADIUS NAS ID of the FA.

Privilege Security Administrator, Administrator

Syntax Description **attribute radius-fa-nas-identifier priority** *priority*

Usage Guidelines RADIUS NAS ID of the FA.

active-charging service edr-format attribute radius-fa-nas-ip-address

Configures the CSV position priority of the radius-fa-nas-ip-address attribute in an EDR or UDR record. Contains the RADIUS IP address of the FA.

Privilege Security Administrator, Administrator

Syntax Description **attribute radius-fa-nas-ip-address priority** *priority*

Usage Guidelines RADIUS IP address of the FA.

active-charging service edr-format attribute radius-nas-identifier

Configures the CSV position priority of the radius-nas-identifier attribute in an EDR or UDR record. Contains the RADIUS NAS identifer.

Privilege Security Administrator, Administrator

Syntax Description **attribute radius-nas-identifier priority** *priority*

Usage Guidelines RADIUS NAS identifer.

active-charging service edr-format attribute radius-nas-ip-address

Configures the CSV position priority of the radius-nas-ip-address attribute in an EDR or UDR record. Contains the RADIUS IP address.

Privilege Security Administrator, Administrator

Syntax Description **attribute radius-nas-ip-address priority** *priority*

Usage Guidelines Configures RADIUS IP address.

active-charging service edr-format attribute radius-user-name

Configures the CSV position priority of the radius-user-name attribute in an EDR or UDR record. Contains the user name associated with this flow.

Privilege Security Administrator, Administrator

Syntax Description `attribute radius-user-name priority priority`

Usage Guidelines User name associated with this flow.

active-charging service edr-format attribute sn-acct-session-id

Configures the CSV position priority of the sn-acct-session-id attribute in an EDR or UDR record. Contains the Session ID.

Privilege Security Administrator, Administrator

Syntax Description `attribute sn-acct-session-id priority priority`

Usage Guidelines Configures session ID.

active-charging service edr-format attribute sn-app-protocol

Configures the CSV position priority of the sn-app-protocol attribute in an EDR or UDR record. Contains the Application protocol for the flow.

Privilege Security Administrator, Administrator

Syntax Description `attribute sn-app-protocol priority priority`

Usage Guidelines Application protocol for the flow.

active-charging service edr-format attribute sn-cf-category-classification-used

Configures the CSV position priority of the sn-cf-category-classification-used attribute in an EDR or UDR record. Contains the ACS Content Filtering category.

Privilege Security Administrator, Administrator

Syntax Description `attribute sn-cf-category-classification-used priority priority`

Usage Guidelines ACS content filtering category.

active-charging service edr-format attribute sn-cf-category-flow-action

Configures the CSV position priority of the sn-cf-category-flow-action attribute in an EDR or UDR record. Contains the ACS Content Filtering action taken.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-cf-category-flow-action priority** *priority*

Usage Guidelines The ACS Content Filtering action taken.

active-charging service edr-format attribute sn-cf-category-policy

Configures the CSV position priority of the sn-cf-category-policy attribute in an EDR or UDR record. Contains the ACS Content Filtering Policy ID.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-cf-category-policy priority** *priority*

Usage Guidelines The ACS Content Filtering Policy ID.

active-charging service edr-format attribute sn-cf-category-rating-type

Configures the CSV position priority of the sn-cf-category-rating-type attribute in an EDR or UDR record. Contains the ACS Content Filtering Rating Mode used.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-cf-category-rating-type priority** *priority*

Usage Guidelines The ACS Content Filtering Rating mode used.

active-charging service edr-format attribute sn-cf-category-unknown-url

Configures the CSV position priority of the sn-cf-category-unknown-url attribute in an EDR or UDR record. Contains the ACS Content Filtering Unknown URL indication.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-cf-category-unknown-url priority** *priority*

Usage Guidelines The ACS Content Filtering Unknown URL indication.

active-charging service edr-format attribute sn-charge-volume

Configures the CSV position priority of the sn-charge-volume attribute in an EDR or UDR record. Excludes the dropped/retransmitted packets/bytes from the total charge volume.

Privilege

Security Administrator, Administrator

Syntax Description

attribute sn-charge-volume

proto *protocol*

Specify the protocol.

Must be one of the following:

- ip

data_type

Specify the data type.

Must be one of the following:

- bytes
- pkts

direction_options

Specify the direction.

Must be one of the following:

- uplink
- downlink

Usage Guidelines

Excludes the dropped/retransmitted packets/bytes from the total charge volume.

active-chargingserviceedr-formatattributesn-charging-action

Configures the CSV position priority of the sn-charging-action attribute in an EDR or UDR record. Contains the name of the last charging action matched against flow.

Privilege

Security Administrator, Administrator

Syntax Description

attribute sn-charging-action priority *priority*

Usage Guidelines

Name of last charging action matched against flow.

active-charging service edr-format attribute sn-closure-reason

Configures the CSV position priority of the sn-closure-reason attribute in an EDR or UDR record. Contains the reason for the termination of the flow.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-closure-reason priority** *priority*

Usage Guidelines Reason for the termination of the flow.

active-charging service edr-format attribute sn-direction

Configures the CSV position priority of the sn-direction attribute in an EDR or UDR record. Contains the direction of the first packet for the flow.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-direction priority** *priority*

Usage Guidelines Direction of the first packet for the flow.

active-charging service edr-format attribute sn-duration

Configures the CSV position priority of the sn-duration attribute in an EDR or UDR record. Contains the duration between the last and first packet for the record.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-duration priority** *priority*

Usage Guidelines Duration between the last and first packet for the record.

active-charging service edr-format attribute sn-end-time

Configures the CSV position priority of the sn-end-time attribute in an EDR or UDR record. Contains the time of last packet of flow.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-end-time**

Usage Guidelines Time of last packet of flow - a string in MM/DD/YYYY HH:MM:SS format.

active-charging service edr-format attribute sn-end-time format

Timestamp format specified using seconds or combinations of "<YY/YYYY>: Year, <MM>: Month, <DD>: Day, <HH>: Hours, <MM>: Minutes, <SS>: seconds, <sss>: milliseconds".

Privilege

Security Administrator, Administrator

Syntax Description

`format`

format

Specify the format.

Must be one of the following:

- MM/DD/YY-HH:MM:SS
- MM/DD/YY-HH:MM:SS:sss
- MM/DD/YYYY-HH:MM:SS
- MM/DD/YYYY-HH:MM:SS:sss
- YYYY/MM/DD-HH:MM:SS
- YYYY/MM/DD-HH:MM:SS:sss
- YYYYMMDDHHMMSS
- YYYYMMDDHHMMSSsss
- seconds

Usage Guidelines

Timestamp format specified using seconds or combinations of "<YY/YYYY>: Year, <MM>: Month, <DD>: Day, <HH>: Hours, <MM>: Minutes, <SS>: seconds, <sss>: milliseconds".

active-charging service edr-format attribute sn-end-time localtime

Configures using local time as against GM time.

Privilege

Security Administrator, Administrator

Syntax Description

`localtime`

Usage Guidelines

Use this command to configure using local time as against GM time.

active-chargingserviceedr-formatattributesn-end-timepriority

Configures the CSV position priority of this field.

Privilege

Security Administrator, Administrator

Syntax Description

`priority`

Usage Guidelines

Use this command to configure the CSV position priority of this field.

active-charging service edr-format attribute sn-flow-end-time

Configures the CSV position priority of the sn-flow-end-time attribute in an EDR or UDR record. Contains the time of flow-end EDR generation.

Privilege

Security Administrator, Administrator

Syntax Description

`attribute sn-flow-end-time`

Usage Guidelines

Time of flow-end EDR generation.

active-charging service edr-format attribute sn-flow-end-time format

Configures the timestamp format.

Privilege

Security Administrator, Administrator

Syntax Description

`format`

timestamp *format*

Specify the timestamp format.

Must be one of the following:

- MM/DD/YY-HH:MM:SS
- MM/DD/YYYY-HH:MM:SS
- YYYY/MM/DD-HH:MM:SS
- YYYYMMDDHHMMSS
- seconds

Usage Guidelines

Use this command to configure the time of flow-end EDR generation timestamp format.

active-charging service edr-format attribute sn-flow-end-time localtime

Configures using local time as against GM time.

Privilege Security Administrator, Administrator

Syntax Description **`localtime`**

Usage Guidelines Use this command to configure using local time as against GM time.

active-charging service edr-format attribute sn-flow-end-time priority

Configures CSV position priority of this field.

Privilege Security Administrator, Administrator

Syntax Description **`priority`**

Usage Guidelines Use this command to configure CSV position priority of this field.

active-charging service edr-format attribute sn-flow-id

Configures the CSV position priority of the sn-flow-id attribute in an EDR or UDR record. Contains the Flow ID of the flow.

Privilege Security Administrator, Administrator

Syntax Description **`attribute sn-flow-id priority`** *`priority`*

Usage Guidelines Flow ID of the flow.

active-charging service edr-format attribute sn-flow-log

Configures the CSV position priority of the sn-flow-log attribute in an EDR or UDR record. Contains the flow log of the flow.

Privilege Security Administrator, Administrator

Syntax Description **`attribute sn-flow-log priority`** *`priority`*

Usage Guidelines Flow log of the flow.

active-charging service edr-format attribute sn-flow-start-time

Configures the CSV position priority of the sn-flow-start-time attribute in an EDR or UDR record. Contains the time of first packet of flow.

Privilege

Security Administrator, Administrator

Syntax Description

```
attribute sn-flow-start-time
```

Usage Guidelines

Time of first packet of flow.

active-charging service edr-format attribute sn-flow-start-time format

Configures the timestamp format specified using seconds or combinations of "<YY/YYYY>: Year, <MM>: Month, <DD>: Day, <HH>: Hours, <MM>: Minutes, <SS>: seconds, <sss>: milliseconds".

Privilege

Security Administrator, Administrator

Syntax Description

```
format
```

timestamp *format*

Specify the timestamp format.

Must be one of the following:

- MM/DD/YY-HH:MM:SS
- MM/DD/YYYY-HH:MM:SS
- YYYY/MM/DD-HH:MM:SS
- YYYYMMDDHHMMSS
- seconds

Usage Guidelines

Timestamp format specified using seconds or combinations of "<YY/YYYY>: Year, <MM>: Month, <DD>: Day, <HH>: Hours, <MM>: Minutes, <SS>: seconds, <sss>: milliseconds".

active-charging service edr-format attribute sn-flow-start-time localtime

Use local time as against GM time.

Privilege

Security Administrator, Administrator

Syntax Description `localtime`

Usage Guidelines Use this command to configure using local time as against GM time.

active-charging service edr-format attribute sn-flow-start-time priority

CSV position priority of this field.

Privilege Security Administrator, Administrator

Syntax Description `priority`

Usage Guidelines Use this command to configure the CSV position priority of this field.

active-charging service edr-format attribute sn-rulebase

Configures the CSV position priority of the sn-rulebase attribute in an EDR or UDR record. Contains the name of the ACS rulebase.

Privilege Security Administrator, Administrator

Syntax Description **`attribute sn-rulebase priority`** *`priority`*

Usage Guidelines Name of the ACS rulebase.

active-charging service edr-format attribute sn-ruledef-name

Configures the CSV position priority of the sn-ruledef-name attribute in an EDR or UDR record. Contains the ruledef name corresponding to last charging action matched.

Privilege Security Administrator, Administrator

Syntax Description **`attribute sn-ruledef-name priority`** *`priority`*

Usage Guidelines Ruledef name corresponding to last charging action matched.

active-charging service edr-format attribute sn-server-port

Configures the CSV position priority of the sn-server-port attribute in an EDR or UDR record. Contains the server port number.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-server-port priority** *priority*

Usage Guidelines Server port number.

active-charging service edr-format attribute sn-service-id

Configures the CSV position priority of the sn-service-id attribute in an EDR or UDR record. Contains the service ID corresponding to last charging action matched.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-service-id priority** *priority*

Usage Guidelines Service ID corresponding to last charging action matched.

active-charging service edr-format attribute sn-start-time

Configures the CSV position priority of the sn-start-time attribute in an EDR or UDR record. Contains the time of first packet of flow.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-start-time**

Usage Guidelines Time of first packet of flow.

active-chargingserviceedr-formatattributesn-start-timeformat

Configures the timestamp format.

Privilege Security Administrator, Administrator

Syntax Description **format**

format

Specify the format.

Must be one of the following:

- MM/DD/YY-HH:MM:SS
- MM/DD/YY-HH:MM:SS:sss
- MM/DD/YYYY-HH:MM:SS
- MM/DD/YYYY-HH:MM:SS:sss
- YYYY/MM/DD-HH:MM:SS

- YYYY/MM/DD-HH:MM:SS:sss
- YYYYMMDDHHMMSS
- YYYYMMDDHHMMSSsss
- seconds

Usage Guidelines Use this command to configure the timestamp format.";

active-charging service edr-format attribute sn-start-time localtime

Configures using local time as against GM time.

Privilege Security Administrator, Administrator

Syntax Description **`localtime`**

Usage Guidelines Use this comamnd to configure using local time as against GM time.

active-charging service edr-format attribute sn-start-time priority

Configures the CSV position priority of the field.

Privilege Security Administrator, Administrator

Syntax Description **`priority`**

Usage Guidelines Use this command to configure CSV position priority of the field.

active-charging service edr-format attribute sn-subscriber-imsi

Configures the CSV position priority of the sn-subscriber-imsi attribute in an EDR or UDR record. Contains the Subscriber IMSI.

Privilege Security Administrator, Administrator

Syntax Description **`attribute sn-subscriber-imsi priority`** *`priority`*

Usage Guidelines Subscriber IMSI.

active-charging service edr-format attribute sn-subscriber-nat-flow-ip

Configures the CSV position priority of the sn-subscriber-nat-flow-ip attribute in an EDR or UDR record. Contains the NAT IP address of the subscriber.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-subscriber-nat-flow-ip priority** *priority*

Usage Guidelines NAT IP address of the subscriber.

active-charging service edr-format attribute sn-subscriber-nat-flow-port

Configures the CSV position priority of the sn-subscriber-nat-flow-port attribute in an EDR or UDR record. Contains the NAT port of the subscriber.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-subscriber-nat-flow-port priority** *priority*

Usage Guidelines NAT port of the subscriber.

active-charging service edr-format attribute sn-subscriber-port

Configures the CSV position priority of the sn-subscriber-port attribute in an EDR or UDR record. Contains the port number of the mobile handling this flow.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-subscriber-port priority** *priority*

Usage Guidelines Port number of the mobile handling this flow.

active-charging service edr-format attribute sn-volume-amt

Configures the CSV position priority of the sn-volume-amt attribute in an EDR or UDR record. Contains the EDR protocol specific uplink/downlink volume amount.

Privilege Security Administrator, Administrator

Syntax Description **attribute sn-volume-amt**

proto *protocol*

Specify the protocol.

Must be one of the following:

- ip
- tcp

data_type

Specify the data type.

Must be one of the following:

- bytes
- pkts

direction

Specify the direction.

Must be one of the following:

- uplink
- downlink

Usage Guidelines EDR protocol specific uplink/downlink volume amount.

active-charging service edr-format attribute transaction-charge-downlink-bytes

Configures the CSV position priority of the transaction-charge-downlink-bytes attribute in an EDR or UDR record. Excludes the dropped/retransmitted bytes from the total transaction downlink bytes.

Privilege Security Administrator, Administrator

Syntax Description **`attribute transaction-charge-downlink-bytes priority`** *`priority`*

Usage Guidelines Excludes the dropped/retransmitted bytes from the total transaction downlink bytes.

active-charging service edr-format attribute transaction-charge-downlink-packets

Configures the CSV position priority of the transaction-charge-downlink-packets attribute in an EDR or UDR record. Excludes the dropped/retransmitted packets from the total transaction downlink packets.

Privilege Security Administrator, Administrator

Syntax Description **attribute transaction-charge-downlink-packets priority** *priority*

Usage Guidelines Excludes the dropped/retransmitted packets from the total transaction downlink packets.

active-charging service edr-format attribute transaction-charge-uplink-bytes

Configures the CSV position priority of the transaction-charge-uplink-bytes attribute in an EDR or UDR record. Excludes the dropped/retransmitted bytes from the total transaction uplink bytes.

Privilege Security Administrator, Administrator

Syntax Description **attribute transaction-charge-uplink-bytes priority** *priority*

Usage Guidelines Excludes the dropped/retransmitted bytes from the total transaction uplink bytes.

active-charging service edr-format attribute transaction-charge-uplink-packets

Configures the CSV position priority of the transaction-charge-uplink-packets attribute in an EDR or UDR record. Excludes the dropped/retransmitted packets from the total transaction uplink packets.

Privilege Security Administrator, Administrator

Syntax Description **attribute transaction-charge-uplink-packets priority** *priority*

Usage Guidelines Excludes the dropped/retransmitted packets from the total transaction uplink packets.

active-charging service edr-format attribute transaction-downlink-bytes

Configures the CSV position priority of the transaction-downlink-bytes attribute in an EDR or UDR record. Contains the total downlink bytes for the transaction.

Privilege Security Administrator, Administrator

Syntax Description **attribute transaction-downlink-bytes priority** *priority*

Usage Guidelines Total downlink bytes for the transaction.

active-charging service edr-format attribute transaction-downlink-packets

Configures the CSV position priority of the transaction-downlink-packets attribute in an EDR or UDR record. Contains the total downlink packets for the transaction.

Privilege Security Administrator, Administrator

Syntax Description **attribute transaction-downlink-packets priority** *priority*

Usage Guidelines Total downlink packets for the transaction.

active-charging service edr-format attribute transaction-uplink-bytes

Configures the CSV position priority of the transaction-uplink-bytes attribute in an EDR or UDR record. Contains the total uplink bytes for the transaction.

Privilege Security Administrator, Administrator

Syntax Description **attribute transaction-uplink-bytes priority** *priority*

Usage Guidelines Total uplink bytes for the transaction.

active-charging service edr-format attribute transaction-uplink-packets

Configures the CSV position priority of the transaction-uplink-packets attribute in an EDR or UDR record. Contains the total uplink packets for the transaction.

Privilege Security Administrator, Administrator

Syntax Description **attribute transaction-uplink-packets priority** *priority*

Usage Guidelines Total uplink packets for the transaction.

active-charging service edr-format event-label

Configures event labels to use as attributes in EDR or UDR.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > EDR Format Configuration

Syntax Description **event-label** *label_name*

label_name

Specify the sequence of characters to be used at EDR attribute.

Must be a string.

Usage Guidelines Use this command to configure event labels to be used as attributes in EDR or UDR.

active-charging service edr-format event-label priority

Configures the CSV position priority of this field in an EDR or UDR record.

Privilege Security Administrator, Administrator

Syntax Description **priority** *priority*

priority

Specify the field's CSV position priority in an EDR or UDR record.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure the CSV position priority of this field in an EDR or UDR record.

active-charging service edr-format rule-variable

Configures the rule variable attribute for EDR or UDR.

Privilege Security Administrator, Administrator

Syntax Description **rule-variable**

Usage Guidelines Use this command to configure the rule variable attribute for EDR or UDR.

active-charging service edr-format rule-variable bearer bearer

Configures bearer-related parameters.

Privilege Security Administrator, Administrator

Syntax Description **bearer**

service *service*

Specify the service.

Must be one of the following:

- 3gpp

Usage Guidelines Use this command to configure bearer-related parameters.

active-charging service edr-format rule-variable bearer bearer imei

Configures IMEI or IMEISV (depending on the case) associated with the bearer flow.

Privilege Security Administrator, Administrator

Syntax Description `imei`

Usage Guidelines Use this command to configure IMEI or IMEISV (depending on the case) associated with the bearer flow.

active-charging service edr-format rule-variable bearer bearer imsi

Configures specific Mobile Station Identification number.

Privilege Security Administrator, Administrator

Syntax Description `imsi`

Usage Guidelines Use this command to configure specific IMSI number.

active-charging service edr-format rule-variable bearer bearer rat-type

Configures RAT Type associated with the bearer flow.

Privilege Security Administrator, Administrator

Syntax Description `rat-type`

Usage Guidelines Use this command to configure the RAT Type associated with the bearer flow.

active-charging service edr-format rule-variable bearer bearer sgsn-address

Configures SGSN associated with the bearer flow.

Privilege Security Administrator, Administrator

Syntax Description `sgsn-address`

Usage Guidelines Use this command to configure the SGSN associated with the bearer flow.

active-charging service edr-format rule-variable bearer bearer user-location-information

Configures the user location information associated with the bearer flow.

Privilege Security Administrator, Administrator

Syntax Description `user-location-information`

Usage Guidelines Use this command to configure the user location information associated with the bearer flow.

active-charging service edr-format rule-variable bearer qci

Configures QCI of bearer data flow is associated with.

Privilege Security Administrator, Administrator

Syntax Description `qci`

Usage Guidelines Use this command to configure QCI of bearer data flow is associated with.

active-charging service edr-format rule-variable flow

Configures flow-related parameters.

Privilege Security Administrator, Administrator

Syntax Description `flow`

Usage Guidelines Use this command to configure flow-related parameters.

active-charging service edr-format rule-variable flow ip-control-param

First eight bytes of IPv6 header.

Privilege Security Administrator, Administrator

Syntax Description `ip-control-param`

Usage Guidelines First eight bytes of IPv6 header.

active-charging service edr-format rule-variable flow tethered

Tethering detected on flow.

Privilege Security Administrator, Administrator

Syntax Description `tethered`

Usage Guidelines Tethering detected on flow.

active-charging service edr-format rule-variable flow tethered-application

Application-based tethering detected on flow.

Privilege Security Administrator, Administrator

Syntax Description `tethered-application`

Usage Guidelines Application-based tethering detected on flow.

active-charging service edr-format rule-variable flow tethered-dns

DNS-based tethering detected on flow. Either 0 or 1.

Privilege Security Administrator, Administrator

Syntax Description `tethered-dns`

Usage Guidelines DNS-based tethering detected on flow. Either 0 or 1.

active-charging service edr-format rule-variable flow tethered-ip-ttl

IP-TTL based tethering detected on flow.

Privilege Security Administrator, Administrator

Syntax Description `tethered-ip-ttl`

Usage Guidelines IP-TTL based tethering detected on flow.

active-charging service edr-format rule-variable flow ttl

Time To Live/Max hops.

Privilege Security Administrator, Administrator

Syntax Description `ttl`

Usage Guidelines Time To Live/Max hops.

active-charging service edr-format rule-variable http content

Content-related configurations.

Privilege Security Administrator, Administrator

Syntax Description `content`

Usage Guidelines Content-related configurations.

active-charging service edr-format rule-variable http content disposition

Content disposition.

Privilege Security Administrator, Administrator

Syntax Description `disposition`

Usage Guidelines Content disposition.

active-charging service edr-format rule-variable http content length

Content length.

Privilege Security Administrator, Administrator

Syntax Description `length`

Usage Guidelines Content length.

active-charging service edr-format rule-variable http content type

Content type.

Privilege Security Administrator, Administrator

Syntax Description `type`

Usage Guidelines Content type.

active-charging service edr-format rule-variable http cookie

Cookie.

Privilege Security Administrator, Administrator

Syntax Description `cookie`

Usage Guidelines Cookie.

active-charging service edr-format rule-variable http header-length

HTTP header length.

Privilege Security Administrator, Administrator

Syntax Description `header-length`

Usage Guidelines HTTP header length.

active-charging service edr-format rule-variable http host

Host.

Privilege Security Administrator, Administrator

Syntax Description `host`

Usage Guidelines Host.

active-charging service edr-format rule-variable http referer

Referer.

Privilege Security Administrator, Administrator

Syntax Description `referer`

Usage Guidelines Referer.

active-charging service edr-format rule-variable http reply code

Response code.

Privilege Security Administrator, Administrator

Syntax Description `code`

Usage Guidelines Response code.

active-charging service edr-format rule-variable http request method

HTTP Request method.

Privilege Security Administrator, Administrator

Syntax Description `method`

Usage Guidelines HTTP Request method.

active-charging service edr-format rule-variable http url

URL.

Privilege Security Administrator, Administrator

Syntax Description **`url`**

Usage Guidelines URL.

active-charging service edr-format rule-variable http url length

Configures the field size as against using the default size of 127.

Privilege Security Administrator, Administrator

Syntax Description **`length`** *`length`*

length

Specify the field size.

Must be an integer in the range of 1-4095.

Usage Guidelines Specify the field size as against using the default size of 127.

active-charging service edr-format rule-variable http url priority

Priority.

Privilege Security Administrator, Administrator

Syntax Description **`priority`**

Usage Guidelines Priority.

active-charging service edr-format rule-variable http user-agent

User agent.

Privilege Security Administrator, Administrator

Syntax Description **`user-agent`**

Usage Guidelines User agent.

active-chargingserviceedr-formatrule-variablehttpuser-agent length

Configures the field size as against using the default size of 127.

Privilege

Security Administrator, Administrator

Syntax Description

length *length*

length

Specify the field size.

Must be an integer in the range of 1-255.

Usage Guidelines

Specify the field size as against using the default size of 127.

active-chargingserviceedr-formatrule-variablehttpuser-agent priority

Priority.

Privilege

Security Administrator, Administrator

Syntax Description

priority

Usage Guidelines

Priority.

active-charging service edr-format rule-variable ip

Configures IP-related parameters.

Privilege

Security Administrator, Administrator

Syntax Description

ip

Usage Guidelines

Use this command to configure IP-related parameters.

active-charging service edr-format rule-variable ip dst-address

Configures IP destination address.

Privilege

Security Administrator, Administrator

Syntax Description `dst-address`

Usage Guidelines Use this command to configure IP destination address.

active-charging service edr-format rule-variable ip protocol

Configures protocol being transported by IP packet.

Privilege Security Administrator, Administrator

Syntax Description `protocol`

Usage Guidelines Use this command to configure protocol being transported by IP packet.

active-charging service edr-format rule-variable ip src-address

Configures IP source address.

Privilege Security Administrator, Administrator

Syntax Description `src-address`

Usage Guidelines Use this command to configure IP source address.

active-charging service edr-format rule-variable ip subscriber-ip-address

Configures subscriber IP address.

Privilege Security Administrator, Administrator

Syntax Description `subscriber-ip-address`

Usage Guidelines Use this command to configure subscriber IP address.

active-charging service edr-format rule-variable ip total-length

Total length of packet, including payload.

Privilege Security Administrator, Administrator

Syntax Description `total-length`

Usage Guidelines Use this command to configure total length of packet, including payload.

active-charging service edr-format rule-variable ip version

IP version

Privilege Security Administrator, Administrator

Syntax Description **`version`**

Usage Guidelines Use this command to configure IP version.

active-charging service edr-format rule-variable p2p app-identifier

Configures TLS-SNI, QUIC-SNI, or any other identifier.

Privilege Security Administrator, Administrator

Syntax Description **`app-identifier`** *`app_id`*

app_id

Specify the P2P app identifier.

Must be a string.

Usage Guidelines Use this command to configure TLS-SNI, QUIC-SNI, or any other identifier.

active-charging service edr-format rule-variable p2p duration

P2P protocol.

Privilege Security Administrator, Administrator

Syntax Description **`duration`**

Usage Guidelines P2P protocol.

active-charging service edr-format rule-variable p2p protocol

P2P protocol.

Privilege Security Administrator, Administrator

Syntax Description **`protocol`**

Usage Guidelines P2P protocol.

active-charging service edr-format rule-variable p2p protocol-group

P2P protocol group.

Privilege Security Administrator, Administrator

Syntax Description `protocol-group`

Usage Guidelines P2P protocol group.

active-charging service edr-format rule-variable p2p protocol-sub-group

P2P protocol sub group.

Privilege Security Administrator, Administrator

Syntax Description `protocol-sub-group`

Usage Guidelines P2P protocol sub group.

active-charging service edr-format rule-variable tcp dst-port

Configures TCP destination port.

Privilege Security Administrator, Administrator

Syntax Description `dst-port`

Usage Guidelines Use this command to configure the TCP destination port.

active-charging service edr-format rule-variable tcp duplicate

Configures TCP retransmitted/duplicate packet.

Privilege Security Administrator, Administrator

Syntax Description `duplicate`

Usage Guidelines Use this command to configure TCP retransmitted/duplicate packet.

active-charging service edr-format rule-variable tcp flag

Configures current packet TCP flag.

Privilege Security Administrator, Administrator

Syntax Description `flag`

Usage Guidelines Use this command to configure current packet TCP flag.

active-charging service edr-format rule-variable tcp os-signature

Configures OS signature string for TCP flow.

Privilege Security Administrator, Administrator

Syntax Description `os-signature`

Usage Guidelines Use this command to configure OS signature string for TCP flow.

active-charging service edr-format rule-variable tcp out-of-order

Configures TCP out-of-order packet analyzed.

Privilege Security Administrator, Administrator

Syntax Description `out-of-order`

Usage Guidelines Use this command to configure TCP out-of-order packet analyzed.

active-charging service edr-format rule-variable tcp payload-length

Configures TCP payload length.

Privilege Security Administrator, Administrator

Syntax Description `payload-length`

Usage Guidelines Use this command to configure TCP payload length.

active-charging service edr-format rule-variable tcp previous-state

Configures previous state of MS.

Privilege Security Administrator, Administrator

Syntax Description `previous-state`

Usage Guidelines Use this command to configure previous state of MS.

active-chargingserviceedr-formatrule-variabletcpsn-tcp-accl

Confgiures TCP acceleration status for the TCP flow.

Privilege Security Administrator, Administrator

Syntax Description `sn-tcp-accl`

Usage Guidelines Use this command to configure TCP acceleration status for the TCP flow.

active-charging service edr-format rule-variable tcp sn-tcp-accl-reject-reason

Configures reason for not accelerating the TCP flow.

Privilege Security Administrator, Administrator

Syntax Description `sn-tcp-accl-reject-reason`

Usage Guidelines Use this command to configure the reason for not accelerating the TCP flow.

active-charging service edr-format rule-variable tcp sn-tcp-min-rtt

Configures minimum RTT observed for accelerated TCP flow.

Privilege Security Administrator, Administrator

Syntax Description `sn-tcp-min-rtt`

Usage Guidelines Use this command to configure the minimum RTT observed for accelerated TCP flow.

active-charging service edr-format rule-variable tcp sn-tcp-rtt

Configures smoothed RTT for accelerated TCP flow.

Privilege Security Administrator, Administrator

Syntax Description `sn-tcp-rtt`

Usage Guidelines Use this command to configure the smoothed RTT for accelerated TCP flow.

active-charging service edr-format rule-variable tcp src-port

Configures TCP source port.

Privilege Security Administrator, Administrator

Syntax Description `src-port`

Usage Guidelines Use this command to configure TCP source port.

active-charging service edr-format rule-variable tcp state

Configures current state of MS.

Privilege Security Administrator, Administrator

Syntax Description `state`

Usage Guidelines Use this command to configure the current state of MS.

active-charging service edr-format rule-variable tcp syn-control-params

Configures eight-bytes following the TCP Acknowledgement in TCP SYN packet displayed as hex string of characters.

Privilege Security Administrator, Administrator

Syntax Description `syn-control-params`

Usage Guidelines Use this command to configure eight-bytes following the TCP Acknowledgement in TCP SYN packet displayed as hex string of characters.

active-chargingserviceedr-formatrule-variabletcpsyn-options

Configure TCP options received in TCP SYN packet displayed as hex string of characters.

Privilege Security Administrator, Administrator

Syntax Description `syn-options`

Usage Guidelines Use this command to configure TCP options received in TCP SYN packet displayed as hex string of characters.

active-charging service edr-format rule-variable tcp syn-seq

Configures sequence number in TCP SYN packet displayed as decimal value.

Privilege Security Administrator, Administrator

Syntax Description `syn-seq`

Usage Guidelines Use this command to configure the sequence number in TCP SYN packet displayed as decimal value.

active-charging service edr-format rule-variable tcp v6-os-signature

Configures OS signature string for IPv6 TCP flow.

Privilege Security Administrator, Administrator

Syntax Description `v6-os-signature`

Usage Guidelines Use this command to configure OS signature string for IPv6 TCP flow.

active-charging service edr-format rule-variable traffic-type

Configures traffic type of flow.

Privilege Security Administrator, Administrator

Syntax Description `traffic-type`

Usage Guidelines Use this command to configure the flow traffic type.

active-charging service group-of-ruledefs

Configures ACS group-of-ruledefs parameters.

Privilege

Security Administrator, Administrator

Syntax Description

group-of-ruledefs *ruledefs_group_name*

ruledefs_group_name

Specify the group-of-ruledefs name.

Must be a string.

Usage Guidelines

Use this command to create/configure/delete a group-of-ruledefs. A group-of-ruledefs is a collection of ruledefs to use in access policy creation. Maximum of 384 group-of-ruledefs can be created.

You can configure a maximum of 384 elements with this command.

Example

The following command creates a group-of-ruledefs named group1, and enters the ACS Group-of-Ruledefs Configuration Mode:

```
group-of-ruledefs group1
```

active-charging service group-of-ruledefs add-ruledef

Adds ruledefs from a group-of-ruledefs.

Privilege

Security Administrator, Administrator

Syntax Description

add-ruledef priority *ruledef_priority* **ruledef** *ruledef_name*

Usage Guidelines

Use this command to add ruledefs to a group-of-ruledefs. A maximum of 512 ruledefs can be added to a group of ruledefs.

active-charging service group-of-ruledefs add-ruledef priority

Configures the priority of the ruledef in the current group-of-ruledefs.

Privilege

Security Administrator, Administrator

Syntax Description

priority *ruledef_priority*

ruledef_priority

Specify the ruledef priority. Priority must be unique within the group-of-ruledefs.

Must be an integer in the range of 1-10000.

ruledef *ruledef_name*

Specify name of the ruledef to add to the current group-of-ruledefs.

Must be a string.

Usage Guidelines Use this command to configure the priority of the ruledef in the current group-of-ruledefs.

You can configure a maximum of 512 elements with this command.

active-charging service host-pool

Configures host pool parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **host-pool** *host_pool_name*

host_pool_name

Specify the host pool name.

Must be a string.

Usage Guidelines Use this command to configure host pool parameters.

active-charging service host-pool ip ipv4-address

Configures IPv4-related configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Host Pool Configuration

Syntax Description **ip** *ipv4_address*

ipv4_address

Specify the IPv4 address.

Must be IPv4 CIDR notation ##.##.##.##/x.

Usage Guidelines Use this command to configure IPv4-related parameters.

active-charging service host-pool ip ipv6-address

Configures IPv6-related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Host Pool Configuration

Syntax Description **ip** *ipv6_address*

ipv6_address

Specify the IPv6 address.

Must be IPv6 CIDR notation ####:####:####:####:####:####:####:####/###.

Usage Guidelines Use this command to configure IPv6-related parameters.

active-charging service host-pool ip range

Configures IP address range.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Host Pool Configuration

Syntax Description **range start** *start_ip_address* **to** *end_ip_address*

start *start_ip_address*

Specify the first IP address of the range.

Must be an IP address.

to *end_ip_address*

Specify the last IP address of the range.

Must be an IP address.

Usage Guidelines Use this command to configure an IP address range.

active-charging service p2p-detection attribute

Configures the detection of SSL renegotiation flows.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **p2p-detection attribute ssl-renegotiation [max-entry-per-sessmgr** *max_entry_per_sessmgr* **| id-reduce-factor** *id_reduce_factor* **]**

Usage Guidelines Use this command to enable or disable the detection of SSL renegotiation flows.

Example

The following command enables SSL renegotiation with SSL session IDs as 40000 and factor as 4:

```
p2p-detection attribute ssl-renegotiation max-entry-per-sessmgr 40000 id-reduce-factor 4
```

active-charging service p2p-detection attribute ssl-renegotiation

Specify the supported attribute of configurable P2P detection attributes populated from the currently loaded P2P plugin.

Privilege Security Administrator, Administrator

Syntax Description **ssl-renegotiation**

max-entry-per-sessmgr ***max_entry_per_sessmgr***

Specify maximum SSL Session IDs tracked per session manager.

Must be an integer in the range of 0-65535.

id-reduce-factor ***id_reduce_factor***

Specify by how much factor the SSL ID is stored in the SSL Session ID tracker table.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to specify the supported attribute of configurable P2P detection attributes populated from the currently loaded P2P plugin.

active-charging service p2p-detection ecs-analysis

Enables or disables ECS analysis for analyzers FTP, HTPP, HTTPS, RTSP and SIP.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **p2p-detection ecs-analysis** *analyzer*

analyzer

Specify the analyzers.

Must be one of the following:

- all: ECS analysis for all analyzers.
- http: ECS analysis for HTTP analyzer.
- sip: ECS analysis for SIP analyzer.
- ftp: ECS analysis for FTP analyzer.
- rtsp: ECS analysis for RTSP analyzer.
- https: ECS analysis for HTTPS analyzer.

Usage Guidelines Use this command to enable or disable ECS analysis for analyzers. This feature is enabled by default if P2P protocols are enabled.

Example

The following command enables ECS analysis for the ftp analyzer:

```
p2p-detection ecs-analysis ftp
```

active-charging service p2p-detection protocol

enables/disables the detection of all or specified peer-to-peer (P2P) protocols.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **`protocol`** *`protocol`*

protocol

Specify the P2P protocol.

Must be one of the following:

- cisco-jabber
- uber
- ufc
- eros
- googlemaps
- yahoo
- skype
- fasttrack
- teamspeak

- all

Usage Guidelines Use this command to specify P2P protocol.

Example

The following command enables detection of all P2P protocols:

```
p2p-detection protocol all
```

active-charging service packet-filter

Configures Active Charging Service Packet Filter parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **packet-filter** *packet_filter_name*

packet_filter_name

Specify the packet filter name.

Must be a string.

direction ***direction***

Specify the direction in which the current packet filter will be applied.

Must be one of the following:

- bi-directional: The filter needs to be applied in uplink as well as downlink direction. This is the default value.
- downlink: The filter needs to be applied in only downlink direction.
- uplink: The filter needs to be applied in only uplink direction.

Default Value: "bi-directional".

priority ***priority***

Specify the current packet filter's priority.

Must be an integer in the range of 0-255.

Usage Guidelines Use this command to configure Active Charging Service Packet Filter parameters.

active-charging service packet-filter ip local-port

Configures port number of the local transport protocol.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Packet Filter Configuration

Syntax Description

`ip local-port`

Usage Guidelines

Configures the IP 5-tuple local port(s) for the current packet filter. Use this command to configure the port number of the local transport protocol.

Example

The following command configures the IP local port as 456:

```
ip local-port 456
```

active-charging service packet-filter ip local-port operator

Configures the operator.

Privilege

Security Administrator, Administrator

Syntax Description

`operator`

operator

Specify how to match.

Must be one of the following:

- =: Equals.

port_number

Specify a TCP or UDP port number to add to the current port map.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this command to specifiy the operator.

active-charging service packet-filter ip local-port range

Configures a port number range.

Privilege

Security Administrator, Administrator

Syntax Description **range start** *start_port_number* **to** *end_port_number*

start *start_port_number*

Specify the first port number for the port number range.

Must be an integer in the range of 0-65535.

to *end_port_number*

Specify the last port number for the port number range.

Must be an integer in the range of 0-65535.

Usage Guidelines Specify a port number range.

active-charging service packet-filter ip protocol

Configures the IP protocol(s) for the current packet filter.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Packet Filter Configuration

Syntax Description **ip protocol** *operator protocol_number*

operator

Specify how to match.

Must be one of the following:

- =: Equals.

protocol_number

Specify the protocol number.

Must be an integer in the range of 0-255.

Usage Guidelines Configures the IP 5-tuple local port(s) for the current packet filter. Use this command to configure the protocol(s) for a packet filter.

Example

The following command configures the protocol assignment number 300:

```
ip protocol = 300
```

active-charging service packet-filter ip remote-address

Configures the IP remote address(es) for the current packet filter.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Packet Filter Configuration

Syntax Description

ip remote-address *operator* **{ {** *ipv4_address* **|** *ipv6_address* **} | {** *ipv4_address/mask* **|** *ipv6_address/mask* **} }**

operator

Specify how to match.

Must be one of the following:

- =: Equals.

Must be IPv4 CIDR notation ##.##.##.##/x or in IPv6 CIDR notation ####:####:####:####:####:####:####:####/###.

Usage Guidelines

Configures the IP 5-tuple local port(s) for the current packet filter. Use this command to configure the remote address(es) for a packet filter.

Example

The following command configures the IP remote address as 10.2.3.4/24:

```
ip remote-address = 10.2.3.4/24
```

active-charging service packet-filter ip remote-port

Configures the IP remote port for the current packet filter.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Packet Filter Configuration

Syntax Description

ip remote-port

Usage Guidelines

Configures the IP 5-tuple local port(s) for the current packet filter. Use this command to configure the remote port for a packet filter.

active-charging service packet-filter ip remote-port operator

Configures the operator.

Privilege Security Administrator, Administrator

Syntax Description **operator**

operator

Specify how to match.

Must be one of the following:

- =: Equals.

port_number

Specify a TCP or UDP port number to add to the current port map.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to specifiy the operator.

active-charging service packet-filter ip remote-port range

Configures a port number range.

Privilege Security Administrator, Administrator

Syntax Description **range start** *start_port_number* **to** *end_port_number*

start *start_port_number*

Specify the first port number for the port number range.

Must be an integer in the range of 0-65535.

to *end_port_number*

Specify the last port number for the port number range.

Must be an integer in the range of 0-65535.

Usage Guidelines Specify a port number range.

active-charging service packet-filter ip tos-traffic-class

Configures the type of service/traffic class under charging action in the Packet filter mode.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Packet Filter Configuration

Syntax Description **tos-traffic-class** *operator traffic_class*

operator

Specify how to match.

Must be one of the following:

- =: Equals.

traffic_class

Specify the traffic class value to filter the traffic.

Must be an integer in the range of 0-255.

mask *operator*

Specify how to match.

Must be one of the following:

- =: Equals.

mask_field

Specify the type-of-service or traffic-class mask field.

Must be an integer in the range of 0-255.

Usage Guidelines Use this command to configure the type of service/traffic class under charging action in the Packet filter mode.

active-charging service policy-control burst-size auto-readjust

Configures policy control burst size parameter.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`auto-readjust duration`** *`duration`*

duration *duration*

Specify the seconds of traffic configured for burst size.

Must be an integer.

Usage Guidelines Use this command to configure the burst size parameter.

active-charging service port-map

Configures port map related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **port-map** *port_map_name*

port_map_name

Specify the name of the port map.

Must be a string.

Usage Guidelines Use this command to configure the port map related parameters.

active-charging service port-map port

Configures the port number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **port** *port_number*

port_number

Specify the port number.

Must be an integer.

Usage Guidelines Use this command to configure the port number.

active-charging service port-map port-range port

Configures the port range.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **port-range**

range *range_start*

Specify the first port number for the port range.

Must be an integer.

to *range_end*

Specify the last port number for the port range.

Must be an integer.

Usage Guidelines Use this command to configure the port number range.

active-charging service rulebase

The ACS Rulebase Configuration Mode is used to configure Active Charging Service (ACS) rulebases.

Privilege Security Administrator, Administrator

Syntax Description **`rulebase`** *`rulebase_name`* **`[ retransmissions-counted ]`**

rulebase_name

Specify the rulebase name. If the named rulebase does not exist, it is created, and the CLI mode changes to the ACS Rulebase Configuration Mode wherein the rulebase can be configured. If the named rulebase already exists, the CLI mode changes to the ACS Rulebase Configuration Mode for that rulebase.

Must be a string.

retransmissions-counted { false | true }

Specify to count retransmissions in all charging modules.

Must be either "false" or "true".

Default Value: true.

transactional-rule-matching

Specify to enable or disable transactional rule matching (TRM), which allows the Enhanced Charging Service (ECS) to bypass per-packet rule matching on a transaction once the transaction is fully classified.

Usage Guidelines Use this command to create/configure/delete an ACS rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow. The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.

Example

The following command creates a rulebase named test1:

```
rulebase test1
```

active-charging service rulebase action

Configures the action priority for a ruledef / group-of-ruledefs in the current rulebase.

Privilege Security Administrator, Administrator

Syntax Description **action priority** *action_priority* **{ dynamic-only | static-and-dynamic | timedef** *timedef_name* **}**

Usage Guidelines Use this command to configure action priorities for ruledefs / group-of-ruledefs in a rulebase. This CLI command can be entered multiple times to specify multiple ruledefs and charging actions. The ruledefs are examined in priority order, until a match is found and the corresponding charging action is applied.

Example

The following command assigns a rule and action with the action priority of 23, a ruledef named test, and a charging action named test1 to the current rulebase:

```
action priority 23 ruledef test charging-action test1
```

active-charging service rulebase action priority

Configire priority for the specified ruledef / group-of-ruledefs in the current rulebase.

Privilege Security Administrator, Administrator

Syntax Description **priority** *action_priority*

action_priority

Specify the action priority.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to assign priority to a rule in a rulebase.

active-charging service rulebase action priority dynamic-only

Enables matching of dynamic rules with static rules for this action priority on a flow.

Privilege Security Administrator, Administrator

Syntax Description **dynamic-only**

Usage Guidelines Use this command to enable matching of dynamic rules with static rules for this action priority on a flow.

active-charging service rulebase action priority dynamic-only group-of-ruledefs

Assigns a group-of-ruledefs to the rulebase.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description **action priority** *action_priority* **static-and-dynamic group-of-ruledefs** *group_of_ruledefs_name*

group_of_ruledefs_name

Specify the group-of-ruledefs name.

Must be a string.

Usage Guidelines Use this command to assign a group-of-ruledefs to the rulebase.

active-charging service rulebase action priority dynamic-only ruledef

Assigns ruledefs to the rulebase.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description **action priority** *action_priority* **static-and-dynamic ruledef** *ruledef_name* **charging-action** *charging_action_name* **ruledef** *ruledef_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

ruledef_name

Specify the ruledef name.

Must be a string.

Usage Guidelines Use this command to assign ruledefs to the rulebase.

active-charging service rulebase action priority group-of-ruledefs

Assigns a group-of-ruledefs to the rulebase.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description **action priority** *action_priority* **static-and-dynamic group-of-ruledefs** *group_of_ruledefs_name*

group_of_ruledefs_name

Specify the group-of-ruledefs name.

Must be a string.

Usage Guidelines Use this command to assign a group-of-ruledefs to the rulebase.

active-charging service rulebase action priority ruledef

Assigns ruledefs to the rulebase.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description **action priority** *action_priority* **static-and-dynamic ruledef** *ruledef_name* **charging-action** *charging_action_name* **ruledef** *ruledef_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

ruledef_name

Specify the ruledef name.

Must be a string.

Usage Guidelines Use this command to assign ruledefs to the rulebase.

active-charging service rulebase action priority static-and-dynamic

The static-and-dynamic option causes the configuration to be defined and enabled, and allows a dynamic protocol to disable or re-enable the configuration.

Privilege Security Administrator, Administrator

Syntax Description **static-and-dynamic**

Usage Guidelines static-and-dynamic

active-charging service rulebase action priority static-and-dynamic group-of-ruledefs

Assigns a group-of-ruledefs to the rulebase.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description **action priority** *action_priority* **static-and-dynamic group-of-ruledefs** *group_of_ruledefs_name*

group_of_ruledefs_name

Specify the group-of-ruledefs name.

Must be a string.

Usage Guidelines Use this command to assign a group-of-ruledefs to the rulebase.

active-charging service rulebase action priority static-and-dynamic ruledef

Assigns ruledefs to the rulebase.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description **action priority** *action_priority* **static-and-dynamic ruledef** *ruledef_name* **charging-action** *charging_action_name* **ruledef** *ruledef_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

ruledef_name

Specify the ruledef name.

Must be a string.

Usage Guidelines Use this command to assign ruledefs to the rulebase.

active-charging service rulebase action priority timedef

Associates a time definition with the ruledef / group-of-ruledefs. Timedefs activate or deactivate ruledefs / groups-of-ruledefs, making them available for rule matching only when they are active.

Privilege Security Administrator, Administrator

Syntax Description **action priority** *action_priority* **timedef group-of-ruledefs** *group_of_ruledefs_name* **charging-action** *charging_action_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

Usage Guidelines Use this command to associate a specified time definition with the ruledef / group-of-ruledefs. Timedefs activate or deactivate ruledefs / groups-of-ruledefs, making them available for rule matching only when they are active.

active-charging service rulebase action priority timedef group-of-ruledefs

Assigns a group-of-ruledefs to the rulebase.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description

action priority *action_priority* **static-and-dynamic group-of-ruledefs** *group_of_ruledefs_name*

group_of_ruledefs_name

Specify the group-of-ruledefs name.

Must be a string.

Usage Guidelines

Use this command to assign a group-of-ruledefs to the rulebase.

active-charging service rulebase action priority timedef ruledef

Assigns ruledefs to the rulebase.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description

action priority *action_priority* **static-and-dynamic ruledef** *ruledef_name* **charging-action** *charging_action_name* **ruledef** *ruledef_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

ruledef_name

Specify the ruledef name.

Must be a string.

Usage Guidelines

Use this command to assign ruledefs to the rulebase.

active-charging service rulebase bandwidth

Configures bandwidth policy parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description **bandwidth default-policy** *default_firewall_policy_name*

default-policy *default_firewall_policy_name*

Specify the default firewall policy.

Must be a string.

Usage Guidelines Use this command to configure the bandwidth policy parameter for default firewall policy.

active-charging service rulebase billing-records

Configures the type of billing to be performed for subscriber sessions.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description **billing-records { egcdr | radius | rf }**

egcdr

Generates an enhanced G-CDR (eG-CDR) for GGSN / P-GW-CDR for P-GW, and/or UDR with specified format on the occurrence of an interim trigger condition at the end of a subscriber session, or an SGSN-to-SGSN handoff

radius

Generates postpaid RADIUS accounting records at the start and end of a subscriber session, and on the occurrence of an interim trigger condition. RADIUS accounting records are generated for each content ID.

rf

Enables Rf accounting.

Usage Guidelines Use this command to generate enhanced G-CDRs (eG-CDRs), P-GW-CDR for P-GW, RADIUS CDRs and/or UDRs for billing records. The format of eG-CDRs for the default GTPP group is controlled by the inspector command in the Context Configuration Mode.

active-charging service rulebase billing-records udr

Generates Usage Data Record (UDR) with specified the format on the occurrence of an interim trigger condition, at the end of a subscriber session, or a handoff.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description **billing-records udr udr-format** *udr_format_name*

udr_format_name

Specify the UDR format name.

Must be a string.

Usage Guidelines Use this command to enable Usage Data Record.

Example

The following command sets the billing record to UDR with UDR format named udr_format1:

```
billing-records udr udr-format udr_format1
```

active-charging service rulebase cca diameter

Specify the Diameter sub-AVPs to be included in "Requested-Service-Unit" the Diameter group AVP sent with DCCA Credit Control Requests (CCRs).

Privilege Security Administrator, Administrator

Syntax Description **cca diameter requested-service-unit sub-avp { time cc-time** *duration* **| units cc-service-specific-units** *charging_unit* **| volume { cc-input-octets** *bytes* **| cc-output-octets** *bytes* **| cc-total-octets** *bytes* **} }**

Usage Guidelines Use this command to include sub-AVPs based on time, volume, and service specific unit in the "Requested-Service-Unit" grouped AVP with CCRs.

Example

The following command sets the time-based sub-AVP with charging duration of 45 seconds in "Requested-Service-Unit" group AVP on DCCA CCRs:

```
cca diameter requested-service-unit sub-avp time cc-time 45
```

active-charging service rulebase cca diameter requested-service-unit

ACS Diameter Credit Control requesting service unit values.

Privilege Security Administrator, Administrator

Syntax Description **requested-service-unit**

Usage Guidelines ACS Diameter Credit Control requesting service unit values.

active-charging service rulebase cca diameter requested-service-unit sub-avp

Configures the sub-AVP of the requesting service unit AVP.

Privilege

Security Administrator, Administrator

Syntax Description

sub-avp

Usage Guidelines

Use this command to configure the sub-AVP of the requesting service unit AVP.

active-charging service rulebase cca diameter requested-service-unit sub-avp time

Configures the ACS Diameter Credit Control requesting service unit - time values.

Privilege

Security Administrator, Administrator

Syntax Description

time

cc-time *duration*

Specify requested service unit for charging time duration in seconds in included sub-AVP.

Must be an integer in the range of 1-4000000000.

Usage Guidelines

Use this command to configure the ACS Diameter Credit Control requesting service unit - time values.

active-charging service rulebase cca diameter requested-service-unit sub-avp units

Specify requested service unit by service specific units in bytes/packets in included sub-AVP.

Privilege

Security Administrator, Administrator

Syntax Description

units cc-service-specific-units *charging_unit*

charging_unit

Specify the service-specific charging units.

Must be an integer in the range of 1-4000000000.

Usage Guidelines

Use this command to configure the ACS Diameter Credit Control requesting service unit - service specific values.

active-charging service rulebase cca diameter requested-service-unit sub-avp volume

Specify the ACS Diameter Credit Control requesting service unit - time values.

Privilege

Security Administrator, Administrator

Syntax Description

volume

cc-input-octets *bytes*

Specify the volume in bytes.

Must be an integer in the range of 1-4000000000.

cc-output-octets *bytes*

Specify the output charging octets in bytes.

Must be an integer in the range of 1-4000000000.

cc-total-octets *bytes*

Specify the total charging octets in bytes.

Must be an integer in the range of 1-4000000000.

Usage Guidelines

Use this command to configure the ACS Diameter Credit Control requesting service unit - time values.

active-charging service rulebase cca quota holding-time

Configures the value for the Quota Holding Time (QHT). QHT is used with both time- and volume-based quotas.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description

cca quota holding-time *holding_time* **content-id** *content_id*

holding_time

Specify the holding time.

Must be an integer in the range of 1-4000000000.

content-id *content_id*

Specify the content ID (Rating group AVP) to use for the Quota holding time for the current rulebase. Must be the content ID specified for Credit Control service in ACS.

Must be an integer in the range of 1-2147483647.

Usage Guidelines Command Description: Configures various time and threshold-based quotas in the Prepaid Credit Control Service (Credit Control Application). Use this command to configure the value for the Quota Holding Time (QHT). QHT is used with both time- and volume-based quotas. After the configured number of seconds has passed without user traffic, the quota is reported back and the charging stops until new traffic starts.

active-charging service rulebase cca quota retry-time

Configures the retry time for the quota request.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description **`cca quota retry-time`** *`retry_time`* **`[ max-retries`** *`max_retries`* **`]`**

retry_time

Specify the retry interval in seconds.

Must be an integer in the range of 0-86400.

max-retries *max_retries*

Specify the maximum number of retries allowed for blacklisted categories.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure credit control quota retry time.

active-charging service rulebase cca quota time-duration

Configures the algorithm to compute time duration for Prepaid Credit Control Application quotas in the current rulebase.

Privilege Security Administrator, Administrator

Syntax Description **`cca quota time-duration algorithm { consumed-time`** *`consumed_time`* **`[ plus-idle ] | continuous-time-periods`** *`seconds`* **`| parking-meter`** *`seconds`* **`} [ content-id`** *`content_id`* **`]`**

algorithm

Specify Credit Control Quota Time Duration Algorithm

Configures the Quota Consumption Time (QCT).

Privilege Security Administrator, Administrator

Syntax Description **consumed-time** *consumed_time*

consumed_time

Specify the credit control consumed time in seconds.

Must be an integer in the range of 1-4294967295.

plus-idle

Specify the idle time for QCT. When used along with consumed-time it indicates the active usage + idle time, when no traffic flow occurs.

Configures the charging quota continuous period.

Privilege Security Administrator, Administrator

Syntax Description **continuous-time-periods** *seconds*

seconds

Specify the charging quota continuous period, in seconds.

Must be an integer in the range of 1-4294967295.

Configures the Parking Meter (PM) period for a specific rating group.

Privilege Security Administrator, Administrator

Syntax Description **parking-meter** *seconds*

seconds

Specify the Parking Meter (PM) period, in seconds.

Must be an integer in the range of 1-4294967295.

content-id *content_id*

Specify the content ID (Rating group AVP) to use for the CCA Quota time duration algorithm selection in the current rulebase. Must be the content ID specified for Credit Control service in ACS.

Must be an integer in the range of 1-2147483647.

Usage Guidelines Use this command to set the various time charging algorithms/schemes for prepaid credit control charging. If operator chooses parking-meter style charging, then time is billed in seconds chunks.

Usage Guidelines Use this command to configure the Quota Consumption Time (QCT). QCT is used with active time-based quotas and to determine chargeable time envelopes for consuming time quota.

Usage Guidelines Use this command to configure the charging quota continuous period in seconds.

Usage Guidelines Use this command to configure the Parking Meter (PM) period for a specific rating group.

Example

The following command configures the QCT to consumed-time duration of 400 seconds:

```
cca quota time-duration algorithm consumed-time 400
```

active-charging service rulebase content-filtering category

Configures the Content Filtering Category Policy Identifier for Policy-based Content Filtering support in the current rulebase.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description

`content-filtering category policy-id` *`cf_policy_id`*

policy-id *cf_policy_id*

Specify the Content Filtering policy ID.

Must be an integer in the range of 1-4294967295.

Usage Guidelines

Use this command to configure the Content Filtering Category Policy ID for Policy-based Content Filtering support in the rulebase.

Example

The following command configures the Content Filtering Category Policy ID 101 in the rulebase:

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

active-charging service rulebase content-filtering flow-any-error

Configures the action to take on Content Filtering packets in the case of ACS error scenarios.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description

`content-filtering flow-any-error { deny | permit }`

permit

Specify the flow-any-error configuration as permit.

deny

Specify the flow-any-error configuration as deny. All the denied packets will be accounted for by the discarded-flow-content-id configuration in the Content Filtering Policy Configuration Mode. This content ID will be used to generate UDRs for packets denied via content filtering.

Usage Guidelines Use this command to allow/discard content filtering packets in case of ACS error scenarios.

Example

The following command allows content filtering packets in case of an ACS error:

```
content-filtering flow-any-error permit
```

active-charging service rulebase content-filtering mode

This command allows you to enable/disable the specified Category-based Content Filtering mode in the current rulebase.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description **`content-filtering mode { category { static-and-dynamic | static-only } | server-group`** *`cf_server_group`* **`}`**

category { static-and-dynamic | static-only }

Using Category-based Content Filtering support requires configuration of the require active-charging content-filtering category command in the Global Configuration Mode.

Must be one of the following:

- static-only: Configures Category-based Content Filtering in static only mode, wherein all URLs are compared against an internal database to categorize the requested content.
- static-and-dynamic: Configures Category-based Content Filtering in Static-and-Dynamic mode, wherein a static rating of the URL is first performed, and only if the static rating fails to find a match, dynamic rating of the content that the server returns is then performed.

server-group *server_group*

Specify the content-filtering server group name.

Must be a string.

Usage Guidelines Use this command to enable and apply the content filtering mode in the rulebase to manage a content filtering server with an ICAP client system.

Example

The following command enables the content filtering mode for external content filtering server group cf_server1 in the rulebase:

```
content-filtering mode server-group cf_server
```

active-charging service rulebase credit-control-group

Configures the credit control group to be used for subscribers who use this rulebase.

Privilege

Security Administrator, Administrator

Syntax Description

credit-control-group *cc_group_name*

cc_group_name

Specify the credit control group name.

Must be a string.

Usage Guidelines

Use this command to specify the desired CC group whenever the rulebase is selected during the subscriber session setup. This is an optional CLI configuration, and used only when customized Assume Positive behavior is required for subscribers. This CLI configuration is applicable only during the session setup. Mid-session change in the CC group is not allowed.

Example

The following command configures the association of a credit-control group named test for the current rulebase:

```
credit-control-group test
```

active-charging service rulebase dynamic-rule

Configfures whether dynamic rules are matched before statically configured rules.

Privilege

Security Administrator, Administrator

Syntax Description

dynamic-rule order *dynamic_rule_order*

order *dynamic_rule_order*

Specify dynamic rule order.

Must be one of the following:

- always-first: Specify to match all the dynamic rules against the flow prior to any static rule. This is the default value.

- first-if-tied: Specify to match rules against the flow based on their priority with the condition that dynamic rules match before a static rule of the same priority. A rule is a combination of a ruledef, charging action, and precedence. Static rules are defined by the "action" CLI command in the ACS Rulebase Configuration Mode, and are applicable to all subscribers that are associated with the rulebase. Dynamic rules are obtained via a dynamic protocol, such as, the Gx-interface for a particular subscriber session.

Usage Guidelines Use this command to configure the order in which rules are selected for matching in between dynamic rules (per subscriber) and static rules (from rulebase).

Example

The following command matches all dynamic rules against the flow prior to any static rule:

```
dynamic-rule order always-first
```

active-charging service rulebase edr transaction-complete

Configures EDR-related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Rulebase Configuration

Syntax Description **edr transaction-complete { dns | http } [charging-edr** *charging_edr_format_name* **| edr-format** *edr_format_name* **| reporting-edr** *reporting_edr_format_name* **]**

dns

DNS protocol related configuration

http

HTTP protocol related configuration

charging-edr *charging_edr_format_name*

Specify to generate charging EDR on transaction completion.

Must be a string.

edr-format *edr_format_name*

Specify to generate EDR on transaction completion for DNS or HTTP protocol.

Must be a string.

reporting-edr *reporting_edr_format_name*

Specify the reporting EDR format name to generate reporting EDR on transaction completion.

Must be a string.

Usage Guidelines Configures the generation of an EDR on the completion of a transaction. Use this command to configure the generation of an EDR when certain application transactions (for example, request/response pairs) complete. EDR generation is supported for DNS or HTTP protocol. Note that these EDRs are in addition to those that might be generated due to other conditions, for example, EDR configurations in a charging action.

Example

The following command configures the generation of charging EDRs on the completion of transactions for HTTP protocol specifying the EDR format as test123:

```
edr transaction-complete http charging-edr test123
```

active-charging service rulebase egcdr threshold

Assigns volume or interval values to the interim G-CDRs.

Privilege Security Administrator, Administrator

Syntax Description **`egcdr threshold interval`** *`duration`*

interval *duration*

Specify the time interval, in seconds, for closing the eG-CDR/PGW-CDR if the minimum time duration thresholds are satisfied.

Must be an integer in the range of 60-40000000.

Usage Guidelines Configures the thresholds for generating eG-CDRs for GGSN and PGW-CDRs for P-GW. Use this command to assign the interval values to the interim G-CDRs.

Example

The following command defines an eG-CDR threshold interval of 600 seconds:

```
egcdr threshold interval 600
```

active-charging service rulebase egcdr threshold volume

Configures the uplink/downlink volume octet counts for the generation of the interim eG-CDRs/PGW-CDRs.

Privilege Security Administrator, Administrator

Syntax Description **`egcdr threshold volume { downlink | total | uplink }`** *`bytes`*

downlink *bytes*

Specify the limit for the number of downlink (from network to subscriber) octets after which the eG-CDR/PGW-CDR is closed.

Must be an integer in the range of 100000-4000000000.

uplink *bytes*

Specify the limit for the number of uplink (from subscriber to network) octets after whichthe eG-CDR/PGW-CDR is closed.

Must be an integer in the range of 100000-4000000000.

total *bytes*

Specify the limit for the total number of octets (uplink+downlink) after which theeG-CDR/PGW-CDR is closed.

Must be an integer in the range of 100000-4000000000.

Usage Guidelines

Configures the thresholds for generating eG-CDRs for GGSN and PGW-CDRs for P-GW. Use this command to configure the uplink/downlink volume octet counts for the generation of the interim GCDRs.

active-charging service rulebase flow

Configures the charge for the control traffic associated with an application.

Privilege

Security Administrator, Administrator

Syntax Description

`flow control-handshaking { charge-to-application { [ all-packets ] [ initial-packets ] [ mid-session-packets ] [ tear-down-packets ] } | charge-separate-from-application }`

Usage Guidelines

Use this command to configure how to charge for the control traffic associated with an application ruledef. Applications like HTTP use TCP to set up and tear down connections before the HTTP application starts. This command controls whether the packets that set up and tear down the connections should use the same content ID as the application's flow. In normal mode 3-way handshake TCP packets (SYN, SYN-ACK, and ACK) and closing or intermittent packets (FIN, RST, etc.) directed and charged based on configured matched rules. This command makes the system to wait for the start and stop of layer 7 packet flow and content ID and charge the initial, intermittent, and closing TCP packets as configured to the same matching rules and content ID as of the flow. This command also affects applications that do not use TCP but use other methods for control packets, for example WAP, where WTP/UDP may be used to set up and tear down connection-oriented WSP.

Example

The following command enables charging all mid-session ACKs as well as tear-down packets to application:

```
flow control-handshaking charge-to-application mid-session-packets tear-down-packets
```

active-charging service rulebase flow control-handshaking

Specify control protocol handshake packets.

Privilege

Security Administrator, Administrator

Syntax Description `flow control-handshaking charge-separate-from-application`

charge-separate-from-application

Specify the charging action to separate the charging of the initial control packets or all subsequent control packets from regular charging.

Usage Guidelines Use this command to specify control protocol handshake packets.

active-charging service rulebase flow control-handshaking charge-to-application

Configures the charging action to include the flow control packets either during initial handshaking only or specified control packets during session for charging.

Privilege Security Administrator, Administrator

Syntax Description `flow control-handshaking charge-to-application { [ all-packets ] [ initial-packets ] [ mid-session-packets ] [ tear-down-packets ] }`

all-packets

Specify that the initial setup packets will wait until the application has been determined before assigning the content-id, and all mid-session ACK packets as well as the final tear-down packets will use that content-id.

mid-session-packets

Specify that the ACK packets after the initial setup will use the application's or content-id assignment.

initial-packets

Specify that only the initial setup packets will wait for content-id assignment.

tear-down-packets

Specify that the final tear-down packets (TCP or WAP) will use the application's or content-id assignment.

Usage Guidelines Use this command to charge control packets to application ruledefs.

active-charging service rulebase flow end-condition

Configures the end condition of the session flows related to a user session and triggers EDR generation.

Privilege Security Administrator, Administrator

Syntax Description `flow end-condition { normal-end-signaling | session-end | timeout | charging-edr` *charging_edr_format_name* `}`

timeout

Creates an EDR with the specified EDR format whenever a flow ends due to a timeout condition.

normal-end-signaling

Creates an EDR with the specified EDR format whenever flow end is signaled normally, for example like detecting FIN and ACK for a TCP flow, or a WSP-DISCONNECT terminating a connection-oriented WSP flow over UDP) and create an EDR for the flow using the specified EDR format.

session-end

Creates an EDR with the specified EDR format whenever a subscriber session ends. By this option ACS creates an EDR with the specified format name for every flow that has had any activity since last EDR was created for the flow on session end.

charging-edr *charging_edr_format_name*

Specify the charging EDR format name.

Must be a string.

Usage Guidelines

Use this command to enable or disable the capturing of EDRs based on flow end condition.

Example

The following command configures the flow end condition as handoff and creates a charging EDR with format named edr_format1:

```
flow end-condition handoff charging-edr edr_format1
```

active-chargingservicerulebaseflowlimit-across-applications

This command allows you to limit the total number of simultaneous flows per Subscriber/APN sent to a rulebase regardless of the flow type, or limit flows based on the protocol type under the Session Control feature.

Privilege

Security Administrator, Administrator

Syntax Description

flow limit-across-applications { *limit* **| non-tcp** *limit* **| tcp** *limit* **}**

tcp *tcp_limit*

Specify the maximum limit of TCP flows.

Must be an integer in the range of 1-4000000000.

non-tcp *limit*

Specify the maximum limit of non-TCP type flows.

Must be an integer in the range of 1-4000000000.

-Or-

Must be an integer in the range of 1-4000000000.

Usage Guidelines Use this command to limit the total number of flows allowed per subscriber for a rulebase regardless of flow type, or limit flows based on the protocol non-TCP (connection-less) or TCP (connection-oriented).

Example

The following command configures the maximum number of 200000 flows for the rulebase:

```
flow limit-across-applications 200000
```

active-charging service rulebase ip

Configures IP parameters related to user session.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`ip reassembly-timeout`** *`reassembly_timeout`*

reassembly-timeout *reassembly_timeout*

Specify the maximum duration for which ip packet fragments are retained, in milliseconds.

Must be an integer in the range of 100-30000.

Default Value: 5000.

Usage Guidelines Use this command to configure IP parameters related to user session.

active-charging service rulebase p2p

Configures enabling/disabling the P2P analyzer to detect peer-to-peer (P2P) applications.

Privilege Security Administrator, Administrator

Syntax Description **`p2p dynamic-flow-detection`**

dynamic-flow-detection

Enables dynamic-flow detection, allowing the P2P analyzer to detect the P2P applications configured for the ACS.

Usage Guidelines Use this command to enable/disable the P2P analyzer to detect peer-to-peer (P2P) applications.";

active-charging service rulebase post-processing

Configures the post-processing action to be taken.

Privilege

Security Administrator, Administrator

Syntax Description

post-processing priority priority { group-of-ruledefs *ruledefs_group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[description** *description* **]**

Usage Guidelines

Use this command to configure the post-processing priority and action to be taken on a ruledef in the rulebase.

active-charging service rulebase post-processing priority

Configures the post-processing priority and action to be taken on specific ruledef in the current rulebase.

Privilege

Security Administrator, Administrator

Syntax Description

post-processing priority *priority_value* **{ group-of-ruledefs** *ruledefs_group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[description** *description* **]**

priority_value

Specify the priority value.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to configure the post-processing priority and action to be taken on a ruledef in the rulebase.

Example

The following command configures the ruledef named test_ruledef with a priority of 10, and the charging action named test_ca for post processing:

```
post-processing priority 10 ruledef test_ruledef charging-action test_ca
```

active-charging service rulebase post-processing priority group-of-ruledefs

Configures group-of-ruledef parameters.

Privilege

Security Administrator, Administrator

Syntax Description

group-of-ruledefs *ruledefs_group_name*

ruledefs_group_name

Specify the group-of-ruledefs to add/configure/delete.

Must be a string.

charging-action *charging_action_name*

Specify the charging action.

Must be a string.

description *description*

Specify an optional description for this configuration.

Must be a string.

Usage Guidelines Use this command to configure group-of-ruledef parameters.

active-charging service rulebase post-processing priority ruledef

Assigns ruledefs to a rulebase.

Privilege Security Administrator, Administrator

Syntax Description **ruledef** *ruledef_name*

ruledef_name

Specify the ruledef name.

Must be a string.

charging-action *charging_action_name*

Specify the charging action name.

Must be a string.

description *description*

Specify an optional description for this configuration.

Must be a string.

Usage Guidelines Use this command to assign ruledefs to a rulebase.";

active-charging service rulebase route

Configures the routing of packets to protocol analyzers.

Privilege

Security Administrator, Administrator

Syntax Description

route priority *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp | rtp | rtsp | sdp | secure-http | sip | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [description** *description* **]**

Usage Guidelines

Instances of this CLI command control which packets are routed to which protocol analyzers. Packets sent to ACS are always passed through the IP protocol analyzer. This CLI command controls which higher layer analyzers are also invoked.

Example

The following command assigns a route and rule action with the route priority of 23, a ruledef named test, and an analyzer test_analyzer with description as route_test1 to the current rulebase:

```
route priority 23 ruledef test analyzer test_analyzer description route_test1
```

active-charging service rulebase route priority

Configures the priority of the route in the rulebase.

Privilege

Security Administrator, Administrator

Syntax Description

priority *route_priority*

route_priority

Specifythe route priority.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this command to configure the priority of the route in the rulebase.

active-charging service rulebase route priority ruledef

Configures the ruledef to evaluate packets to determine analyzer.

Privilege

Security Administrator, Administrator

Syntax Description

ruledef *ruledef_name*

ruledef_name

Specify the ruledef name.

Must be a string.

analyzer *analyzer*

Specify the analyzer for the ruledef.

Must be one of the following:

- dns: Configure the primary and secondary IPv4 or IPv6 address of the DNS servers.
- file-transfer: Allows you to enter descriptive text for this configuration.
- ftp-control: Charge volume for FTP-Control.
- ftp-data: Charge volume for FTP-Data.
- h323: Enables/disables H323 NAT ALG.
- http: Specify to detect HTTP protocol.
- imap: Route to IMAP protocol analyzer.
- mipv6: Route to MIPv6 protocol analyzer.
- mms: Route to MMS protocol analyzer.
- pop3: Route to POP3 protocol analyzer.
- pptp: Route to PPTP protocol analyzer.
- radius: Route to RADIUS protocol analyzer.
- rtcp: Route to RTCP protocol analyzer.
- rtsp: Route to RTSP protocol analyzer.
- rtp: Route to RTP protocol analyzer.
- sdp: Route to SDP protocol analyzer.
- sip: Route to SIP protocol analyzer.
- secure-http: Route to secure HTTP protocol analyzer.
- smtp: Route to SMTP protocol analyzer.
- tftp: Route to TFTP protocol analyzer.
- wsp-connection-less: Route to WSP connection-less protocol analyzer.
- wsp-connection-oriented: Route to WSP connection-oriented protocol analyzer.

description *description*

Enables to add a description to the rule and action for later reference in saved configuration file.

Must be a string.

Usage Guidelines

Use this command to assign a ruledef to a rulebase,

active-charging service rulebase rtp

This command allows you to enable/disable the Real Time Streaming Protocol (RTSP) and Session Description Protocol (SDP) analyzers to detect the start/stop of RTP and RTCP flows.

Privilege

Security Administrator, Administrator

Syntax Description

```
rtp dynamic-flow-detection
```

dynamic-flow-detection

Controls whether dynamic RTP/RTCP flow detection is enabled or not.

Usage Guidelines

Use this command to enable the RTSP and SDP analyzer to detect the start/stop of RTP and RTCP flows. This command is used in conjunction with the route priority command.

Example

```
rtp dynamic-flow-detection
```

active-charging service rulebase tcp

Configures TCP window size checking.

Privilege

Security Administrator, Administrator

Syntax Description

```
tcp check-window-size
```

check-window-size

Enables/Disables TCP window-size check.

Usage Guidelines

Use this command to enable/disable TCP window-size check for packets out of TCP window.

Example

The following command enables TCP window-size check:

```
tcp check-window-size
```

active-charging service rulebase tcp mss

Configures the TCP Maximum Segment Size (MSS) in TCP SYN packets.

Privilege

Security Administrator, Administrator

Syntax Description `tcp mss mss_value { [ add-if-not-present ] [ limit-if-present ] }`

mss_value

Specify the TCP MSS.

Must be an integer in the range of 496-65535.

add-if-not-present

Specify to add the TCP MSS if not present in the packet.

limit-if-present

Specify to limit the TCP MSS if present in the packet.

Usage Guidelines Using this command, TCP MSS can be limited if already present in the TCP SYN packets. If there are no errors detected in IP header/TCP mandatory header and there are no memory allocation failures, TCP optional header is parsed. If TCP MSS is present in the optional header and its value is greater than the configured MSS value, the value present in the TCP packet is replaced with the configured one.

Example

The following command limits the TCP maximum segment size to 3000, and if not present adds it to the packets:

```
tcp mss 3000 limit-if-present add-if-not-present
```

active-charging service rulebase tcp packets-out-of-order

Configures processing of TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

Privilege Security Administrator, Administrator

Syntax Description `tcp packets-out-of-order timeout timeout_duration`

timeout *timeout_duration*

Specify the timeout duration for re-assembly of TCP out-of-order packets in milliseconds.

Must be an integer in the range of 100-30000.

Default Value: 5000.

Usage Guidelines Use this command to configure how to process TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

Example

The following command sets the timeout timer to 10000 milliseconds:

```
tcp packets-out-of-order timeout 10000
```

active-charging service rulebase tcp packets-out-of-order transmit

Configures the TCP out-of-order segment behavior after buffering a copy.

Privilege

Security Administrator, Administrator

Syntax Description

transmit *transmit_behavior*

transmit *transmit_behavior*

Specify the TCP out-of-order segment behavior after buffering a copy.

Must be one of the following:

- after-reordering: Delivers the TCP out-of-order segments in-sequence to the ECS analyzer after all packets are received and successfully reordered. The 'after-reordering' feature is doing this by buffering out-of-order packets, and only releasing them after the missing out-of-order packets are received (or after OOO timeout). When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is done, and then the last packet is forwarded (as the latest). If reordering is not successful within the specified OOO timeout, all the subsequent received packets in that TCP flow are forwarded without being passed through the analysers (except the L3/L4 analyzer). As a consequence, only L3/L4 rule matching will take place. If memory allocation fails or the received packet is partial retransmitted data, the packet will also be forwarded immediately without being passed through the protocol analyzers, except for the L3/L4 analyzers.
- immediately: Delivers the TCP out-of-order segments in-sequence to the ECS analyzer after all packets are received and successfully reordered. The 'immediately' feature is accomplishing this by making a copy of out-of-order packets, and buffering those, while transmitting the original data packets through the outgoing interface immediately. When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is done, and then the last packet is forwarded. If reordering of the buffered packets is not successful within the specified OOO timeout, all the subsequent received packets in that TCP flow are forwarded without being passed through the analysers (except the L3/L4 analyzer). As a consequence only L3/L4 rule matching will take place. If memory allocation fails or the received packet is partial retransmitted data, the packet will also be forwarded immediately without being passed through the protocol analyzers, except for the L3/L4 analysers.

Usage Guidelines

Use this command to configure the TCP out-of-order segment behavior after buffering a copy.

active-charging service rulebase tethering-detection

Enables or disables the Tethering Detection feature for the current rulebase, and specifies the database to use.

Privilege

Security Administrator, Administrator

Syntax Description

tethering-detection [application | dns-based | ip-ttl value *ttl_value* **| max-syn-packet-in-flow** *max_syn_packets* **| tether-db** *database* **]**

max-syn-packet-in-flow *max_syn_packets*

Specify the number of SYN packets applicable for tethering detection in a flow.

Must be an integer in the range of 1-3.

application

Specify to perform tethering detection based on App-based method.

dns-based

Specify to perform tethering detection based on DNS-based method.

tether-db *database*

Specify to perform tethering detection using the specified database.

Must be one of the following:

- ua-db-only: Specify to perform tethering detection using only the UA signature database.
- os-ua-db: Specify to perform tethering detection using IPv4 OS, IPv6 OS, and UA signature databases.
- os-db-only: Specify to perform tethering detection using IPv4 and IPv6 OS signature databases.

This command allows you to perform tethering detection using IP-TTL configuration.

Privilege

Security Administrator, Administrator

Syntax Description

`ip-ttl value` *`ttl_value`*

ttl_value

Specify TTL values for tethered flows.

Must be an integer in the range of 1-255.

Usage Guidelines

Use this command to enable/disable the Tethering Detection feature for a rulebase, and configures the database to use. Tethering Detection can be done for IPv4, IPv6, TCP and UDP flows.

Usage Guidelines

Use this command to perform tethering detection using ip-ttl configuration.

Example

The following command enables the Tethering Detection feature in the rulebase, and specifies to use only the OS database:

```
tethering-detection os-db-only
```

active-charging service rulebase url-blacklisting

This command allows you to enable/disable URL Blacklisting functionality for the current rulebase, and configures the action to be taken when there is a URL match.

Privilege

Security Administrator, Administrator

Syntax Description

`url-blacklisting action { discard | redirect-url` *`url`* **`| terminate-flow | www-reply-code-and-terminate-flow`** *`reply_code`* **`} [ content-id`** *`content_id`* **`]`**

Usage Guidelines

Use this command to enable/disable URL Blacklisting at the rulebase level, and configure the action to be taken.

Example

The following command enables URL Blacklisting in the rulebase, and configures the terminate-flow action with reply code 300:

```
url-blacklisting action www-reply-code-and-terminate-flow 300
```

active-charging service rulebase url-blacklisting action

Configures URL Blacklisting action.

Privilege

Security Administrator, Administrator

Syntax Description

`action { content-id` *`content_id`* **`| discard | redirect-url`** *`redirect_url`* **`| terminate-flow | www-reply-code-and-terminate-flow`** *`reply_code`* **`}`**

redirect-url *redirect_url*

Specify the redirect URL/URI, which must be a fully qualified URL/URI.

Must be a string.

discard

Specify the URL Blacklisting action as "discard".

terminate-flow

Specify the URL Blacklisting action as "terminate-flow".

www-reply-code-and-terminate-flow *reply_code*

Specify the URL Blacklisting action as "terminate-flow action with reply code".

Must be an integer in the range of 400-599.

content-id *content_id*

Specify the content ID, a number assigned to URL Blacklisting.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to configure the URL Blacklisting action.

active-chargingservicerulebaseurl-blacklistingmatch-method

Configures URL Blacklisting match-method.

Privilege

Security Administrator, Administrator

Syntax Description

match-method *match_method*

match_method

Specify the match method.

Must be one of the following:

- exact
- generic

Usage Guidelines

Use this command to configure the URL Blacklisting match method.

active-charging service ruledef

Configures ACS rule definitions (ruledef).

Privilege

Security Administrator, Administrator

Syntax Description

ruledef *ruledef_name* **[rule-application** *ruledef_purpose* **]**

ruledef_name

Specify the ruledef name. If the named ruledef does not exist, it is created, and the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured. If the named ruledef already exists, the CLI mode changes to the ACS Ruledef Configuration Mode for that ruledef.

Must be a string.

rule-application *ruledef_purpose*

Specify the purpose of the ruledef, such as for charging, post-processing, routing, and so on. When a ruledef is evaluated, if the multi-line-or all-lines command is configured, the logical OR.

Must be one of the following:

- charging: Specify that the current ruledef is for charging purposes.
- post-processing: Specify that the current ruledef is for post-processing purposes. This enables processing of packets even if the rule matching for them has been disabled.
- routing: Specify that the current ruledef is for routing purposes. Up to 256 ruledefs can be defined for routing in an Active Charging Service.

Usage Guidelines Use this command to create/configure/delete an ACS ruledef. A ruledef represents a set of matching conditions across multiple L3 L7 protocol based on protocol fields and state information. Each ruledef can be used across multiple rulebases within the active charging service.

Example

The following command creates/configures an ACS ruledef named test1:

```
ruledef test1
```

active-charging service ruledef bearer

Configures rule expression to match Radio Access Technology (RAT) in the bearer flow.

Privilege Security Administrator, Administrator

Syntax Description **bearer service-3gpp rat-type** *operator rat_type*

Usage Guidelines Use this command to define rule expressions to match a RAT type.

Example

The following command defines a rule expression to match user traffic based on RAT type "wlan":

```
bearer service-3gpp rat-type = wlan
```

active-charging service ruledef bearer service-3gpp

Specify 3GPP service.

Privilege Security Administrator, Administrator

Syntax Description **service-3gpp**

Usage Guidelines service-3gpp

active-charging service ruledef bearer service-3gpp rat-type

Specify RAT type associated with the bearer flow.

Privilege Security Administrator, Administrator

Syntax Description **rat-type**

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- =: Equals.

rat_type

Specify the RAT type.

Must be one of the following:

- geran: GSM EDGE Radio Access Network type.
- utran: UMTS Terrestrial Radio Access Network type.
- wlan: Wireless LAN type.

Usage Guidelines Use this command to configure the RAT type associated with the bearer flow.

active-charging service ruledef dns

Configures rule expression to match answer name in the answer section of DNS response messages.";

Privilege Security Administrator, Administrator

Syntax Description **`dns answer-name [ case-sensitive ]`** *`operator value`*

Usage Guidelines Use this command to define rule expressions to match an answer name from the answer section of DNS response messages.

Example

The following command defines a rule expression to match user traffic for answer name test:

```
dns answer-name = test
```

active-charging service ruledef dns answer-name

Specify DNS answer name.

Privilege Security Administrator, Administrator

Syntax Description **`answer-name`**

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- !contains: Does not contains.
- !ends-with: Does not end with.
- !starts-with: Does not start with.
- =: Equals.
- case-sensitive: Strings will be matched in case-sensitive manner.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.

value

Specify the value.

Must be a string.

Usage Guidelines Use this command to configure the DNS answer name. This depends upon the query type.

active-charging service ruledef dns any-match

Configures any-match.

Privilege Security Administrator, Administrator

Syntax Description **`wsp any-match`** *`operator condition`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

condition

Specify the condition.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Use this command to configure any match.

active-charging service ruledef dns previous-state

Configures rule expression to match previous state of the DNS FSM.

Privilege

Security Administrator, Administrator

Syntax Description

dns previous-state *operator previous_state*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

previous_state

Specify the previous state to match.

Must be one of the following:

- dns-timeout: DNS timeout.
- init: Init.
- req-sent: Request sent.
- resp-error: Response error.
- resp-success: Response sucess..

Usage Guidelines

Use this command to define rule expressions to match previous state of DNS FSM.

Example

The following command defines a rule expression to match the DNS FSM previous state "req-sent":

```
dns previous-state = req-sent
```

active-charging service ruledef dns query-name

Configures rule expression to match query name in DNS request messages.

Privilege

Security Administrator, Administrator

Syntax Description

dns query-name [case-sensitive] *operator query_name*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- !contains: Does not contain.
- !ends-with: Does not end with.
- !starts-with: Does not start with.
- =: Equals.
- case-sensitive: Strings will be matched in case-sensitive manner.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.

query_name

Specify the query name to match.

Must be a string.

Usage Guidelines Use this command to define rule expressions to match query name in DNS request messages.

Example

The following command defines a rule expression to match DNS query name "test":

```
dns query-name = test
```

active-charging service ruledef dns query-type

Configures rule expression to match the query type in the DNS request messages.

Privilege Security Administrator, Administrator

Syntax Description **`dns query-type`** *`operator query_type`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

query_type

Specify the previous state to match.

Must be one of the following:

- a: Support query-type 'A'.
- aaaa: Support query-type 'AAAA'.
- cname: Support query-type 'CNAME'.
- ns: Support query-type 'NS'.
- null: Support query-type 'NULL'.
- ptr: Support query-type 'PTR'.
- srv: Support query-type 'SRV'.
- txt: Support query-type 'TXT'.

Usage Guidelines Use this command to define rule expressions to match the query type in the DNS request messages.

Example

The following command defines a rule expression to match the DNS query type "txt":

```
dns query-type = txt
```

active-charging service ruledef dns return-code

Configures rule expression to match response code in DNS response messages.

Privilege Security Administrator, Administrator

Syntax Description **dns return-code** *operator return_code*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

return_code

Specify the response code to match.

Must be one of the following:

- format-error: DNS response: Format Error.

- name-error: DNS response: Name Error.
- no-error: DNS response: No Error.
- not-implemented: DNS response: Name server does not support the requested query.
- refused: DNS response: Refused to perform specified operation.
- server-failure: DNS response: Server Failure.

Usage Guidelines Use this command to define rule expressions to match response code in DNS response messages.

Example

The following command defines a rule expression to match a DNS response code "refused":

```
dns return-code = refused
```

active-charging service ruledef dns state

Configures rule expressions to match current state of DNS FSM.

Privilege Security Administrator, Administrator

Syntax Description **`dns state`** *`operator current_state`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

current_state

Specify the state to match.

Must be one of the following:

- dns-timeout
- init
- req-sent
- resp-error
- resp-success

Usage Guidelines Use this command to define rule expressions to match DNS FSM current state.

Example

The following command defines a rule expression to match DNS FSM current state of "req-sent":

```
dns state = req-sent
```

active-charging service ruledef dns tid

Configures rule expressions to match Transaction Identifier (TID) field in DNS messages.

Privilege

Security Administrator, Administrator

Syntax Description

dns tid *operator tid_value*

operator

Specify how to match.

Must be one of the following:

- '!=': Does not equal.
- <=: Lesser than or equals.
- =: Equals.
- >=: Greater than or equals.

value

Specify the query name to match.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this command to define rule expressions to match a TID field of DNS messages.

Example

The following command defines a rule expression to match DNS TID field value of "test":

```
dns tid = test
```

active-charging service ruledef http

Configures rule expression to match the User-Agent request-header field of HTTP packets.

Privilege

Security Administrator, Administrator

Syntax Description

http user-agent [case-sensitive] *operator user_agent*

Usage Guidelines Use this command to define rule expressions to match value in HTTP user-agent header field.

Example

The following command defines a rule expression to match "xyz.123" in HTTP user-agent header field:

```
http user-agent = xyz.123
```

active-charging service ruledef http content

Configures rule expression to match value in HTTP Content-Type entity-header field.

Privilege Security Administrator, Administrator

Syntax Description **`http content type [ case-sensitive ]`** *`operator content_type`*

Usage Guidelines Use this command to define rule expressions to match value in HTTP Content-Type entity-header field.

Example

```
http content type = abc100
```

active-charging service ruledef http content type

Specify HTTP Content-Type.

Privilege Security Administrator, Administrator

Syntax Description **`type`** *`operator content_type`*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- !contains: Does not contain.
- !ends-with: Does not end with.
- !starts-with: Does not start with.
- =: Equals.
- contains: Contains.
- ends-with: Ends with.

- starts-with: Starts with.

content_type

Specify the content type to match.

Must be a string.

case-sensitive

Specify that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

Usage Guidelines Use this command to configure rule expressions to match HTTP content type.

active-charging service ruledef http host

Configures rule expression to match value in HTTP Host Request header field.

Privilege Security Administrator, Administrator

Syntax Description **`http host [ case-sensitive ]`** *`operator host_name`*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- !contains: Does not contain.
- !ends-with: Does not end with.
- !starts-with: Does not start with.
- =: Equals.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.
- regex: Regular expression.

host-string *host_name*

Specify the host name to match.

Must be a string.

case-sensitive

Specify that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

Usage Guidelines Use this command to define rule expressions to match value in HTTP Host request-header field.

Example

The following command defines a rule expression to match "host1" in HTTP Host request-header field:

```
http host = host1
```

active-charging service ruledef http referer

Configures rule expression to match the value in the HTTP Referer request-header field.

Privilege Security Administrator, Administrator

Syntax Description

```
http referer [ case-sensitive ] operator referer_name
```

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- !contains: Does not contain.
- !ends-with: Does not end with.
- !present: Not present.
- !starts-with: Does not start with.
- =: Equals.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.
- regex: Regular expression.

referer_name

Specify the HTTP referer name to match.

Must be a string.

case-sensitive

Specify that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

Usage Guidelines Use this command to define rule expressions to match value in HTTP Referer request-header field. This feature allows an operator to collect or track all URLs visited during a particular subscriber session. These URLs

include the entire string of visited URLs, including all referral links. This information is output in an Event Data Record (EDR) format to support reporting or billing functions.

Example

The following command defines a rule expression to match the HTTP referer "cricket.espn.com":

```
http referer = cricket.espn.com
```

active-charging service ruledef http url

Configures rule expression to match HTTP URL.

Privilege

Security Administrator, Administrator

Syntax Description

`http url [ case-sensitive ]` *`operator url`*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- !contains: Does not contain.
- !ends-with: Does not end with.
- !present: Does not present.
- !starts-with: Does not start with.
- =: Equals.
- case-sensitive: Is case sensitive.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.
- regex: Regular expression.

url

Specify the HTTP URL to match.

Must be a string.

Usage Guidelines

Use this command to define rule expressions to match HTTP URL.";

active-charging service ruledef http user-agent

Rule expressions to match the User-Agent.

Privilege

Security Administrator, Administrator

Syntax Description

user-agent *operator user_agent*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- !contains: Does not contain.
- !ends-with: Does not end with.
- !starts-with: Does not start with.
- =: Equal.
- present: Present.
- !present: Not present.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.
- regex: Regular expression.

user_agent

Specify the HTTP user agent value to match.

Must be a string.

case-sensitive

Specify that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

Usage Guidelines

Use this command to configure rule expressions to match user agent.

active-charging service ruledef icmpv6 any-match

Configures any-match.

Privilege

Security Administrator, Administrator

Syntax Description **wsp any-match** *operator condition*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

condition

Specify the condition.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Use this command to configure any match.

active-charging service ruledef ip

This command allows you to define rule expressions to match the IP address of the destination end of the connection.

Privilege Security Administrator, Administrator

Syntax Description **ip server-ip-address {** *ipv4_address* **|** *ipv6_address* **}**

Usage Guidelines Use this command to define rule expressions to match the IP address of the destination end of the connection.

Example

The following command defines a rule expression to match user traffic based on IPv4 server address 10.1.1.1:

```
ip server-ip-address = 10.1.1.1
```

active-charging service ruledef ip any-match

Configures rule expressions to match all IPv4/IPv6 packets.

Privilege Security Administrator, Administrator

Syntax Description **ip any-match** *operator condition*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- =: Equals.

condition

Specify the condition.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Use this command to define rule expressions to match IPv4/IPv6 packets.

Example

The following command defines a rule expression to match IPv4/IPv6 packets:

```
ip any-match = TRUE
```

active-charging service ruledef ip dst-address

Configures rule expressions to match IP destination address field within IP headers.

Privilege Security Administrator, Administrator

Syntax Description **`ip dst-address { `** *`ipv4_address`* **`| `** *`ipv6_address`* **`}`**

dst-address { *ipv4_address* | *ipv6_address* }

Specify the destination IP address.

Must be one of the following:

- dst-address: DST address.

operator

Specify how to match.

Must be one of the following:

- '!=': Does not equal.
- !range: Not in the range.
- <=: Lesser than or equal to.

- =: Equals.
- >=: Greater than or equal to.
- range: In the range.

ip-address-prefix *prefix*

Specify the IP address prefix.

Must be IPv4 CIDR notation ##.##.##.##/x or in IPv6 CIDR notation ####:####:####:####:####:####:####:####/###.

-Or-

Must be an IP address.

address-group *ipv6_address*

Specify a group of IPv6 addresses configured with wildcard input and/or specialized range input. Multiple wildcard characters can be accepted as input and only one 2 byte range input will be accepted. Both wildcard character input and 2 byte range input can be configured together within an IPv6 address.

Must be a string.

host-pool *host_pool_name*

Specify the host pool name.

Must be a string.

Usage Guidelines Use this command to define rule expressions to match the IP destination address field within IP headers.

Example

The following command defines a rule expression to match user traffic based on the IPv4 destination address 10.1.1.1:

```
ip dst-address = 10.1.1.1
```

active-charging service ruledef ip protocol

Configures rule expression to match based on protocol being transported by IP packet.

Privilege Security Administrator, Administrator

Syntax Description **ip protocol** *operator protocol*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.
- <=: Lesser than or equal to.
- >=: Greater than or equal to.

protocol

Specify the protocol.

Must be an integer in the range of 0-255.

-Or-

Must be one of the following:

- ah
- esp
- gre
- icmp
- icmpv6
- tcp
- udp

Usage Guidelines Use this command to define rule expressions to match based on protocol being transported by IP packet.

active-charging service ruledef ip server-ip-addr

Specify the server's IP address.

Privilege Security Administrator, Administrator

Syntax Description **`server-ip-address`**

{ *ipv4_address* | *ipv6_address* }

Specify the server IP address.

Must be one of the following:

- server-ip-address: server-ip-address.

operator

Specify how to match.

Must be one of the following:

- '!=': Does not equal.
- !range: Not in the range.
- <=: Lesser than or equal to.
- =: Equals.
- >=: Greater than or equal to.
- range: In the range.

ip-address-prefix *prefix*

Specify the IP address prefix.

Must be IPv4 CIDR notation ##.##.##.##/x or in IPv6 CIDR notation ####:####:####:####:####:####:####:####/###.

-Or-

Must be an IP address.

address-group *ipv6_address*

Specify a group of IPv6 addresses configured with wildcard input and/or specialized range input. Multiple wildcard characters can be accepted as input and only one 2 byte range input will be accepted. Both wildcard character input and 2 byte range input can be configured together within an IPv6 address.

Must be a string.

host-pool *host_pool_name*

Specify the host pool name.

Must be a string.

Usage Guidelines Use this command to configure the server IP address.

active-charging service ruledef ip uplink

Configures rule expression to match IP uplink packets.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **uplink** *operator condition*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.

- =: Equals.

condition

Specify the condition to match.

Must be one of the following:

- TRUE: Analyzed.
- FALSE: Not analyzed.

Usage Guidelines Use this command to configure matching IP uplink packets based on condition.

active-charging service ruledef ip version

Configures rule expression to match based on IP version.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`version`** *`operator ip_version`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.

ip_version

Specify the condition to match.

Must be one of the following:

- ipv4
- ipv6

Usage Guidelines Use this command to configure rule expression to match based on the IP version.

active-charging service ruledef multi-line-or

This command applies the OR operator to all lines in the current ruledef.

Privilege Security Administrator, Administrator

Syntax Description **`multi-line-or all-lines`**

all-lines

Applies the OR operator to all lines in the current ruledef.

Usage Guidelines

When a ruledef is evaluated, if the multi-line-or all-lines command is configured, the logical OR operator is applied to all the rule expressions in the ruledef to decide if the ruledef matches or not. If the multi-line-or all-lines command is not configured, the logical AND operator is applied to all the rule expressions.";

active-charging service ruledef p2p

This command allows you to define rule expressions to match P2P protocol. This command must be used for charging purposes. It must not be used for detection purposes.

Privilege

Security Administrator, Administrator

Syntax Description

`p2p protocol` *`operator protocol`*

p2p set-app-proto *app_protocol_name*

Specify the custom-defined protocol (CDP) name. CDP name specifies the name of the custom defined protocol (CDP) for TLS/SSL flows, QUIC flows or any app-identifier matching the ruledef. If the flow/packet matches the rule, the CDP name specified in the ruledef will be taken and the flow will be marked as CDP. If no CDP is configured in the rule, then the flow will be treated as TLS/SSL or QUIC flow.

Must be a string.

Usage Guidelines

Use this command to define rule expressions to detect P2P protocols for charging purposes. For detection purposes use the "p2p-detection protocol" command in the ACS Configuration Mode.

Example

The following command specifies to detect "skype" protocol for charging purposes:

```
p2p protocol = skype
```

active-charging service ruledef p2p app-identifier

Configures application identifiers populated from the plugin and mark the matching flows to a custom-defined protocol (CDP) name.

Privilege

Security Administrator, Administrator

Syntax Description

`p2p app-identifier app-type` *`app_type operator string`*

app-type *app_type*

Specify the app type.

Must be one of the following:

- tls-sni: Specify the TLS/SSL Server Name Indication (SNI) field.

- quic-sni: Specify the QUIC Server Name Indication (SNI) field value.
- tls-cname: Specify the common name in the Server Hello message of TLS. SSL renegotiation is supported for the flows that are marked using "tls-cname" rules.

operator

Specify how to match.

Must be one of the following:

- !=: Not equals.
- =: Equals.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.

string

Specify the string.

Must be a string.

Usage Guidelines Use this command to configure application identifiers populated from the plugin and mark the matching flows to a custom-defined protocol (CDP) name. The SNI ruledef supports multi-line-or all-lines or default multi-line-and rule lines. The rule lines configured with "!=" operator will not be optimized.

Example

The following command configures the QUIC SNI app-identifier that is set to fb.com:

```
p2p app-identifier quic-sni = fb.com
```

active-charging service ruledef p2p protocol

Configures the protocol to match.

Privilege Security Administrator, Administrator

Syntax Description **`protocol`** *`operator protocol`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.

protocol

Specify the P2P protocol.

Must be one of the following:

- skype: P2P detection protocol for "Skype" application.
- bittorrent: P2P detection protocol for "bittorrent" application.
- edonkey: P2P detection protocol for "edonkey" application.
- msn: P2P detection protocol for "msn" application.
- yahoo: P2P detection protocol for "yahoo" application.
- orb: P2P detection protocol for "orb" application.
- gnutella: P2P detection protocol for "gnutella" application.
- jabber: P2P detection protocol for "jabber" application.
- slingbox: P2P detection protocol for "slingbox" application.
- winny: P2P detection protocol for "winny" application.
- fasttrack: P2P detection protocol for "fasttrack" application.
- manolito: P2P detection protocol for "manolito" application.
- pando: P2P detection protocol for "pando" application.
- filetopia: P2P detection protocol for "filetopia" application.
- soulseek: P2P detection protocol for "soulseek" application.
- ppstream: P2P detection protocol for "ppstream" application.
- qqlive: P2P detection protocol for "qqlive" application.
- qq: P2P detection protocol for "qq" application.
- mute: P2P detection protocol for "mute" application.
- gadugadu: P2P detection protocol for "gadugadu" application.
- feidian: P2P detection protocol for "feidian" application.
- applejuice: P2P detection protocol for "applejuice" application.
- zattoo: P2P detection protocol for "zattoo" application.
- skinny: P2P detection protocol for "skinny" application.
- sopcast: P2P detection protocol for "sopcast" application.
- ares: P2P detection protocol for "ares" application.
- directconnect: P2P detection protocol for "directconnect" application.
- imesh: P2P detection protocol for "imesh" application.
- pplive: P2P detection protocol for "pplive" application.

- oscar: P2P detection protocol for "oscar" application.
- popo: P2P detection protocol for "popo" application.
- irc: P2P detection protocol for "irc" application.
- steam: P2P detection protocol for "steam" application.
- ddlink: P2P detection protocol for "ddlink" application.
- halflife2: P2P detection protocol for "halflife2" application.
- hamachivpn: P2P detection protocol for "hamachivpn" application.
- tvants: P2P detection protocol for "tvants" application.
- tvuplayer: P2P detection protocol for "tvuplayer" application.
- uusee: P2P detection protocol for "uusee" application.
- vpnx: P2P detection protocol for "vpnx" application.
- vtun: P2P detection protocol for "vtun" application.
- winmx: P2P detection protocol for "winmx" application.
- wofwarcraft: P2P detection protocol for "wofwarcraft" application.
- xbox: P2P detection protocol for "xbox" application.
- iskoot: P2P detection protocol for "iskoot" application.
- fring: P2P detection protocol for "fring" application.
- oovoo: P2P detection protocol for "oovoo" application.
- gtalk: P2P detection protocol for "gtalk" application.
- freenet: P2P detection protocol for "freenet" application.
- aimini: P2P detection protocol for "aimini" application.
- battlefld: P2P detection protocol for "battlefld" application.
- openft: P2P detection protocol for "openft" application.
- qqgame: P2P detection protocol for "qqgame" application.
- quake: P2P detection protocol for "quake" application.
- secondlife: P2P detection protocol for "secondlife" application.
- actsync: P2P detection protocol for "actsync" application.
- nimbuzz: P2P detection protocol for "nimbuzz" application.
- iax: P2P detection protocol for "iax" application.
- paltalk: P2P detection protocol for "paltalk" application.
- warcft3: P2P detection protocol for "warcft3" application.
- rdp: P2P detection protocol for "rdp" application.

- iptv: P2P detection protocol for "iptv" application.
- pandora: P2P detection protocol for "pandora" application.
- icecast: P2P detection protocol for "icecast" application.
- kontiki: P2P detection protocol for "kontiki" application.
- meebo: P2P detection protocol for "meebo" application.
- shoutcast: P2P detection protocol for "shoutcast" application.
- truphone: P2P detection protocol for "truphone" application.
- thunder: P2P detection protocol for "thunder" application.
- armagettron: P2P detection protocol for "armagettron" application.
- blackberry: P2P detection protocol for "blackberry" application.
- citrix: P2P detection protocol for "citrix" application.
- clubpenguin: P2P detection protocol for "clubpenguin" application.
- crossfire: P2P detection protocol for "crossfire" application.
- dofus: P2P detection protocol for "dofus" application.
- fiesta: P2P detection protocol for "fiesta" application.
- florensia: P2P detection protocol for "florensia" application.
- funshion: P2P detection protocol for "funshion" application.
- guildwars: P2P detection protocol for "guildwars" application.
- isakmp: P2P detection protocol for "isakmp" application.
- maplestory: P2P detection protocol for "maplestory" application.
- mgcp: P2P detection protocol for "mgcp" application.
- octoshape: P2P detection protocol for "octoshape" application.
- off: P2P detection protocol for "off" application.
- ps3: P2P detection protocol for "ps3" application.
- rmstream: P2P detection protocol for "rmstream" application.
- rfactor: P2P detection protocol for "rfactor" application.
- splashfighter: P2P detection protocol for "splashfighter" application.
- ssdp: P2P detection protocol for "ssdp" application.
- stealthnet: P2P detection protocol for "stealthnet" application.
- stun: P2P detection protocol for "stun" application.
- teamspeak: P2P detection protocol for "teamspeak" application.
- tor: P2P detection protocol for "tor" application.

- veohtv: P2P detection protocol for "veohtv" application.
- wii: P2P detection protocol for "wii" application.
- wmstream: P2P detection protocol for "wmstream" application.
- wofkungfu: P2P detection protocol for "wofkungfu" application.
- xdcc: P2P detection protocol for "xdcc" application.
- yourfreetunnel: P2P detection protocol for "yourfreetunnel" application.
- facebook: P2P detection protocol for "facebook" application.
- gamekit: P2P detection protocol for "gamekit" application.
- facetime: P2P detection protocol for "facetime" application.
- gmail: P2P detection protocol for "gmail" application.
- itunes: P2P detection protocol for "itunes" application.
- myspace: P2P detection protocol for "myspace" application.
- teamviewer: P2P detection protocol for "teamviewer" application.
- twitter: P2P detection protocol for "twitter" application.
- viber: P2P detection protocol for "viber" application.
- antsp2p: P2P detection protocol for "antsp2p" application.
- imo: P2P detection protocol for "imo" application.
- netmotion: P2P detection protocol for "netmotion" application.
- ogg: P2P detection protocol for "ogg" application.
- openvpn: P2P detection protocol for "openvpn" application.
- quicktime: P2P detection protocol for "quicktime" application.
- spotify: P2P detection protocol for "spotify" application.
- tango: P2P detection protocol for "tango" application.
- ultrabac: P2P detection protocol for "ultrabac" application.
- usenet: P2P detection protocol for "usenet" application.
- tunnelvoice: P2P detection protocol for "tunnelvoice" application.
- scydo: P2P detection protocol for "scydo" application.
- whatsapp: P2P detection protocol for "whatsapp" application.
- flash: P2P detection protocol for "flash" application.
- mojo: P2P detection protocol for "mojo" application.
- pcanywhere: P2P detection protocol for "pcanywhere" application.
- mypeople: P2P detection protocol for "mypeople" application.

- webex: P2P detection protocol for "webex" application.
- netflix: P2P detection protocol for "netflix" application.
- implus: P2P detection protocol for "implus" application.
- ebuddy: P2P detection protocol for "ebuddy" application.
- msrp: P2P detection protocol for "msrp" application.
- ficall: P2P detection protocol for "ficall" application.
- gotomeeting: P2P detection protocol for "gotomeeting" application.
- mig33: P2P detection protocol for "mig33" application.
- comodounite: P2P detection protocol for "comodounite" application.
- goober: P2P detection protocol for "goober" application.
- iplayer: P2P detection protocol for "iplayer" application.
- operamini: P2P detection protocol for "operamini" application.
- rdt: P2P detection protocol for "rdt" application.
- kakaotalk: P2P detection protocol for "kakaotalk" application.
- nateontalk: P2P detection protocol for "" application.nateontalk
- naverline: P2P detection protocol for "naverline" application.
- callofduty: P2P detection protocol for "callofduty" application.
- thunderhs: P2P detection protocol for "thunderhs" application.
- avi: P2P detection protocol for "avi" application.
- wuala: P2P detection protocol for "wuala" application.
- wechat: P2P detection protocol for "wechat" application.
- soribada: P2P detection protocol for "soribada" application.
- icloud: P2P detection protocol for "icloud" application.
- googleplay: P2P detection protocol for "googleplay" application.
- kugou: P2P detection protocol for "kugou" application.
- instagram: P2P detection protocol for "instagram" application.
- voipdiscount: P2P detection protocol for "voipdiscount" application.
- vopium: P2P detection protocol for "vopium" application.
- plingm: P2P detection protocol for "plingm" application.
- pinterest: P2P detection protocol for "pinterest" application.
- magicjack: P2P detection protocol for "magicjack" application.
- spdy: P2P detection protocol for "spdy" application.

- amazoncloud: P2P detection protocol for "amazoncloud" application.
- smartvoip: P2P detection protocol for "smartvoip" application.
- rynga: P2P detection protocol for "rynga" application.
- icall: P2P detection protocol for "icall" application.
- actionvoip: P2P detection protocol for "actionvoip" application.
- jumblo: P2P detection protocol for "" application.jumblo
- talkatone: P2P detection protocol for "talkatone" application.
- mapi: P2P detection protocol for "mapi" application.
- imessage: P2P detection protocol for "imessage" application.
- linkedin: P2P detection protocol for "linkedin" application.
- google: P2P detection protocol for "google" application.
- poco: P2P detection protocol for "poco" application.
- ultrasurf: P2P detection protocol for "ultrasurf" application.
- snapchat: P2P detection protocol for "snapchat" application.
- truecaller: P2P detection protocol for "truecaller" application.
- cyberghost: P2P detection protocol for "cyberghost" application.
- googleplus: P2P detection protocol for "googleplus" application.
- adobeconnect: P2P detection protocol for "adobeconnect" application.
- ustream: P2P detection protocol for "ustream" application.
- siri: P2P detection protocol for "siri" application.
- softether: P2P detection protocol for "softether" application.
- sudaphone: P2P detection protocol for "sudaphone" application.
- svtplay: P2P detection protocol for "svtplay" application.
- hyves: P2P detection protocol for "hyves" application.
- silverlight: P2P detection protocol for "silverlight" application.
- blackdialer: P2P detection protocol for "blackdialer" application.
- rodi: P2P detection protocol for "rodi" application.
- skydrive: P2P detection protocol for "skydrive" application.
- vtok: P2P detection protocol for "vtok" application.
- flickr: P2P detection protocol for "flickr" application.
- kuro: P2P detection protocol for "kuro" application.
- dropbox: P2P detection protocol for "dropbox" application.

- heytell: P2P detection protocol for "heytell" application.
- bitcasa: P2P detection protocol for "bitcasa" application.
- clubbox: P2P detection protocol for "clubbox" application.
- tumblr: P2P detection protocol for "tumblr" application.
- youtube: P2P detection protocol for "youtube" application.
- voxer: P2P detection protocol for "voxer" application.
- hotspotvpn: P2P detection protocol for "hotspotvpn" application.
- baidumovie: P2P detection protocol for "baidumovie" application.
- badoo: P2P detection protocol for "badoo" application.
- vine: P2P detection protocol for "vine" application.
- yahoomail: P2P detection protocol for "yahoomail" application.
- outlook: P2P detection protocol for "outlook" application.
- monkey3: P2P detection protocol for "monkey3" application.
- foursquare: P2P detection protocol for "foursquare" application.
- jap: P2P detection protocol for "jap" application.
- applemaps: P2P detection protocol for "applemaps" application.
- regram: P2P detection protocol for "regram" application.
- bbm: P2P detection protocol for "bbm" application.
- chikka: P2P detection protocol for "chikka" application.
- box: P2P detection protocol for "box" application.
- imgur: P2P detection protocol for "imgur" application.
- oist: P2P detection protocol for "oist" application.
- vchat: P2P detection protocol for "vchat" application.
- youku: P2P detection protocol for "youku" application.
- cisco-jabber: P2P detection protocol for "cisco-jabber" application.
- waze: P2P detection protocol for "waze" application.
- hls: P2P detection protocol for "hls" application.
- lync: P2P detection protocol for "lync" application.
- path: P2P detection protocol for "path" application.
- bittorrent-sync: P2P detection protocol for "bittorrent-sync" application.
- apple-store: P2P detection protocol for "apple-store" application.
- samsung-store: P2P detection protocol for "samsung-store" application.

- blackberry-store: P2P detection protocol for "blackberry-store" application.
- igo: P2P detection protocol for "igo" application.
- mozy: P2P detection protocol for "mozy" application.
- mapfactor: P2P detection protocol for "mapfactor" application.
- opendrive: P2P detection protocol for "opendrive" application.
- windows-azure: P2P detection protocol for "windows-azure" application.
- nokia-store: P2P detection protocol for "nokia-store" application.
- windows-store: P2P detection protocol for "windows-store" application.
- navigon: P2P detection protocol for "navigon" application.
- weibo: P2P detection protocol for "weibo" application.
- hulu: P2P detection protocol for "hulu" application.
- telegram: P2P detection protocol for "telegram" application.
- didi: P2P detection protocol for "didi" application.
- xing: P2P detection protocol for "xing" application.
- kik-messenger: P2P detection protocol for "kik-messenger" application.
- friendster: P2P detection protocol for "friendster" application.
- tagged: P2P detection protocol for "tagged" application.
- idrive: P2P detection protocol for "idrive" application.
- hike-messenger: P2P detection protocol for "hike-messenger" application.
- google-music: P2P detection protocol for "google-music" application.
- apple-push: P2P detection protocol for "apple-push" application.
- google-push: P2P detection protocol for "google-push" application.
- twitch: P2P detection protocol for "twitch" application.
- rhapsody: P2P detection protocol for "rhapsody" application.
- speedtest: P2P detection protocol for "speedtest" application.
- upc-phone: P2P detection protocol for "upc-phone" application.
- iheartradio: P2P detection protocol for "iheartradio" application.
- hbogo: P2P detection protocol for "hbogo" application.
- slacker-radio: P2P detection protocol for "slacker-radio" application.
- radio-paradise: P2P detection protocol for "radio-paradise" application.
- beatport: P2P detection protocol for "beatport" application.
- soundcloud: P2P detection protocol for "soundcloud" application.

- amazonmusic: P2P detection protocol for "amazonmusic" application.
- ssl: P2P detection protocol for "ssl" application.
- slingtv: P2P detection protocol for "slingtv" application.
- vessel: P2P detection protocol for "vessel" application.
- 8tracks: P2P detection protocol for "8tracks" application.
- quic: P2P detection protocol for "quic" application.
- tunein-radio: P2P detection protocol for "tunein-radio" application.
- go90: P2P detection protocol for "go90" application.
- vudu: P2P detection protocol for "vudu" application.
- periscope: P2P detection protocol for "periscope" application.
- hbonow: P2P detection protocol for "hbonow" application.
- crackle: P2P detection protocol for "crackle" application.
- espn: P2P detection protocol for "espn" application.
- amazonvideo: P2P detection protocol for "amazonvideo" application.
- showtime: P2P detection protocol for "showtime" application.
- vevo: P2P detection protocol for "vevo" application.
- mlb: P2P detection protocol for "mlb" application.
- starz: P2P detection protocol for "starz" application.
- tmo-tv: P2P detection protocol for "tmo-tv" application.
- hgtv: P2P detection protocol for "hgtv" application.
- nbc-sports: P2P detection protocol for "nbc-sports" application.
- univision: P2P detection protocol for "univision" application.
- dish-anywhere: P2P detection protocol for "dish-anywhere" application.
- fox-sports: P2P detection protocol for "fox-sports" application.
- newsy: P2P detection protocol for "newsy" application.
- fandor: P2P detection protocol for "fandor" application.
- odnoklassniki: P2P detection protocol for "odnoklassniki" application.
- http: P2P detection protocol for "http" application.
- kidoodle: P2P detection protocol for "kidoodle" application.
- mega: P2P detection protocol for "mega" application.
- fubotv: P2P detection protocol for "fubotv" application.
- wwe: P2P detection protocol for "wwe" application.

- curiosity-stream: P2P detection protocol for "curiosity-stream" application.
- dns-tunneling: P2P detection protocol for "dns-tunneling" application.

Usage Guidelines Use this command to specify the protocol to match.

active-charging service ruledef p2p traffic-type

Configures rule expression to match the traffic type.

Privilege Security Administrator, Administrator

Syntax Description **p2p traffic-type** *operator traffic_type*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- =: Equals.

traffic_type

Specify the traffic type to match.

Must be one of the following:

- unclassified
- audio
- video
- im
- file-transfer
- voipout
- ads
- streaming-video
- streaming-audio
- tunnel

Usage Guidelines Use this command to configure the system to detect voice or non-voice P2P traffic. When the detection of a protocol is enabled then the detection of sub-type is enabled by default.

Example

The following command configures the system to detect video traffic:

```
p2p traffic-type = video
```

active-charging service ruledef rtp

Configures rule expression to match all Real-time Transport Protocol (RTP) packets.

Privilege

Security Administrator, Administrator

Syntax Description

`rtp any-match` *`operator condition`*

Usage Guidelines

Use this command to define rule expressions to match all RTP packets.

Example

The following command defines a rule expression to match all RTP packets:

```
rtp any-match = TRUE
```

active-charging service ruledef rtp any-match

Configures any-match.

Privilege

Security Administrator, Administrator

Syntax Description

`wsp any-match` *`operator condition`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

condition

Specify the condition.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Use this command to configure any match.

active-charging service ruledef rtsp

Configures rule expression to match all Real Time Streaming Protocol (RTSP) packets.

Privilege Security Administrator, Administrator

Syntax Description **`rtsp any-match`** *`operator condition`*

Usage Guidelines Use this command to define rule expressions to match all RTSP packets.

Example

The following command defines a rule expression to match all RTSP packets:

```
rtsp any-match = TRUE
```

active-charging service ruledef rtsp any-match

Configures any-match.

Privilege Security Administrator, Administrator

Syntax Description **`wsp any-match`** *`operator condition`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

condition

Specify the condition.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Use this command to configure any match.

active-charging service ruledef secure-http

Configures rule expression to match uplink (subscriber to network) HTTPS packets.

Privilege

Security Administrator, Administrator

Syntax Description

`secure-http uplink` *`operator condition`*

Usage Guidelines

Use this command to define rule expressions to match uplink HTTPS packets.

Example

The following command defines a rule expression to match all uplink HTTPS packets:

```
secure-http uplink = TRUE
```

active-charging service ruledef secure-http any-match

Configures any-match.

Privilege

Security Administrator, Administrator

Syntax Description

`wsp any-match` *`operator condition`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

condition

Specify the condition.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines

Use this command to configure any match.

active-charging service ruledef secure-http uplink

Specify HTTPS uplink packet.

Privilege Security Administrator, Administrator

Syntax Description **`uplink`**

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

condition

Specify the condition to match.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Use this command to specify the HTTPS uplink packets.

active-charging service ruledef tcp

Configures rule expression to match bit within the flag field of TCP headers.

Privilege Security Administrator, Administrator

Syntax Description **`tcp flag`** *`operator flag`*

Usage Guidelines Use this command to configure the rule expression to match bit within the flag field of TCP headers.

Example

The following command defines a rule expression to match "reset" within flag field of TCP headers:

```
tcp flag = reset
```

active-charging service ruledef tcp any-match

Configures any-match.

Privilege Security Administrator, Administrator

Syntax Description **`wsp any-match`** *`operator condition`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

condition

Specify the condition.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Use this command to configure any match.

active-charging service ruledef tcp either-port

Configures either-port.

Privilege Security Administrator, Administrator

Syntax Description **`either-port`**

Usage Guidelines Use this command to configure either-port.

active-charging service ruledef tcp either-port with-portMap-range

With port map range.

Privilege Security Administrator, Administrator

Syntax Description **`with-portMap-range`** *`operator`* **`port-map`** *`port_map_name`*

operator

Specify how to match.

Must be one of the following:

- range: In the range of.
- !range: Not in the range of.

port-map *port_map_name*

Specify the port map name.

Must be a string.

Usage Guidelines Use this command to configure with port map range.

active-charging service ruledef tcp either-port with-range

Configures operator start to-node end.

Privilege Security Administrator, Administrator

Syntax Description **with-range** *operator* **start** *start_range* **to-node end** *end_range*

operator

Specify how to match.

Must be one of the following:

- range: In the range of.
- !range: Not in the range of.

start *start_range*

Specify the start range.

Must be an integer in the range of 1-65535.

to-node

Specify the to node.

Must be one of the following:

- to

end *end_range*

Specify the end range.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure operator start to-node end.

active-charging service ruledef tcp either-port without-range

Configures without-range.

Privilege Security Administrator, Administrator

Syntax Description **`without-range`** *`operator`* **`port`** *`port_range`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- <=: Lesser than or equal to.
- !=: Does not equal.
- >=: Greater than or equal to.

port *port_range*

Specify the port range.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure without-range.

active-charging service ruledef tcp flag

Flag field of TCP headers.

Privilege Security Administrator, Administrator

Syntax Description **`flag`** *`operator flag`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.
- contains: Contains.
- !contains: Does not contain.

flag

Specify the flag to match.

Must be one of the following:

- ack
- push

- fin
- reset
- sync

Usage Guidelines Use this command to configure the Flag field of TCP headers.

active-charging service ruledef tcp state

Configures rule expression to match current state of TCP connections.

Privilege Security Administrator, Administrator

Syntax Description **`tcp state`** *`operator current_state`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- '!=': Does not equal.

current_state

Specify the state to match.

Must be one of the following:

- close
- close-wait
- closing
- established
- fin-wait1
- fin-wait2
- last-ack
- listen
- syn-received
- syn-sent
- time-wait

Usage Guidelines Use this command to define rule expressions to match a current state of TCP connections.

Example

The following command defines a rule expression to match user traffic based on current state "close":

```
tcp state = close
```

active-charging service ruledef tethering-detection

Configures rule expression to match tethered or non-tethered flows.

Privilege

Security Administrator, Administrator

Syntax Description

`tethering-detection [ application | dns-based | ip-ttl | os-ua ] { tether-flow }`

flow-opt

Specify flow options.

Must be one of the following:

- flow-tethered: If tethering is detected on flow.
- flow-not-tethered: If tethering is not detected on flow.

Usage Guidelines

Use this command to define rule expressions to match tethered/non-tethered flows. Note that in order for the rule containing the tethering-detection configuration to get matched, at least one valid rule line has to be present in it.

Example

The following command defines a rule expression to match tethered flows:

```
tethering-detection flow-tethered
```

active-charging service ruledef tethering-detection application

Configures application-based tethering detection.

Privilege

Security Administrator, Administrator

Syntax Description

`application`

flow-opt

Specify flow options.

Must be one of the following:

- flow-tethered: If tethering is detected on flow.

- flow-not-tethered: If tethering is not detected on flow.

Usage Guidelines Use this command to select flows that were tethered or non-tethered based on application-based detection solution.

active-charging service ruledef tethering-detection dns-based

Configures DNS query pattern based tethering detection.

Privilege Security Administrator, Administrator

Syntax Description `dns-based`

flow-opt

Specify flow options.

Must be one of the following:

- flow-tethered: If tethering is detected on flow.
- flow-not-tethered: If tethering is not detected on flow.

Usage Guidelines Use this command to select flows that were tethered or non-tethered based on DNS-based detection solution.

active-charging service ruledef tethering-detection ip-ttl

Configures IP-TTL based tethering detection.

Privilege Security Administrator, Administrator

Syntax Description `ip-ttl`

flow-opt

Specify flow options.

Must be one of the following:

- flow-tethered: If tethering is detected on flow.
- flow-not-tethered: If tethering is not detected on flow.

Usage Guidelines Use this command to select flows that were tethered or non-tethered as per IP-TTL values.

active-charging service ruledef tethering-detection os-ua

Configures OS-UA based tethering detection.

Privilege Security Administrator, Administrator

Syntax Description **`os-ua`**

flow-opt

Specify flow options.

Must be one of the following:

- flow-tethered: If tethering is detected on flow.
- flow-not-tethered: If tethering is not detected on flow.

Usage Guidelines Use this command to select flows that were tethered or non-tethered as per OS-UA lookups.

active-charging service ruledef udp

Configures rule expression to match all UDP packets.

Privilege Security Administrator, Administrator

Syntax Description **`udp any-match`** *`operator condition`*

Usage Guidelines Use this command to define rule expressions to match all UDP packets.

Example

The following command defines a rule expression to match all UDP packets:

```
udp any-match = TRUE
```

active-charging service ruledef udp any-match

Configures any-match.

Privilege Security Administrator, Administrator

Syntax Description **`wsp any-match`** *`operator condition`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

condition

Specify the condition.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Use this command to configure any match.

active-charging service ruledef udp either-port

Configures either-port.

Privilege Security Administrator, Administrator

Syntax Description **`either-port`**

Usage Guidelines Use this command to configure either-port.

active-charging service ruledef udp either-port with-portMap-range

With port map range.

Privilege Security Administrator, Administrator

Syntax Description **`with-portMap-range`** *`operator`* **`port-map`** *`port_map_name`*

operator

Specify how to match.

Must be one of the following:

- range: In the range of.
- !range: Not in the range of.

port-map *port_map_name*

Specify the port map name.

Must be a string.

Usage Guidelines Use this command to configure with port map range.

active-charging service ruledef udp either-port with-range

Configures operator start to-node end.

Privilege

Security Administrator, Administrator

Syntax Description

with-range *operator* **start** *start_range* **to-node end** *end_range*

operator

Specify how to match.

Must be one of the following:

- range: In the range of.
- !range: Not in the range of.

start *start_range*

Specify the start range.

Must be an integer in the range of 1-65535.

to-node

Specify the to node.

Must be one of the following:

- to

end *end_range*

Specify the end range.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to configure operator start to-node end.

active-charging service ruledef udp either-port without-range

Configures without-range.

Privilege

Security Administrator, Administrator

Syntax Description

without-range *operator* **port** *port_range*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- <=: Lesser than or equal to.
- !=: Does not equal.
- >=: Greater than or equal to.

port *port_range*

Specify the port range.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure without-range.

active-charging service ruledef wsp

Configures rule expression to match all Wireless Session Protocol (WSP) packets.

Privilege Security Administrator, Administrator

Syntax Description **`wsp any-match`** *`operator condition`*

Usage Guidelines Use this command to specify a rule expression to match all WSP packets.

Example

The following command defines a rule expression to match all WSP packets:

```
wsp any-match = TRUE
```

active-charging service ruledef wsp any-match

Configures any-match.

Privilege Security Administrator, Administrator

Syntax Description **`wsp any-match`** *`operator condition`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

condition

Specify the condition.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Use this command to configure any match.

active-charging service ruledef wtp

Configures rule expression to match all Wireless Transaction Protocol (WTP) packets.

Privilege Security Administrator, Administrator

Syntax Description **`wtp any-match`** *`operator condition`*

Usage Guidelines Use this command to define rule expressions to match all WTP packets.

Example

The following command defines a rule expression to match all WTP packets:

```
wtp any-match = TRUE
```

active-charging service ruledef wtp any-match

Configures any-match.

Privilege Security Administrator, Administrator

Syntax Description **`wsp any-match`** *`operator condition`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

condition

Specify the condition.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Use this command to configure any match.

active-charging service ruledef www

Configures rule expression to match URL for any Web protocol analyzer HTTP, WAP1.X, WAP2.0.

Privilege Security Administrator, Administrator

Syntax Description **`www url [ case-sensitive ]`** *`operator url`*

Usage Guidelines Use this command to define rule expressions to match the URL for any Web protocol analyzer HTTP, WAP1.X, WAP2.0.

Example

The following command defines a rule expression to match user traffic based on WWW URL "www.abc.com":

```
www url = www.abc.com
```

active-charging service ruledef www any-match

Configures rule expression to match all WWW packets. It is true for HTTP, WAP1.x, and WAP2.0 protocols.

Privilege Security Administrator, Administrator

Syntax Description **`www any-match`** *`operator condition`*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- =: Equals.

condition

Specify the condition to match.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Use this command to define rule expressions to match all WWW packets. This expression is true for HTTP, WAP1.x, and WAP2.0 protocols

Example

The following command defines a rule expression to match all WWW packets:

```
www any-match = TRUE
```

active-charging service ruledef www host

Configures rule expression to match the "host name" header field present in HTTP/WSP headers.

Privilege Security Administrator, Administrator

Syntax Description **`www host [ case-sensitive ]`** *`operator host_name`*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- !contains: Does not contain.
- !ends-with: Does not end with.
- !starts-with: Does not start with.
- =: Equals.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.
- regex: Regular expression.

host_name

Specify the WWW host name to match.

Must be a string.

case-sensitive

Specify that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

Usage Guidelines Use this command to define rule expressions to match the host name header field present in HTTP/WSP headers.

Example

The following command defines a rule expression to match user traffic based on WWW host name "host1":

```
www host = host1
```

active-charging service ruledef www url

Configures rule expressions to match URL.

Privilege

Security Administrator, Administrator

Syntax Description

`url`

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- !contains: Does not contain.
- !ends-with: Does not end with.
- !starts-with: Does not start with.
- =: Equals.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.
- regex: Regular expression.

url

Specify the URL to match.

Must be a string.

case-sensitive

Specify that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

Usage Guidelines

Use this command to configure the rule expressions to match URLs.

active-charging service service-scheme

Service scheme configuration, enable association of service-scheme based on triggers.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Service Scheme Configuration

Syntax Description

service-scheme *service_scheme_format_name*

service_scheme_format_name

Specify the service scheme format name.

Must be a string.

Usage Guidelines

Service scheme configuration, enable association of service-scheme based on triggers.

active-charging service service-scheme trigger

Trigger at which service-scheme need to be updated.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Service Scheme Configuration

Syntax Description

trigger *attribute*

attribute

Specify the attribute.

Must be one of the following:

- sess-setup
- nsh-response-received
- monitor-bearer-bandwidth
- loc-update
- flow-create
- bearer-creation

Usage Guidelines

Trigger at which service-scheme need to be updated.

active-charging service service-scheme trigger priority

Configures priority to the triggers in service-scheme. This priority must be unique within a trigger.

Privilege

Security Administrator, Administrator

Syntax Description

priority *priority*

priority

Specify the priority.

Must be an integer in the range of 1-127.

Usage Guidelines

Use this command to assign priority to the triggers in service-scheme. This priority must be unique within a trigger.

active-charging service service-scheme trigger priority trigger-condition

Assign trigger condition definition.

Privilege

Security Administrator, Administrator

Syntax Description

trigger-condition

name ***trigger_condition_name***

Specify the trigger condition name.

Must be a string.

trigger-action ***trigger_action***

Specify the trigger action.

Must be a string.

Usage Guidelines

Use this command to assign trigger condition definition.

active-charging service statistics-collection

Configures ruledef statistics collection.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration

Syntax Description `statistics-collection`

all

Specify to configure all stats.

Usage Guidelines Use this command to configure the ruledef statistics collection.

active-charging service statistics-collection ruledef

Configures ruledef stats collection.

Privilege Security Administrator, Administrator

Syntax Description `ruledef ruledef-option` *ruledef_option*

ruledef-option *ruledef_option*

Specify the ruledef option.

Must be one of the following:

- all
- charging
- firewall
- post-processing

Usage Guidelines Use this command to configure ruledef stats collection.

active-charging service subs-class

Configures ACS Subscriber Class configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description `subs-class` *subscriber_class_format_name*

name *subscriber_class_format_name*

Specify the subscriber class format name.

Must be a string.

Usage Guidelines Use this command to configure ACS Subscriber Class configuration.

active-charging service subs-class multi-line-or

Configures to check if the OR operator must be applied to all lines in a trigger-condition.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Subs-Class Configuration

Syntax Description

`multi-line-or all-lines`

all-lines

Applies the OR operator to all lines in the current ruledef.

Usage Guidelines

Use this command to check if the OR operator must be applied to all lines in a trigger-condition.

active-charging service subs-class rulebase

Configures rulebase name as a condition.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Subs-Class Configuration

Syntax Description

`rulebase` *`operator value`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

value

Specify the value.

Must be a string.

Usage Guidelines

Configures rulebase name as a condition.

active-charging service subscriber-base

Configures ACS subscriber base configuration.

Privilege

Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **subscriber-base** *subscriber_base_name*

subscriber_base_name

Specify thesubscriber base name.

Must be a string.

Usage Guidelines Use this command to configure ACS subscriber base configuration.

You can configure a maximum of one element with this command.

active-charging service subscriber-base priority

Assigns priority to the service-scheme association. This priority has to be unique within a subscriber-base.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Subscriber Base Configuration

Syntax Description **priority** *priority*

priority

Specify the priority to the service-scheme association.

Must be an integer in the range of 1-127.

Usage Guidelines Use this command to assign a priority to the service-scheme association. This priority must be unique within a subscriber-base.

active-charging service subscriber-base priority subs-class

Assigns subs-class definition to a subscriber base.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Subscriber Base Configuration

Syntax Description **priority** *priority* **subs-class** *subs_class_name* **bind service-scheme** *service_scheme_name*

subs_class_name

Specify the subs-class name.

Must be a string.

bind

Specify the association of service scheme with subs-class.

service-scheme *service_scheme_name*

Specify the service scheme definition.

Must be a string.

Usage Guidelines Use this command to assign subs-class definition to a subscriber base.

active-charging service tethering-database

Configures tethering detection databases.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **`tethering-database ipv6-os-signature`** *`file_name`*

ipv6-os-signature *file_name*

Specify the IPv6 OS signature database file name.

Must be a string.

os-signature *file_name*

Specify the IPv4 OS signature database file name.

Must be a string.

tac *file_name*

Specify the TAC database file name.

Must be a string.

ua-signature *file_name*

Specify the ua-signature database file name.

Must be a string.

Usage Guidelines Use this command to configure the tethering detection databases.

active-charging service tethering-detection

Enables TAC-db lookup for tethering detection.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **`tethering-detection tac-db`**

tac-db

Specify TAC-db lookup for tethering detection.

Usage Guidelines Use this command to enable TAC-db lookup for tethering detection.

active-charging service tethering-detection bypass

Configures bypass tethering detection.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **`bypass interface-id`** *`interface_id`*

interface-id *interface_id*

Specify the 64-bit interface ID from IPv6 address.

Must be a string in the pattern ([0-9a-fA-F]{2}[-]){7}([0-9a-fA-F]{2}).

Usage Guidelines Use this command to configure bypass tethering detection.

active-charging service tethering-detection dns-based nat64

Configures the NAT64 IPv6 address for DNS-based lookup for tethering detection.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **`nat64 ipv6-network-prefix`** *`ipv6_address_with_mask`*

ipv6-network-prefix *ipv6_address_with_mask*

Specify the IPv6 address with mask.

Must be IPv4 CIDR notation ##.##.##.##/x or in IPv6 CIDR notation ####:####:####:####:####:####:####:####/###.

Usage Guidelines Use this command to configure the NAT64 IPv6 address for DNS-based lookup for tethering detectionNAT64 IPv6 address.

active-charging service trigger-action

Configures Active Charging Service (ACS) trigger actions.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration

Syntax Description

trigger-action *trigger_action_name*

trigger_action_name

Specify the active-charging trigger action name.

Must be a string.

activate-predef-rule ***predefined_rule_name***

Activates predefined rule or group of rules for a trigger action. When this CLI command is configured, the dedicated bearer is created by service flow at a specific location.

Must be a string.

throttle-suppress

Enables suppressing throttling when the subscriber is in a particular LAC or TAC location. Use this command to perform throttle suppression to provide unlimited bandwidth based on the subscriber location.

service-chain ***service_chain_name***

Associates a service chain to a trigger action.

Must be a string.

Usage Guidelines

Use this command to configure ACS trigger actions.

active-charging service trigger-action charge-request-to-response http

Configures the delay charging request to response.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration

Syntax Description

charge-request-to-response http all

all

Specify delay enagagement of TRM till HTTP method responses.

Usage Guidelines Use this command to delay charging until HTTP response for the configured HTTP request method(s).

Example

The following command is configured to delay charging for all HTTP methods:

```
charge-request-to-response http all
```

active-charging service trigger-action step-down

Allows you to step down the initial configured value of committed data rate.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Action Configuration

Syntax Description **`step-down committed-data-rate`** *`negotiated_value`*

committed-data-rate *negotiated_value*

Defines the committed data rate.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to step down the initial configured value of committed data rate.

Example

The following command steps down the committed data rate by 30% of initial configured committed-data-rate value:

```
step-down committed-data-rate 30
```

active-charging service trigger-action step-up

Enables step up the initial configured value of committed data rate.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Action Configuration

Syntax Description **`step-up committed-data-rate`** *`negotiated_value`*

committed-data-rate *negotiated_value*

Specify the committed data rate.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to step up the initial configured value of committed data rate.

Example

The following command steps up the committed data rate by 20% of initial configured committed-data-rate value:

```
step-up committed-data-rate 20
```

active-charging service trigger-action transactional-rule-matching response http

Specify HTTP protocol.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Action Configuration

Syntax Description **`http`**

all

Specify to delay enagagement of TRM till HTTP method responses.

Usage Guidelines This command allows you to delay engagement of TRM till the specified HTTP response method(s) for the flow received.

Example

The following command is configured to delay engagement of TRM for all HTTP methods:

```
transactional-rule-matching response http all
```

active-charging service trigger-condition

Configures trigger-condition parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration

Syntax Description **`trigger-condition`** *`trigger_condition_name`*

trigger_condition_name

Specify the trigger condition name.

Must be a string.

Usage Guidelines Use this command to configure trigger-condition parameters.

active-charging service trigger-condition any-match

Applicable for all.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Syntax Description **any-match** *operator condition*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- !=: Does not equal.

condition

Specify the condition.

Must be one of the following:

- TRUE
- FALSE

Usage Guidelines Applicable for all.

active-charging service trigger-condition committed-data-rate

Configures the ommitted data rate of a bearer.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Syntax Description **committed-data-rate [lower-threshold** *lower_threshold* **| upper-threshold** *upper_threshold* **]**

lower-threshold *lower_threshold*

Specify the lower threshold as a percentage of the current negotiated value.

Must be an integer in the range of 1-100.

upper-threshold *upper_threshold*

Specify the upper threshold as a percentage of the current negotiated value.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure the committed data rate of a bearer.

active-charging service trigger-condition content-type

Configures content-type value to be matched.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Syntax Description **`content-type`** *`operator content_type`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.

content_type

Specify the content type.

Must be a string.

Usage Guidelines Use this command to configure the content-type value to be matched.

active-charging service trigger-condition delay

Configures delay action for configured period of time.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Syntax Description **`delay`** *`operator delay_duration`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.

delay_duration

Specify the delay in seconds.

Must be an integer in the range of 1-600.

Usage Guidelines Use this command to configure the delay action for configured period of time.

active-chargingservicetrigger-conditionflow-lengththreshold

Configures flow length threshold condition.

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Privilege Security Administrator, Administrator

Syntax Description **`flow-length exceed`**

exceed

Specify flow length threshold exceeded.

Usage Guidelines Use this command to configure the flow length threshold condition.

active-charging service trigger-condition ip protocol

Configures protocol being transported by IP packet.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Syntax Description **`protocol`** *`operator protocol`*

operator

Specify how to match.

Must be one of the following:

- =: Equals.

protocol

Specify the protocol.

Must be one of the following:

- tcp
- udp

Usage Guidelines Use this command to configure protocol being transported by IP packet.

active-charging service trigger-condition local-policy-rule

Configures the local policy rule name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Syntax Description **`local-policy-rule`**

operator

Specify how to match.

Must be one of the following:

- =: Equals.

policy_rule_name

Specify the policy rule name.

Must be a string.

Usage Guidelines Use this command to configure the local policy rule name.

active-charging service trigger-condition multi-line-or

Whether to apply the OR operator to all lines in a ruledef.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Syntax Description **`multi-line-or`**

all-lines

Specify to apply the OR operator to all lines in a ruledef.

Usage Guidelines Use this command to configure whether to apply the OR operator to all lines in a ruledef.

active-charging service trigger-condition post-processing-rule-name

Will be applicable for a particular post-processing rule.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Syntax Description **post-processing-rule-name** *operator rule_name*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- =: Equals.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.

rule_name

Specify the rule name to match.

Must be a string.

Usage Guidelines Will be applicable for a particular post-processing rule.

active-charging service trigger-condition qci

Configures QCI value.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Syntax Description **qci** *operator qci*

operator

Specify how to match.

Must be one of the following:

- =: Equals.

qci

Specify the QCI to match.

Must be an integer in the range of 1-254.

to

to

Must be a string.

Usage Guidelines Use this command to specfiy the QCI to match.

active-charging service trigger-condition rule-name

Will be applicable for a particular rule/GoR.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Syntax Description **rule-name** *operator rule_name*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- =: Equals.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.

rule_name

Specify the rule name.

Must be a string.

Usage Guidelines Will be applicable for a particular rule/GoR.

active-charging service trigger-condition tdf-appid

Configures TDF App ID value to be matched.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > ACS Configuration > Trigger Condition Configuration

Syntax Description

tdf-appid *operator tdf_appid*

operator

Specify how to match.

Must be one of the following:

- !=: Does not equal.
- =: Equals.
- contains: Contains.
- ends-with: Ends with.
- starts-with: Starts with.

tdf_appid

Specify the TDF App ID to match.

Must be a string.

Usage Guidelines

Use this command to specify the TDF App ID value to match.

active-charging service url-blacklisting

Enable URL Blacklisting functionality.

Privilege

Security Administrator, Administrator

Syntax Description

url-blacklisting

match-method *match_method*

Specify the match method to look up for URLs in the URL Blacklisting database.

Must be one of the following:

- exact
- generic

Default Value: exact.

Usage Guidelines Use this command to enable URL Blacklisting functionality.

active-charging service urr-list

Configures ACS URR list configuration.

Privilege Security Administrator, Administrator

Syntax Description **urr-list** *urr_list_name*

urr_list_name

Specify the URR list name.

Must be a string.

Usage Guidelines Use this command to configure the ACS URR list configuration. Enters ACS URR List Configuration mode. This mode allows mapping of URR-ID with Rating Group and Service-ID

You can configure a maximum of one element with this command.

active-charging service urr-list urr-list-data

Configures URR list data.

Privilege Security Administrator, Administrator

Syntax Description **urr-list-data**

rating group *group_number*

Specify the rating ID used in prepaid charging.

Must be an integer in the range of 0-2147483647.

urr-id *urr_id_range*

Specify the URR identifier for rating/service group.

Must be an integer in the range of 1-8388607.

Usage Guidelines Use this command to configure the URR list data.

active-charging service urr-list urr-list-data service-identifier

Configures the service identifier.

Privilege Security Administrator, Administrator

Syntax Description **service-identifier** *service_id*

service_id

Specify the service ID.

Must be an integer in the range of 0-2147483647.

urr-id ***urr_id_range***

Specify the URR identifier for rating/service group.

Must be an integer in the range of 1-8388607.

Usage Guidelines Use this command to configure the servoce identifier.

active-charging service xheader-format

Enables ACS x-header Format Configuration Mode. This mode is used to create and configure extension-header (x-header) formats.

Privilege Security Administrator, Administrator

Syntax Description **xheader-format** *xheader_format_name*

xheader_format_name

Specify the Xheader format name.

Must be a string.

Usage Guidelines Use this command to create/configure/delete an x-header format specification in the active charging service. Each x-header format must have a unique name.

Example

The following command creates an x-header format named test, and enters the ACS X-header Format Configuration Mode:

```
xheader-format test
```

active-charging service xheader-format insert

This command inserts xheader field.

Privilege Security Administrator, Administrator

Syntax Description **insert** *xheader_field_name*

xheader_field_name

Specify the Xheader field name.

Must be a string.

string-constant *xheader_field_value*

Specify the constant string value of xheader field to be inserted.

Must be a string.

delete-existing

Enables detection of spoofing in xheader fields, valid for Request packet.

Usage Guidelines

Use this command to configure the x-header fields to be inserted in HTTP/WSP GET and POST request packets. The x-headers would be inserted at the end of the HTTP/WSP header. This CLI command may be used up to 10 times. There is no control over the order of the fields that are to be inserted. Any of the indicated ruledef variables may be inserted using the variable option, or a static string may be inserted using the string-constant option. Operators may insert x-headers in some HTTP/WSP packets, for which some rules will be configured. The charging-action associated with these rules will contain the list of x-headers to be inserted in the packets.

You can configure a maximum of 10 elements with this command.

Example

The following command configures an x-header field named test12 with a constant string value of testing to be inserted in HTTP/WSP GET and POST request packets:

```
insert test12 string-constant testing
```

active-charging service xheader-format insert variable

Configures name of the x-header field whose value must be inserted in the packets.

Privilege

Security Administrator, Administrator

Syntax Description

`variable`

Usage Guidelines

Use this command to specify name of the x-header field whose value must be inserted in the packets.

active-charging service xheader-format insert variable bearer

Configures bearer-related configuration.

Privilege

Security Administrator, Administrator

Syntax Description

`bearer`

Usage Guidelines Use this command to configure bearer-related configuration.

active-charging service xheader-format insert variable bearer ggsn-address

GGSN IP address.

Privilege Security Administrator, Administrator

Syntax Description `ggsn-address`

Usage Guidelines Use this command to configure the GGSN IP address field.

active-charging service xheader-format insert variable bearer ggsn-address encrypt

Configures encryption of x-header field.

Privilege Security Administrator, Administrator

Syntax Description `encrypt`

Usage Guidelines Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer imsi

Specify the Mobile Station ID.

Privilege Security Administrator, Administrator

Syntax Description `imsi`

Usage Guidelines Use this command to specify the Mobile Station ID.

active-charging service xheader-format insert variable bearer imsi encrypt

Configures encryption of x-header field.

Privilege Security Administrator, Administrator

Syntax Description `encrypt`

Usage Guidelines Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer msisdn-no-cc

MSISDN of the mobile handling the flow without the country code.

Privilege Security Administrator, Administrator

Syntax Description `msisdn-no-cc`

Usage Guidelines Use this command to configure the MSISDN of the mobile handling the flow without the country code.

active-charging service xheader-format insert variable bearer msisdn-no-cc encrypt

Configures encryption of x-header field.

Privilege Security Administrator, Administrator

Syntax Description `encrypt`

Usage Guidelines Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer radius-calling-station-id

Calling Station ID of the mobile handling the flow. Use this for MSISDN of the mobile handling the flow with the country code.

Privilege Security Administrator, Administrator

Syntax Description `radius-calling-station-id`

Usage Guidelines Use this command to specify the Calling Station ID of the mobile handling the flow.

active-charging service xheader-format insert variable bearer radius-calling-station-id encrypt

Configures encryption of x-header field.

Privilege Security Administrator, Administrator

Syntax Description `encrypt`

Usage Guidelines Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer sgsn-address

Specify the SGSN associated with the bearer flow. This field is deprecated from under bearer sgsn-address and has been moved within bearer three-gpp sgsn-address. The SGSN address as added via bearer three-gpp sgsn-address.

Privilege Security Administrator, Administrator

Syntax Description `sgsn-address`

Usage Guidelines Use this command to specify the SGSN associated with the bearer flow.

active-charging service xheader-format insert variable bearer sgsn-address encrypt

Configures encryption of x-header field.

Privilege Security Administrator, Administrator

Syntax Description `encrypt`

Usage Guidelines Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer sn-rulebase

Specify the ACS rulebase.

Privilege Security Administrator, Administrator

Syntax Description `sn-rulebase`

Usage Guidelines Use this command to specify the ACS rulebase name.

active-charging service xheader-format insert variable bearer sn-rulebase encrypt

Configures encryption of x-header field.

Privilege Security Administrator, Administrator

Syntax Description `encrypt`

Usage Guidelines Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer subscriber-ip-address

Specify the subscriber IP address.

Privilege Security Administrator, Administrator

Syntax Description `subscriber-ip-address`

Usage Guidelines Use this command to specify the subscriber IP address.

active-charging service xheader-format insert variable bearer subscriber-ip-address encrypt

Configures encryption of x-header field.

Privilege Security Administrator, Administrator

Syntax Description `encrypt`

Usage Guidelines Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer three-gpp

Specify the 3GPP service to be configured.

Privilege Security Administrator, Administrator

Syntax Description **`three-gpp`**

Usage Guidelines Use this command to specify the 3GPP service to be configured.

active-charging service xheader-format insert variable bearer three-gpp charging-id

Specify charging ID of the bearer flow.

Privilege Security Administrator, Administrator

Syntax Description **`charging-id`**

Usage Guidelines Use this command to configure the charging ID of the bearer flow.

active-charging service xheader-format insert variable bearer three-gpp charging-id encrypt

Configures encryption of x-header field.

Privilege Security Administrator, Administrator

Syntax Description **`encrypt`**

value

Usage Guidelines Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer three-gpp imei

Specify IMEI or IMEISV (depending on the case) associated with the bearer flow.

Privilege Security Administrator, Administrator

Syntax Description `imei`

Usage Guidelines Use this command to specify the IMEI or IMEISV (depending on the case) associated with the bearer flow.

active-charging service xheader-format insert variable bearer three-gpp imei encrypt

Configures encryption of x-header field.

Privilege Security Administrator, Administrator

Syntax Description `encrypt`

value

Usage Guidelines Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer three-gpp imsi

Specify the Mobile Station Identification number.

Privilege Security Administrator, Administrator

Syntax Description `imsi`

Usage Guidelines Use this command to specify the Mobile Station Identification number.

active-charging service xheader-format insert variable bearer three-gpp imsi encrypt

Configures encryption of x-header field.

Privilege Security Administrator, Administrator

Syntax Description `encrypt`

value

Usage Guidelines Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer three-gpp s-mcc-mnc

Specify the 3GPP serving node MCC + MNC associated with the bearer.

Privilege Security Administrator, Administrator

Syntax Description **`s-mcc-mnc`**

Usage Guidelines Use this command to specify the 3GPP serving node MCC + MNC associated with the bearer.

active-charging service xheader-format insert variable bearer three-gpp s-mcc-mnc encrypt

Configures encryption of x-header field.

Privilege Security Administrator, Administrator

Syntax Description **`encrypt`**

value

Usage Guidelines Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer three-gpp sgsn-address

SGSN associated with the bearer flow.

Privilege Security Administrator, Administrator

Syntax Description **`sgsn-address`**

Usage Guidelines Use this command to specify the SGSN associated with the bearer flow.

active-charging service xheader-format insert variable bearer three-gpp sgsn-address encrypt

Configures encryption of x-header field.

Privilege

Security Administrator, Administrator

Syntax Description

`encrypt`

value

Usage Guidelines

Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format insert variable bearer three-gpp uli

3GPP User Location Info (ULI) associated with the bearer.

Privilege

Security Administrator, Administrator

Syntax Description

`uli`

Usage Guidelines

Use this command to specify the 3GPP ULI associated with the bearer.

active-charging service xheader-format insert variable bearer three-gpp uli encrypt

Configures encryption of x-header field.

Privilege

Security Administrator, Administrator

Syntax Description

`encrypt`

value

Usage Guidelines

Use this command to configure encryption of x-header field. This option must only be configured when x-header encryption is enabled.

active-charging service xheader-format msisdn-no-cc-length

Configures the length of msisdn-no-cc.

Privilege

Security Administrator, Administrator

Syntax Description

msisdn-no-cc-length *msisdn_no_cc_length*

msisdn_no_cc_length

Specify the msisdn-no-cc length.

Must be an integer in the range of 1-14.

Usage Guidelines

Use this command to configure the length of msisdn-no-cc.

apn

Configures Access Point Name (APN) templates.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

Syntax Description

apn *apn_name*

apn_name

Specify the APN name.

Must be a string.

Usage Guidelines

Use this command to create and configure an APN.

Example

The following command creates an APN template named isp1:

```
apn isp1
```

apn active-charging

Enables a configured ACS rulebase.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

Syntax Description **active-charging rulebase** *rulebase_name*

rulebase *rulebase_name*

Specify the rulebase name.

Must be a string.

Usage Guidelines Use this command to enable a configured ACS rulebase.

apn authorize-with-hss

Configures s6b authentication.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **authorize-with-hss [report-ipv6** *ipv6_address* **]**

Usage Guidelines Use this command to configure s6b authentication. Enables IPv6 reporting through AAR towards s6b interface.

apn authorize-with-hss egtp

Enables s6b authorization for all the interfaces of EGTP along with GN-GP Handover except 3G initial attach.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration > Redundancy Group Configuration

Syntax Description **authorize-with-hss egtp [report-ipv6]**

Usage Guidelines Use this command to enable s6b authorization for all the interfaces of EGTP along with GN-GP Handover except 3G initial attach.

apn authorize-with-hss egtp gn-gp-enabled

Enables s6b authorization for 3G initial attach and GNGP handover.

Privilege Security Administrator, Administrator

Syntax Description **gn-gp-enabled report-ipv6** *ipv6_address*

Usage Guidelines Use this command to enable s6b authorization for 3G initial attach and GNGP handover.

apn authorize-with-hss egtp s2b

Enables s6b authorization for egtp-s2b.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`authorize-with-hss egtp s2b report-ipv6-addr`**

Usage Guidelines Use this command to enable s6b authorization for egtp-s2b.

apn authorize-with-hss egtp s2b gn-gp-enabled

Enables s6b authorization for 3G initial attach and GNGP handover.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **`gn-gp-enabled report-ipv6`** *`ipv6_address`*

Usage Guidelines Use this command to enable s6b authorization for 3G initial attach and GNGP handover.

apn authorize-with-hss egtp s2b s5-s8

Enables s6b authorization for egtp-s5s8.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **`authorize-with-hss egtp s2b s5-s8 [`** *`gn_gp_option`* **`| report-ipv6-addr ]`**

Usage Guidelines Use this command to enable s6b authorization for egtp-s5s8.

apn authorize-with-hss egtp s5-s8

Enables s6b authorization for egtp-s5s8.

Privilege Security Administrator, Administrator

Syntax Description **`s5-s8`**

Usage Guidelines Use this command to enable s6b authorization for egtp-s5s8.

apn authorize-with-hss egtp s5-s8 s2b

Enables s6b authorization for egtp-s2b.

Command Modes Exec > Global Configuration > Context Configuration

Privilege Security Administrator, Administrator

Syntax Description **`s2b`**

Usage Guidelines Use this command to enable s6b authorization for egtp-s2b.

apn authorize-with-hss lma

Enables IPv6 reporting through AAR towards s6b.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`lma [ report-ipv6`** *`ipv6_address`* **`| s6b-aaa-group`** *`group_name`* **`]`**

s6b-aaa-group *group_name*

Specify the AAA group name for s6b authorization.

Must be a string.

Usage Guidelines Use this command to enable IPv6 reporting through AAR towards s6b.

apn cc-profile

Configures the subscriber charging characteristics profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`cc-profile`** *`index`* **`{ credit-control-group`** *`cc_group_name`* **`| prepaid-prohibited }`**

index

Specify the charging characterstics profile index.

Must be an integer.

-Or-

Must be one of the following:

- any

credit-control-group *cc_group_name*

Specify the credit control group name.

Must be a string.

prepaid-prohibited

Specify to disable prepaid for the configured profile index.

Usage Guidelines Use this command to configure the subscriber charging characteristics profile parameters.

apn content-filtering category

Configures Content Filtering category.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`category policy-id`** *`policy_id`*

policy-id *policy_id*

Specify the Content Filtering policy ID.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Use this command to configure Content Filtering category.

apn data-tunnel

Configures the data tunnel MTU parameter.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`data-tunnel mtu`** *`max_transmission_unit`*

mtu *max_transmission_unit*

Specify the data tunnel MTU value, in octets.

Must be an integer.

Usage Guidelines Use this command to configure the data tunnel MTU parameter.

apn gtpp group

Enables and configures the GTPP group to be used by this APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **gtpp group** *gtpp_group_name*

group *gtpp_group_name*

Specify the GTPP group name.

Must be a string.

Usage Guidelines Use this command to enable and configure the GTPP group to be used by this APN.

apn ip

Configures IP-related parameters.

Privilege Security Administrator, Administrator

Syntax Description **ip context-name** *context_name*

context-name *context_name*

Specify name of the destination context to use for subscribers accessing this APN.

Must be a string.

Usage Guidelines Use this command to configure IP-related parameters.

apn ip access-group

Configures the access group to be used by this APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **ip access-group** *access_group_name* **[in | out]**

access_group_name

Specify the access group name.

Must be a string.

in

Specify the access group as inbound.

out

Specify the access group as outbound.

Usage Guidelines Use this command to specify the access group to be used by this APN.

You can configure a maximum of eight elements with this command.

apn ip source-violation

Enables packet source validation.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`source-violation [ ignore ]`**

ignore

Specify to disable source address checking for this APN.

Usage Guidelines Use this command to enable packet source validation.

apn ppp

Configures PPP parameters for specified APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **`ppp mtu`** *`max_transmission_unit`*

mtu *max_transmission_unit*

Specify the maximum transmission unit. Default: 1500.

Must be an integer.

Usage Guidelines Use this command to configure the PPP parameters for specified APN.

apn redundancy-group

Configures redundancy group parameters.

Privilege Security Administrator, Administrator

Syntax Description **redundancy-group** *group_name*

group_name

Specify the redundancy group name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group parameters.

apn redundancy-group active-charging

Enables a configured ACS rulebase.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **active-charging rulebase** *rulebase_name*

rulebase *rulebase_name*

Specify the rulebase name.

Must be a string.

Usage Guidelines Use this command to enable a configured ACS rulebase.

apn redundancy-group authorize-with-hss

Configures s6b authentication.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **authorize-with-hss [report-ipv6** *ipv6_address* **]**

Usage Guidelines Use this command to configure s6b authentication. Enables IPv6 reporting through AAR towards s6b interface.

apn redundancy-group authorize-with-hss egtp

Enables s6b authorization for all the interfaces of EGTP along with GN-GP Handover except 3G initial attach.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration > Redundancy Group Configuration

Syntax Description **`authorize-with-hss egtp [ report-ipv6 ]`**

Usage Guidelines Use this command to enable s6b authorization for all the interfaces of EGTP along with GN-GP Handover except 3G initial attach.

apn redundancy-group authorize-with-hss egtp gn-gp-enabled

Enables s6b authorization for 3G initial attach and GNGP handover.

Privilege Security Administrator, Administrator

Syntax Description **`gn-gp-enabled report-ipv6`** *`ipv6_address`*

Usage Guidelines Use this command to enable s6b authorization for 3G initial attach and GNGP handover.

apn redundancy-group authorize-with-hss egtp s2b

Enables s6b authorization for egtp-s2b.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`authorize-with-hss egtp s2b report-ipv6-addr`**

Usage Guidelines Use this command to enable s6b authorization for egtp-s2b.

apn redundancy-group authorize-with-hss egtp s2b gn-gp-enabled

Enables s6b authorization for 3G initial attach and GNGP handover.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **`gn-gp-enabled report-ipv6`** *`ipv6_address`*

Usage Guidelines Use this command to enable s6b authorization for 3G initial attach and GNGP handover.

apn redundancy-group authorize-with-hss egtp s2b s5-s8

Enables s6b authorization for egtp-s5s8.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **authorize-with-hss egtp s2b s5-s8 [** *gn_gp_option* **| report-ipv6-addr]**

Usage Guidelines Use this command to enable s6b authorization for egtp-s5s8.

apn redundancy-group authorize-with-hss egtp s5-s8

Enables s6b authorization for egtp-s5s8.

Privilege Security Administrator, Administrator

Syntax Description **s5-s8**

Usage Guidelines Use this command to enable s6b authorization for egtp-s5s8.

apn redundancy-group authorize-with-hss egtp s5-s8 s2b

Enables s6b authorization for egtp-s2b.

Command Modes Exec > Global Configuration > Context Configuration

Privilege Security Administrator, Administrator

Syntax Description **s2b**

Usage Guidelines Use this command to enable s6b authorization for egtp-s2b.

apn redundancy-group authorize-with-hss lma

Enables IPv6 reporting through AAR towards s6b.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **lma [report-ipv6** *ipv6_address* **| s6b-aaa-group** *group_name* **]**

s6b-aaa-group *group_name*

Specify the AAA group name for s6b authorization.

Must be a string.

Usage Guidelines Use this command to enable IPv6 reporting through AAR towards s6b.

apn redundancy-group cc-profile

Configures the subscriber charging characteristics profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`cc-profile`** *`index`* **`{ credit-control-group`** *`cc_group_name`* **`| prepaid-prohibited }`**

index

Specify the charging characterstics profile index.

Must be an integer.

-Or-

Must be one of the following:

- any

credit-control-group *cc_group_name*

Specify the credit control group name.

Must be a string.

prepaid-prohibited

Specify to disable prepaid for the configured profile index.

Usage Guidelines Use this command to configure the subscriber charging characteristics profile parameters.

apn redundancy-group content-filtering category

Configures Content Filtering category.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`category policy-id`** *`policy_id`*

policy-id *policy_id*

Specify the Content Filtering policy ID.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Use this command to configure Content Filtering category.

apn redundancy-group data-tunnel

Configures the data tunnel MTU parameter.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`data-tunnel mtu`** *`max_transmission_unit`*

mtu *max_transmission_unit*

Specify the data tunnel MTU value, in octets.

Must be an integer.

Usage Guidelines Use this command to configure the data tunnel MTU parameter.

apn redundancy-group gtpp group

Enables and configures the GTPP group to be used by this APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **`gtpp group`** *`gtpp_group_name`*

group *gtpp_group_name*

Specify the GTPP group name.

Must be a string.

Usage Guidelines Use this command to enable and configure the GTPP group to be used by this APN.

apn redundancy-group ip

Configures IP-related parameters.

Privilege Security Administrator, Administrator

Syntax Description **ip context-name** *context_name*

context-name *context_name*

Specify name of the destination context to use for subscribers accessing this APN.

Must be a string.

Usage Guidelines Use this command to configure IP-related parameters.

apn redundancy-group ip access-group

Configures the access group to be used by this APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **ip access-group** *access_group_name* **[in | out]**

access_group_name

Specify the access group name.

Must be a string.

in

Specify the access group as inbound.

out

Specify the access group as outbound.

Usage Guidelines Use this command to specify the access group to be used by this APN.

You can configure a maximum of eight elements with this command.

apn redundancy-group ip source-violation

Enables packet source validation.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **source-violation [ignore]**

ignore

Specify to disable source address checking for this APN.

Usage Guidelines Use this command to enable packet source validation.

apn redundancy-group ppp

Configures PPP parameters for specified APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > APN Configuration

Syntax Description **ppp mtu** *max_transmission_unit*

mtu *max_transmission_unit*

Specify the maximum transmission unit. Default: 1500.

Must be an integer.

Usage Guidelines Use this command to configure the PPP parameters for specified APN.

apn redundancy-group timeout

Configures session timeout parameters for the current APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **timeout idle** *idle_timeout*

idle *idle_timeout*

Specify the session idle timeout period for the current APN.

Must be an integer in the range of 0-4294967295.

Usage Guidelines Use this command to configure the session timeout parameters for the current APN.

apn timeout

Configures session timeout parameters for the current APN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

Syntax Description **timeout idle** *idle_timeout*

idle *idle_timeout*

Specify the session idle timeout period for the current APN.

Must be an integer in the range of 0-4294967295.

Usage Guidelines Use this command to configure the session timeout parameters for the current APN.

clear-all

Clears all subscriber data.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `clear subscriber all [ purge { false | true } ]`

purge { false | true }

Specify whether to purge data locally.

Must be either "false" or "true".

Default Value: false.

Usage Guidelines Use this command to clear all subscriber data.

coverage

Enable or disable code coverage utilities.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `coverage container-stop` *`string`*

container-stop *string*

Specify to enable or disable code coverage utilities.

Must be a string.

Default Value: "false".

Usage Guidelines Use this command to enable or disable code coverage utilities.

echo

Enables GTP-C path management.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

`echo`

interval *echo_interval*

Specify the echo interval in seconds.

Must be an integer in the range of 60-360.

Default Value: 60.

retransmission-timeout *retransmission_timeout*

Specify the retransmission timeout period in seconds.

Must be an integer in the range of 1-20.

Default Value: 5.

max-retransmissions *max_retransmissions*

Specify the maximum number of retires for GTP echo request.

Must be an integer in the range of 0-10.

Default Value: 3.

Usage Guidelines

Use this command to enable GTP-C path management.

gtpp group

Configures GTPP group related parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

Syntax Description

`gtpp` *`gtpp_group_name`*

gtpp_group_name

Specify the GTPP group name.

Must be a string.

Usage Guidelines

Use this command to configure GTPP group related parameters.

gtpp group gtpp

Disables GTPP trigger conditions that cause either partial CDR record closure or opening of a new CDR record container. GTPP Triggers are specified in 3GPP TS 32.251 v6.6.0. All GTPP trigger changes take effect immediately, except volume-limit.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

gtpp trigger { time-limit | volume-limit }

Usage Guidelines

Use this command to disable or enable GTTP triggers that can cause partial CDR record closure or cause a new CDR to be created.

Example

The following command disables partial record closure when a configured time limit is reached:

```
gtpp trigger time-limit
```

gtpp group gtpp egcdr

Configures the eG-CDR and P-CDR (P-GW CDR) parameters and triggers.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

gtpp egcdr { service-data-flow threshold { interval *duration* **| volume { downlink** *bytes* **| uplink** *bytes* **| total** *bytes* **} } | service-idle-timeout { 0 |** *service_idle_timeout* **} }**

Usage Guidelines

Use this command to configure individual triggers for eG-CDR/P-CDR generation. Use the service-data-flow threshold option to configure the thresholds for closing a service data flow container within an eG-CDR (eG-CDRs for GGSN and P-CDRs for P-GW) during flow-based charging (FBC). A service data flow container has statistics regarding an individual content ID.

gtpp group gtpp egcdr final-record closing-cause

Configures closing cause for final EGCDR.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description `gtpp egcdr final-record closing-cause { same-in-all-partials | unique }`

unique

Specify unique closing cause for final EGCDR.

same-in-all-partials

Specify same closing cause for multiple final EGCDR(s).

Usage Guidelines Use this command to configure closing cause for final EGCDR.

gtpp group gtpp egcdr losdv-max-containers

Configures maximum number of LoSDV containers in one EGCDR.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description `losdv-max-containers` *max_containers*

max_containers

Specify the number of LOSDV containers.

Must be an integer in the range of 1-255.

Usage Guidelines Use this command to configure the maximum number of LoSDV containers in one EGCDR.

gtpp group gtpp egcdr service-data-flow threshold

Configures service data flow related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description `threshold interval` *duration*

interval *duration*

Specify the time interval, in seconds, to close the eG-CDR/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging. By default, this option is disabled.

Must be an integer in the range of 60-40000000.

Usage Guidelines Use this command to assign volume or interval values to the interim GCDRs.

gtpp group gtpp egcdr service-data-flow threshold volume

Configures the uplink/downlink volume octet counts for the generation of interim GCDRs.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

`volume { downlink` *`bytes`* **`| uplink`** *`bytes`* **`| total`** *`bytes`* **`}`**

downlink *bytes*

Specify the limit for the number of downlink octets after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

uplink *bytes*

Specify the limit for the number of uplink octets after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

total *bytes*

Specify the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

Usage Guidelines

Use this command to configure the uplink/downlink volume octet counts for the generation of interim GCDRs.

gtpp group gtpp egcdr service-idle-timeout

Enables configuration for service idle out closure of LOSDV container.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

`gtpp egcdr service-idle-timeout { zero |` *`service_idle_timeout`* **`}`**

service_idle_timeout

Specify time limit in seconds for service-idle-timeout.

Must be an integer in the range of 10-86400.

zero

Specify no service-idle-timeout trigger.

Must be one of the following:

- 0

Usage Guidelines Use this command to enable configuration for service idle out closure.

gtpp group gtpp storage-server ip-address

Configures IP address of the external GTPP storage server for storing CDRs.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **gtpp storage-server { { *ipv4_address* | *ipv6_address* } | port *port_number* }**

{ *ipv4_address* | *ipv6_address* }

Specify the IP address.

Must be IPv4 CIDR notation ##.##.##.##/x or in IPv6 CIDR notation ####:####:####:####:####:####:####:####/###.

-Or-

Must be an IP address.

port *port_number*

Specify the UDP port number that the GTPP Backup server is using.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure the IP address of the external GTPP storage server for storing CDRs.

gtpp group gtpp storage-server local

Configures storage-server local-mode configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **local aaamgr-wait-time** *aaamgr_wait_time*

aaamgr-wait-time *aaamgr_wait_time*

Specify the time in seconds that AAAmgr has to wait trying to accumlate 255 CDRs.

Must be an integer in the range of 1-300.

Default Value: 300.

Usage Guidelines Use this command to configure the storage-server local-mode configuration.

gtpp group gtpp storage-server local file

Configures GTPP file related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`file compression {`** *`file_compression`* **`| format`** *`file_format`* **`}`**

compression *file_compression*

Specify the GTPP file compression related configurations. By default, GZIP file compression is disabled.

Must be one of the following:

- gzip
- none

Default Value: "none".

format *file_format*

Specify the file format to be used for local storage.

Must be one of the following:

- custom1
- custom2
- custom3
- custom4
- custom5
- custom6
- custom7
- custom8

Default Value: "custom1".

Usage Guidelines Use this command to configure the GTPP file related parameters.

gtpp group gtpp storage-server local file name

Configures file name related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`name { format`** *`file_name_format`* **`| prefix`** *`file_name_prefix`* **`}`**

format *file_name_format*

Specify the file name format to be used.

Must be a string.

prefix *file_name_prefix*

Specify the file name prefix to be used.

Must be a string.

Usage Guidelines Use this command to configure the file name related parameters.

gtpp group gtpp trigger

Configures triggers for CDR.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`trigger { time-limit | volume-limit }`**

time-limit

When this trigger is disabled, no partial record closure occurs when the configured time limit is reached. Default: Enabled.

volume-limit

When this trigger is disabled no partial record closure occurs when volume limit is reached. Default: Enabled.

Usage Guidelines Use this command to configure triggers for CDR.

gtpp group gtpp trigger egcdr

Enables or disables and configures eGCDR-related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`egcdr max-losdv`**

max-losdv

Enable trigger for eGCDR release at MAX LoSDV containers.

Usage Guidelines Use this command to enable or disable and configure eGCDR-related parameters.

gtpp group redundancy-group

Configures redundancy group parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **redundancy-group** *group_name*

group_name

Specify the redundancy group name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group parameters.

gtpp group redundancy-group host

Configures redundancy group host parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **host** *host_name*

host_name

Specify the host name.

Must be a string.

Usage Guidelines Use this command to configure the redundancy group host parameters.

gtpp group redundancy-group host gtpp

Disables GTPP trigger conditions that cause either partial CDR record closure or opening of a new CDR record container. GTPP Triggers are specified in 3GPP TS 32.251 v6.6.0. All GTPP trigger changes take effect immediately, except volume-limit.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **gtpp trigger { time-limit | volume-limit }**

Usage Guidelines Use this command to disable or enable GTTP triggers that can cause partial CDR record closure or cause a new CDR to be created.

Example

The following command disables partial record closure when a configured time limit is reached:

```
gtpp trigger time-limit
```

gtpp group redundancy-group host gtpp egcdr

Configures the eG-CDR and P-CDR (P-GW CDR) parameters and triggers.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **gtpp egcdr { service-data-flow threshold { interval** *duration* **| volume { downlink** *bytes* **| uplink** *bytes* **| total** *bytes* **} } | service-idle-timeout { 0 |** *service_idle_timeout* **} }**

Usage Guidelines Use this command to configure individual triggers for eG-CDR/P-CDR generation. Use the service-data-flow threshold option to configure the thresholds for closing a service data flow container within an eG-CDR (eG-CDRs for GGSN and P-CDRs for P-GW) during flow-based charging (FBC). A service data flow container has statistics regarding an individual content ID.

gtpp group redundancy-group host gtpp egcdr final-record closing-cause

Configures closing cause for final EGCDR.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **gtpp egcdr final-record closing-cause { same-in-all-partials | unique }**

unique

Specify unique closing cause for final EGCDR.

same-in-all-partials

Specify same closing cause for multiple final EGCDR(s).

Usage Guidelines Use this command to configure closing cause for final EGCDR.

gtpp group redundancy-group host gtpp egcdr losdv-max-containers

Configures maximum number of LoSDV containers in one EGCDR.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`losdv-max-containers`** *`max_containers`*

max_containers

Specify the number of LOSDV containers.

Must be an integer in the range of 1-255.

Usage Guidelines Use this command to configure the maximum number of LoSDV containers in one EGCDR.

gtpp group redundancy-group host gtpp egcdr service-data-flow threshold

Configures service data flow related parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`threshold interval`** *`duration`*

interval *duration*

Specify the time interval, in seconds, to close the eG-CDR/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging. By default, this option is disabled.

Must be an integer in the range of 60-40000000.

Usage Guidelines Use this command to assign volume or interval values to the interim GCDRs.

gtpp group redundancy-group host gtpp egcdr service-data-flow threshold volume

Configures the uplink/downlink volume octet counts for the generation of interim GCDRs.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`volume { downlink`** *`bytes`* **`| uplink`** *`bytes`* **`| total`** *`bytes`* **`}`**

downlink *bytes*

Specify the limit for the number of downlink octets after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

uplink *bytes*

Specify the limit for the number of uplink octets after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

total *bytes*

Specify the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

Usage Guidelines Use this command to configure the uplink/downlink volume octet counts for the generation of interim GCDRs.

gtpp group redundancy-group host gtpp egcdr service-idle-timeout

Enables configuration for service idle out closure of LOSDV container.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description **`gtpp egcdr service-idle-timeout { zero |`** *`service_idle_timeout`* **`}`**

service_idle_timeout

Specify time limit in seconds for service-idle-timeout.

Must be an integer in the range of 10-86400.

zero

Specify no service-idle-timeout trigger.

Must be one of the following:

- 0

Usage Guidelines Use this command to enable configuration for service idle out closure.

gtpp group redundancy-group host gtpp storage-server ip-address

Configures IP address of the external GTPP storage server for storing CDRs.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

gtpp storage-server { { *ipv4_address* | *ipv6_address* } | port *port_number* }

{ ipv4_address | ipv6_address }

Specify the IP address.

Must be IPv4 CIDR notation ##.##.##.##/x or in IPv6 CIDR notation ####:####:####:####:####:####:####:####/###.

-Or-

Must be an IP address.

port *port_number*

Specify the UDP port number that the GTPP Backup server is using.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to configure the IP address of the external GTPP storage server for storing CDRs.

gtpp group redundancy-group host gtpp storage-server local

Configures storage-server local-mode configuration.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

local aaamgr-wait-time *aaamgr_wait_time*

aaamgr-wait-time *aaamgr_wait_time*

Specify the time in seconds that AAAmgr has to wait trying to accumlate 255 CDRs.

Must be an integer in the range of 1-300.

Default Value: 300.

Usage Guidelines

Use this command to configure the storage-server local-mode configuration.

gtpp group redundancy-group host gtpp storage-server local file

Configures GTPP file related parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

`file compression {` *`file_compression`* **`|`** **`format`** *`file_format`* **`}`**

compression *file_compression*

Specify the GTPP file compression related configurations. By default, GZIP file compression is disabled.

Must be one of the following:

- gzip
- none

Default Value: "none".

format *file_format*

Specify the file format to be used for local storage.

Must be one of the following:

- custom1
- custom2
- custom3
- custom4
- custom5
- custom6
- custom7
- custom8

Default Value: "custom1".

Usage Guidelines

Use this command to configure the GTPP file related parameters.

gtpp group redundancy-group host gtpp storage-server local file name

Configures file name related parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

`name { format` *`file_name_format`* **`| prefix`** *`file_name_prefix`* **`}`**

format *file_name_format*

Specify the file name format to be used.

Must be a string.

prefix *file_name_prefix*

Specify the file name prefix to be used.

Must be a string.

Usage Guidelines

Use this command to configure the file name related parameters.

gtpp group redundancy-group host gtpp trigger

Configures triggers for CDR.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

`trigger { time-limit | volume-limit }`

time-limit

When this trigger is disabled, no partial record closure occurs when the configured time limit is reached. Default: Enabled.

volume-limit

When this trigger is disabled no partial record closure occurs when volume limit is reached. Default: Enabled.

Usage Guidelines

Use this command to configure triggers for CDR.

gtpp group redundancy-group host gtpp trigger egcdr

Enables or disables and configures eGCDR-related parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Group Configuration

Syntax Description

`egcdr max-losdv`

max-losdv

Enable trigger for eGCDR release at MAX LoSDV containers.

Usage Guidelines

Use this command to enable or disable and configure eGCDR-related parameters.

heartbeat

Enables PFCP path management.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

`heartbeat { interval` *`heartbeat_interval`* **`| retransmission-timeout`** *`retransmission_timeout`* **`}`**

interval *heartbeat_interval*

Specify the heartbeat interval in seconds.

Must be an integer in the range of 60-360.

Default Value: 60.

retransmission-timeout *retransmission_timeout*

Specify the heartbeat retransmission timeout period in seconds.

Must be an integer in the range of 1-20.

Default Value: 5.

max-retransmissions *max_retransmissions*

Specify the maximum number of retries for PFCP heartbeat request.

Must be an integer in the range of 0-10.

Default Value: 3.

Usage Guidelines

Use this command to enable PFCP path management.

ipam

Clears IPAM operational data.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `clear ipam`

Usage Guidelines Use this command to clear IPAM operational data.

nrf

Configures NRF Client operational data.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `nrf`

Usage Guidelines Use this command to configure the NRF Client operational data.

nrf discovery-info

Displays discovery information.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `show discovery-info`

Usage Guidelines Use this command to view discovery information.

Must be a string.

nrf discovery-info discovery-filter

Displays NF discovery filter information.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `show discovery-filter`

Usage Guidelines Use this command to view NF discovery filter information.

Must be a string.

-Or-

Must be a string.

nrf discovery-info discovery-filter nf-discovery-profile

Displays discovery profile information.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `show nf-discovery-profile`

Usage Guidelines Use this command to view NF discovery profile information.

Must be a string.

-Or-

Must be a string.

-Or-

Must be a string.

-Or-

Must be a string.

-Or-

Must be an integer.

-Or-

Must be an integer.

-Or-

Must be an integer.

-Or-

Must be a string.

-Or-

Must be a string.

-Or-

Must be a string.

nrfdiscovery-infodiscovery-filtemf-discovery-profilenf-service

Displays NF service information.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `show nf-service`

Usage Guidelines Use this command to view NF service information.

Must be a string.

-Or-

Must be a string.

-Or-

Must be a string.

-Or-

Must be a string.

-Or-

Must be an integer.

-Or-

Must be an integer.

-Or-

Must be an integer.

-Or-

Must be a string.

-Or-

Must be a string.

nrf registration-info

Displays registration information.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `show registration-info`

Usage Guidelines Use this command to view registration information.

Must be a string.

-Or-

Must be a string.

-Or-

Must be a string.

-Or-

Must be an integer.

-Or-

Must be a string.

-Or-

Must be a string.

nrf subscription-info

Displays NF subscription information.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `show subscription-info`

Usage Guidelines Use this command to view NF subscription information.

Must be a string.

-Or-

Must be a string.

-Or-

Must be a string.

-Or-

Must be a string.

nssai

Configures the list of DNN profile names.

Privilege Administrator, Security Administrator

Command Modes Exec > Global Configuration

Syntax Description

nssai name *name* **[[dnn** *profile_names_list* **] [sst** *slice/service_type* **] [sdt slice_differentiator_type>]]**

name *slice_name*

Specify the slice name.

Must be a string.

sst *slice/service_type*

Specify the Slice/Service Type (SST).

Must be a 2-digit string in the pattern [0-9a-fA-F].

sdt *slice_differentiator_type*

Specify the Slice Differentiator Type (SDT).

Must be a 6-digit string in the pattern [0-9a-fA-F].

dnn *profile_names_list*

Specify the list of actual DNN profile names configured.

Must be a string.

Usage Guidelines

Use this command to configure the list of actual DNN profile names.

policy dnn

Configures the virtual DNN to operator DNN mapping.

Privilege

Security Administrator, Administrator

Syntax Description

dnn *policy_name* **[profile** *dnn_profile_name* **]**

dnn *policy_name*

Specify the DNN name.

Must be a string.

profile *dnn_profile_name*

Specify the DNN profile name.

Must be a string.

Usage Guidelines

Use this command to configure the virtual DNN to operator DNN mapping.

policy dnn dnn

Configures the virtual DNN to a network DNN.

Privilege

Security Administrator, Administrator

Syntax Description

dnn *dnn_name* **[profile** *dnn_profile_name* **]**

dnn *dnn_name*

Specify the DNN name.

Must be a string.

profile *dnn_profile_name*

Specify the DNN profile name.

Must be a string.

Usage Guidelines

Use this command to configure the virtual DNN to a network DNN.

policy network-capability

Configures Network Capability Policy configuration.

Privilege

Security Administrator, Administrator

Command Modes

Exec

Syntax Description

network-capability *policy_name* **[nw-support-local-address-tft { false | true }]**

policy_name

Specify the network capability policy name.

Must be a string.

nw-support-local-address-tft { false | true }

Enable or disable network support for local address in TFT.

Must be either "false" or "true".

Default Value: false.

Usage Guidelines

Use this command to configure Network Capability Policy configuration.

policy operator

Configures the operator policy configuration.

Privilege

Security Administrator, Administrator

Syntax Description

operator *policy_name*

operator *policy_name*

Specify the operator policy name.

Must be a string.

Usage Guidelines

Use this command to configure the operator policy specific configuration.

policy operator policy

Configures DNN policy parameters.

Privilege

Security Administrator, Administrator

Syntax Description

policy dnn *dnn_policy_name* **[network-capability** *network_capability* **]**

dnn *dnn_policy_name*

Specify the DNN policy name.

Must be a string.

network-capability *network_capability*

Specify the network capability.

Must be a string.

Usage Guidelines

Use this command to configure DNN policy parameters.

policy subscriber

Configures subscriber parameters.

Privilege

Security Administrator, Administrator

Syntax Description

subscriber *policy_name*

subscriber *policy_name*

Specify the subscriber policy name.

Must be a string.

Usage Guidelines Use this command to configure subscriber parameters.

policy subscriber list-entry

Configures operator policy selection match criteria definition.

Privilege Security Administrator, Administrator

Syntax Description

precedence *precedence_number* **[sst** *slice/service_type* **| sdt** *slice_differentiator_type* **| supi-start-range** *supi_start_range* **| supi-stop-range** *supi_stop_range* **| gpsi-start-range** *gpsi_start_range* **| gpsi-stop-range** *gpsi_stop_range* **| pei-start-range** *pei_start_range* **| pei-stop-range** *pei_stop_range* **| operator-policy** *operator_policy_name* **]**

precedence *precedence_number*

Specify the precedence for entry.

Must be an integer in the range of 1-512.

sst *slice/service_type*

Specify the Slice/Service Type (SST).

Must be a 2-digit string in the pattern [0-9a-fA-F].

sdt *slice_differentiator_type*

Specify the Slice Differentiator Type (SDT).

Must be a 6-digit string in the pattern [0-9a-fA-F].

supi-start-range *supi_start_range*

Specify the SUPI start range. The supi-stop-range value must be greater than the supi-start-range value.

Must be an integer in the range of 100000000000000-999999999999999.

supi-stop-range *supi_stop_range*

Specify the SUPI stop range. The supi-stop-range value must be greater than the supi-start-range value.

Must be an integer in the range of 100000000000000-999999999999999.

gpsi-start-range *gpsi_start_range*

Specify the GPSI start range. The gpsi-stop-range value must be greater than the gpsi-start-range value.

Must be an integer in the range of 1000000000-9999999999.

gpsi-stop-range *gpsi_stop_range*

Specify the GPSI stop range. The gpsi-stop-range value must be greater than the gpsi-start-range value.

Must be an integer in the range of 1000000000-9999999999.

pei-start-range *pei_start_range*

Specify the PEI start range. The pei-stop-range value must be greater than pei-start-range.

Must be an integer in the range of 100000000000000-9999999999999999.

pei-stop-range *pei_stop_range*

Specify the PEI stop range. The pei-stop-range value must be greater than pei-start-range.

Must be an integer in the range of 100000000000000-9999999999999999.

operator-policy *operator_policy_name*

Specify the operator policy to be associated with the subscriber policy.

Must be a string.

Usage Guidelines Use this command to configure operator policy selection match criteria definition.

policy subscriber list-entry serving-plmn

Configures serving PLMN parameters.

Privilege Security Administrator, Administrator

Syntax Description **serving-plmn [mcc** *mobile_country_code* **| mnc** *mobile_network_code* **| supi-start-range** *supi_start_range* **| supi-stop-range** *supi-stop-range* **| gpsi-start-range** *gpsi_start_range* **| gpsi-stop-range** *gpsi-stop-range* **| operator-policy** *operator_policy_name* **]**

mcc *mobile_country_code*

Specify the mobile country code (MCC) portion of the PLMN ID.

Must be a 3-digit integer.

mnc *mobile_network_code*

Specify the mobile network code (MNC) portion of the PLMN ID.

Must be a 2- or 3-digit integer.

Usage Guidelines Use this command to configure serving PLMN parameters.

profile

Configures the SMF NF profile that the configured Data Network Name (DNN) uses.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **profile dnn** *profile_name*

Usage Guidelines Use this command to configure the NF profile.

profile access

Configures the Access profile.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **access** *profile_name*

profile_name

Specify the Access profile name.

Must be a string.

Usage Guidelines Use this command to configure the Access profile.

profile access eps-fallback cbr

Configures Create Dedicated Bearer parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Access Profile Configuration

Syntax Description **eps-fallback cbr delay** *delay_period* **max-retry** *max_retry* **timeout** *timeout_interval*

delay_period

Specify the Create Dedicated Bearer delay time in milliseconds.

Must be an integer in the range of 0-10000.

Default Value: 0.

max-retry ***max_retry***

Specify the Create Dedicated Bearer maximum retry count.

Must be an integer in the range of 0-10.

Default Value: 0.

timeout *timeout_interval*

Specify the Create Dedicated Bearer Retry interval in seconds.

Must be an integer in the range of 1-3.

Default Value: 1.

Usage Guidelines Use this command to configure Create Dedicated Bearer parameters.

profile access eps-fallback guard

Configures handling EPS fallback expiry.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Access Profile Configuration

Syntax Description **eps-fallback guard timeout** *eps_fallback_timer*

eps_fallback_timer

Specify the EPS fallback guard timer in milliseconds.

Must be an integer in the range of 500-15000.

Default Value: 10000.

Usage Guidelines Use this command to configure handling EPS fallback expiry.

profile access gtpc

Configures the GTPC Failure profile.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **gtpc gtpc-failure-profile** *profile_name*

gtpc-failure-profile *profile_name*

Specify the GTPC Failure profile name.

Usage Guidelines Use this command to configure the GTPC Failure profile.

profile access n1 t3591-pdu-mod-cmd

Configures the n1 timer t3591 - PDU Session Modify Command Retransmission Timer.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **t3591-pdu-mod-cmd { timeout** *timeout_period* **| max-retry** *max_retries* **}**

timeout *timeout_period*

Specify the PDU Modify Command timer in seconds.

Must be an integer in the range of 1-16.

Default Value: 4.

max-retry *max_retries*

Specify the PDU Modify Command maximum retry count.

Must be an integer in the range of 0-10.

Default Value: 4.

Usage Guidelines Use this command to configure the n1 timer t3591 - PDU Session Modify Command Retransmission Timer.

profile access n1 t3592-pdu-rel-cmd

Configures the n1 timer t3592 - PDU Sess Rel Command retransmission timer for cause 39 - retransmission required.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **t3592-pdu-rel-cmd { timeout** *timeout* **| max-retry** *max_retry* **}**

timeout *timeout*

Specify the PDU Release Command timer in seconds for cause 39.

Must be an integer in the range of 1-16.

Default Value: 4.

max-retry *max_retry*

Specify the PDU Release Command Max Retry Count.

Must be an integer in the range of 0-10.

Default Value: 4.

Usage Guidelines Use this command to configure the n1 timer t3592 - PDU Sess Rel Command retransmission timer for cause 39 - retransmission required.

profile access n2 idft

Configures n2 indirect forwarding tunnel support.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

`idft { enable | timeout` *`idft_timeout`* **`}`**

enable

Specify to enable IDFT support.

timeout *idft_timeout*

Specify the IDFT timeout period in seconds.

Must be an integer in the range of 15-60.

Usage Guidelines

Use this command to configure n2 indirect forwarding tunnel support.

profile access n26 idft

Configures the N26 indirect forwarding tunnel support parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Access Profile Configuration

Syntax Description

`n26 idft enable timeout` *`idft_timeout`*

enable

Specify to enable IDFT support.

timeout *idft_timeout*

Specify the IDFT timeout period in seconds.

Must be an integer in the range of 15-60.

Usage Guidelines

Use this command to configure the N26 indirect forwarding tunnel support parameters.

profile charging

Configures the charging profile.

Privilege

Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`profile charging`** *`profile_name`*

profile_name

Specify the charging profile configuration.

Must be a string.

method *charging_method*

Specify the charging method. Default Value: none.

Must be one of the following:

- online
- offline
- none

offline-interim-timer *timer_duration*

Specify the offline interim timer duration in seconds.

Must be an integer.

Default Value: 60.

max-charging-condition *max_changes*

Specify the maximum number of charging condition changes.

Must be an integer in the range of 0-500.

Default Value: 20.

tight-interworking-mode

Specify to enable or disable tight interworking mode for online/offline charging methods.

Must be either "false" or "true".

Default Value: false.

max-deferred-urr *max_deferred_urr*

Specify the maximum number of deferred USU containers.

Must be an integer in the range of 1-200.

Default Value: 50.

metering-method *metering_method*

Specify the parameters to be metered.

Must be one of the following:

- duration
- volume
- duration-volume

Default Value: duration-volume.

Usage Guidelines Use this command to configure the charging profile.

profile charging limit

Configures the duration and volume thresholds.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Charging Profile Configuration

Syntax Description **`limit { duration | volume }`**

volume *volume_threshold*

Specify the volume threshold for charging.

Must be an integer.

duration *duration_threshold*

Specify the duration threshold for charging.

Must be an integer.

Usage Guidelines Use this command to configure the duration and volume thresholds.

profile charging limit rating-group

Configures the rating group volume and duration thresholds.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Charging Profile Configuration

Syntax Description **`limit rating-group { duration`** *`duration_threshold`* **`| volume`** *`volume_threshold`* **`}`**

volume *volume_threshold*

Specify the volume threshold for charging.

Must be an integer.

duration *duration_threshold*

Specify the duration threshold for charging.

Must be an integer.

Usage Guidelines Use this command to configure the rating group duration and volume thresholds.

profile charging quota

Configures the charging quota parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`quota request`** *`request_quota`*

request *request_quota*

Specify the request quota from CHF.

Must be one of the following:

- always
- standard

Default Value: standard.

Usage Guidelines Use this command to configure the charging quota parameters.

profile charging quota suppress

Configures the list of triggers to be suppressed.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`suppress triggers`** *`triggers_to_suppress`*

triggers *triggers_to_suppress*

Specify the list of triggers to be suppressed.

Must be one of the following:

- qht

Usage Guidelines Use this command to configure the list of triggers to be suppressed.

profile charging reporting-level

Configures the usage reporting level to be used if not sent by the PCF.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Charging Profile Configuration

Syntax Description

`reporting-level { online` *`reporting_level`* **`| offline`** *`reporting_level`* **`}`**

online *reporting_level*

Specify the reporting level configuration for online.

Must be one of the following:

- rating-group
- service-id

Default Value: rating-group.

offline *reporting_level*

Specify the reporting level configuration for offline.

Must be one of the following:

- rating-group
- service-id

Default Value: rating-group.

Usage Guidelines

Use this command to configure the usage reporting level to be used if not sent by the PCF.

profile charging requested-service-unit

Configures the Requested Service Unit time parameter.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Charging Profile Configuration

Syntax Description

`requested-service-unit time` *`rsu_time`*

time *rsu_time*

Specify the Requested Service Unit time value in seconds.

Must be an integer in the range of 1-4000000000.

Usage Guidelines Use this command to configure the Requested Service Unit time parameter.

profile charging requested-service-unit volume

Configures the Requested Service Unit volume parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Charging Profile Configuration

Syntax Description **requested-service-unit volume { uplink** *uplink_volume* **| downlink** *downlink_volume* **| total** *total_volume* **}**

uplink *uplink_volume*

Specify the uplink volume in bytes.

Must be an integer in the range of 1-4000000000.

downlink *downlink_volume*

Specify the downlink volume in bytes.

Must be an integer in the range of 1-4000000000.

total *total_volume*

Specify the total volume in bytes.

Must be an integer in the range of 1-4000000000.

Usage Guidelines Use this command to configure the Requested Service Unit volume parameters.

profile charging tariff-time-change

Configures timestamps for tariff-time change.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **tariff-time-change hour** *hour* **minute** *minute*

minute *minute*

Specify the minute timestamp for tariff-time change.

Must be an integer in the range of 0-59.

hour *hour*

Specify the hour timestamp for tariff-time change.

Must be an integer in the range of 0-23.

Usage Guidelines Use this command to configure timestamps for tariff-time change.

profile charging triggers

Configures the list of triggers.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Charging Profile Configuration

Syntax Description **`triggers session`** *`trigger`*

session *trigger*

Specify the list of session-level triggers.

Must be one of the following:

- ambr-change
- qos-change
- serv-node-change
- ue-pra-change
- 3gpp-ps-change
- tarrif-time-change
- max-number-of-changes-in-charging-conditions
- user-loc-change
- ue-time-change
- plmn-change
- rat-change
- upf-add
- upf-rem

Usage Guidelines Use this command to configure the list of triggers.

profile charging-characteristics

Configures the charging characteristics profile.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **charging-characteristics** *cc_profile_name* **[charging-profile** *charging_profile_name* **]**

cc_profile_name

Specify the charging characteristics profile name. For example, 1, 2, 3, 12, 14, till 16.

Must be an integer.

charging-profile ***charging_profile_name***

Specify the charging profile name.

Must be a string.

Usage Guidelines Use this command to configure the charging characteristics profile.

profile charging-characteristics network-element-profile-list

Configures the network elements profile list.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Charging Characteristics Profile Configuration

Syntax Description **network-element-profile-list chf** *charging_server*

chf ***charging_server***

Specify the list of charging servers.

Must be a string.

Usage Guidelines Use this command to configure the network elements profile list.

profile compliance

Configures 3GPP compliance configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **compliance** *profile_name*

profile_name

Specify the compliance profile name.

Must be a string.

Usage Guidelines Use this command to configure the 3GPP compliance configuration.

profile compliance service

Configures the SMF service names. The service names are specified in 3GPPTS 29.510 V15.2.0, Section 6.1.6.3.11.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **service** *service_name*

service_name

Specify the service names.

Must be one of the following:

- nsmf-pdusession
- namf-comm
- n1
- n2
- nudm-sdm
- nudm-uecm
- nnrf-disc
- nnrf-nfm
- npcf-smpolicycontrol
- nchf-convergedcharging
- threegpp23502

Usage Guidelines Use this command to configure the SMF service names.

profile compliance service n1-version

Configures the 3GPP n1 specification version number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **n1-version spec** *3gpp_spec_version*

uri *version_uri*

Specify the version URI.

Must be a string in the pattern v\d.

full *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string in the pattern \d+.\d+.\d+^?(.alpha-\d+)?.

spec *3gpp_spec_version*

Specify the 3GPP n1 specification version number.

Must be one of the following:

- 15.2.0
- 15.4.0

Default Value: "15.2.0".

Usage Guidelines Use this command to configure the 3GPP n1 specification version number.

profile compliance service n2-version

Configures the 3GPP n2 service specification version number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Compliance Profile Configuration

Syntax Description **n2-version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **}**

uri *version_uri*

Specify the version URI.

Must be a string in the pattern v\d.

full *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string in the pattern \d+.\d+.\d+^?(.alpha-\d+)?.

spec *3gpp_spec_version*

Specify the 3GPP n2 service specification version number.

Must be one of the following:

- 15.0.0
- 15.2.0
- 15.4.0

Default Value: "15.0.0".

Usage Guidelines Use this command to configure the 3GPP n2 service specification version number.

profile compliance service namf-version

Configures the 3GPP namf-comm specification version number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Compliance Profile Configuration

Syntax Description **`service namf-comm version { full`** *`full_version`* **`| spec`** *`3gpp_spec_version`* **`| uri`** *`version_uri`* **`}`**

uri *version_uri*

Specify the version URI.

Must be a string in the pattern v\d.

full *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string in the pattern \d+.\d+.\d+^?(.alpha-\d+)?.

spec *3gpp_spec_version*

Specify the 3GPP namf-comm specification version number.

Must be one of the following:

- 15.0.0
- 15.2.0
- 15.4.0

Default Value: "15.0.0".

Usage Guidelines Use this command to configure the 3GPP namf-comm specification version number.

profile compliance service nchf-version

Configures the 3GPP nchf-convergedcharging service specification version number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Compliance Profile Configuration

Syntax Description **service nchf-convergedcharging version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **}**

uri *version_uri*

Specify the version URI.

Must be a string in the pattern v\d.

full *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string in the pattern \d+.\d+.\d+^?(.alpha-\d+)?.

spec *3gpp_spec_version*

Specify the 3GPP nchf-convergedcharging service specification version number.

Must be one of the following:

- 15.0.0
- 15.1.0
- 15.2.1
- 15.3.0

Default Value: "15.0.0".

Usage Guidelines Use this command to configure the 3GPP nchf-convergedcharging service specification version number.

profile compliance service nnrf-disc-version

Configures the 3gpp nnrf-disc service specification version number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Compliance Profile Configuration

Syntax Description **service nnrf-disc version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **}**

uri *version_uri*

Specify the version URI.

Must be a string in the pattern v\d.

full *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string in the pattern \d+.\d+.\d+^?(.alpha-\d+)?.

spec *3gpp_spec_version*

Specify the 3gpp nnrf-disc service specification version number.

Must be one of the following:

- 15.0.0
- 15.2.0
- 15.4.0

Default Value: "15.2.0".

Usage Guidelines Use this command to configure the 3GPP nnrf-disc service specification version number.

profile compliance service nnrf-nfm-version

Configures the 3GPP nnrf-nfm service specification version number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Compliance Profile Configuration

Syntax Description **`service nnrf-nfm version { full`** *`full_version`* **`| spec`** *`3gpp_spec_version`* **`| uri`** *`version_uri`* **`}`**

uri *version_uri*

Specify the version URI.

Must be a string in the pattern v\d.

full *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string in the pattern \d+.\d+.\d+^?(.alpha-\d+)?.

spec *3gpp_spec_version*

Specify the 3GPP nnrf-nfm service specification version number.

Must be one of the following:

- 15.0.0
- 15.2.0
- 15.4.0

Default Value: "15.2.0".

Usage Guidelines Use this command to configure the 3GPP nnrf-nfm service specification version number.

profile compliance service npcf-version

Configures the 3GPP npcf-smpolicycontrol service specification version number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Compliance Profile Configuration

Syntax Description **version npcf-smpolicycontrol version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **}**

uri *version_uri*

Specify the version URI.

Must be a string in the pattern v\d.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string in the pattern \d+.\d+.\d+^?(.alpha-\d+)?.

spec *3gpp_spec_version*

Specify the 3GPP npcf-smpolicycontrol service specification version number.

Must be one of the following:

- 15.0.0
- 15.2.0
- 15.4.0

Default Value: "15.2.0".

Usage Guidelines Use this command to configure the 3GPP npcf-smpolicycontrol service specification version number.

profile compliance service nsmf-version

Configures the 3GPP nsmf-pdusession specification version number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Compliance Profile configuration

Syntax Description **service nsmf-version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **}**

uri *version_uri*

Specify the version URI.

Must be a string in the pattern v\d.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string in the pattern \d+.\d+.\d+^?(.alpha-\d+)?.

spec *3gpp_spec_version*

Specify the 3GPP nsmf-pdusession specification version number.

Must be one of the following:

- 15.0.0
- 15.2.0
- 15.4.0

Default Value: "15.0.0".

Usage Guidelines Use this command to configure the 3GPP nsmf-pdusession specification version number.

profile compliance service nudm-sdm-version

Configures the 3GPP nudm-sdm service specification version number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Compliance Profile Configuration

Syntax Description **service nudm-sdm version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **}**

uri *version_uri*

Specify the version URI.

Must be a string in the pattern v\d.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string in the pattern \d+.\d+.\d+^?(.alpha-\d+)?.

spec *3gpp_spec_version*

Specify the 3GPP nudm-sdm service specification version number.

Must be one of the following:

- 15.1.0
- 15.2.1
- 15.4.0

Default Value: "15.2.1".

Usage Guidelines Use this command to configure the 3GPP nudm-sdm service specification version number.

profile compliance service nudm-uecm-version

Configures the 3GPP nudm-uecm service specification version number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Compliance Profile Configuration

Syntax Description **service nudm-uecm version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **}**

uri *version_uri*

Specify the version URI.

Must be a string in the pattern v\d.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string in the pattern \d+.\d+.\d+^?(.alpha-\d+)?.

spec *3gpp_spec_version*

Specify the 3GPP nudm-uecm service specification version number.

Must be one of the following:

- 15.1.0
- 15.2.1
- 15.4.0

Default Value: "15.2.1".

Usage Guidelines Use this command to configure the 3GPP nudm-uecm service specification version number.

profile compliance service threegpp23502-version

Configures the 3GPP 23.502 Stage-2 5GS specification version number.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Compliance Profile Configuration

Syntax Description

service threegpp23502 version { full *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **}**

uri *version_uri*

Specify the version URI.

Must be a string in the pattern v\d.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string in the pattern \d+.\d+.\d+^?(.alpha-\d+)?.

spec *3gpp_spec_version*

Specify the 3GPP 23.502 Stage-2 5GS specification version number.

Must be one of the following:

- 15.4.0
- 15.6.0

Default Value: "15.4.0".

Usage Guidelines

Use this command to configure the 3GPP 23.502 Stage-2 5GS specification version number.

profile dnn

Configures DNN profile.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

profile dnn *profile_name* **[always-on { false | true } | charging-profile** *profile_name* **| dcnr { false | true } | pcscf-profile** *profile_name* **| ppd-profile** *profile_name* **| qos-profile** *qos_profile* **| userplane-inactivity-timer | virtual-mac** *mac_address* **| wps-profile** *profile_name* **]**

dnn *profile_name*

Specify the DNN profile name.

Must be a string.

charging-profile *profile_name*

Specify the charging profile name.

Must be a string.

virtual-mac *mac_address*

Specify the remote virtual MAC address used to generate interface ID for UE.

Must be a 17-digit string in the pattern [0-9a-fA-F:-].

Default Value: "00:14:22:01:23:45".

pcscf-profile *profile_name*

Specify the P-CSCF profile association.

Must be a string.

ppd-profile *profile_name*

Specify the Paging-Policy differentition.

Must be a string.

wps-profile *profile_name*

Specify the Wireless Priority Service (WPS).

Must be a string.

qos-profile *qos_profile*

Specify the QoS Profile configuration.

Must be a string.

always-on { false | true }

Specify to enable or disable Always On PDU session.

Must be either "false" or "true".

Default Value: false.

dcnr { false | true }

Specify to enable or disable support for dual connectivity with new radio.

Must be either "false" or "true".

Default Value: false.

userplane-inactivity-timer

Specify the user plane inactivity timer in seconds.

Must be an integer in the range of 0-86400.

Default Value: 0.

Usage Guidelines Use this command to configure the DNN profile. The CLI prompt changes to the DNN Profile Configuration mode.

profile dnn authentication secondary

Configures the secondary authentication method.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > DNN Profile Configuration

Syntax Description `authentication secondary radius`

radius

Specify to use RADIUS as secondary authentication method.

Usage Guidelines Use this command to configure the secondary authentication method.

profile dnn authorization

Configures authorization method.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > DNN Profile Configuration

Syntax Description `authorization local`

local

Specify to use local policy configuration.

Usage Guidelines Use this command to configure the authorization method.

profile dnn dnn

Configures a Virtual DNN profile under a DNN profile and NF user list.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > DNN Profile Configuration

Syntax Description **dnn** *profile_name* **network-function-list** *network_function_list*

Usage Guidelines Use this command to configure a DNN profile that is used to map a UE-requested DNN to a Virtual DNN. The SMF sends "Mapped" DNNs for configured network functions and "UE-requested" DNNs for other network functions. The UE-requested DNN is always sent on the N1 interface.

Example

The following command configures a DNN profile named "testdnn" and the network interface as "upf":

```
dnn testdnn network-function-list upf
```

profile dnn dnn nw-fu-conf

Configures network function parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **nw-fu-conf { nwfunc-dnn** *dnn_name* **| network-function-list** *nf_list* **}**

nwfunc-dnn *dnn_name*

Specify the DNN name.

Must be a string.

network-function-list *nf_list*

Specify the list of network functions that the selected DNN profile will be sent. The list of network functions supported are CHF, PCF, and UPF.

Must be a string.

Usage Guidelines Use this command to configure the network function parameters.

profile dnn dnn rmgr-conf

Configures the RMGR parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **rmgr-conf rmgr** *rmgr_nf*

rmgr *rmgr_nf*

Specify the RMGR Network Function.

Must be a string.

Usage Guidelines Use this command to configure the RMGR parameters.

profile dnn dns

Configures the DNS server details.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **dns { primary { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | secondary { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} }**

Usage Guidelines Use this command to configure the DNS server details.

profile dnn dns primary

Configures the primary DNS server details.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > DNN Profile Configuration

Syntax Description **dns primary { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **}**

ipv4 *ipv4_address*

Specify the primary DNS server's ipv4 address.

Must be an IPv4 address.

ipv6 *ipv6_address*

Specify the primary DNS server's ipv6 address.

Must be an IPv6 address.

Usage Guidelines Use this command to configure the primary DNS server details.

profile dnn dns secondary

Configures the secondary DNS server details.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > DNN Profile Configuration

Syntax Description **dns secondary { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **}**

ipv4 ***ipv4_address***

Specify the secondary DNS server's ipv4 address.

Must be an IPv4 address.

ipv6 ***ipv6_address***

Specify the secondary DNS server's ipv6 address.

Must be an IPv6 address.

Usage Guidelines Use this command to configure the secondary DNS server details.

profile dnn network-element-profiles

Configures network element profiles.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > DNN Profile Configuration

Syntax Description **profile dnn** *dnn_name* **network-element-profiles { amf | chf | pcf | udm }** *profile_name*

chf ***profile_name***

Specify the CHF network element profile name.

Must be a string.

amf ***profile_name***

Specify the AMF network element profile name.

Must be a string.

pcf ***profile_name***

Specify the PCF network element profile name.

Must be a string.

udm ***profile_name***

Specify the UDM network element profile name.

Must be a string.

Usage Guidelines Use this command to configure network element profiles.

profile dnn nssai

Configures the default NSSAI configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **nssai**

sst *slice/service_type*

Specify the S-NSSAI Slice/Service Type (SST).

Must be an integer in the range of 0-255.

sd *slice_differentiator*

Specify the S-NSSAI Slice Differentiator (SD).

Must be a 6-digit string in the pattern [0-9a-fA-F].

Usage Guidelines Use this command to configure the default NSSAI configuration.

profile dnn session type

Configures the PDU session type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > DNN Profile Configuration

Syntax Description **session type** *default_session_type* **[allowed** *allowed_session_type* **]**

type *default_session_type*

Specify the default session type.

Must be one of the following:

- IPV4
- IPV6
- IPV4V6

allowed *allowed_session_type*

Specify the SMF allowed session types. Up to two allowed session types can be configured in addition to the default session type. The same session type cannot be configured both as allowed and default.

Must be one of the following:

- IPV4
- IPV6
- IPV4V6

Usage Guidelines Use this command to configure the PDU session type.

You can configure a maximum of two elements with this command.

profile dnn ssc-mode

Configures Session and Service Continuity (SSC) Mode parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > DNN Profile Configuration

Syntax Description **`ssc-mode`** *`default_ssc_mode`* **`[ allowed`** *`allowed_ssc_mode`* **`]`**

default_ssc_mode

Specify the default SSC mode.

Must be one of the following:

- 1
- 2
- 3

allowed *allowed_ssc_mode*

Specify the allowed SSC Modes. Up to two allowed modes can be configured in addition to the default SSC mode. The same SSC mode cannot be configured both as allowed and default.

Must be one of the following:

- 1
- 2
- 3

Usage Guidelines Use this command to configure SSC mode parameters.

You can configure a maximum of two elements with this command.

profile dnn timeout

Configures session time-to-live (TTL) configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > DNN Profile Configuration

Syntax Description **`timeout { absolute`** *`max_duration`* **`| idle-only { false | true } }`**

absolute *max_duration*

Specify the maximum duration of the session in seconds, before the system automatically terminates the session. Value of 0 disables the function.

Must be an integer in the range of 0-2147483647.

Default Value: 0.

idle-only { false | true }

Specify whether to terminate only idle sessions.

Must be either "false" or "true".

Default Value: false.

Usage Guidelines Use this command to configure session time-to-live (TTL) configuration.

profile dnn upf

Configures the UPF APN profile.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > DNN Profile Configuration

Syntax Description **`upf apn`** *`apn_name`*

apn *apn_name*

Specify the APN name.

Must be a string.

Usage Guidelines Use this command to configure the UPF APN profile.

profile dns-proxy

Configures DNS proxy parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > DNN Profile Configuration

Syntax Description **dns-proxy**

query-type *query_type*

Specify the DNS query type.

Must be one of the following:

- ipv4
- ipv6
- ipv4-ipv6

Default Value: ipv4.

timeout *dns_timeout*

Specify the DNS timeout.

Must be an integer.

Default Value: 500.

cache-ttl *ttl*

Specify the TTL value of DNS responses in cache, in seconds.

Must be an integer in the range of 60-86400.

round-robin-answers

Specify to enable round-robin address fetch.

Usage Guidelines Use this command to configure DNS proxy parameters.

profile dns-proxy servers

Configures DNS server parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **servers** *dns_server_name* **[ip** *ip_address* **| port** *port_number* **| protocol** *protocol* **| priority** *priority* **]**

dns_server_name

Specify the name of the DNS server.

Must be a string.

ip *ip_address*

Specify the IP address of the DNS server.

Must be an IP address.

port *port_number*

Specify the port number of the DNS server.

Must be an integer in the range of 1-65535.

protocol *protocol*

Specify the protocol type for the DNS server.

Must be one of the following:

- udp
- tcp

Default Value: tcp.

priority *priority*

Specify the priority for the DNS server.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure the DNS server parameters.

profile ecgi-group

Configures ECGI Group profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`ecgi-group`** *`profile_name`*

profile_name

Specify the ECGI Group profile name.

Must be a string.

Usage Guidelines Use this command to configure ECGI Group profile parameters.

profile ecgi-group ecgis

Configures the list of MCC, MNC, TAC, and ECGI groups.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

ecgis { mcc *mobile_country_code* **| mnc** *mobile_network_code* **| tac** *tracking_area_code* **}**

mcc *mobile_country_code*

Specify the Mobile Country Code (MCC). For example, 01, 001.

Must be a 3-digit integer.

mnc *mobile_network_code*

Specify the Mobile Network Code (MNC). For example, 23, 456.

Must be a 2- or 3-digit integer.

tac *tracking_area_code*

Specify the Tracking Area Code (TAC). For example, A1a2, AaBbF1.

Must be a 4-digit string in the pattern [0-9a-fA-F], or a 6-digit string in the pattern [0-9a-fA-F].

Usage Guidelines

Use this command to configure the list of MCC, MNC, TAC, and ECGI groups.

You can configure a maximum of 16 elements with this command.

profile ecgi-group ecgis ecgi

Configures ECGI group parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

ecgi list *ecgi_values*

ecgi_values

Specify the list of ECGI values.

Must be a 7-digit string in the pattern [0-9a-fA-F].

Usage Guidelines

Use this command to configure ECGI group parameters.

You can configure a maximum of 64 elements with this command.

profile ecgi-group ecgis ecgi range

Configures an ECGI range.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

range start *ecgi_range_start* **end** *ecgi_range_end*

start *ecgi_range_start*

Specify the ECGI range start value.

Must be a 7-digit string in the pattern [0-9a-fA-F].

end *ecgi_range_end*

Specify the ECGI range end value.

Must be a 7-digit string in the pattern [0-9a-fA-F].

Usage Guidelines

Use this command to configure an ECGI range.

You can configure a maximum of 64 elements with this command.

profile emergency-profile

Configures Emergency profile parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

emergency-profile *profile_name* **[udm-profile** *profile_name* **]**

profile_name

Specify the Emergency profile name.

Must be a string.

udm-profile *profile_name*

Specify the UDM profile name.

Must be a string.

Usage Guidelines

Use this command to configure Emergency profile parameters.

profile failure-handling

Configures the Failure Handling profile.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **failure-handling** *profile_name*

profile_name

Specify the Failure Handling profile name.

Must be a string.

Usage Guidelines Use this command to configure the Failure Handling profile.

profile failure-handling interface gtpc message

Configures GTPC failure-handling template message types.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Failure Handling Profile Configuration

Syntax Description **interface gtpc message** *message_type*

message_type

Specify the message type.

Must be one of the following:

- S5S8CreateBearerReq
- S5S8UpdateBearerReq
- S5S8DeleteBearerReq

Usage Guidelines Use this command to configure GTPC failure-handling template message types.

profilefailure-handlinginterfacegtpcmessagecause-code-type cause-code

Configures GTPC interface cause-code types.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Failure Handling Profile Configuration

Syntax Description **cause-code** *cause_code_type*

cause_code_type

Specify the cause code type.

Must be one of the following:

- temp-fail

Usage Guidelines Use this command to configure GTPC interface cause-code types.

profilefailure-handlinginterfacegtpcmessagecause-code-type cause-code action

Configures the action type for the cause.

Privilege Security Administrator, Administrator

Syntax Description **action** *action_type* **[timeout** *retry_interval* **| max-retry** *max_retry* **]**

action_type

Specify the action type for the cause.

Must be one of the following:

- retry
- clear
- terminate

timeout *retry_interval*

Specify the retry interval in milliseconds.

Must be an integer in the range of 1000-5000.

Default Value: 1000.

max-retry *max_retry*

Specify the maximum retry count.

Must be an integer in the range of 0-5.

Default Value: 1.

Usage Guidelines Use this command to configure the action type for the cause.

profile failure-handling interface n11

Configures the N11 interface - SMF/PGW-C timer for reattempting bearer creation/updation.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **n11 message** *message_types message_type*

Usage Guidelines Use this command to configure the N11 interface - SMF/PGW-C timer for reattempting bearer creation/updation.

profile failure-handling interface n11 message

Configures N11 message types.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **message** *message_type*

message_type

Specify the message type.

Must be one of the following:

- n1n2transfer

Usage Guidelines Use this command to configure n11 message types.

profile failure-handling interface n11 message cause-code-value cause-code

Configures the n11 interface cause-code types.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **cause-code-value cause-code** *cause_code_type*

cause_code_type

Specify the cause code type.

Must be one of the following:

- temp-reject-register
- temp-reject-handover

Usage Guidelines Use this command to configure the n11 interface cause-code types.

profile failure-handling interface n11 message cause-code-value cause-code action

Configures the action type for the cause.

Privilege Security Administrator, Administrator

Syntax Description **action** *action_type* **[timeout** *retry_interval* **| max-retry** *max_retry* **]**

action_type

Specify the action type for the cause.

Must be one of the following:

- retry
- clear
- terminate

timeout *retry_interval*

Specify the retry interval in milliseconds.

Must be an integer in the range of 1000-5000.

Default Value: 1000.

max-retry *max_retry*

Specify the maximum retry count.

Must be an integer in the range of 0-5.

Default Value: 1.

Usage Guidelines Use this command to configure the action type for the cause.

profile failure-handling interface pfcp message

Configures PFCP message types.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **message** *message_type*

message_type

Specify the message type.

Must be one of the following:

- N4SessionEstablishmentReq
- N4SessionModificationReq

Usage Guidelines Use this command to configure PFCP message types.

profile failure-handling interface pfcp message cause-code-type-est cause-code

Configures PFCP interface cause code types.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **cause-code** *cause_code_type*

cause_code_type

Specify the cause code type.

Must be one of the following:

- pfcp-entity-in-congestion
- system-failure
- service-not-supported
- no-resource-available
- no-response-received
- reject

Usage Guidelines Use this command to configure PFCP interface cause code types.

profile failure-handling interface pfcp message cause-code-type-est cause-code action

Configures the action type for the cause.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

action *action_type* **[timeout** *retry_interval* **| max-retry** *max_retry* **]**

action_type

Specify the action type for the cause.

Must be one of the following:

- retry-terminate
- terminate

max-retry ***max_reties***

Specify the maximum reties count for the retry-terminate action.

Must be an integer in the range of 0-5.

Default Value: 1.

Usage Guidelines

Use this command to configure the action type for the cause.

profile failure-handling interface pfcp message cause-code-type-mod cause-code

Configures PFCP interface cause code types.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

cause-code *cause_code_type*

cause_code_type

Specify the cause code type.

Must be one of the following:

- no-response-received

- mandatory-ie-incorrect
- session-ctx-not-found
- reject

Usage Guidelines Use this command to configure PFCP cause code type.

profile failure-handling interface pfcp message cause-code-type-mod cause-code action

Configures the action type for the cause.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`action`** *`action_type`*

action_type

Specify the action type for the cause.

Must be one of the following:

- terminate

Usage Guidelines Use this command to configure the action type for the cause.

profile icmpv6

Configuration used in ICMPv6 messages.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **`profile icmpv6`** *`profile_name`*

profile_name

Specify the ICMPv6 profile name.

Must be a string.

Usage Guidelines Use this command to configure the ICMPv6 profile name.

profile icmpv6 options

Configures ICMPv6 configuration parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Profile Configuration

Syntax Description

options { hop-limit *hop_limit* **| mtu** *mtu_size* **| reachable-time** *reachable_period* **| retrans-timer** *retransmission_period* **| router-lifetime** *lifetime_period* **| virtual-mac** *mac_address* **}**

virtual-mac *mac_address*

Specify the local virtual MAC address.

Must be a 17-digit string in the pattern [0-9a-fA-F:-].

hop-limit *hop_limit*

Specify the hop limit.

Must be an integer in the range of 0-255.

Default Value: 255.

router-lifetime *lifetime_period*

Specify the router lifetime in seconds.

Must be an integer in the range of 0-65535.

Default Value: 65535.

reachable-time *reachable_period*

Specify the reachable time in milliseconds.

Must be an integer.

Default Value: 0.

retrans-timer *retransmission_period*

Specify the retransmission time in milliseconds.

Must be an integer.

Default Value: 0.

mtu *mtu_size*

Specify the MTU size.

Must be an integer.

Default Value: 1500.

Usage Guidelines Use this command to configure the ICMPv6 configuration parameters.

profile location-area-group

Configures the Location Area Group profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **location-area-group** *profile_name* **[tai-group** *tai_group_name* **| ecgi-group** *ecgi_group_name* **| ncgi-group** *ncgi_group_name* **]**

profile_name

Specify the Location Area Group profile name.

Must be a string.

tai-group *tai_group_name*

Specify the TAI group name.

Must be a string.

ecgi-group *ecgi_group_name*

Specify the ECGI Group name.

Must be a string.

ncgi-group *ncgi_group_name*

Specify the NCGI Group name.

Must be a string.

Usage Guidelines Use this command to configure the Location Area Group profile parameters.

profile n3-tunnel

Configures N3 tunnelling information profile configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **profile n3-tunnel** *profile_name* **[notify]**

profile_name

Specify the N3 tunnelling profile name.

Must be a string.

notify

Specify to enable downlink data notification.

Usage Guidelines Use this command to configure N3 tunnelling information profile configuration.

profile n3-tunnel buffer

Configures the buffering for downlink direction.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **buffer** *node*

node

Specify to enable buffering in UPF.

Must be one of the following:

- upf

Usage Guidelines Use this command to configure the buffering for downlink direction.

profile ncgi-group

Configures NCGI Group profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **ncgi-group** *profile_name*

profile_name

Specify the NCGI Group profile name.

Must be a string.

Usage Guidelines Use this command to configure NCGI Group profile parameters.

profile ncgi-group ncgis

Configures the list of MCC, MNC, TAC, and NCGI groups.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **ncgis { mcc** *mobile_country_code* **| mnc** *mobile_network_code* **| tac** *tracking_area_code* **}**

mcc *mobile_country_code*

Specify the Mobile Country Code (MCC). For example, 01, 001.

Must be a 3-digit integer.

mnc *mobile_network_code*

Specify the Mobile Network Code (MNC). For example, 23, 456.

Must be a 2- or 3-digit integer.

tac *tracking_area_code*

Specify the Tracking Area Code (TAC). For example, A1a2, AaBbF1.

Must be a 4-digit string in the pattern [0-9a-fA-F], or a 6-digit string in the pattern [0-9a-fA-F].

Usage Guidelines Use this command to configure the list of MCC, MNC, TAC, and NCGI groups.

You can configure a maximum of 16 elements with this command.

profile ncgi-group ncgis ncgi

Configures NCGI Group parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **ncgi** *ncgi_values* **[range** *ncgi_range* **]**

ncgi_values

Specify the list of NCGI values - 9 digit hex string NR Cell ID.

Must be a 9-digit string in the pattern [0-9a-fA-F].

Usage Guidelines Use this command to configure NCGI Group parameters.

You can configure a maximum of 64 elements with this command.

profile ncgi-group ncgis ncgi range

Configures an NCGI range.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **range** *ncgi_range*

start *ncgi_range_start*

Specify the NCGI range start value.

Must be a 9-digit string in the pattern [0-9a-fA-F].

end *ncgi_range_end*

Specify the NCGI range end value.

Must be a 9-digit string in the pattern [0-9a-fA-F].

Usage Guidelines Use this command to configure an NCGI range.

You can configure a maximum of 64 elements with this command.

profile network-element amf

Configures peer AMF parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **network-element amf** *peer_amf_name* **[nf-client-profile** *profile_name* **| failure-handling-profile** *profile_name* **]**

peer_amf_name

Specify name of the peer AMF.

Must be a string.

nf-client-profile *profile_name*

Specify the NF client profile name.

Must be a string.

failure-handling-profile *profile_name*

Specify the failure handling profile name.

Must be a string.

Usage Guidelines Use this command to configure peer AMF configuration.

profile network-element amf query-params

Configures the query parameter for AMF discovery.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Profile Configuration

Syntax Description

query-params { dnn | supi | tai | target-nf-instance-id | target-plmn }

query-params *query_params*

Specify the query parameters.

Must be one of the following:

- supi
- dnn
- tai
- target-plmn
- target-nf-instance-id

Usage Guidelines

Use this command to configure the query parameter for AMF discovery.

profile network-element chf

Configures peer CHF parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > CHF Network Element Profile Configuration

Syntax Description

chf *peer_chf_name* **[failure-handling-profile** *profile_name* **| failure-handling-profile-offline** *profile_name* **| nf-client-profile** *profile_name* **| nf-client-profile-offline** *profile_name* **| nf-client-profile** *profile_name* **]**

peer_chf_name

Specify the peer CHF name.

Must be a string.

nf-client-profile *profile_name*

Specify the NF Client profile name.

Must be a string.

failure-handling-profile *profile_name*

Specify the Failure Handling profile name.

Must be a string.

nf-client-profile-offline *profile_name*

Specify the NF Client profile name for offline server.

Must be a string.

failure-handling-profile-offline *profile_name*

Specify the Failure Handling profile name for offline server.

Must be a string.

Usage Guidelines Use this command to configure peer CHF parameters.

profile network-element chf query-params

Configures UDM discovery query parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **`query-params`** *`query_parameters`*

query-params *query_params*

Specify the query parameters.

Must be one of the following:

- supi
- dnn
- tai
- target-plmn
- target-nf-instance-id

Usage Guidelines Use this command to configure UDM discovery query parameter.

profile network-element pcf

Configures peer PCF parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > PCF Network Element Profile Configuration

Syntax Description **pcf** *peer_pcf_name* **[failure-handling-profile** *profile_name* **| nf-client-profile** *profile_name* **| predefined-rule-prefix** *prefix_name* **| rulebase-prefix** *rulebase_prefix* **| use-amf-provided-pcf [false | true]]**

peer_pcf_name

Specifes the peer PCF name.

Must be a string.

nf-client-profile ***profile_name***

Specify the NF client profile name.

Must be a string.

failure-handling-profile ***profile_name***

Specify the Failure Handling profile name.

Must be a string.

rulebase-prefix ***rulebase_prefix***

Specify the rulebase prefix string.

Must be a string.

predefined-rule-prefix ***prefix_name***

Specify the predefined rule prefix to be added.

Must be a string.

use-amf-provided-pcf [false | true]

Specify to enable or disable discovery of PCF using PCF ID provided by AMF.

Must be either "false" or "true".

Default Value: true.

Usage Guidelines Use this command to configure peer PCF parameters.

profile network-element pcf query-params

Configures query parameter for PCF discovery.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **query-params** *query_parameters*

query-params *query_params*

Specify the query parameters.

Must be one of the following:

- supi
- dnn
- tai
- target-plmn
- target-nf-instance-id

Usage Guidelines Use this command to configure the query parameter for PCF discovery.

profile network-element udm

Configures peer UDM configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **udm** *peer_udm_name* **[nf-client-profile** *profile_name* **| failure-handling-profile** *profile_name* **]**

peer_udm_name

Specify the peer UDM name.

Must be a string.

nf-client-profile *profile_name*

Specify the NF client profile name.

Must be a string.

failure-handling-profile *profile_name*

Specify the failure handling profile name.

Must be a string.

Usage Guidelines Use this command to configure the peer UDM configuration.

profile network-element udm query-params

Configures query parameter for UDM discovery.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **query-params** *query_parameters*

query-params *query_params*

Specify the query parameters.

Must be one of the following:

- supi
- dnn
- tai
- target-plmn
- target-nf-instance-id

Usage Guidelines Use this command to configure the query parameter for UDM discovery.

profile network-element upf

Configures peer UPF parameters.

Privilege Security Administrator, Administrator

Syntax Description **upf** *peer_upf_name* **[node-id** *node_id* **]**

peer_upf_name

Specify the UPF peer name.

Must be a string.

node-id *node_id*

Specify the node ID for the UPF peer node.

Must be a string.

n4-peer-port *port_number*

Specify the UPF N4 peer port number.

Must be an integer in the range of 0-65535.

Default Value: 8809.

upf-group-profile *profile_name*

Specify the UPF Group profile name.

dnn-list *dnn_list*

Specify the list of DNNs supported by the UPF node.

Must be a string.

downlink-data-report [false | true]

Specify to enable or disable notification from UPF for downlink data.

Must be either "false" or "true".

Default Value: true.

downlink-data-buffer [false | true]

Specify to enable or disable buffering in UPF for downlink data.

Must be either "false" or "true".

Default Value: true.

capacity *lb_capacity*

Specify the static capacity relative to other UPFs used for load balancing.

Must be an integer in the range of 0-65535.

Default Value: 10.

priority *lb_priority*

Specify the static priority relative to other UPFs used for load balancing.

Must be an integer in the range of 0-65535.

Default Value: 1.

Usage Guidelines Use this command to configure peer UPF parameters.

profile network-element upf n4-peer-address

Configures the N4 peer address.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`n4-peer-address [ ipv4-address`** *`ipv4_address`* **`| ipv6-address`** *`ipv6_address`* **`| n4-peer-port`** *`port_number`* **`| keepalive`** *`heartbeat_interval`* **`| dnn-list`** *`dnn_list`* **`| downlink-data-report [ false | true ] | downlink-data-buffer [ false | true ] | capacity`** *`lb_capacity`* **`| priority`** *`lb_priority`* **`]`**

ipv4-address *ipv4_address*

Specify the N4 peer IPv4 address.

Must be an IPv4 address.

ipv6-address *ipv6_address*

Specify the N4 peer IPv6 address.

Must be an IPv6 address.

Usage Guidelines Use this command to confgure the N4 peer address.

profile nf-client

Configures the network function client parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`nf-client nf-type udm udm-profile`** *`profile_name`*

Usage Guidelines Use this command to configure the NF client parameters.

profile nf-client nf-type

Configures the NF client type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`nf-type`**

Usage Guidelines Use this command to configure the NF client type.

profile nf-client nf-type amf amf-profile

Configures AMF profile configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`amf amf-profile`** *`profile_name`*

profile_name

Specify the AMF profile name

Must be a string.

Usage Guidelines Use this command to configure the AMF profile.

profile nf-client nf-type amf amf-profile locality

Configures the locality information.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **locality** *locality_name* **[priority** *priority* **]**

locality_name

Specify the locality name.

Must be a string.

priority ***priority***

Specify the priority for the locality configuration.

Must be an integer.

Usage Guidelines Use this command to configure the locality information.

profile nf-client nf-type amf amf-profile locality service name type

Configures AMF service name type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **type** *amf_service_name_type*

type ***amf_service_name_type***

Specify the service name type.

Must be one of the following:

- namf-comm
- namf-evts
- namf-mt

- namf-loc

responsetimeout *response_timeout*

Specify the response timeout period in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines Use this command to configure the AMF service name type.

profile nf-client nf-type amf amf-profile locality service name type endpoint-profile

Configures endpoint profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *priority_value* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

endpoint_profile_name

Specify the endpoint profile name.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

priority *priority_value*

Specify the profile priority.

Must be an integer in the range of 0-65535.

Default Value: 1.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

api-root *api_root*

Specify the API root.

Must be a string.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- http: HTTP.
- https: HTTPS.

Usage Guidelines Use this command to configure endpoint profile parameters.

profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name

Configures the endpoint name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *priority_value* **| capacity** *capacity_value* **]**

endpoint_name

Specify the endpoint name. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority *priority_value*

Specify the node priority for endpoint.

Must be an integer in the range of 0-65535.

capacity *capacity_value*

Specify the node capacity.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this configuration to configure the endpoint name.

profile nf-client nf-type amf amf-profile locality service name type endpoint-profile version uri-version

Configures the URI version.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description

`version uri-version {` *`uri_version`* **`|`** **`full-version`** *`full_version`* **`}`**

uri_version

Specify the URI version.

Must be a string in the pattern v\d.

full-version *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string.

Usage Guidelines

Use this command to configure the URI version information.

profile nf-client nf-type ausf ausf-profile

Configures the AuSF profile parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

`ausf-profile` *`profile_name`*

profile_name

Specify the profile name.

Must be a string.

Usage Guidelines

Use this command to configure the AuSF profile parameters.

profile nf-client nf-type ausf ausf-profile locality

Configures the locality parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`locality`** *`locality_name`* **`[ priority`** *`priority`* **`]`**

locality_name

Specify the locality name.

Must be a string.

priority *priority*

Specify the locality configuration priority.

Must be an integer.

Usage Guidelines Use this command to configure the locality parameters.

profile nf-client nf-type ausf ausf-profile locality service name type

Configures AuSF service name type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`type`** *`ausf_service_name_type`*

type *ausf_service_name_type*

Specify the AuSF service name type.

Must be one of the following:

- nausf-auth

Usage Guidelines Use this command to configure AuSF service name type.

profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile

Configures endpoint profile parameters.

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

endpoint-profile *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *priority_value* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

endpoint_profile_name

Specify the endpoint profile name.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

priority *priority_value*

Specify the profile priority.

Must be an integer in the range of 0-65535.

Default Value: 1.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

api-root *api_root*

Specify the API root.

Must be a string.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- http: HTTP.
- https: HTTPS.

Usage Guidelines

Use this command to configure endpoint profile parameters.

profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name

Configures the endpoint name.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

endpoint-name *endpoint_name* **[priority** *priority_value* **| capacity** *capacity_value* **]**

endpoint_name

Specify the endpoint name. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority ***priority_value***

Specify the node priority for endpoint.

Must be an integer in the range of 0-65535.

capacity ***capacity_value***

Specify the node capacity.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this configuration to configure the endpoint name.

profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile version uri-version

Configures the URI version.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description

version uri-version { *uri_version* **| full-version** *full_version* **}**

uri_version

Specify the URI version.

Must be a string in the pattern v\d.

full-version *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string.

Usage Guidelines Use this command to configure the URI version information.

profile nf-client nf-type chf chf-profile

Configures the CHF profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **chf chf-profile name** *profile_name*

name *profile_name*

Specify the CHF profile name.

Must be a string.

Usage Guidelines Use this command to configure the CHF profile parameters.

profile nf-client nf-type chf chf-profile locality

Configures the CHF locality parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **locality name** *locality_name* **[priority** *priority* **]**

name *locality_name*

Specify the locality name.

Must be a string.

priority *priority*

Specify the priority for the locality configuration.

Must be an integer.

Usage Guidelines Use this command to configure the locality parameters.

profile nf-client nf-type chf chf-profile locality service name type

Configures the CHF service name type.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

type *service_name_type*

type *service_name_type*

Specify the CHF service name type.

Must be one of the following:

- nchf-spendinglimitcontrol
- nchf-convergedcharging

responsetimeout *response_timeout*

Specify the response timeout period in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines

Use this command to configure the CHF service name type.

profile nf-client nf-type chf chf-profile locality service name type endpoint-profile

Configures endpoint profile parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

endpoint-profile *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *priority_value* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

endpoint_profile_name

Specify the endpoint profile name.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

priority *priority_value*

Specify the profile priority.

Must be an integer in the range of 0-65535.

Default Value: 1.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

api-root *api_root*

Specify the API root.

Must be a string.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- http: HTTP.
- https: HTTPS.

Usage Guidelines Use this command to configure endpoint profile parameters.

profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name

Configures the endpoint name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *priority_value* **| capacity** *capacity_value* **]**

endpoint_name

Specify the endpoint name. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority *priority_value*

Specify the node priority for endpoint.

Must be an integer in the range of 0-65535.

capacity *capacity_value*

Specify the node capacity.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this configuration to configure the endpoint name.

profile nf-client nf-type chf chf-profile locality service name type endpoint-profile version uri-version

Configures the URI version.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description **`version uri-version {`** *`uri_version`* **`|`** **`full-version`** *`full_version`* **`}`**

uri_version

Specify the URI version.

Must be a string in the pattern v\d.

full-version *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string.

Usage Guidelines Use this command to configure the URI version information.

profile nf-client nf-type pcf pcf-profile

PCF profile configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **pcf pcf-profile name** *profile_name*

name *profile_name*

Specify the PCF profile name.

Must be a string.

Usage Guidelines Use this command to configure the PCF profile.

profile nf-client nf-type pcf pcf-profile locality

Configures the locality information.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **pcf locality** *locality_name* **[priority** *priority_value* **]**

locality_name

Specify the locality name.

Must be a string.

priority *priority*

Specify the priority for the locality configuration.

Must be an integer.

Usage Guidelines Use this command to configure the locality information.

profile nf-client nf-type pcf pcf-profile locality service name type

Configures the PCF service name type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **type** *service_name_type*

type *service_name_type*

Specify the PCF service name parameters.

Must be one of the following:

- npcf-am-policy-control
- npcf-smpolicycontrol
- npcf-policyauthorization
- npcf-bdtpolicycontrol
- npcf-eventexposure
- npcf-ue-policy-control

responsetimeout *response_timeout*

Specify the response timeout period in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines Use this command to configure the PCF service name type.

profile nf-client nf-type smf smf-profile

Configures SMF profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **smf-profile** *smf_profile_name*

smf_profile_name

Specify the SMF profile name.

Must be a string.

Usage Guidelines Use this command to configure the SMF profile parameters.

profile nf-client nf-type smf smf-profile locality

Configures locality parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **locality** *locality_name*

locality_name

Specify the locality name.

Must be a string.

priority ***priority***

Specify the priority of the locality configuration.

Must be an integer.

Usage Guidelines Use this command to configure the locality parameters.

profile nf-client nf-type udm udm-profile

Configures UDM profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **udm-profile** *udm_profile_name*

udm_profile_name

Specify the UDM profile name.

Must be a string.

Usage Guidelines Use this command to configure the UDM profile for an NF client.

profile nf-client nf-type udm udm-profile locality

Configures locality information.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **locality** *locality_name* **[priority** *priority* **]**

locality_name

Specify the locality name.

Must be a string.

priority *priority*

This keyword sets the priority for the locality configuration.

Must be an integer.

Usage Guidelines Use this command to configure the locality information.

profile nf-client nf-type udm udm-profile locality service name type

Configures the UDM service type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **type** *service_name_type*

type *service_name_type*

Specify the UDM service name type.

Must be one of the following:

- nudm-sdm
- nudm-uecm
- nudm-ueau
- nudm-ee
- nudm-pp

responsetimeout *response_timeout*

Specify the response timeout period in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines Use this command to configure the UDM service type.

profile nf-client-failure nf-type amf profile failure-handling

Configures the AMF failure handling template name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`failure-handling name`** *`template_name`*

name *template_name*

Specify the AMF failure handling template name.

Must be a string.

Usage Guidelines Use this command to configure the failure handling template for AMF profile.

profile nf-client-failure nf-type amf profile failure-handling service name type

Configures the AMF service name type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`type`** *`amf_service_name_type`*

type *amf_service_name_type*

Specify the AMF service name type.

Must be one of the following:

- namf-comm
- namf-evts
- namf-mt
- namf-loc

responsetimeout *response_timeout*

Specify the response timeout period in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines Use this command to configure AMF service name type.

profile nf-client-failure nf-type amf profile failure-handling service name type message type

Configures the AMF message type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **message type** *amf_message_type*

amf_message_type

Specify the AMF message type.

Must be one of the following:

- AmfCommEBIAssignment
- AmfCommN1N2MessageTransfer
- AmfCommSMStatusChangeNotify

Usage Guidelines Use this command to configure the AMF message type.

profile nf-client-failure nf-type ausf profile failure-handling

Configures the failure handling template name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **failure-handling** *template_name*

template_name

Specify the failure handling template name.

Must be a string.

Usage Guidelines Use this command to configure the failure handling template for AuSF profile.

profile nf-client-failure nf-type ausf profile failure-handling service name type

Configures the AuSF service name type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **service name type** *ausf_service_name_type*

ausf_service_name_type

Specify the AuSF service name type.

Must be one of the following:

- nausf-auth

Usage Guidelines Use this command to configure the AuSF service name type.

profile nf-client-failure nf-type ausf profile failure-handling service name type message type

Configures the AuSF message type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **message type** *ausf_message_type*

ausf_message_type

Specify the AuSF message type.

Must be one of the following:

- AusfAuthenticationReq
- AusfAuthenticationCfm

Usage Guidelines Use this command to configure the AuSF message type.

profile nf-client-failure nf-type chf profile failure-handling

Configures the failure handling template name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **failure-handling** *template_name*

template_name

Specify the CHF failure handling template name.

Must be a string.

Usage Guidelines Use this command to configure the failure handling template for CHF profile.

profile nf-client-failure nf-type chf profile failure-handling service name type

Configures the CHF service name type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **type** *chf_service_name_type*

type *chf_service_name_type*

Specify the CHF service name type.

Must be one of the following:

- nchf-spendinglimitcontrol
- nchf-convergedcharging

responsetimeout *response_timeout*

Specify the response timeout period in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines Use this command to configure the CHF service name type.

profile nf-client-failure nf-type chf profile failure-handling service name type message type

Specify the CHF message type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **message type** *chf_message_type*

chf_message_type

Specify the CHF message type.

Must be one of the following:

- ChfConvergedchargingCreate
- ChfConvergedchargingUpdate
- ChfConvergedchargingDelete

Usage Guidelines Use this command to configure the CHF message type.

profile nf-client-failure nf-type pcf profile failure-handling

Configures the failure handling template name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **failure-handling** *template_name*

template_name

Specify the PCF failure handling template name.

Must be a string.

Usage Guidelines Use this command to configure the failure handling template for PCF profile.

profile nf-client-failure nf-type pcf profile failure-handling service name type

Configures PCF service name type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **type** *pcf_service_name_type*

pcf_service_name_type

Specify the PCF service name type.

Must be one of the following:

- npcf-am-policy-control

- npcf-smpolicycontrol
- npcf-policyauthorization
- npcf-bdtpolicycontrol
- npcf-eventexposure
- npcf-ue-policy-control

responsetimeout *response_timeout*

Specify the response timeout period in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines Use this command to configure the PCF service name type.

profile nf-client-failure nf-type udm profile failure-handling

Configures the failure handling template name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **failure-handling** *template_name*

template_name

Specify the UDM failure handling template name.

Must be a string.

Usage Guidelines Use this command to configure the failure handling template for UDM profile.

profile nf-client-failure nf-type udm profile failure-handling service name type

Configures UDM service name type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **type** *udm_service_name_type* **[responsetimeout** *response_timeout* **]**

udm_service_name_type

Specify the UDM service name type.

Must be one of the following:

- nudm-sdm
- nudm-uecm
- nudm-ueau
- nudm-ee
- nudm-pp

responsetimeout ***response_timeout***

Specify the response timeout period in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines Use this command to configure the UDM service name type.

profile nf-pair nf-type

Configures the NF client pair type parameter.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`nf-pair nf-type type`** *`nf_type`*

type ***nf_type***

Specify the NF client pair type.

Must be one of the following:

- NRF
- UDM
- AMF
- SMF
- AUSF
- NEF
- PCF
- SMSF

- NSSF
- UDR
- LMF
- GMLC
- 5G_EIR
- SEPP
- UPF
- N3IWF
- AF
- UDSF
- BSF
- CHF
- NWDAF

nrf-discovery-group *group_name*

Specify the NRF discovery group name.

Must be a string.

Usage Guidelines Configures Nf client pair parameters. Use this command to configure the NF client pair type parameter.

profile nf-pair nf-type cache

Configures the NF client pair cache.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `Use this command to configure the NF client pair cache.`

Usage Guidelines Use this command to configure the NF client pair cache.

profile nf-pair nf-type cache invalidation

Configures the invalidation cache parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `invalidation { false | true }`

Usage Guidelines Use this command to configure the invalidation cache parameters.

profile nf-pair nf-type cache invalidation true

Configures the invalidation cache for "true" case.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `true`

true-value

true-value.

timeout *timeout_period*

Specify the invalidation cache timeout period in milliseconds.

Must be an integer.

Default Value: 0.

Usage Guidelines Use this command to configure the true case parameters for invaldation cache.

profile nf-pair nf-type capacity-threshold

Configures the capacity threshold.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description `capacity-threshold { warn value_percentage | critical value_percentage }`

warn *percentage*

Specify the threshold warning percentage.

Must be an integer in the range of 1-100.

critical *percentage*

Specify the threshold critical percentage.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure the capacity threshold.

profile nf-pair nf-type failover

Configures the SLA failover time.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

`failover sla` *`time`*

sla *time*

Specify the failover SLA value in milliseconds.

Must be an integer.

Default Value: 0.

Usage Guidelines

Use this command to configure the SLA failover time.

profile nf-pair nf-type locality

Configures client locality parameter.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

`locality { client` *`locality_name`* **`| geo-server`** *`locality_name`* **`| preferred-server`** *`locality_name`* **`}`**

client *locality_name*

Specify the Client locality information.

Must be a string.

preferred-server *locality_name*

Specify the preferred server locality information.

Must be a string.

geo-server *locality_name*

Specify the Geo service locality information.

Must be a string.

Usage Guidelines

Use this command to configure the client locality parameter.

profile nf-pair nf-type reconnect

Configures the reconnect interval.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **reconnect interval** *time*

interval *time*

Specify the reconnect interval in milliseconds.

Must be an integer.

Default Value: 0.

Usage Guidelines Use this command to configure the reconnect interval.

profile pcscf

Configures the P-CSCF profile.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **pcscf** *profile_name*

profile_name

Specify the P-CSCF profile name.

Must be a string.

Usage Guidelines Use this command to configure the P-CSCF profile.

profile pcscf fqdn

Configures the P-CSCF server's FQDN.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **fqdn** *fqdn*

fqdn

Specify the P-CSCF server's FQDN.

Must be a string.

Usage Guidelines Use this command to configure the P-CSCF server's FQDN.

profile pcscf pcscf-selection

Configures the P-CSCF server selection algorithm.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`pcscf-selection`** *`algorithm`*

algorithm

Specify the P-CSCF server selection algorithm.

Must be one of the following:

- round-robin

Default Value: round-robin.

Usage Guidelines Use this command to configure the P-CSCF server selection method. NOTE: In this release, round-robin is the only supported algorithm for server selection.";

profile pcscf v4-list

Configures the P-CSCF IPv4 server details in the P-CSCF profile.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`v4-list`**

Usage Guidelines Use this command to configure the P-CSCF IPv4 server details in the P-CSCF profile.";

profile pcscf v4-list list-entry

Configures the P-CSCF IPv4 server list entries.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`v4-list list-entry precedence`** *`precedence_number`*

precedence *precedence_number*

Specify the precedence number for P-CSCF IPv4 server configuration.

Must be an integer in the range of 1-64.

Usage Guidelines Use this command to configure the P-CSCF IPv4 server list entries.

profile pcscf v4-list list-entry primrary

Configures the IPv4 address of the primary P-CSCF server.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`primary ipv4`** *`ipv4_address`*

ipv4 *ipv4_address*

Specify the IPv4 address of the primary P-CSCF server in dotted-decimal notation.

Must be an IPv4 address.

Usage Guidelines Use this command to configure the IPv4 address of the primary P-CSCF server.

Example

The following command configures the primary P-CSCF server with IPv4 address 30.22.21.44:

```
primary ipv4 30.22.21.44
```

profile pcscf v4-list list-entry secondary

Configures the IPv4 address of the secondary P-CSCF server.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`secondary ipv4`** *`ipv4_address`*

ipv4 *ipv4_address*

Specify the IPv4 address of the secondary P-CSCF server in dotted-decimal notation.

Must be an IPv4 address.

Usage Guidelines Use this to command configure the IPv4 address of the secondary P-CSCF server.

Example

The following command configures the secondary P-CSCF server with IPv4 address 30.22.21.44:

```
secondary ipv4 30.22.21.44
```

profile pcscf v4v6-list

Configures the P-CSCF IPv4v6 server details.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`v4v6-list`**

Usage Guidelines Use this command to configure the P-CSCF IPv4v6 server details in the P-CSCF profile.";

profile pcscf v4v6-list list-entry

Configures the P-CSCF IPv4v6 server list entries.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`v4v6-list list-entry precedence`** *`precedence_number`*

precedence *precedence_number*

Specify the precedence of entries in the P-CSCF IPv4v6 server list.

Must be an integer in the range of 1-64.

Usage Guidelines Use this command to configure the P-CSCF IPv4v6 server list entries.

profile pcscf v4v6-list list-entry primrary

Configures the IPv4v6 address of the primary P-CSCF server.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **primary ipv4** *ipv4_address* **ipv6** *ipv6_address*

ipv4 *ipv4_address*

Specify the IPv4 address of the primary P-CSCF server in dotted-decimal notation.

Must be an IPv4 address.

ipv6 *ipv6_address*

Specify the IPv6 address of the primary P-CSCF server in colon-separated hexadecimal notation.

Must be an IPv6 address.

Usage Guidelines Use this command to configure the IPv4v6 address of the primary P-CSCF server.

Example

The following command configures the primary P-CSCF server with IPv4 address as 30.22.21.44 and IPv6 address as 123:345:456::6578:

```
primary ipv4 30.22.21.44 ipv6 123:345:456::6578
```

profile pcscf v4v6-list list-entry secondary

Configures the IPv4v6 address of the secondary P-CSCF server.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **secondary { [ipv4** *ipv4_address* **] [ipv6** *ipv6_address* **] }**

ipv4 *ipv4_address*

Specify the IPv4 address of the secondary P-CSCF server in dotted-decimal notation.

Must be an IPv4 address.

ipv6 *ipv6_address*

Specify the IPv6 address of the secondary P-CSCF server in colon-separated hexadecimal notation.

Must be an IPv6 address.

Usage Guidelines Use this command to configure the IPv4v6 address of the secondary P-CSCF server.

Example

The following command configures the secondary P-CSCF server with IPv4 address as 30.22.21.44 and IPv6 address as 123:345:456::6578:

```
secondary ipv4 30.22.21.44 ipv6 123:345:456::6578
```

profile pcscf v6-list

Configures the P-CSCF IPv6 server details.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`v6-list list-entry precedence`** *`precedence`*

Usage Guidelines Use this command to configure the P-CSCF IPv6 server details in the P-CSCF profile.";

profile pcscf v6-list list-entry

Configures the P-CSCF IPv6 server list entries.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`v6-list list-entry precedence`** *`precedence_number`*

precedence_number

Specify the precedence of entries in the P-CSCF IPv6 server list.

Must be an integer in the range of 1-64.

Usage Guidelines Use this command to configure the P-CSCF IPv6 server list entries.

profile pcscf v6-list list-entry primrary

Configures the IPv6 address of the primary P-CSCF server.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`primary ipv6`** *`ipv6_address`*

ipv6 *ipv6_address*

Specify the IPv6 address of the primary P-CSCF server in colon-separated hexadecimal notation.

Must be an IPv6 address.

Usage Guidelines Use this command to configure the IPv6 address of the primary P-CSCF server.

Example

The following command configures the primary P-CSCF server with IPv6 address 123:345:456::6578:

```
primary ipv6 123:345:456::6578
```

profile pcscf v6-list list-entry secondary

Configures the IPv6 address of the secondary P-CSCF server.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

`secondary ipv6` *`ipv6_address`*

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be an IPv6 address.

Usage Guidelines

Use this command to configure the IPv6 address of the secondary P-CSCF server.

Example

The following command configures the secondary P-CSCF server with IPv6 address 123:345:456::6578:

```
secondary ipv6 123:345:456::6578
```

profile ppd

Configures the PPD profile in the DNN profile configuration.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

`ppd` *`ppd_profile_name`*

ppd_profile_name

Specify the PPD profile name.

Must be a string.

fqi *5qi_values*

Specify the range of 5G QoS Identifier (5QI) priority levels. To list multiple priority levels, use commas and hyphens as needed. For example, 5QI 3,10-15,65.

Must be an integer.

-Or-

Must be a string.

Usage Guidelines

Use this command to specify the PPD profile to be associated with the DNN profile.

Example

The following command defines the PPD profile ppdtest within the DNN profile:

```
ppd ppdtest
```

profile ppd dscp-list

Configures the Differentiated Services Code Point (DSCP) values.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

dscp-list dscp *dscp_value* **ppi** *ppi_value*

dscp *dscp_value*

Specify the DSCP value. To list the different priority levels, use comma and hyphen as needed. For example, 5QI 3,10-15,65.

Must be an integer in the range of 0-63.

ppi *ppi_value*

Specify the Paging Policy Indicator value.

Must be an integer in the range of 0-7.

Usage Guidelines

Use this command to configure the DSCP and Paging Policy Indicator values.

Example

The following command sets the DSCP value as 10 and the paging profile indicator value as 7:

```
dscp 10 ppi 7
```

profile qos

Configures a Quality of Service (QoS) profile.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Profile Configuration

Syntax Description

qos *profile_name* **[priority** *qos_priority* **| qi5** *5qi_value* **]**

profile_name

Specify the QoS profile's name.

Must be a string.

qi5 ***5qi_value***

Specify the 5G QoS Identifier (5QI) for authorized QoS parameters.

Must be an integer in the range of 0-255.

priority ***qos_priority***

Specify the 5QI priority level for the QoS profile.

Must be an integer in the range of 1-127.

Usage Guidelines

Use this command to create a QoS profile and configure the QoS parameters.

Example

The following command creates a QoS profile named qos1:

```
qos qos1
```

profile qos ambr

Configures the Aggregate Maximum Bit Rate (AMBR) for the uplink (subscriber-to-network) and the downlink (network-to-subscriber) traffic.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Profile Configuration

Syntax Description

ambr { ul *uplink_ambr* **| dl** *downlink_ambr* **}**

ul ***uplink_ambr***

Specify the AMBR uplink threshold.

Must be a string in the pattern [0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps).

dl *downlink_ambr*

Specify the AMBR downlink threshold.

Must be a string in the pattern [0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps).

Usage Guidelines Use this command to configure the AMBR threshold values for uplink and downlink traffic.

Example

The following command configures the uplink and downlink AMBR for the QoS profile to 1024 bps:

```
ambr ul 1024 dl 1024
```

profile qos arp

Configures the Allocation and Retention Priority (ARP) for the service data.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **arp { preempt-cap** *preemption_capability* **| preempt-vuln** *preemption_vulnerability* **| priority-level** *priority_level* **}**

priority-level *priority_level*

Specify the ARP for the service data.

Must be an integer in the range of 1-15.

preempt-cap *preemption_capability*

Specify the preemption capability flag.

Must be one of the following:

- NOT_PREEMPT: Bearer cannot be preempted
- MAY_PREEMPT: Bearer may be preempted

Default Value: MAY_PREEMPT.

preempt-vuln *preemption_vulnerability*

Specify the preemption vulnerability flag.

Must be one of the following:

- NOT_PREEMPTABLE: Bearer cannot be preempted

- PREEMPTABLE: Bearer may be preempted

Default Value: NOT_PREEMPTABLE.

Usage Guidelines This command sets the Allocation and Retention Priority (ARP) for the service data.

Example

The following command sets the ARP Preemption capability flag as MAY_PREEMPT:

```
arp preempt-cap MAY_PREEMPT
```

profile qos dscp-map qi5 arp-priority-level dscp-info

Configures the DSCP type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`dscp-info`**

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- uplink
- downlink

dl-encaps-header

Specify the DSCP value be applied to encaps header.

dl-encap-copy-inner

Specify to copy inner DSCP to outer.

dl-encap-dscp-marking *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the pattern 0x[0-3][0-9a-fA-F].

user-datagram1

Specify the DSCP value to be applied to user datagram.

dl-ud-dscp *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the pattern 0x[0-3][0-9a-fA-F].

encsp-header

Specify the DSCP value to be applied to encaps header.

dl-ud-encap-copy-inner

Specify to copy inner DSCP to outer.

dl-ud-encap-dscp *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the pattern 0x[0-3][0-9a-fA-F].

Usage Guidelines Use this command to configure the DSCP type.

profile qos dscp-map qi5 arp-priority-level dscp-info user-datagram

Configures the DCSP value to be applied to user datagram.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`user-datagram ul-uD-dscp-marking`** *`dscp_marking`*

ul-uD-dscp-marking *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the pattern 0x[0-3][0-9a-fA-F].

Usage Guidelines Use this command to configure the DCSP value to be applied to user datagram.

profile qos dscp-map qi5 dscp-info

Configures the DSCP type.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`dscp-info`**

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- uplink
- downlink

dl-encaps-header

Specify the DSCP value be applied to encaps header.

dl-encap-copy-inner

Specify to copy inner DSCP to outer.

dl-encap-dscp-marking *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the pattern 0x[0-3][0-9a-fA-F].

user-datagram1

Specify the DSCP value to be applied to user datagram.

dl-ud-dscp *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the pattern 0x[0-3][0-9a-fA-F].

encsp-header

Specify the DSCP value to be applied to encaps header.

dl-ud-encap-copy-inner

Specify to copy inner DSCP to outer.

dl-ud-encap-dscp *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the pattern 0x[0-3][0-9a-fA-F].

Usage Guidelines Use this command to configure the DSCP type.

profile qos dscp-map qi5 dscp-info user-datagram

Configures the DCSP value to be applied to user datagram.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`user-datagram ul-uD-dscp-marking`** *`dscp_marking`*

ul-uD-dscp-marking *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the pattern 0x[0-3][0-9a-fA-F].

Usage Guidelines Use this command to configure the DCSP value to be applied to user datagram.

profile qos max

Configures the maximum data burst volume.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **`max data-burst`** *`burst_volume`*

data-burst *burst_volume*

Specify the maximum data burst volume in bps.

Must be an integer in the range of 1-4095.

Usage Guidelines Use this command to configure the maximum data burst volume.

Example

The following command configures the maximum data burst volume to 2048:

```
max data-burst 2048
```

profile radius

Enables RADIUS client configuration.

Privilege Security Administrator, Administrator

Syntax Description **`radius { algorithm`** *`radius_algorithm`* **`|`** **`deadtime`** *`deadtime_duration`* **`|`** *`max_retries`* **`|`** *`timeout_duration`* **`}`**

algorithm *radius_algorithm*

Specify the algorithm for RADIUS server selection.

Must be one of the following:

- first-server

- round-robin

Default Value: first-server.

deadtime *deadtime_duration*

Specify the RADIUS server deadtime duration - the time duration, in minutes, after a RADIUS server is marked as unreachable and before connection can be reattempted.

Must be an integer in the range of 0-65535.

Default Value: 10.

max_retries

Specify the maximum number of times the system will attempt retry with the RADIUS server.

Must be an integer in the range of 0-65535.

Default Value: 2.

timeout_duration

Specify the time duration to elapse for a response from the RADIUS server before re-transmitting.

Must be an integer in the range of 1-65535.

Default Value: 2.

Usage Guidelines Use this command to enable RADIUS client configuration.

profile radius attribute

Configures RADIUS identification parameters.

Privilege Security Administrator, Administrator

Syntax Description **`attribute nas-identifier`** *`nas_id`*

nas-identifier *nas_id*

Specify the attribute name by which the system will be identified in Access-Request messages.

Must be a string.

Usage Guidelines Use this command to configure RADIUS identification parameters.

profile radius detect-dead-server

Configures the response timeout duration, in seconds, to wait for a response from the RADIUS server after which it is marked as unreachable/dead.

Privilege Security Administrator, Administrator

Syntax Description **detect-dead-server** *response_timeout_duration*

response_timeout_duration

Specify the response timeout duration, in seconds.

Must be an integer in the range of 0-65535.

Default Value: 0.

Usage Guidelines Use this command to configure the response timeout duration, in seconds, to wait for a response from the RADIUS server after which it is marked as unreachable/dead.

profile radius server

Configures RADIUS server parameters.

Privilege Security Administrator, Administrator

Syntax Description **server secret** *secret_key* **[** *ipv4_address* **| port** *port_number* **| priority** *priority_number* **]**

ipv4_address

Specify the IPv4 address of the RADIUS server.

Must be an IP address.

secret ***secret_key***

Specify the secret key for the RADIUS server.

Must be an aes-cfb-128-encrypted string.

port ***port_number***

Specify the port number of the RADIUS server.

Must be an integer in the range of 1-65535.

priority ***priority_number***

Specify the priority of the RADIUS server.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure RADIUS server parameters.

profile smf

Configures the SMF network function profile configuration parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Profile Configuration

Syntax Description

smf *profile_name* **[dnn-profile-list** *dnn_profile_list* **| locality** *locality* **| nf-services** *nf_services* **| node-id** *node_id* **]**

profile_name

Specify the SMF profile name.

Must be a string.

mode ***mode_of_operation***

Specify the mode of operation.

Must be one of the following:

- offline

node-id ***node_id***

Specify the SMF's node ID.

Must be a 6-digit string in the pattern [0-9a-fA-F].

locality ***locality***

Specify the locality for geo support.

Must be a string.

nf-services ***nf_services***

Specify the NF services.

Must be a string.

fqdn ***fqdn***

Specify the SMF+PGW-C FQDN.

Must be a string.

dnn-selection-mode ***dnn_selection_mode***

Specify the selection mode for subscription.

Must be one of the following:

- verified
- network-provided
- ue-provided

allowed-nassi *nssai*

Specify the Network Slice Selection Assistance Information (NSSAI).

Must be a string.

ue-authorization *ue_authorization*

The SMF supports the PDU sessions with IPv4v6 type in addition to IPv4 and IPv6 PDU session types for UEs. When a UE requests establishment of PDU session with a specific session type, the SMF checks the UE request against the UE subscription information maintained as default and allowed listPDU session types in the UDM. The SMF performs UE authorization and allocates IP address when the requested PDN type is matching with the values in the UDM. The SMF communicates about the allocated IP address to all other network functions.

Must be one of the following:

- none

Usage Guidelines Use this command to configure the SMF network function profile configuration parameters.

profile smf plmn-id

Configures the definition for public land mobile network identifier (PLMN ID) and the preferred radio access technology (RAT). This is one of PLMNs which is considered by the mobile as equivalent to the visited PLMN for cell reselection and network selection. When configured, the equivalent PLMN list will be sent to the UE in NAS ATTACH ACCEPT / TAU ACCEPT messages.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **`plmn-id { [ mcc`** *`mobile_country_code`* **`] [ mnc`** *`mobile_network_code`* **`] }`**

mcc *mobile_country_code*

Specify the mobile country code (MCC) portion of the PLMN ID.

Must be a 3-digit integer.

mnc *mobile_network_code*

Specify the mobile network code (MNC) portion of the PLMN ID.

Must be a 2- or 3-digit integer.

Usage Guidelines Use the command to identify a PLMN and assign it a priority to define the preferred PLMN to be used. This command can be entered multiple times to set priorities of usage.

profile smf service

Configures the session management network function services. The service names as specified in 3GPPTS 29.510 V15.2.0, Section 6.1.6.3.11.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Profile Configuration

Syntax Description

service *service_name*

nf-service *nf_service_name*

Specify the NF service name.

Must be a string.

type *service_type*

Specify the service type.

Must be one of the following:

- pdu-session
- sm-event-exposure

schema *schema_name*

Specify the schema name.

Must be a string.

service-id *service_id*

Specify the service ID.

Must be a string.

Default Value: "1".

version *version*

Specify the version.

Must be a string.

icmpv6-profile *profile_name*

Specify the ICMPv6 profile name.

Must be a string.

compliance-profile *compliance_profile_name*

Specify the compliance profile name.

Must be a string.

capacity *capacity*

Specify the static weight relative to other NFs of the same type.

Must be an integer in the range of 0-65535.

Default Value: 10.

priority *priority*

Specify the priority relative to other NFs of the same type.

Must be an integer in the range of 0-65535.

Default Value: 1.

access-profile *profile_name*

Specify the access profile name.

subscriber-policy *policy_name*

Specify the subscriber policy name.

Must be a string.

Usage Guidelines Use this command to configure the N1, N2, and N11 interfaces in compliance with the 3GPP.

profile smf service http-endpoint

Configures the SMF HTTP REST endpoint parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`http-endpoint base-url`** *`base_url`*

base-url *base_url*

Specify the SMF base URL that is exposed and accessible externally.

Must be a string.

Usage Guidelines Use this command to configure the SMF HTTP REST endpoint parameters.

profile tai-group

Configures TAI Group profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **profile tai-group** *profile_name*

profile_name

Specify the TAI group profile name.

Must be a string.

Usage Guidelines Use this command to configure the TAI Group profile parameters.

profile tai-group tais

Configures the list of MCC, MNC, and possible TACs.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > TAI Group Profile Configuration

Syntax Description **tais { mcc** *mobile_country_code* **| mnc** *mobile_network_code* **}**

mcc *mobile_country_code*

Specify the Mobile Country Code (MCC). For example, 01, 001.

Must be a 3-digit integer.

mnc *mobile_network_code*

Specify the Mobile Network Code (MNC). For example, 23, 456.

Must be a 2- or 3-digit integer.

Usage Guidelines Use this command to configure the list of MCC, MNC, and possible TACs.

You can configure a maximum of 16 elements with this command.

profile tai-group tais tac

Configures the TAC Group parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > TAI Group Profile Configuration

Syntax Description **tac list** *tac_values*

list *tac_values*

Specify the list of TAC values.

Must be a 4-digit string in the pattern [0-9a-fA-F], or a 6-digit string in the pattern [0-9a-fA-F].

Usage Guidelines Use this command to configure the TAC Group parameters.

You can configure a maximum of 64 elements with this command.

profile tai-group tais tac range

Configures TAC ranges.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > TAI Group Profile Configuration

Syntax Description **range start** *tac_range_start* **end** *tac_range_end*

Usage Guidelines Use this command to configure a TAC range.

You can configure a maximum of 16 elements with this command.

profile upf-group

Configures the UPF group parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **upf-group** *upf_group_name*

upf_group_name

Specify the UPF group name.

Must be a string.

Usage Guidelines Use this command to configure the UPF group parameters.

profile upf-group failure-profile

Configures the UPF failure profile.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **failure** *failure_profile_name*

failure_profile_name

Specify the UPF failure profile name.

Must be a string.

Usage Guidelines Use this command to configure the UPF failure profile.

profile upf-group heartbeat

Enables PFCP path management.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **heartbeat [interval** *heartbeat_interval* **| retransmission-timeout** *retransmission_timeout* **| max-retransmissions** *max_retransmissions* **]**

interval *heartbeat_interval*

Specify the heartbeat interval in seconds. To disable, set to 0.

Must be an integer.

Default Value: 60.

retransmission-timeout *retransmission_timeout*

Specify the heartbeat retransmission timeout period in seconds.

Must be an integer in the range of 1-20.

Default Value: 5.

max-retransmissions *max_retransmissions*

Specify the maximum number retries for PFCP heartbeat request.

Must be an integer in the range of 0-10.

Default Value: 3.

Usage Guidelines Use this command to enable PFCP path management.

profile wps

Configures the Wireless Priority Service (WPS) profile parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

wps *wps_service_name*

wps_service_name

Specify the WPS service name.

Must be a string.

arp ***arp_level_range***

Specify the range of ARP levels (separated by , or -).

Must be an integer.

-Or-

Must be a string.

message-priority ***message_priority***

Specify the message priority for GTP-C and UP.

Must be one of the following:

- pfcp
- gtpc

Usage Guidelines

Use this command to configure the WPS profile parameters.

You can configure a maximum of two elements with this command.

profile wps dscp

Configures the DSCP marking value for n3.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

dscp n3 *dscp_marking_value*

n3 ***dscp_marking_value***

Specify the UP DSCP marking value in the range 0 to 0x3F.

Must be an integer in the range of 0-63.

Usage Guidelines Use this command to confgiure the DSCP marking value for n3.

retransmission

Configures PFCP retransmission.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`retransmission { timeout`** *`pfcp_retransmission_interval`* **`| max-retry`** *`max_retries`* **`}`**

timeout *pfcp_retransmission_interval*

Specify the PFCP retransmission interval in seconds. To disable retransmission, configure to 0.

Must be an integer in the range of 0-10.

Default Value: 2.

max-retry *max_retries*

Specify the maximum number of times PFCP request retry attempts. To disable retransmission, configure to 0.

Must be an integer in the range of 0-5.

Default Value: 3.

Usage Guidelines Use this command to configure PFCP retransmission.

smf deployment component

Configures microservice name of the SMF deployment.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`component`** *`component_name`*

component *component_name*

Specify the microservice name of the SMF deployment.

Must be a string.

Usage Guidelines Use this command to configure the microservice name of the SMF deployment.

smf deployment component pod

Configure pod parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **pod** *pod_group_name* **[repository** *path* **]**

pod_group_name

Specify the pod group name.

Must be a string in the pattern [a-zA-Z][a-zA-Z0-9-]*.

repository *path*

Specify to override Helm Repository.

Usage Guidelines Use this command to configure pod parameters.

smf local

Configures the SMF local parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **local { coverage-build { false | true } | datastore-endpoint** *ep_config* **}**

datastore-endpoint *ep_config*

Specifes the data store endpoint configuration.

Must be a string.

Default Value: "datastore-ep-session:8882".

coverage-build { false | true }

Specify the coverage build setting.

Must be either "false" or "true".

Default Value: false.

Usage Guidelines Use this command to configure the SMF local etcd endpoint.

smf local etcd endpoint

Configures the SMF local etcd endpoint.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **etcd endpoint { host** *host_name* **| port** *port_number* **}**

host *host_name*

Specify the host name.

Must be a string.

Default Value: "etcd".

port *port_number*

Specify the port number.

Must be an integer.

Default Value: 2379.

Usage Guidelines Use this command to configure the SMF local etcd endpoint.

smf local tracing

Enables or disables and configures tracing.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **tracing { append-messages { false | true } | enable { false | true } | enable-trace-percent** *percentage* **}**

enable { false | true }

Specify to enable or disable tracing.

Must be either "false" or "true".

enable-trace-percent *percentage*

Specify the tracing percentage.

Must be an integer in the range of 0-100.

Default Value: 100.

append-messages { false | true }

Specify whether to append the messages or not.

Must be either "false" or "true".

Default Value: true.

Usage Guidelines Use this command to enable or disable and to configure tracing.

smf local tracing endpoint

Configures the endpoint parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **endpoint { host** *host_name* **| port** *port_number* **}**

host *host_name*

Specify the host name.

Must be a string.

Default Value: "jaeger-collector".

port *port_number*

Specify the port number.

Must be an integer.

Default Value: 9411.

Usage Guidelines Use this command to configure endpoint parameters.

smf profile gtp-ep

Configures the GTP endpoint node label.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **k8 smf profile gtp-ep node-label** *node_label*

node-label *node_label*

Specify the GTP endpoint node label.

Must be a string.

Usage Guidelines Use this command to configure the GTP endpoint node label.

smf profile protocol

Configures the protocol node label.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **k8 smf profile protocol node-label** *node_label*

node-label *node_label*

Specify the node label.

Must be a string.

Usage Guidelines Use this command to configure the protocol node label.

smf profile rcm-bfd-ep bfd-monitor group

Configures BFD application.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **k8 smf profile rcm-bfd-ep bfd-monitor group** *group_id* **[min-rx-int** *min_receive_interval* **| min-tx-int** *min_send_interval* **| multiplier** *multiplier_value* **| standby** *standby_upf* **]**

group_id

Specify the group ID.

Must be an integer.

min-tx-int *min_send_interval*

Specify the minimum send interval capability.

Must be an integer in the range of 50-10000.

min-rx-int *min_receive_interval*

Specify the minimum receive interval capability.

Must be an integer in the range of 50-10000.

multiplier *multiplier_value*

Specify the multiplier value used to compute holddown.

Must be an integer in the range of 3-50.

standby *standby_upf*

Specify the standby UPFs for N:M redundancy group.

Must be an integer in the range of 0-10.

Usage Guidelines Use this command to configure BFD application.

smf profile rcm-bfd-ep bfd-monitor group endpoint

Configures the endpoint address.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **endpoint** *endpoint_ip_address*

endpoint_ip_address

Specify the endpoint IP address.

Must be an IP address.

Usage Guidelines Use this command to configure the endpoint IP address.

smf profile rcm-config-ep

Configures the RCM configuration endpoint parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **k8 smf profile rcm-config-ep { [username** *user_name* **] [password** *password* **] }**

username *user_name*

Specify the RCM configuration endpoint user name.

Must be a string.

password *password*

Specify the RCM configuration endpoint password.

Must be a string.

Usage Guidelines Use this command to configure the GTP endpoint node label.

smf profile rcm-config-ep disable-cm

Disables specific configmaps.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description

```
k8 smf profile rcm-config-ep disable-cm { apn | chargingAction | creditCtrl
 | global | gtpp | gtpuService | miscacs | packetFilter | rulebase |
ruledef | sxService | upSvcs | upfCpg | upfIfc | urrList }
```

apn

Specify to disable APN configmaps.

gtpp

Specify to disable GTPP group configmaps.

creditCtrl

Specify to disable credit control configmaps.

packetFilter

Specify to disable packet filter configmaps.

urrList

Specify to disable URR ID configmaps.

ruledef

Specify to disable ruledef configmaps.

rulebase

Specify to disable rulebase configmaps.

miscacs

Specify to disable global config under ACS.

global

Specify to disable global config outside ACS.

chargingAction

Specify to disable charging action configmaps.

upfCpg

Specify to disable UPF control plane group configmaps.

upSvcs

Specify to disable UPF service configmaps.

sxService

Specify to disable Sx service configmaps.

gtpuService

Specify to disable GTPU service configmaps.

upfIfc

Specify to disable UPF interface configmaps.

Usage Guidelines Use this command to disable specific configmaps.

smf profile rcm-controller-ep endpoint grpc

Configures GRPC endpoint parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **k8 smf profile rcm-controller-ep endpoint grpc { name** *endpoint_name* **| port** *port_number* **| host** *host_name* **}**

name *endpoint_name*

Specify the GRPC endpoint name.

Must be a string.

port *port_number*

Specify the port number.

Must be an integer.

host *host_name*

Specify the host name.

Must be a string.

Usage Guidelines Use this command to configure TCP endpoint parameters.

smf profile rcm-controller-ep endpoint tcp

Configures TCP endpoint parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **k8 smf profile rcm-controller-ep endpoint tcp { name** *endpoint_name* **| port** *port_number* **| host** *host_name* **}**

name *endpoint_name*

Specify the TCP endpoint name.

Must be a string.

port *port_number*

Specify the port number.

Must be an integer.

host *host_name*

Specify the host name.

Must be a string.

Usage Guidelines Use this command to configure TCP endpoint parameters.

smf-tools

Enables or disables SMF tools.

Privilege Security Administrator, Administrator

Syntax Description **smf-tools enable { false | true }**

enable { false | true }

Specify to enable or disable SMF tools.

Must be either "false" or "true".

Default Value: false.

Usage Guidelines Use this command to enable or disable SMF tools.

smf-tools lfs

Configures the kubernetes node on which Lattice will be deployed.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

lfs [sctp-k8-node-name *name* **| sctp-ip-address** *ip_address* **| lattic-tar-url** *url* **| test-companion-tar-url** *url* **| ngap-spec-ver** *version* **| n1-spec-ver** *version* **| n7-spec-ver** *version* **| n10-spec-ver** *version* **| n11-spec-ver** *version* **| nrf-spec-ver** *version* **| chf-spec-ver** *version* **]**

sctp-k8-node-name *name*

Specify the kubernetes node name on which Lattice will be deployed.

Must be a string.

sctp-ip-address *ip_address*

Specify the external IP address for SCTP.

Must be an IP address.

lattic-tar-url *url*

Specify the Lattice TAR URL.

Must be a string.

test-companion-tar-url *url*

Specify the test companion TAR URL.

Must be a string.

ngap-spec-ver *version*

Specify the ngap interface specification version.

Must be a string.

n1-spec-ver *version*

Specify the N1 interface specification version.

Must be a string.

n7-spec-ver *version*

Specify the N7 interface specification version.

Must be a string.

n10-spec-ver *version*

Specify the N10 interface specification version.

Must be a string.

n11-spec-ver *version*

Specify the N11 interface specification version.

Must be a string.

nrf-spec-ver *version*

Specify the NRF specification version.

Must be a string.

chf-spec-ver *version*

Specify the N40 interface specification version.

Must be a string.

Usage Guidelines Use this command to configure the kubernetes node on which Lattice will be deployed.

supi-opt

Displays subscriber data.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **show subscriber supi [psid** *pdu_session_id* **|** *supi_option* **]**

psid *pdu_session_id*

Specify the PDU Session ID (PSID).

Must be an integer in the range of 1-15.

supi_option

Specify the SUPI option.

Must be one of the following:

- charging
- full
- policy
- userplane

Usage Guidelines Use this command to view subscriber data.

supi-opt

Clears subscriber data.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **clear subscriber supi [psid** *pdu_session_id* **| ebi** *eps_bearer_id* **]**

psid *pdu_session_id*

Specify the PDU Session ID (PSID).

Must be an integer in the range of 1-15.

ebi *eps_bearer_id*

Specify the EPS Bearer ID (EBI).

Must be a string.

Usage Guidelines Use this command to clear subscriber data.

supi-opt policy-opt

Displays subscriber data.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **policy** *policy_option*

policy *policy_option*

Specify the policy option.

Must be one of the following:

- flow
- rules

Usage Guidelines Use this command to view subscriber data.

traffic service

Configures Traffic Steering for SMF.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`traffic service default-destination`** *`default_destination`*

default-destination *default_destination*

Specify the default smf-service group to receive traffic.

Must be a string in the pattern [a-zA-Z][a-zA-Z0-9-]*.

Usage Guidelines Use this command to configure Traffic Steering for SMF.

traffic service rule

Configures traffic routing rule.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`traffic service rule`** *`rule_name`* **`{ [ destination`** *`destination_address`* **`] [ hash-prefix`** *`hash_prefix`* **`] }`**

rule *rule_name*

Specify the traffic routing rule name.

Must be a string.

hash-prefix *hash_prefix*

Specify the route on 2-digit hash.

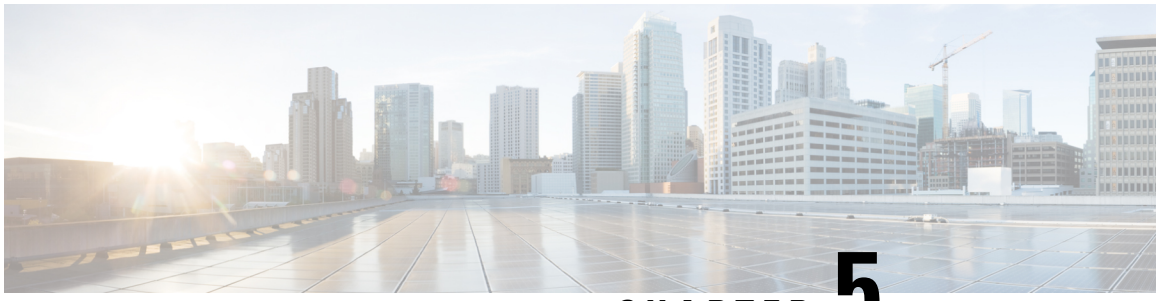
Must be a string.

destination *destination_address*

Specify the smf-service group to receive traffic.

Must be a string in the pattern [a-zA-Z][a-zA-Z0-9-]*.

Usage Guidelines Use this command to configure traffic routing rule.



CHAPTER 5

SMF NRF CLI Commands

group nf-mgmt

Configures NF management group name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **nf-mgmt** *mgmt_group_name* **{ nrf-mgmt-group** *nrf_mgmt_group_name* **| nrf-auth-group** *nrf_auth_group_name* **| locality** *locality_name* **| re-register { false | true } }**

mgmt_group_name

Specify the NRF management group name.

Must be a string.

nrf-mgmt-group ***nrf_mgmt_group_name***

Specify the NRF management group name.

Must be a string.

locality ***locality_name***

Specify locality information.

Must be a string.

Usage Guidelines Use this command to configure NF management group name.

group nf-mgmt failover

Configures failover SLA time duration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **failover sla** *failover_sla*

sla ***failover_sla***

Specify the failover sla time duration in milliseconds.

Must be an integer.

Usage Guidelines Use this command to configure the failover SLA time duration.

group nf-mgmt heartbeat

Configures heartbeat interval time in seconds.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **heartbeat interval** *heartbeat_interval*

interval *heartbeat_interval*

Specify the heartbeat interval time in seconds.

Must be an integer.

Usage Guidelines Use this command to configure the heartbeat interval time in seconds.

group nf-mgmt reconnect

Configures reconnect interval configuration.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **reconnect interval** *reconnect_interval*

interval *reconnect_interval*

Specify the reconnect interval time in milliseconds.

Must be an integer.

Usage Guidelines Use this command to configure reconnect interval time in milliseconds.

group nrf auth

Configures NRF auth group parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **auth** *group_name* **[nrf-type** *nrf_type* **]**

group_name

Specify the NRF auth group name.

Must be a string.

nrf-type *nrf_type*

Specify the NRF type.

Must be one of the following:

- PLMN: PLMN.
- SHARED: SHARED.
- SLICE-LOCAL: SLICE-LOCAL.

Usage Guidelines Use this command to configure NRF auth group parameters.

group nrf auth service type nrf

Configures NRF service auth name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **nrf nrf-service-name** *nrf_service_auth_name*

nrf-service-name *nrf_service_auth_name*

Specify the NRF service auth name.

Must be one of the following:

- oauth2

Usage Guidelines Use this command to configure the NRF service auth name.

group nrf auth service type nrf endpoint-profile

Configures endpoint profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *priority_value* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

endpoint_profile_name

Specify the endpoint profile name.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

priority *priority_value*

Specify the profile priority.

Must be an integer in the range of 0-65535.

Default Value: 1.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

api-root *api_root*

Specify the API root.

Must be a string.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- http: HTTP.
- https: HTTPS.

Usage Guidelines Use this command to configure endpoint profile parameters.

group nrf auth service type nrf endpoint-profile endpoint-name

Configures the endpoint name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *priority_value* **| capacity** *capacity_value* **]**

endpoint_name

Specify the endpoint name. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority *priority_value*

Specify the node priority for endpoint.

Must be an integer in the range of 0-65535.

capacity *capacity_value*

Specify the node capacity.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this configuration to configure the endpoint name.

group nrf auth service type nrf endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

group nrf auth service type nrf endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

group nrf auth service type nrf endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

ip-address { { ipv4 *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this command to configure the endpoint IP address and port number.

group nrf auth service type nrf endpoint-profile version uri-version

Configures the URI version.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description

version uri-version { *uri_version* **| full-version** *full_version* **}**

uri_version

Specify the URI version.

Must be a string in the pattern v\d.

full-version *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string.

Usage Guidelines

Use this command to configure the URI version information.

group nrf discovery

Configures NRF discovery group parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

discovery *group_name* **[nrf-type** *nrf_type* **]**

group_name

Specify the NRF discovery group name.

Must be a string.

nrf-type *nrf_type*

Specify the NRF type.

Must be one of the following:

- PLMN: PLMN.
- SHARED: SHARED.
- SLICE-LOCAL: SLICE-LOCAL.

Usage Guidelines

Use this command to configure the NRF discovery group configuration.

group nrf discovery service type nrf

Configures the NRF discovery service name.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

nrf *nrf_service_name* **[responsetimeout** *response_timeout* **]**

nrf_service_name

Specify the NRF discovery service name.

Must be one of the following:

- nnrf-disc

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines Use this command to configure the NRF discovery service name.

group nrf discovery service type nrf endpoint-profile

Configures endpoint profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

endpoint_profile_name

Specify the endpoint profile name.

Must be a string.

api-root *api_root*

Specify the API root.

Must be a string.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- http
- https

Usage Guidelines Use this command to configure endpoint profile parameters.

group nrf discovery service type nrf endpoint-profile endpoint-name

Configures endpoint parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *priority* **| capacity** *endpoint_capacity* **]**

endpoint_name

Specify the endpoint name.

Must be a string.

priority ***priority***

Specify the node priority for endpoint.

Must be an integer in the range of 0-65535.

capacity ***endpoint_capacity***

Specify the endpoint capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

Usage Guidelines Use this command to configure endpoint parameters.

group nrf discovery service type nrf endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

port ***port_number***

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

group nrf discovery service type nrf endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

ip-address { { ipv4 *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this command to configure the endpoint IP address and port number.

group nrf discovery service type nrf endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

ip-address { { ipv4 *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this command to configure the endpoint IP address and port number.

group nrf discovery service type nrf endpoint-profile version uri-version

Configures URI version information.

Privilege

Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **uri-version** *uri_version* **[full-version** *full_version* **]**

uri_version

Specify the URI version.

Must be a string in the pattern v\d.

full-version *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string.

Usage Guidelines Use this command to configure URI version information.

group nrf mgmt

Configures the NRF self-management group parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **mgmt** *group_name* **[nrf-type** *nrf_type* **]**

group_name

Specify the NRF self-management group name.

Must be a string.

nrf-type *nrf_type*

Specify the NRF type.

Must be one of the following:

- PLMN: PLMN.
- SHARED: SHARED.
- SLICE-LOCAL: SLICE-LOCAL.

Usage Guidelines Use this command to configure the NRF self-management group parameters.

group nrf mgmt service type nrf

Configures the NRF self-management service name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **nrf nrf-service-name** *nrf_service_name* **[responsetimeout** *response_timeout* **]**

nrf-service-name *nrf_service_name*

Specify the NRF service name.

Must be one of the following:

- nnrf-nfm

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines Use this command to configure the NRF self-management service name.

group nrf mgmt service type nrf endpoint-profile

Configures endpoint profile parameters.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

endpoint_profile_name

Specify the endpoint profile name.

Must be a string.

api-root *api_root*

Specify the API root.

Must be a string.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- http
- https

Usage Guidelines Use this command to configure endpoint profile parameters.

group nrf mgmt service type nrf endpoint-profile endpoint-name

Configures the endpoint name.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *priority* **]**

endpoint_name

Specify the endpoint name.

Must be a string.

priority *priority*

Specify the node priority for endpoint.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint name.

group nrf mgmt service type nrf endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be an IPv4 address.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be an IPv6 address.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

group nrf mgmt service type nrf endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Syntax Description **`ip-address { { ipv4`** *`ipv4_address`* **`| ipv6`** *`ipv6_address`* **`} | port`** *`port_number`* **`}`**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be an IPv4 address.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be an IPv6 address.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

group nrf mgmt service type nrf endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

ip-address { { ipv4 *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 ***ipv4_address***

Specify the IPv4 address.

Must be an IPv4 address.

ipv6 ***ipv6_address***

Specify the IPv6 address.

Must be an IPv6 address.

port ***port_number***

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this command to configure the endpoint IP address and port number.

group nrf mgmt service type nrf endpoint-profile version uri-version

Configures version information.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Syntax Description

uri-version *uri_version* **[full-version** *full_version* **]**

uri_version

Specify the URI version.

Must be a string in the pattern v\d.

full-version *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string.

Usage Guidelines

Use this command to configure the version information.