Global Configuration Mode Commands (L-S)

The Global Configuration Mode is used to configure basic system-wide parameters.

Command Modes

This section includes the commands **license** through **system**.

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

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

- license, on page 3
- line, on page 5
- link-aggregation, on page 5
- local-policy-service, on page 7
- local-user allow-aaa-authentication, on page 8
- local-user lockout-time, on page 9
- local-user max-failed-logins, on page 10
- local-user password, on page 11
- local-user username, on page 14
- logging console, on page 18
- logging disable, on page 19
- logging display, on page 20
- logging filter, on page 21
- logging include-ueid, on page 32
- logging monitor, on page 35
- logging runtime, on page 36
- logging syslog, on page 36
- lte-policy, on page 37
- mediation-device, on page 38
- mme-manager, on page 38

- msisdn-group, on page 38
- network-overload-protection mme-new-connections-per-second, on page 39
- network-overload-protection mme-tx-msg-rate-control, on page 42
- network-overload-protection sgsn-new-connections-per-second, on page 43
- network-service-entity, on page 45
- nsh, on page 46
- ntp, on page 47
- ntsr pool-id, on page 48
- operator-policy, on page 49
- orbem force , on page 50
- pac-standby-priority, on page 51
- pco-options, on page 51
- pdu-session-recovery, on page 54
- peer-profile, on page 55
- plugin, on page 57
- port ethernet, on page 57
- port rs232, on page 58
- profile-id-qci-mapping, on page 59
- ps-network, on page 60
- qci, on page 62
- qci-qos-mapping, on page 64
- qos ip-dscp-iphb-mapping, on page 65
- qos l2-mapping-table, on page 66
- qos npu inter-subscriber traffic bandwidth, on page 67
- qos npu inter-subscriber traffic bandwidth-sharing, on page 69
- qos npu inter-subscriber traffic priority, on page 70
- quality-of-service-profile, on page 72
- ran-peer-map, on page 73
- require active-charging, on page 74
- require aes-ni, on page 75
- require crypto, on page 76
- require demux, on page 77
- require detailed-rohc-stats, on page 79
- require diameter origin-host-abbreviation, on page 80
- require diameter-proxy, on page 81
- require ecs credit-control, on page 84
- require graceful-cleanup-during-audit-failure, on page 85
- require ipsec-large, on page 87
- require segregated li-configuration, on page 87
- require session ipsecmgr-per-vcpu, on page 87
- require session recovery, on page 88
- require session sessmgr-per-vcpu, on page 90
- reveal disabled commands, on page 91
- rlf-template, on page 92
- rohc-profile, on page 94
- sccp-network, on page 95

- sctp-param-template, on page 96
- security, on page 97
- service-chain, on page 97
- session disconnect-reasons bucket-interval, on page 98
- session trace, on page 99
- sgsn-global, on page 101
- sgsn-operator-policy, on page 102
- snmp authentication-failure-trap, on page 104
- snmp community, on page 104
- snmp discard-snmpv3-pdu, on page 106
- snmp engine-id, on page 106
- snmp heartbeat, on page 107
- snmp history heartbeat, on page 108
- snmp mib, on page 109
- snmp notif-threshold, on page 109
- snmp runtime-debug, on page 111
- snmp server, on page 112
- snmp target, on page 113
- snmp trap, on page 115
- snmp trap-pdu-v1tov2, on page 117
- snmp trap-timestamps, on page 117
- snmp user, on page 118
- ss7-routing-domain, on page 120
- ssh key-gen wait-time, on page 121
- ssh key-size, on page 122
- statistics-backup , on page 123
- stats-profile, on page 125
- statistics-backup-interval, on page 126
- support collection, on page 127
- support record, on page 128
- suspend local-user, on page 130
- system, on page 130

license

Configures the license keys on the system.

In Release 21.3 and higher, this command also enables or disables Cisco Smart Licensing on this system.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

[no] license { key *key_value* **[-force] session-limit | smart { enable | call-home destination url** *https link* **}**

no

Removes the license key(s) installed.

no smart license enable disables smart licensing on this system.

no smart license call-home destination url removes the configured URL where Cisco Smart Software Manager (CSSM) can be reached.

key *key_value*

Installs the license key specified by *key_value*. *key_value* is enclosed with double quotation marks (" "). The license is provided by the Cisco operations staff.

-force

Sets the license key even if resources are not available. The system supports the dynamic resizing of demultiplexor software tasks based on the licensed session capacity and feature type. When installing a license, the system automatically attempts to resize currently functioning tasks. Warning messages are displayed if there is an issue. Though its use is not recommended, the **-force** keyword can be used to suppress these warning messages.

Using the **-force** keyword to install an invalid license key automatically places the license in a 30-day grace period.

Caution Use of this option is not recommended.

session-limit

Use this keyword to suppress fail-over calls from being rejected if the licensed threshold is crossed.

Important This is a customer-specific command that is available for HA, PDSN, EHA, and PDIF. Please contact your local Cisco sales representative for more information.

smart { enable | call-home destination url *https link* }

- **enable:** Enables Cisco Smart Licensing on this system. By default this feature is disabled. No communication with Cisco is triggered when this command is issued.

  For more information, refer to the **license smart register** Exec mode command, as well as the *Licensing* chapter in the *System Administration Guide*.

- **call-home destination url *https link* :** This optional keyword configures the destination URL where Cisco Smart Software Manager (CSSM) can be reached. By default, this is set to the public CSSM URL and does not need to be updated unless a Smart Software Manager satellite is installed on premise.

Usage Guidelines

Install or update system session keys when necessary due to expiration and/or capacity needs.

In Release 21.3 and higher, this command also enables or disables Cisco Smart Licensing on this system and configures the optional CSSM Call-Home destination URL.

Example

The following command installs the license key that appears within double quotation marks:

```
license key
"\VER=1|C1M=StarentSimCF|C1S=10000020|DOI=1339011659|DOE=1354866669|ISS=3
|NUM=52612|CMT=BxB_HSGW|LEC=1000|FIS=Y|FR4=Y|FTC=Y|FSR=Y|FI6=Y|FLI=Y
|FCA=Y|FTM=Y|FTP=Y|FDC=Y|FGR=Y|FAA=Y|FDQ=Y|BEP=Y|FAI=Y|FLS=Y|LGW=1000|FVN=Y|
FRE=Y|FUR=Y|FAL=Y|FST=Y|FLP=Y|FSE=Y|FIT=Y|LSE=2000|FUZ=Y|SIG=MC0CFAZdtHcnRL/
SN4hXY3CJFQy/e/JXAhUA3JWMbauC7RMF7hVJxzS0fCSXCMQ"
```

line

Enters the terminal display Line Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

line

Usage Guidelines

Change the terminal display configuration based upon the users own terminal characteristics.

The following command enters the Line Configuration mode.

line

link-aggregation

Configures system MAC address and priority for Link Aggregation. These parameters are usually changed to match the feature requirements of the remote Ethernet switch.

Product

WiMAX

PDSN

HA

FA

GGSN

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

link-aggregation { system-mac { *mac_address* | auto } | system-priority *priority* **} [-noconfirm]**
{ default | no } link-aggregation { system-mac | system-priority } [-noconfirm]

default

Resets the configuration to the default.

system-mac { *mac_address* | auto }

Sets the system MAC address used along with the system priority to form the system ID.

mac_address is manually entered as six groups of two hexadecimal digits separated by hyphens (for example, 01-23-45-67-89-ab).

Auto is the default and is the MAC address of the LAG master port.

system-priority *priority*

This command sets the system priority used by Link Aggregation Control Protocol (LACP) to form the system ID.

priority is a hexadecimal value from 0x0000 through 0xFFFF. Default is 0x8000 (32768).

-noconfirm

Executes the command without additional prompting for command confirmation.

Usage Guidelines

The system MAC address (6 bytes) and system priority (2 bytes) combine to form the system ID. A system consists of a packet processing card and its associated QGLC or XGLC traffic ports. The highest system ID priority (the lowest number) handles dynamic changes.

For additional usage and configuration information for the link aggregation feature, refer to the *System Administration Guide*.

Important Not supported on all platforms

Example

The following command configures the link aggregation system-priority to 10640 (0x2990):

```
link-aggregation system-priority 0x2990
```

local-policy-service

This command enables creating, configuring, or deleting a local QoS policy.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
local-policy-service name [ -noconfirm ]
no local-policy-service name
```

no

Deletes the specified local QoS policy service from the system.

name

Specifies name of the local QoS policy service as an alphanumeric string of 1 through 63 characters.

Important

The *name* must be unique across all contexts.

If the named local QoS policy service does not exist, it is created, and the CLI mode changes to the Local Policy Service Configuration Mode wherein the local QoS policy service can be configured.

If the named local QoS policy service already exists, the CLI mode changes to the Local Policy Service Configuration Mode for that local QoS policy service.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to specify a local QoS policy service name to allow configuration of a local QoS policy service.

Important This feature is license dependent. Please contact your local sales representative for more information.

A local QoS policy service can be used to control different aspects of a session, such as QoS, data usage, subscription profiles, or server usage, by means of locally defined policies.

Local QoS policies are triggered when certain events occur and the associated conditions are satisfied. For example, when a new call is initiated, the QoS to be applied for the call could be decided based on the IMSI, MSISDN, and APN.

Important A maximum of 16 local QoS policy services are supported.

Entering this command results in the following prompt:

```
[context_name]hostname(config-local-policy-service)#
```

Local Policy Service Configuration Mode commands are defined in the *Local Policy Service Configuration Mode Commands* chapter.

Example

The following command creates a local QoS policy service named *lctest* and enters the Local Policy Service Configuration Mode:

```
local-policy-service lctest
```

local-user allow-aaa-authentication

Enables or disables the use of administrative accounts other than local-user administrative accounts.

Important In a release 20.0 or higher Trusted build, this command is not available.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
[ default | no ] local-user allow-aaa-authentication [ noconsole ]
```

default

Returns this parameter to its default setting of enabled.

no

Disables administrative user accounts other than local-user accounts.

noconsole

Prevents authentication via non-local-user mechanisms when logging into a Console port.

Since local user authentication is always performed before AAA-based authentication, if **local-user allow-aaa-authentication noconsole** is configured, the behavior is the same as if **no local-user allow-aaa-authentication** is configured. However, there is no impact on SSH or tenet logins (vty lines).

Usage Guidelines

Local-user administrative accounts are separate from other administrative user accounts configured at the context level (Security Administrator, Administrator, Operator, and Inspector).

Context-level administrative users rely on the system's AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS server.

Since the T1.276-2003 password security mechanisms are supported only for local-user administrative accounts and not for the AAA-based administrative accounts, this command provides a mechanism for disabling AAA-based administrative accounts.

By default, AAA-based administrative accounts are allowed.

Example

The following command forces the system to authenticate local-user accounts based only on the information in the security account file on its CompactFlash:

```
no local-user allow-aaa-authentication
```

local-user lockout-time

Configures the lockout period for local-user administrative accounts.

Important In a release 20.0 or higher Trusted build, this command is not available.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

local-user lockout-time *time*
default local-user lockout-time

default

Restores the parameter to its default setting.

time

Default: 60

Specifies the amount of time (in minutes) that must elapse before a previously locked-out local-user account can attempt to login again. *time* is an integer from 1 through 10080.

Usage Guidelines

Local-user administrative accounts can become locked for reasons such as exceeding the configured maximum number of login failures.

Once an account is locked, this parameter specifies the lockout duration. Once the amount of time configured by this parameter has elapsed, the local-user can once again attempt to login.

Example

The following command configures a lockout time of *120* minutes (2 hours):

```
local-user lockout-time 120
```

local-user max-failed-logins

Configures the maximum number of failed login attempts a local-user can have before their account is locked out.

Important In a release 20.0 or higher Trusted build, this command is not available.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

local-user max-failed-logins *number*
[default | no] local-user max-failed-logins

no

Disables this functionality.

default

Restores this parameter to its default setting of 5.

number

Specifies the maximum number of times a local-user could experience a login failure before their account is locked out. *number* is an integer from 2 through 100. Default: 5

Usage Guidelines

This command configures the maximum number of failed login attempts a local-user can have before their account is locked out. For example if, this parameter is configured to "3" then after the third failed login attempt, the account would be locked.

Important

Local-user accounts can be configured to either enforce or reject a lockout due to the maximum number of failed login being reached. Refer to the **local-user username** command for more information.

Refer to the **local-user lockout-time** command for more information.

Example

The following command configures a maximum of three login attempts:

```
local-user max-failed-logins 3
```

local-user password

Configures local-user administrative account password properties.

Important

In a release 20.0 or higher Trusted build, this command is not available.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
local-user password { [ complexity { ansi-t1.276-2003 | none } ] [ history
 length number [ duration days ] ] [ max-age days ] [ min-change-char number
```

] [min-change-interval *days* **] [min-length** *number* **] [exp-warn-interval** *days* **] [exp-grace-interval** *days* **] [security-admin | administrator | inspector | operator] [auto-generate [none | length** *password-length*] **}**
no local-user password { [history] [max-age] [min-change-interval] [exp-warn-interval] [exp-grace-interval] }
default local-user password { [complexity] [history] [max-age] [min-change-char] [min-change-interval] [min-length] [exp-warn-interval] [auto-generate] [exp-grace-interval] }

no

Disables the specified parameter.

default

Restores the specified parameter to its default setting.

[complexity { ansi-t1.276-2003 | none }]

Default: ansi-t1.276-2003

Specifies the password strength as one of the following:

- **ansi-t1.276-2003:** If this option is selected, the following rules are enforced:
- Passwords may not contain the username or the reverse of the username
- Passwords may contain no more than three of the same characters used consecutively
- Passwords must contain at least three of the following:
  - uppercase alpha character (A, B, C, D ... Z)
  - lowercase alpha character (a, b, c, d ... z)
  - numeric character (0, 1, 2, 3 ...)
  - special character (see the *Alphanumeric Strings* section of the *Command Line Interface Overview* chapter)
- **none:** Only the password length is checked. No additional password checks are performed.

[history length *number* [duration *days*]]

Default: length is 5

Specifies the number of previous password entries kept in the history list maintained by the system. A password cannot be reused if it is one of the entries kept in the history list unless the time it was last used was more than the number of days specified by the **duration** keyword.

If the duration keyword is not used, the only check performed by the system is that it is not in the history list.

number is the number of entries for each account stored in the history list entered as an integer from 1 through 100. *days* is the number of days during which a password can not be reused entered an integer from 1 through 365.

[max-age *days*]

Specifies the maximum age for a password. Users logging in with a password older than the specified limit are locked out. Once the lockout period expires, at their next login attempt, they are prompted to change their password before accessing the CLI. Default: 90

Important Local-user accounts can be configured to either enforce or reject a lockout due to a password's maximum age being reached. Refer to the **local-user username** command for more information.

days is the number of days that passwords remain valid entered as an integer from 1 through 365.

[min-change-char *number*]

Specifies the minimum number of characters that must be changed (in comparison to the current password) when a user changes their password. Default: 2

Important Changes in password length are counted as "character" changes. For example: changing a password from "password" to "passwo" is a 2-character change, changing a password from "password" to "password2" is a 1-character change, and changing a password from "password" to "apassword" is a 9-character change.

number is the number of characters entered as an integer from 0 through 16.

[min-change-interval *days*]

Specifies the frequency that passwords can be changed (other than first login).

days is the minimum number of days that must pass before a user can change their password. It is an integer from 1 through 365. Default: 1

Important If the **no local-user password min-change-interval** command is used, users may change their password as often as desired which could allow them to circumvent the password history function.

[min-length *number*]

Specifies the minimum length allowed for user-defined password.

number is the minimum number of alphanumeric characters that the password must contain, entered as an integer from 3 through 32. Default: 8

[exp-warn-interval *days*]

Specifies the password expiry warning interval in days.

days is the number of days before which password expiry warning is issued. The default is 30 days.

[exp-grace-interval *days*]

Specifies the password expiry grace interval in days. The default is 3 days after expiry.

days is the number of days beyond password expiry date at which the account is locked. The valid values range from 1 to 7 days. The default is 3 days.

[security-admin | administrator | inspector | operator]

Configures as follows:

security-admin: Configures all local users with security administrator rights.

administrator: Configures all local users with administrator rights.

inspector: Configures all local users with inspector rights.

operator: Configures all local users with operator rights.

[auto-generate [none | length *password-length*]

Presents an automatically generated password to the user at login when password is expired or found weak.

The auto-generate option is enabled by default with the password length of 8.

none : Specifies that the user must not be presented with the option to automatically generate a password.

length *password-length* : Specifies the length of the automatically-generated password for the user. The length of the automatically-generated password is an integer between 6 to 127.

Usage Guidelines

This command is used to set the property requirements for user-defined passwords and system behavior in relation to those passwords.

Information pertaining to user passwords, login failures, and password history are stored on the packet processing cards and in the software's Shared Configuration Task (SCT).

The system uses the information in the SCT for runtime operations such as determining password ages and determining if new passwords meet the criteria specified by this command.

Example

The following command configures a minimum password length requirement of *6* characters:

```
local-user password min-length 6
```

The following command configures the system to store the *4* most recently used passwords per user-account in the history list:

```
local-user password history length 4
```

The following command configures the password expiry warning interval.

```
local-user password exp-warn-interval 15
```

The following command configures the auto-generated password with the specified length.

```
local-user password auto-generate length 10
```

local-user username

Adds or removes local-user administrative accounts.

Important In a release 20.0 or higher Trusted build, this command is not available.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

local-user username *name* **[authorization-level { administrator | inspector | operator | security-admin }] [ecs | noecs] [ftp [sftp-server]** *sftp-name* **] | noftp] [timeout-min-absolute** *time* **] [max sessions** *number* **] [no-lockout-login-failure] [no-lockout-password-aging] [noconsole | novty][suspend-date** *YYYY:MM:DD:HH:MM:SS* **[no warn-date | warn-date** *YYYY:MM:DD:HH:MM:SS* **]] [max-age** *days* **[no exp-warn-interval | exp-warn-interval** *days* **] | [no-exp-grace-interval | exp-grace-interval** *days* **]] [password** *password* **| nopassword] [timeoute-min-idle** *time* **]**
no local-user username *name*

no

Removes a previously configured user.

name

Specifies the name of the user as an alphanumeric string of 3 through 16 characters that is case sensitive.

[ecs | noecs]

Specifies whether or not the user has access to Active Charging Service configuration parameters.

- **ecs**: The user has access.
- **noecs**: The user does not have access.

Default: **ecs**

[ftp | noftp]

Default: ftp

Specifies whether or not the user is allowed to access the system via the File Transfer Protocol (FTP) and/or the Secure File Transfer Protocol (SFTP).

- **ftp**: The user has access.
- **noftp**: The user does not have access.

[sftp-server *sftp_name*]

Assigns an optional root directory and access privilege to this user. *sftp_name* must have been previously created via the SSH Server Configuration mode **subsystem sftp** command.

[max-sessions number

Default: Disabled

max-sessions *number*: Configures the maximum number of simultaneous CLI sessions for one user. *number* must be an alphanumeric integer from 1 to 100. **Default:** No limit.

Important The only way to change the configured max-sessions number is to delete the user and then re-configure user with a different max-sessions number.

Important The user is requested to change their password upon their first login.

[no-lockout-login-failure]

Default: Disabled

Specifies that this user will never be locked out due to login attempt failures.

[no-lockout-password-aging]

Default: Disabled

Specifies that this user will never be locked out due to the age of their password.

[noconsole | novty]

Specifies whether or not a user can login through a Console port or SSH/telnet (vty line).

- **noconsole** denies login via a Console port
- **novty** denies login via SSH or telnet

By default logins to Console and vty lines are allowed.

[suspend-date *YYYY:MM:DD:HH:MM:SS* [no warn-date | warn-date *YYYY:MM:DD:HH:MM:SS*]]

Specifies the date and time when the local-user account should be suspended.

YYYY:MM:DD:HH:MM:SS is the clock in format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.

no warn-date : Disables impending password expiry warnings.

warn-date *YYYY:MM:DD:HH:MM:SS*: Specifies the date and time when the local-user account suspension warning notification starts.

YYYY:MM:DD:HH:MM:SS is the clock in format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.

[max-age *days* [no exp-warn-interval | exp-warn-interval *days*]]

max-age *days*: Specifies the maximum age for a password. Users logging in with a password older than the specified limit are locked out. After the lockout period expires, at their next login attempt, they are prompted to change their password before accessing the CLI.

Important Local-user accounts can be configured to either enforce or reject a lockout due to a password's maximum age being reached. Refer to the **local-user username** command for more information.

days is the number of days that passwords remain valid entered as an integer from 1 to 365. The global or user group value is considered as the default value.

no exp-warn-interval: Disables impending password expiry warnings.

exp-warn-interval *days*: Specifies the password expiry warning interval in days.

days is the number of days before which password expiry warning is issued. The valid values range from 7 to 90 days. The global or user group value is considered as the default value.

[no-exp-grace-interval | exp-grace-interval *days*]

no exp-grace-interval : Disables grace period of expired password.

exp-grace-interval *days*: Specifies the password expiry grace interval in days.

days is the number of days beyond password expiry date at which the account is locked. The valid values range from 1 to 7 days. The global or user group value is considered as the default value.

[password *password* | nopassword]

Specifies the initial password for this user. *password* must an alphanumeric string of 6 through 32 characters that is case sensitive.

Important The user is requested to change their password upon their first login.

[timeout-min-absolute *time*]

Default: 0

Specifics the maximum session time (in minutes) for this user. *time* is an integer from 0 through 525600. A value of "0" indicates no limit.

Important This limit applies only to the user's CLI sessions.

[timeout-min-idle *time*]

Default: 0

Specifics the maximum idle time (in minutes) for this user. *time* is an integer from 0 through 525600. A value of "0" indicates no limit.

Important This limit applies only to the user's CLI sessions.

Usage Guidelines

The ability to configure administrative local-users is provided in support of the login security mechanisms specified in ANSI T1.276-2003.

Like administrative users configured at the context level, local-users can be assigned one of 4 security levels:

Local-User Level User	Context Level User
Security Administrator	Administrator
Administrator	Config-Administrator
Operator	Operator
Inspector	Inspector

Local-user configuration support is handled differently from that provided for administrative users configured at the context level.

Context-level administrative users rely on the system's AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS server. Passwords for these user types are assigned once and are accessible in the configuration file.

Local-user account information (passwords, password history, lockout states, etc.) is maintained in non-volatile memory and in the software's Shared Configuration Task (SCT). This information is maintained in a separate file – not in configuration files used by the system. As such, the configured local-user accounts are not visible with the rest of the system configuration.

Local-user and context-level administrative accounts can be used in parallel.

Example

The following command configures a security-administrator level local-user administrative account for a user named *User672* that has FTP privileges, a temporary password of *abc123*, and that does not lockout due to either login attempt failures or password aging:

```
local-user username User672 authorization-level security-admin ftp
no-lockout-login-failure no-lockout-password-aging password abc123
```

The following command deletes a previously configured local-user administrative account called admin32:

```
no local-user username admin32
```

logging console

Enables the output of logged events to be displayed on the console terminal.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

`[ no ] logging console`

no

Disables the output of events to the console port.

Usage Guidelines

Log console output to allow for offline review during system monitoring and/or trouble shooting.

logging disable

Enables/disables the logging of the specified event ID or range of IDs.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

`[ no ] logging disable eventid` *`id`* **`[ to`** *`to_id`* **`]`**

no

Indicates the event IDs specified are to be enabled for logging.

eventid *id*

Specifies the event for which no logging is to occur.

In 14.1 and earlier releases, *id* is an integer from 1 through 202699.

In 15.0, *id* is an integer from 1 through 204999.

In 17.0 and later releases, *id* is an integer from 1 through 215999.

to *to_id*

Specifies the end ID of the events when a range of event ID is to be disabled from being logged. *to_id* must be an integer from 1 through 204999. The *to_id* must be equal to or larger than the *id* specified.

Usage Guidelines Disable common events which may occur with a normal frequency are not of interest in monitoring the system for troubles.

Example

The following command disables the logging the range of events from 4500 through 4599, respectively.

```
logging disable eventid 4500 to 4599
```

logging display

Configures the level of detail for information to be logged.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **`logging display ( event-verbosity ( min | concise | full } | pdu-data { none | hex | hex-ascii } | pdu-verbosity`** *`pdu_level`* **`}`**

event-verbosity (min | concise | full }

Specifies the level of verboseness to use in logging of events as one of:

- **min**: displays minimal detail.
- **concise**: displays summary detail.
- **full**: dislays all details.

pdu-data { none | hex | hex-ascii }

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

- **none**: output in raw format.
- **hex**: displays output in hexadecimal format.
- **hex-ascii**: displays output in hexadecimal and ASCII similar to a main-frame dump.

pdu-verbosity *pdu_level*

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

Usage Guidelines Tune the level of information to be logged so as to avoid flooding a log file with information which is not useful or critical.

Example

The following sets event logging to display the maximum amount of detail.

```
logging display event-verbosity full
```

logging filter

Configures the logging of events to be performed in real time for the specified facility.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **logging filter runtime facility** *facility* **level** *report_level* **[critical-info | no-critical-info]**

facility *facility*

Specifies the facility to modify the filtering of logged information. The following list displays the valid facilities for this command:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: Authentication, Authorization and Accounting (AAA) client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
- **acl-log**: Access Control List (ACL) logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: ACS Manager facility
- **afctrl**: Fabric Controller facility [ASR 5500 only]
- **afmgr**: Fabric Manager logging facility [ASR 5500 only]

- **alarmctrl**: Alarm Controller facility
- **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility
- **alcapmgr**: ALCAP manager logging facility
- **all**: All facilities
- **asngwmgr**: Access Service Network (ASN) Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-Demux Manager logging facility
- **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **callhome**: Call Home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]
- **cdf**: Charging Data Function (CDF) logging facility
- **cgw**: Converged Access Gateway (CGW) logging facility
- **cli**: Command Line Interface (CLI) logging facility
- **cmp**: Certificate Management Protocol (IPSec) logging facility
- **connectedapps**: SecGW ASR 9000 oneP communication procotol
- **connproxy**: Controller Proxy logging facility
- **credit-control**: Credit Control (CC) facility
- **csp**: Card/Slot/Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: CSS RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility [CSCF <--> HSS]
- **data-mgr**: Data Manager Framework logging facility
- **dcardctrl**: IPSec Daughter Card Controller logging facility
- **dcardmgr**: IPSec Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility

- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diactrl**: Diameter Controller proclet logging facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-engine**: Diameter version2 engine logging facility
- **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSec Data Path facility
- **drvctrl**: Driver Controller facility
- **dpath**: IPSec Data Path logging facility
- **drvctrl**: Driver Controller logging facility
- **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
- **eap-diameter**: Extensible Authentication Protocol (EAP) IP Sec urity facility
- **eap-ipsec**: Extensible Authentication Protocol (EAP) IPSec facility
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
- **egtpu**: eGTP-U logging facility
- **embms**: evolved Multimedia Broadcast Multicast Service Gateway facility
- **embms**: eMBMS Gateway Demux facility
- **epdg**: evolved Packet Data (ePDG) gateway logging facility
- **event-notif**: Event Notification Interface logging facility
- **evlog**: Event log facility

- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: Femto Network Gateway (FNG) logging facility
- **gbmgr**: SGSN Gb Interface Manager facility
- **gmm**:
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  - For 3G: Logs the access application layer (above the RANAP layer)
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol manager logging facility
- **gtpp**: GTP-prime protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTP-U Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **h248prt**: H.248 port manager facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **henbapp**: Home Evolved NodeB (HENB) App facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgw**: HENB-GW facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgw-pws**: HENB-GW Public Warning System logging facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgw-sctp-acs**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgw-sctp-nw**: HENBGW network SCTP facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgwdemux**: HENB-GW Demux facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **henbgwmgr**: HENB-GW Manager facility

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

- **hnb-gw**: HNB-GW (3G Femto GW) logging facility

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

- **hnbmgr**: HNB-GW Demux Manager logging facility

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

- **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
- **igmp**: Internet Group Management Protocol (IGMP)
- **ikev2**: Internet Key Exchange version 2 (IKEv2)
- **ims-authorizatn**: IP Multimedia Subsystem (IMS) Authorization Service facility
- **ims-sh**: HSS Diameter Sh Interface Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMS User Equipment (IMSUE) facility
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
- **ipne**: IP Network Enabler (IPNE) facility
- **ipsec**: IP Security logging facility
- **ipsecdemux**: IPSec demux logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: Key/Value Store (KVSTORE) Store facility
- **l2tp-control**: Layer 2 Tunneling Protocol (L2TP) control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: Link Aggregation Group (LAG) manager logging facility
- **lcs**: Location Services (LCS) logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)

- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **location-service**: Location Services facility
- **m3ap**: M3 Application Protocol facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: Mobile Application Part (MAP) protocol logging facility
- **megadiammgr**: MegaDiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity (MME) Application logging facility
- **mme-embms**: MME evolved Multimedia Broadcast Multicast Service facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
- **mrme**: Multi Radio Mobility Entity (MRME) logging facility
- **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
- **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
- **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
- **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
- **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
- **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
- **netwstrg**: Network Storage facility
- **npuctrl**: Network Processor Unit Control facility
- **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager facility

- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-drv**: NPUMGR DRV logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-lc**: NPUMGR LC logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **npumgr-rri**: NPUMGR RRI (Reverse Route Injection) logging facility
- **npumgr-vpn**: NPUMGR VPN logging facility
- **npusim**: NPUSIM logging facility [ASR 5500 only]
- **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
- **ocsp**: Online Certificate Status Protocol logging facility.
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pagingmgr**: PAGINGMGR logging facility
- **pccmgr**: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
- **pdg**: Packet Data Gateway (PDG) logging facility
- **pdgdmgr**: PDG Demux Manager logging facility
- **pdif**: Packet Data Interworking Function (PDIF) logging facility
- **pgw**: Packet Data Network Gateway (PGW) logging facility
- **pmm-app**: Packet Mobility Management (PMM) application logging facility
- **ppp**: Point-To-Point Protocol (PPP) link and packet facilities
- **pppoe**: PPP over Ethernet logging facility
- **proclet-map-frwk**: Proclet mapping framework logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)

- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Diameter Rf interface messages facility
- **rip**: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
- **rlf**: Rate Limiting Function (RLF) logging facility
- **rohc**: Robust Header Compression (RoHC) facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
- **s102**: S102 protocol logging facility
- **s102mgr**: S102Mgr logging facility
- **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
- **sabp**: Service Area Broadcast Protocol (SABP) logging facility
- **saegw**: System Architecture Evolution (SAE) Gateway facility
- **sbc**: SBc protocol logging facility
- **sccp:** Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **sct**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef_ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN "glue" interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility

- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSN System Components logging facility (used infrequently)
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sls**: Service Level Specification (SLS) protocol logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
- **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
- **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
- **ssl**: Secure Socket Layer (SSL) message logging facility
- **stat**: Statistics logging facility
- **supserv**: Supplementary Services logging facility [H.323]
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility
- **threshold**: threshold logging facility
- **ttg**: Tunnel Termination Gateway (TTG) logging facility
- **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
- **udr**: User Data Record (UDR) facility (used with the Charging Service)
- **user-data**: User data logging facility

- **user-l3tunnel**: User Layer 3 tunnel logging facility
- **usertcp-stack**: User TCP Stack
- **vim**: Voice Instant Messaging (VIM) logging facility
- **vinfo**: VINFO logging facility
- **vmgctrl**: Virtual Media Gateway (VMG) controller facility
- **vmgctrl**: VMG Content Manager facility
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6
- **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)
- **x2gw-app**: X2GW (X2 proxy Gateway, eNodeB) application logging facility
- **x2gw-demux**: X2GW demux task logging facility

level *report_level* [critical-info | no-critical-info]

level *report_level*: specifies the level of information to be logged, *report_level*, as one of:

- critical
- debug
- error
- info
- trace
- unusual
- warning

critical-info | **no-critical-info**: indicates if critical information is to be displayed or not. The keyword **critical-info** specifies that events with a category attribute of critical information are to be displayed. Examples of these types of events can be seen at bootup when system processes and tasks are being initiated. The **no-critical-info** keyword specifies that events with a category attribute of critical information are not to be displayed.

Usage Guidelines

This command is useful when it is necessary to get real time output of events. Event output may be cached otherwise which may make it difficult to trouble shoot problems which do not allow the last cache of events to be output prior to system problems.

Caution Issuing this command could negatively impact system performance depending on system loading, the log level, and/or the type of facility(ies) being logged.

Example

Set real time output for the point-to-point protocol facility and all facilities, respectively, to avoid logging of excessive information.

```
logging filter runtime facility ppp
logging filter runtime facility all level warning
```

logging include-ueid

Enables the sending of the International Mobile Station Identifier (IMSI) and International Mobile Equipment Identifier (IMEI) in logging details of event log types error and critical.

Product

P-GW

SAEGW

Privilege

Administrator, Security Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
[ no ] logging include-ueid
```

no

Disables the sending of the IMSI/IMEI in logging details of event log types error and critical.

include-ueid

Enables the sending of the IMSI/IMEI in logging details of event log types error and critical. When enables, the following event logs of type error and critical will contain the IMSI/IMEI in the logging details.

Table 1: System Event Logs of Type Error and Critical with IMSI/IMEI in System Event Log Details

Event Log #	Description
12225	Represents misc_error3 in format "[IMSI <IMSI>] Misc Error3: %s, error code %d"
12226	Represents recover_call_from_crr_failed1 error in format "[IMSI <IMSI>]Sessmgr-%d Recover call from CRR failed for callid:0x%x reason=%s"
12227	Represents aaa_create_session_failed_no_more_sessions1 error in format "[IMSI <IMSI>] Sessmgr-%d Ran out of session handles"
140075	Represents error_log1 in format "[IMSI <IMSI>]%s"

Event Log #	Description
139001	To print miscellaneous PGW error log.
191006	To print miscellaneous SAEGW error log.
10034	Represents FSM error in format "[IMSI <IMSI>] default call fsm error: ostate=%s(%d) state=%s(%d) event=%s(%d)"
10035	Represents FSM INVALID event in format "[IMSI <IMSI>] default call fsm invalid event: state=%s(%d) event=%s(%d)"
12382	Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format "[IMSI <IMSI>] Sessmgr-%d: Request to %s bearer rejected. Reason: %s". For example "[IMSI 112233445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress"
12668	Represents fsm_event_error in format "[IMSI <IMSI>] Misc Error: Bad event in sessmgr fsm, event code %d"
12774	Represents pgw_purge_invalid_crr in format "[IMSI <IMSI>] Local %s TEID [%lu] Collision: Clp Connect Time: %lu, Old Clp Callid: %d, Old Clp Connect Time: %lu %s"
12855	Represents ncqos_nrspca_trig_err in format "[IMSI <IMSI>] NCQOS NRSPCA trig rcvd in invalid bcm mode."
12857	Represents ncqos_nrupc_tft_err in format "[IMSI <IMSI>] NCQOS NRUPC Trig : TFT validation failed for nsapi <%u>."
12858	Represnts ncqos_nrxx_trig_already in format "[IMSI <IMSI>] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi <%u>."
12859	Represents ncqos_nrxx_tft_check_fail in format "[IMSI <IMSI>] NCQOS TFT check failed as TFT has invalid opcode for nsapi <%u>:pf_id_bitmap 0x%x and tft_opcode: %d"
12860	Represents ncqos_sec_rej in format "[IMSI <IMSI>] NCQOS Secondary ctxt with nsapi <%u> rejected, due to <%s>."
12861	Represents ncqos_upc_rej in format "[IMSI <IMSI>] UPC Rejected for ctxt with nsapi <%u>, due to <%s>."
12862	Represents ggsn_subsession_invalid_state in format "[IMSI <IMSI>] GGSN subsession invalid state state:<%s>,[event:<%s>]"
11830	Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format "[IMSI <IMSI>] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN doesnt support Deffered allocation for IPv4v6, dropping the call."

Event Log #	Description
11832	Represents gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection in format "[IMSI <IMSI>] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GBR bearer to be selected as Default bearer."
11834	Represents gngp_handoff_from_ggsn_rejected_no_ggsn_call in format "[IMSI <IMSI>] Sessmgr-%d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC <0x%x> not found."
12960	Represents gtp_pdp_type_mismatch in format "[IMSI <IMSI>] Mismatch between PDP type of APN %s and in create req. Rejecting call"
11282	Represents pcc_intf_error_info in format "[IMSI <IMSI>] %s"
11293	Represents collision_error in format "[IMSI <IMSI>] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code %d"
11917	Represents rcvd_invalid_bearer_binding_req_from_acs in format "[IMSI <IMSI>] Sessmgr %d: Received invalid bearer binding request from ACS."
11978	Represents saegw_uid_error in format "[IMSI <IMSI>] %s"
11994	Represents unwanted_pcc_intf_setup_req error in format "[IMSI <IMSI>] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface "
140005	Represents ue_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled UE event <%s> in state <%s>"
140006	Represents pdn_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled PDN event <%s> in state <%s>"
140007	Represents epsb_fsm_illegal_event in format "[IMSI <IMSI>] Invalid/unhandled EPSB event <%s> in state <%s>"
10726	Represents saegwdrv_generic_error "[IMSI <IMSI>] %s"

Usage Guidelines

Use this command to enable the logging of the UE's IMSI/IMEI in event log types of error and critical. This is useful in identifying the specific UE affected by events that can potentially affect service.

Example

The following command enables the sending of the IMSI/IMEI in the logging details of event logs of type error and critical.

```
logging include-ueid
```

logging monitor

Enables or disables the monitoring of a specified user.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ no ] logging monitor { ipaddr` *`ip_address`* **`| ipv6addr`** *`ipv6_address`* **`| msid`** *`ms_id`* **`| username`** *`user_name`* **`}`**

no

Disables the monitoring of the user specified by the options given.

ipaddr *ip_address*

Specifies the IP address of the user for which the monitoring filter is to be set. *ip_address* must entered using IPv4 dotted-decimal notation.

ipv6addr *ipv6_address*

Specifies the IPv6 address of the user for which the monitoring filter is to be set. *ipv6_address* must be followed by IPv6 address in a xx:yy::zz format .

msid *ms_id*

msid *ms_id*: specifies the mobile subscriber ID for which the monitoring filter is to be set. *ms_id* must be from 7 to 16 digits.

This keyword/option can be used to specify the International Mobile Subscriber Identity (IMSI) which enables logging based on IMSI.

username *user_name*

username *user_name*: specifies a user for which the monitoring filter is to be set. *user_name* must refer to a previously configured user.

Usage Guidelines

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

Caution

Issuing this command could negatively impact system performance depending on the number of subscribers for which monitoring is performed and/or the amount of data they're passing.

Example

The following command enables the monitoring of user *user1* and mobile subscriber ID 4441235555, respectively.

```
logging monitor username user1
logging monitor msid 44441235555
```

The following disables the monitoring of user *user1*.

```
no logging monitor username user1
```

logging runtime

Enables events to be filtered and logged in real time.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
logging runtime buffer store { all-events | filtered-events-only }
```

all-events

Logging daemon runtime buffer stores all logs that come to it.

filtered-events-only

Logging daemon runtime buffer stores only logs that pass the runtime filter.

Usage Guidelines

Sets the filtering of logged information to log in real time.

Example

The following command enables storage of logs that pass the runtime filter:

```
logging runtime buffer store filtered-events-only
```

logging syslog

Enables or disables syslog configuration.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **`[ no ] logging syslog hostname`**

no

Disables syslog configuration.

hostname

Enables the hostname to appear in the syslog messages after the time stamp.

Usage Guidelines The hostname keyword enables or disables the hostname to appear in the syslog messages after the time stamp. This feature is disabled by default.

lte-policy

This command enters the LTE Policy Configuration Mode where LTE policy parameters can be configured.

Product MME

SAEGW

S-GW

SGSN

Privilege Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **`lte-policy`**

Usage Guidelines Enters the LTE Policy Configuration Mode.

Entering this command results in the following prompt:

[*context_name*]*hostname*(lte-policy)#

LTE Policy Configuration Mode commands are defined in the *LTE Policy Configuration Mode Commands* chapter.

mediation-device

Important This command is obsolete. Even though the CLI accepts the command no function is performed.

mme-manager

This command configures MME Manager(s) and enters the MME Manager Configuration mode.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **mme-manager**

Usage Guidelines Enters the LTE Policy Configuration Mode.

Entering this command results in the following prompt:

```
[context_name]host_name(mme-manager)#
```

The related commands are defined in the *MME Manager Configuration Mode Commands* chapter.

msisdn-group

This command configures the Mobile Subscriber Integrated Services Digital Network (MSISDN) group.

Product MME

SGSN

Privilege Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **msisdn-group** *group_name*
no msisdn-group *group_name*

no

Deletes the configured MSISDN group.

msisdn-group *group_name*

Specifies the MSISDN group name. *group_name* must be an alphanumeric string of 1 through 64 characters. It can have a maximum of 50 groups.

Usage Guidelines

Use this command to create a new MSISDN group. the MSISDN is used to decide whether to allow or block the subscribers.

An MSISDN group can contain up to 500 elements of either individual MSISDN or range of MSISDNs. Once an MSISDN group is created, each group can be configured with up to 500 unique MSISDN values. Multiple lines of MSISDN and MSISDN-range can be up to 20 lines per group.

This command allows you to enter the MSISDN Group Configuration Mode.

Entering this command results in the following prompt:

[*context_name*]*hostname*(msisdn-group)#

MSISDN Group Configuration Mode commands are defined in the *MSISDN Group Configuration Mode Commands* chapter.

network-overload-protection mme-new-connections-per-second

This command configures an attach rate throttle mechanism to control the number of new connections allowed on a per second basis.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
network-overload-protection mme-new-connections-per-second #_new_connections
 action attach { drop | reject-with-emm-cause { congestion |
network-failure | no-suitable-cell-in-tracking-area } } tau { drop |
reject-with-emm-cause { congestion | network-failure | no-sec-ctxt-in-nw
 | no-suitable-cell-in-tracking-area } } fwd-reloc { drop | reject } [
ddn { drop | reject-with-cause { unable-to-page-ue | context-not-found }
 } ] [ queue-size queue_size ] [ wait-time wait_time ]
default network-overload-protection mme-new-connections-per-second
```

default

Disables the MME attach rate throttle feature.

mme-new-connections-per-second *#_new_connections*

Define the number of new connections to be accepted per second.

#_new_connections: Must be an integer from 50 to 5000.

action

Specifies the action to be taken by the MME when the new connection queue is full. Specific actions can be defined for each of the following connection types:

- UE-initated attaches (see **attach** keyword).
- UE-initatied inter-CN node TAU requests (see **tau** keyword).
- Peer SGSN/MME intiated forward relocation requests (see **fwd-reloc** keyword).

attach { drop | reject-with-emm-cause { congestion | network-failure | no-suitable-cell-in-tracking-area } }

Specifies the action to be taken for all types of UE-initiated initial attaches (IMSI, local GUTI, foreign GUTI, mapped GUTI, etc.). Select one of the following actions:

- **drop:** Drop the new connection request.
- **reject-with-cause:** Reject the new connection request. Include one of the following as the cause in the reject message:
  - **congestion**
  - **network-failure**
  - **no-suitable-cell-in-tracking-area**

tau { drop | reject-with-emm-cause { congestion | network-failure | no-sec-ctxt-in-nw | no-suitable-cell-in-tracking-area } }

Specifies the action to be taken for UE-initiated inter-CN TAU requests requiring context transfer from old MME/SGSN, including TAU requests with foreign GUTI or mapped GUTI. Select one of the following actions:

- **drop:** Drop the new connection request.
- **reject-with-cause:** Reject the new connection request. Include one of the following as the cause in the reject message:
  - **congestion**
  - **network-failure**
  - **no-sec-ctxt-in-nw**
  - **no-suitable-cell-in-tracking-area**

fwd-reloc { drop | reject }

Specifies the action to be taken for peer SGSN/MME initiated forward relocation requests via Gn/S10/S3. Select one of the following actions:

- **drop:** Drop the new connection request.

- **reject:** Reject the new connection request. If the inbound forward-relocation requests are rejected, the following cause codes shall be used:
  - GTPv1 - No resources available (199)
  - GTPv2 - No resources available (73)

ddn { drop | reject-with-cause { unable-to-page-ue | context-not-found } }

In the event of an MME failure, the surviving MME in the pool may receive a very large number of IMSI requests, which may overwhelm the IMSI Manager. To avoid congestion, the MME can be configured using this keyword to throttle the IMSI-based DDN requests it receives if the configured *#_new_connections* rate is exceeded. Select one of the following actions:

- **drop**: Drop new IMSI-based DDN requests.
- **reject**: Reject the IMSI-based DDN request. Include one of the following as the cause in the reject message:
  - **unable-to-page-ue**
  - **context-not-found**

Important Beginning with Release 19.4, the **dnn** keyword behavior changes from mandatory to optional. If the **dnn** option is not configured, then the default action is to drop the Downlink Data Notification.

queue-size *queue_size*

Defines the maximum size of the pacing queue used for buffering the packets. If configured, the queue-size should be greater than or equal to the *#_new_connections* value and less than or equal to the optimal value (the *wait_time* * *#_new_connections*). This validation is done in the CLI.

queue_size Must be an integer from 250 to 25000.

Default: unconfigured. The default value is the *#_new_connections* * *wait-time*. This will be the optimal value.

wait-time *wait_time*

Defines the maximum life-time (number of seconds) of the packets in the queue beyond which the packets are considered to be "stale" and are dropped.

wait_time Must be an integer from 1 to 15

Default: 5

Usage Guidelines

Use this command to configure attach rate throttling on the MME.

When enabled, new connections (except emergency requests) are buffered and paced through the queue. Messages in the queue are processed (FIFO) until they age-out when the queued message's lifetime crosses the configured wait-time. The wait-time and the attach rate decide the optimal size of the queue. If the queue is full, packets are rejected or dropped based on the configured action.

This feature functions at a system (chassis) level for all MME services. All MME services on the system are controlled by a single pacing queue. For a combo MME-SGSN node, each type of service shall be controlled by its own queue and its own configuration.

Emergency attaches are not be throttled when this feature is enabled.

Important This command is available only if a valid license (MME Resiliency) is installed. Contact your Cisco account representative for more information.

Example

Configure the new connections per second rate at 2500, reject all (non-emergency) attaches and TAU requests, and drop forward relocation requests if the new connection rate is exceeded. Rejects will return emm cause code "Congestion".

```
network-overload-protection mme-new-connections-per-second 2500 action
attach reject-with-emm-cause congestion tau reject-with-emm-cause
congestion fwd-reloc drop ddn drop wait-time 5
```

Set the attach rate to 500 per second, the same actions as the previous example, but set the wait time to 5 seconds, and the queue size to be calculated (as follows: *wait_time * #_new_connections* - i.e., 2500)

```
 network-overload-protection
mme-new-connections-per-second
500 action attach reject-with-emm-cause
congestion tau reject-with-emm-cause
congestion fwd-reloc drop ddn drop wait-time 5 5
```

network-overload-protection mme-tx-msg-rate-control

Enables and configures the S1 Paging Rate Limit feature as well as UE Deactivation Rates upon EGTPC path failure feature.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
network-overload-protection  mme-tx-msg-rate-control { egtp-pathfail
ecm-idle rate ecm-connected rate | enb s1-paging rate }
[  default ] network-overload-protection  mme-tx-msg-rate-control
```

default

Applies the default MME message rate control configuration; S1 paging rate limit is disabled and a path failure processing rate of 1000 per second per session manager without distinguishing between ECM idle/connected sessions.

egtp-pathfail ecm-idle *rate* ecm-connected *rate*

Configures the UE deactivation pacing rate for MME S11/S10/S3 interfaces (any EGTPC service with interface type "interface-mme").

ecm-idle *rate*: This keyword defines the deactivation rate for UEs in ECM Idle mode.

ecm-connected *rate*: This keyword defines the deactivation rate for UEs in ECM Connected mode.

rate specifies a rate threshold in sessions per second per session manager (SessMgr) as an integer from 1 through 5000.

Note: Configuring a high deactivation rate can have a negative effect on performance. Appropriate dimensioning exercises should be performed to arrive at the optimum rate.

enb s1-paging *rate*

Configures an S1 paging rate limit applicable to all eNodeBs connected all MME services. S1 Paging requests to an eNodeB will be rate limited at this threshold value. S1 Paging requests to an eNodeB exceeding this threshold will be dropped.

rate specifies the rate threshold in messages per second per eNodeB as an integer from 1 through 65535.

Usage Guidelines

Use this command to enable and configure the S1 Paging Rate Limit feature as well as UE Deactivation Rates upon EGTPC path failure feature.

Example

The following command configures S1 Paging rate limit of 150 messages per second per eNodeB.

```
network-overload-protection mme-tx-msg-rate-control enb s1-paging 150
```

The following command configures EGTP path failure processing rate limit for UE sessions in ECM-Idle mode to 10 sessions per second per session manager and for UE sessions in ECM-Connected mode to 20 sessions per second per session manager.

```
network-overload-protection mme-tx-msg-rate-control egtp-pathfail ecm-idle
 10 ecm-connected 20
```

network-overload-protection sgsn-new-connections-per-second

This command configures an attach rate throttle mechanism to control the number of new connections (attaches or inter-SGSN RAUs), through the SGSN, on a per second basis.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
network-overload-protection sgsn-new-connections-per-second #_new_connections
 action { drop | reject with cause { congestion | network failure } } [
queue-size queue_size ] [ wait-time wait_time ]
default network-overload-protection sgsn-new-connections-per-second
```

default

Using **default** in the command, disables this attach rate throttle feature that provides network overload protection.

sgsn-new-connections-per-second *#_new_connections*

Define the number of new connections to be accepted per second.

#_new_connections: Must be an integer from 50 to 5000.

action

Specifies the action to be taken by the SGSN when the attach rate exceeds the configured limit on the number of attaches. Select one of the following actions:

- **drop:** Drop the new connection request.
- **reject-with-cause:** Reject the new connection request. Include one of the following as the cause in the reject message:
- **congestion**
- **network failure**

queue-size *queue_size*

Defines the maximum size of the pacing queue used for buffering the packets. If configured, the queue-size should be greater than or equal to the *#_new_connections* value and less than or equal to the optimal value (the *wait_time* * *#_new_connections*). This validation is done in the CLI.

queue_size Must be an integer from 250 to 25000.

Default: unconfigured. The default value is the *#_new_connections* * *wait-time*. This will be the optimal value.

wait-time *wait_time*

Defines the maximum life-time (number of seconds) of the packets in the queue beyond which the packets are considered to be "stale".

wait_time Must be an integer from 1 to 15

Default: 5

Usage Guidelines

Use this command to configure the rate at which the SGSN must process new connection requests. The rate is the number of new connections to be accepted per second.

With basic network overload protection, the incoming new connection rate is higher than this configured rate. When this occurs, all of the new connection requests cannot be processed. This command can also be used to configure the action to be taken when the rate limit is exceeded. The new connection requests, which cannot be processed, can be either dropped or rejected with a specific reject cause.

The SGSN's *optimized* network overload protection performs attach-rate throttling to avoid overloading Gr, Gn and Gf interfaces. This is enabled with **queue-size** and **wait-time** keywords so that the IMSIMgr throttles the attach rate to values configured with these keywords.

If the SGSN receives more than the configured number of attaches in a second, then the attaches are buffered in the pacing queue and requests are only dropped when the buffer overflows due to high incoming attach rate. Messages in the queue are processed (FIFO) until they age-out when the queued message's lifetime crosses the configured wait-time. The wait-time and the attach rate decide the optimal size of the queue.

Counters for this feature are available in the **show gmm-sm statistics** command display in the Network Overload Protection portion of the table.

Example

Configure the throttle rate or limit to 2500 attaches per second and to drop all requests if the limit is exceeded.

```
network-overload-protection sgsn-new-connections-per-second 2500 action
drop
```

Disables the network-overload protection feature and set the default queue size to 1000 and the wait time to 5 seconds:

```
default network-overload-protection
sgsn-new-connections-per-second
```

Set the attach rate to 500 per second, the action to drop, the wait time to 5 seconds, and the queue size to be calculated (as follows: *wait_time * #_new_connections* - i.e., 2500)

```
network-overload-protection
sgsn-new-connections-per-second
500 action drop wait-time 5
```

network-service-entity

This command creates a new instance of an SGSN network service entity (NSE) for either the IP environment or the Frame Relay environment.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ no ] network-service-entity ( ip-local | peer-nsei` *peer_nsei_number* **`frame-relay )`**

no

Deletes the network service entity definition from the system configuration.

ip-local

Configures the local endpoint for NS/IP and enters the NSE-IP configuration mode. The prompt will change to:

```
[local]<hostname>(nse-ip-local)#
```

peer-nsei *peer_nsei_number* frame-relay

Configures a peer NSE with frame relay connectivity. This set of keywords also provides access to the NSE-FR Configuration mode. The prompt will change to:

```
[local]<hostname>(nse-fr-peer-nsei-<peer_nsei_number>)#
```

Usage Guidelines

Use this command to access the configuration modes for either the IP or Frame Relay network service entities.

Example

Enter the NSE for a Frame Relay configuration instance identified as 4554:

```
network-service-entity peer-nsei 4554 frame-relay
```

nsh

This command enters the NSH Configuration Mode. It enables you to encode or decode Network Services Headers (NSH).

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`nsh`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-nsh)#
```

Syntax Description **`[ no ] nsh { nsh-field`** *`<nsh_field_name>`* **`| nsh format`** *`<nsh_format_name>`* **`}`**

no

Disables the NSH options.

nsh-field

This command defines NSH fields tag value. Entering the above command sequence results in the following prompt:

```
[local]<hostname>(nsh-nshfields)#
```

nsh-format

This command define NSH format for encoding and decoding NSH header. Entering the above command sequence results in the following prompt:

```
[local]<hostname>(nsh-nshformat)#
```

Usage Guidelines Use this command to encode or decode Network Services Headers or associate tag values with NSH headers.

Example

The following command enters the NSH configuration mode: :

```
nsh
```

The following command helps you come out of the NSH configuration mode: :

```
no nsh
```

ntp

Enters the Network Time Protocol (NTP) configuration mode or disables the use of NTP on the system.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **`[ no ] ntp`**

no

Disables the use of NTP for clock synchronization. When omitted, NTP client support is enabled on the chassis. By default NTP synchronization to external servers is disabled.

Important If the use of NTP is disabled the system clock may drift over a period of time. This may require manual updates to the system clock to synchronize the clock with other network elements.

Usage Guidelines Used when it is necessary to enable or configure NTP settings. For additional information refer to the *NTP Configuration Mode Commands* chapter and the *System Administration Guide*.

Example

The following command enters the NTP configuration mode:

```
ntp
```

The following disables the use of the network timing protocol for system clock synchronization.

```
no ntp
```

ntsr pool-id

Configures a pool ID and pool type (either MME or S4-SGSN) for Network Triggered Service Restoration (NTSR). Once executed, the user is placed in NTSR Pool Configuration Mode.

Product S-GW

Privilege Administrator, Security Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
ntsr pool-id number pool-type [ mme | s4-sgsn ]
no ntsr pool-id
```

ntsr pool-id *number*

Specifies an ID number for this NTSR pool. Valid entries are from 1 to 65535.

pool-type

Specifies the type of pool for the pool-id. Options are MME or S4-SGSN.

Usage Guidelines

This command is used to configure a pool ID and pool type (either MME or S4-SGSN) for NTSR. Once executed, the operator must configure a peer IP address in NTSR Pool Configuration mode using the **peer-ip-address** command.

Example

This example configures an NTSR pool ID of 1 and a pool type of mme.

```
ntsr pool-id 1 pool-type mme
```

operator-policy

This command creates an operator policy and enters the operator policy configuration mode. Commands for configuration of the policies are available in the *Operator Policy Configuration Mode Commands* chapter.

Product

MME

SGSN

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
operator-policy ( default | name policy_name } [ -noconfirm ]
no operator-policy ( default | name policy_name }
```

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

no

Removes the specified operator policy from the system configuration.

default

default, in this case, is the *name* of a specific operator policy. This default policy is used when no other operator policy matches the incoming IMSI.

Important

You should configure this default operator policy to make it available to handle IMSIs that are not matched with other policies.

name *policy_name*

Specifies the unique name of an operator policy. *policy_name* is entered as an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to create an operator policy and to enter the operator policy configuration mode to define or modify policies.

An operator policy associates APNs, APN profiles, IMEI ranges, IMEI profiles, an APN remap table and a call-control profile to ranges of IMSIs. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules governing the services, facilities and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements such as DNS servers and HLRs.

The system supports up to 1,000 operator policies, including the *default* operator policy.

Important An operator policy is ***the*** key element of the Operator Policy feature. After defining an instance of an operator policy, you must go to the SGSN Global Configuration Mode (from the Global Configuration mode) to define the IMSI range(s). This requirement does not hold if you are using a *default* operator policy.

To see what operator policies have already been created, return to the Exec mode and enter the **show operator-policy all** command.

Example

The following command accesses the default operator policy and enters the operator policy configuration mode to view or modify the specified policy:

```
operator-policy default
```

orbem force

Attention

- With Release 21.16 onwards, the **force** keyword has to be appended to the **orbem** CLI command to enter the ORBEM mode and enable the feature. The **orbem** keyword is now hidden.
- Support for the end-of-life ORBEM/WEM feature will be fully discontinued in future releases.

Enters the Object Request Broker Element Manager (ORBEM) Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **orbem force**

Usage Guidelines Set the configuration mode to allow modification of the ORBEM configuration data.

Example

The following command enters the Object Request Broker Element Manager (ORBEM) Configuration mode:

orbem force

pac-standby-priority

This command has been renamed to **card-standby-priority**. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.

pco-options

The following commands are explained below:

Note custom1 container ID is not configurable at Global configuration mode using CLI as its container value is fixed to FF00.

pco-options custom2

This command controls the sending of customized PCO (Protocol Configuration Options) options in the network to MS GTP messages at Global configuration mode..

Product GGSN

P-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **[no] pco-options { custom2 } container-id** *container_id_value*

no

Removes PCO configuration at Global configuration mode

custom2

Enable sending of customized PCO options in the network to MS messages.

container-id

Configures the operator defined container ID. The value ranges from FF03 to FFFF.

Usage Guidelines

Use this command to enable or disable sending of customized PCO options in the network to MS GTP messages and configure link MTU size PCO value.

Example

The following command enables sending customized PCO options:

```
pco-options custom2
```

pco-options custom3

This command controls the sending of customized PCO (Protocol Configuration Options) options in the network to MS GTP messages at Global configuration mode..

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ no ] pco-options { custom3 } container-id` *container_id_value*

no

Removes PCO configuration at Global configuration mode

custom3

Enable sending of customized PCO options in the network to MS messages.

container-id

Configures the operator defined container ID. The value ranges from FF03 to FFFF.

Usage Guidelines

Use this command to enable or disable sending of customized PCO options in the network to MS GTP messages and configure link MTU size PCO value.

Example

The following command enables sending customized PCO options:

pco-options custom3

pco-options custom4

This command controls the sending of customized PCO (Protocol Configuration Options) options in the network to MS GTP messages at Global configuration mode..

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

[no] pco-options { custom4 } container-id *container_id_value*

no

Removes PCO configuration at Global configuration mode

custom4

Enable sending of customized PCO options in the network to MS messages.

container-id

Configures the operator defined container ID. The value ranges from FF03 to FFFF.

Usage Guidelines

Use this command to enable or disable sending of customized PCO options in the network to MS GTP messages and configure link MTU size PCO value.

Example

The following command enables sending customized PCO options:

pco-options custom4

pco-options custom5

This command controls the sending of customized PCO (Protocol Configuration Options) options in the network to MS GTP messages at Global configuration mode..

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ no ] pco-options { custom5 } container-id` *container_id_value*

no

Removes PCO configuration at Global configuration mode

custom5

Enable sending of customized PCO options in the network to MS messages.

container-id

Configures the operator defined container ID. The value ranges from FF03 to FFFF.

Usage Guidelines

Use this command to enable or disable sending of customized PCO options in the network to MS GTP messages and configure link MTU size PCO value.

Example

The following command enables sending customized PCO options:

```
pco-options custom5
```

pdu-session-recovery

Enables or disables support for early PDU recovery of VoLTE calls during Transaction Protocol Data Unit. (TPDU) based session recovery. When this CLI is enabled, data is allowed for VoLTE-only calls when Session Manager is recovering.

Product

GGSN

P-GW

S-GW

SAE-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
pdu-session-recovery call-type ims-media services { ggsn [pgw] [sgw] |
pgw [ggsn] [sgw] | sgw [ggsn] [pgw] }
no pdu-session-recovery call-type ims-media
```

no

Disables early PDU recovery of VoLTE calls during session recovery.

{ ggsn [pgw] [sgw] | pgw [ggsn] [sgw] | sgw [ggsn] [pgw] }

Specifies one or more services for which this feature can be enabled.

Usage Guidelines

usage

Use this command to enable or disable support for early PDU recovery of VoLTE calls during TPDU based session recovery. When this CLI is enabled, data is allowed for VoLTE-only calls when Session Manager is recovering.

Even with GnGp association, the **pgw** option needs to be explicitly configured for PGW calls.

Example

The following command enables early PDU recovery for P-GW services:

```
pdu-session-recovery call-type ims-media services pgw
```

peer-profile

This command creates a peer profile based on service type and interface and enters the Peer-Profile Configuration mode. Commands for configuration of the policies are available in the *Peer Profile Configuration Mode Commands* chapter.

Product

GGSN

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
peer-profile service-type { ggsn-access | pgw-access | sgw-access |
sgw-network } { default | name peer_profile_name } [ -noconfirm ]
no peer-profile service-type { ggsn-access | pgw-access | sgw-access |
sgw-network } name peer_profile_name
```

[-noconfirm]

Indicates that the command is to execute without any additional prompt and confirmation from the user.

no

Removes the specified peer profile for specific service type from the system configuration.

service-type

Specifies service type for which peer profile is being configured.

ggsn-access configure profile for peer nodes of GGSN.

pgw-access configures profile for peer nodes of P-GW.

sgw-access configures profile for peer nodes of S-GW toward S4/S11 interfaces.

sgw-network configures profile for peer nodes of S-GW toward S5/S8 interfaces.

name *peer_profile_name*

Specifies the unique name of a peer profile for specific service type.

peer_profile_name is entered as an alphanumeric string of 1 through 64 characters.

default

default, in this case, is the *name* of a specific peer profile. This default profile is used when no other defined peer profile matches.

Important When there is no association of peer-map in any of the services, then "default" peer profile of the corresponding service-interface type shall be applied, except for GTP-C parameters. In addition, GTP-C parameter configuration shall be applied from eGTP service-level configuration for P-GW/S-GW service and GGSN service-level configuration for GGSN.

Usage Guidelines

Use this command to create a peer profile for specific service type and to enter the service specific Peer Profile configuration mode to define or modify the peer profile parameters.

The peer profile feature allows flexible profile-based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of GGSN/P-GW/S-GW. With this feature, configuration of GTP-C echo parameters and disabling/enabling of Lawful intercept per MCC/MNC or IP address based on rules can be managed.

Before StarOS Release 15.0, the GGSN service allowed operator to configure list of SGSNs. Using this configuration, operator can also control some parameters associated with the configured SGSN, such as RAT type. This would be taken from configuration if CPC request does not have RAT type.

Important The system supports up to 64 peer profiles configured for each of the peer profile types; there can be up to 1024 peer map rules configured, including all the peer maps.

Example

The following command accesses the default peer profile for GGSN service and enters the GGSN Peer Profile configuration mode to view or modify the specified profile:

```
peer-profile service-type ggsn-access default
```

plugin

Specifies a previously installed software plugin module and enters the Plugin Configuration Mode. This function is associated with the patch process for dynamic software upgrades. A plugin module is a loadable dynamic link library (DLL) of shared objects.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

plugin *module_name*

module_name

Specifies the name of an existing plugin module that you want to downgrade as an alphanumeric string of 1 through 16 characters. If the named module is not known to the sytem, an error message is displayed.

Usage Guidelines

Specify a previously loaded software plugin module that you wish to configure. The specified module must have been previously copied onto the system and unpacked/verified via the **patch plugin** and **install patch plugin** commands.

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

Example

To specify the plugin module named *p2p_odyssey* enter the following command:

```
plugin p2p_odyssey
```

port ethernet

Enters the Ethernet Port Configuration mode for the identified port.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

port ethernet *slot/port*

ethernet

Indicates the port identified is an Ethernet interface port.

slot/port

Specifies the slot and port for which Ethernet Port Configuration mode is being entered. The slot and port must refer to an installed card and port.

Important The range of slot and port numbers varies by platform type – ASR 5500 versus VPC.

Usage Guidelines

Change the current configuration mode to Ethernet Port Configuration mode.

Example

The following command enters the Ethernet Port Configuration mode for ethernet port 11 in slot 5 (ASR 5500):

```
port ethernet 5/11
```

port rs232

Enters the RS-232 Port Configuration mode for the RS-232 console port on the specified SPIO card. Not available on the XT2 platform.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

port rs232 *slot* **3**

rs232

Indicates the port identified is an RS-232 port on a SPIO card.

***slot* 3**

Specifies the slot of the SPIO for which RS-232 Port Configuration mode is being entered. The slot must refer to an installed SPIO card. The specified port must always be 3 for an RS-232 port.

The value for *slot* must be either 24 or 25.

Usage Guidelines

Change the current configuration mode to RS-232 Port Configuration mode.

Example

The following command enters the RS-232 Port Configuration mode for the SPIO in slot 24;

```
port rs232 24 3
```

profile-id-qci-mapping

Creates a Qos Class-Identifier-Radio Access Network (QCI-RAN) ID mapping table or specifies an existing table and enters the QCI Mapping Configuration mode for the system.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

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

no

Removes the specified mapping table from the system

name

Creates a new or enters an existing mapping table configuration. *name* must be an alphanumeric string of 1 through 63 alphanumeric.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Enters the QCI-RAN ID mapping configuration mode for an existing table or for a newly defined table. This command is also used to remove an existing table.

Entering this command results in the following prompt:

```
[context_name]hostname(config-hsgw-association-table)#
```

QCI Mapping Configuration Mode commands are defined in the *QCI Mapping Configuration Mode Commands* chapter.

Use this command when configuring the HSGW eHRPD component.

Important This command creates a mapping table available to any HSGW context configured on the system.

Example

The following command enters the existing QCI mapping configuration mode (or creates it if it doesn't already exist) for a mapping table named *qci_table1*:

```
profile-id-qci-mapping qci_table1
```

The following command will remove *qci_table1* from the system:

```
no profile-id-qci-mapping qci_table1
```

ps-network

This command creates/removes an HNB-PS network configuration instance for Femto UMTS access over Iu-PS/Iu-Flex interface between Home NodeB Gateway (HNB-GW) service and PS networks elements; i.e. SGSN. This command also configures an existing HNB-CS network instance and enters the HNB-CS Network Configuration mode on a system.

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

Product HNBGW

Privilege Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
[ no ] ps-network ps_instance [ -noconfirm ]
no ps-network ps_instance
```

no

Removes the specified HNB-PS network instance from the system.

Caution Removing the HNB-PS network instance is a disruptive operation and it will affect all UEs accessing SGSN(s) in specific PS core network through the HNB-GW service.

Caution If any HNB-PS Network instance is removed from the system, all parameters configured in that mode will be deleted and Iu-PS/Iu-Flex interface will be disabled.

ps_instance

Specifies the name of the Packet Switched Core Networks instance which needs to be associated with HNB Radio Network PLMN in HNB RN-PLMN configuration mode. If *ps_instance* does not refer to an existing HNB-PS instance, the new HNB-PS network instance is created.

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

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to enter the HNB-PS Network Configuration mode for an existing PS network instance or for a newly defined HNB-PS network instance. This command is also used to remove an existing HNB-PS network instance.

This configuration enables the Iu-PS/Iu-Flex interface on HNB-GW service with CS core network elements; i.e. MSC/VLR.

A maximum of 1 HNB-PS networks instance which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution This is a critical configuration. The HNBs can not access SGSNs in PS core network without this configuration. Any change to this configuration would lead to disruption in HNB access to PS core network.

Entering this command results in the following prompt:

```
[context_name]hostname(config-ps-network)#
```

The various parameters available for configuration of an HNB-PS network instance are defined in the *HNB-PS Network Configuration Mode Commands* chapter.

Example

The following command enters the existing HNB-PS Network configuration mode (or creates it if it doesn't already exist) for the instance named *hnb-ps1*:

```
ps-network hnb-ps1
```

The following command will remove HNB-PS network instance *hnb-ps1* from the system without any prompt to user:

```
no ps-network hnb-ps1
```

qci

Defines QCI value.

Product

ePDG

HSGW

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > qci-qos-mapping

configure > qci-qos-mapping *mapping_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

qci *num* **[delay-class** *delay-class-value* **[precedence-class** *precedence-class-value* **[reliability-class** *reliability-class-value* **]]] [downlink [802.1p-value** *value* **] [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **| copy-outer}] [gbr] [max-packet-delay** *max-packet-delay-value* **max-error-rate** *max-error-rate* **] [non-gbr] [traffic-policing interval** *value* **] [uplink [802.1p-value** *value* **] [encaps-header { copy-inner | dscp-marking** *dscp-marking-value* **| copy-outer }] [mpls-exp-value** *value* **] [user-datagram dscp-marking** *dscp-marking-value* **]]**
no | default qci *num*

no

Removes the specified QCI value.

default

Sets the default QCI value.

qci *num*

num must be an integer from 1 through 256.

delay-class *delay-class-value*

Defines Pre Release 8 value for configuring packet delay.

delay-class *delay-class-value*: Defines Pre Release 8 value for configuring packet delay as an integer from 1 through 9.

precedence-class ***precedence-class-value***

Defines Pre Release 8 value for configuring packet precedence.

precedence-class *precedence-class-value*: Defines Pre Release 8 value for configuring packet precedence as an integer from 1 through 32.

reliability-class ***reliability-class-value***

Defines Pre Release 8 value for configuring packet reliability.

reliability-class *reliability-class-value*: Defines Pre Release 8 value for configuring packet reliability as an integer from 1 through 32.

downlink

Configures for downlink traffic.

802.1p-value*value*

802.1p-value*value*: Configures for downlink traffic 802.1p-value as an integer from 1 through 7.

encaps-header { copy-inner | dscp-marking ***dscp-marking-value*** **| copy-outer}**

encaps-header: Defines the DSCP value to be applied to encaps header.

copy-inner: Copy inner DSCP to outer.

dscp-marking *dscp-marking-value*: Defines the DSCP value to be applied to packets with this QCI.

dscp-marking-value: A Hexadecimal number between 0x0 and 0x3F.

copy-outer Copies the DSCP value coming in an encapsulation header from the S1u interface to the encapsulation header sent on the S5 interface and vice-versa.

gbr

Sets the type of the QCI to GBR.

max-packet-delay ***max-packet-delay-value***

Defines the maximum packet delay in ms for the data with the QCI as an integer from 10 through 1000.

max-error-rate ***max-error-rate***

Defines the maximum error rate that the data stream can handle in power of 10 as an integer from 1 through 6.

non-gbr

Sets the type of the QCI to non GBR.

traffic-policing interval ***value***

Sets the parameters for traffic policing interval in seconds as an integer from 1 through 100.

uplink

Configures for uplink traffic.

mpls-exp-value *value*

Configures for uplink traffic mpls-exp-value as an integer from 1 through 7.

user-datagram

Defines DSCP value to be applied to user data gram.

Usage Guidelines

Use this command to define QCI value in qci-qos-mapping.

Example

The following command defines QCI value as *56*:

```
qci 56
```

qci-qos-mapping

Global QCI-QoS mapping tables are used to map QoS Class Identifier (QCI) values to appropriate Quality of Service (QoS) parameters.

Product

ePDG

GGSN

HSGW

P-GW

SAEGW

S-GW

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
qci-qos-mapping name [ -noconfirm ]
no qci-qos-mapping name
```

no

Removes the specified mapping configuration from the system

name

Creates a new or enters an existing mapping configuration. *name* must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the QCI-QoS mapping configuration mode for an existing table or for a newly defined table. This command is also used to remove an existing table.

Entering this command results in the following prompt:

```
[context_name]hostname(config-qci-qos-mapping)#
```

QCI - QoS Mapping Configuration Mode commands are defined in the *QCI - QoS Mapping Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD component: HSGW, P-GW, SAEGW, S-GW.

Important This command creates a mapping configuration available to any GGSN,HSGW, P-GW, SAEGW, S-GW context configured on the system.

Example

The following command enters the existing QCI - QoS mapping configuration mode (or creates it if it doesn't already exist) for a mapping configuration named *qci-qos3*:

```
qci-qos-mapping qci-qos3
```

qos ip-dscp-iphb-mapping

Manages internal QoS (Internal-Per-Hop-Behavior/IPHB).

Product

ePDG

HSGW

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

qos ip-dscp-iphb-mapping dscp *dscp_value* **internal-priority cos** *class_of_service_value*
default qos ip-dscp-iphb-mapping dscp *dscp_value*

default

Map any IP Differentiated Services Code Point (DSCP) to an IPHB value of 0.

dscp *dscp_value*

Map IP DSCP values into internal QoS.

dscp_value must be a Hexadecimal number between 0x0 and 0x3F.

internal-priority cos *class_of_service_value*

Maps to the internal QoS priority/class of service.

class_of_service_value must be a Hexadecimal number between 0x0 and 0x7.

Usage Guidelines

Use this command to manage internal QoS.

Example

The following command maps DSCP values in a packet to internal-QoS COS marking values:

```
qos ip-dscp-iphb-mapping dscp 0x3 internal-priority cos 0x5
```

qos l2-mapping-table

Creates or modifies a Level 2 mapping table and enters the QoS L2 Mapping Configuration Mode to map internal QoS priority.

Product

ePDG

HSGW

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local] host_name (config)#
```

Syntax Description

qos l2-mapping-table { name *map_table_name* **| system-default }**
no qos l2-mapping-table name *map_table_name*

no

Deletes the specified L2 mapping table.

Important The system-default table ca not be deleted. Only named tables that were previously created using this CLI command can be deleted.

name *map_table_name*

Specifies the name of an internal table from which to map QoS to L2 values.

map_table_name must be an alphanumeric string of 0 through 80 characters.

system-default

Configure the system default mapping.

Usage Guidelines

Use this command to create or modify an L2 mapping table and enter the QoS L2 Mapping Configuration Mode, which is used to map internal QoS values to L2 values.

Entering this command results in the following prompt:

```
[context_name]host(config-qos-l2-mapping)#
```

QoS L2 Mapping Configuration Mode commands are defined in the QoS L2 Mapping Configuration Mode Commands chapter.

Example

The following command creates an L2 mapping table and enters the QoS L2 Mapping Configuration Mode:

```
qos l2-mapping-table name qostable1
```

qos npu inter-subscriber traffic bandwidth

Configures NPU QoS bandwidth allocations for the system.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

qos npu inter-subscriber traffic bandwidth gold *percent* **silver** *percent* **bronze** *percent* **best-effort** *percent*
no qos npu inter-subscriber traffic bandwidth

no

Removes a previous bandwidth allocation.

gold *percent*

Default: 10%

Specifies the maximum percentage of bandwidth to be allocated to the gold queue priority.

percent can be configured to an integer from 0 through 100.

silver *percent*

Default: 20%

Specifies the maximum percentage of bandwidth to be allocated to the silver queue priority.

percent can be configured to an integer from 0 through 100.

bronze *percent*

Default: 30%

Specifies the maximum percentage of bandwidth to be allocated to the bronze queue priority.

percent can be configured to an integer from 0 through 100.

best-effort *percent*

Default: 40%

Specifies the maximum percentage of bandwidth to be allocated to the best-effort queue priority.

percent can be configured to an integer from 0 through 100.

Usage Guidelines

The bandwidth of a subscriber queue is maintained by rate limiting functions which implement packet-rate limiting at the first level and bit-rate limiting at the next level.

The packet-rate limit of a queue is defined by the number of packets-per-second (PPS) permitted for queuing. Before queuing a packet on a subscriber queue, the NPU ensures that the packet falls within the limit. If the packet to be queued exceeds the packet rate limit, it is dropped.

Each subscriber queue is configured with a bit rate limit, measured in megabits-per-second (Mbps), referred to as CP-BPS (bit-per-second to CP). The CP-BPS is available as the total bandwidth for the subscriber traffic that a CP can sustain. Each subscriber queue receives an allocation of a certain percentage of the CP-BPS. The following maximum CP-BPS values are supported:

- Lead CP (CP0) = 128 Mbps
- Remaining CPs (CP1, CP2, CP3) = 256 Mbps

For additional information on the NPU QoS functionality, refer to the System Administration and Configuration Guide.

Example

The following command configures bandwidth allocations of 20, 30, 40, and 50% for the gold, silver, bronze, and best-effort queues respectively:

```
qos npu inter-subscriber traffic bandwidth gold 20 silver 30 bronze 40
best-effort 50
```

Upon executing this command, the priority queues will have the following packet processing card CP bandwidth allocations based on the maximum CP bandwidth specifications:

Priority	Lead CP (CP 0) Bandwidth (Mbps)	CP 1 through CP 3 Bandwidth (Mbps)
Gold	25.6	51.2
Silver	38.4	76.8
Bronze	51.2	102.4
Best-effort	64	128

qos npu inter-subscriber traffic bandwidth-sharing

Configures NPU QoS bandwidth sharing properties for the system.

Product

GGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

qos npu inter-subscriber traffic bandwidth-sharing { { enable | disable } { all | slot *slot_num* **cpu** *cpu_num* **} }**

enable

Enables bandwidth sharing for the specified criteria.

disable

Disables bandwidth sharing for the specified criteria.

all

Specifies that the bandwidth action is to be applied to all packet processing cards and every CPU on each packet processing card.

slot *slot_num*

Specifies that the bandwidth action is to be applied to a packet processing card in a specific chassis slot number.

slot_num is the slot in which a packet processing card is installed. These cards can be installed in slots 1 through 4 and 7 through 10 on the ASR 5500.

cpu *cpu_num*

Specifies a specific control processor (CP) on a packet processing card for which to perform the bandwidth action.

cpu_num is an integer value from 0 to 3. 0 represents the lead CP.

Usage Guidelines

The available bandwidth of a subscriber queue can be shared equally among the other subscriber queues. Any unutilized bandwidth of a queue can be shared with the other queues equally. For example, if only one DSCP is configured and it is mapped to best-effort, that DSCP would get the bandwidth allocated to the best-effort in addition to the rest of the bandwidth allocated to the gold, silver, and bronze.

By default, the system enables sharing for all packet processing cards and their CPs.

For additional information on the NPU QoS functionality, refer to the *System Administration Guide*.

Example

The following command disables bandwidth sharing for the fourth CP (CP 3) on a packet processing card installed in chassis slot 3:

```
qos npu inter-subscriber traffic bandwidth-sharing disable slot 4 cpu 3
```

qos npu inter-subscriber traffic priority

Configures the DSCP-to-Priority assignments for the system.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
qos npu inter-subscriber traffic priority { best-effort | bronze | gold
| silver } assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 |
af31 | af32 | af33 | af41 | af42 | af43 | be | ef | dscp_num } }
no qos npu inter-subscriber traffic priority [ assigned-to dscp { af11 |
 af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 |
af43 | be | ef } ]
```

best-effort

Specifies the best-effort queue priority.

bronze

Specifies the bronze queue priority.

gold

Specifies the gold queue priority.

silver

Specifies the silver queue priority.

af*XX*

Assigns the Assured Forwarding *XX* PHB (per-hop behavior) DSCP.

Each Assured Forwarding PHB has a corresponding DSCP value as follows:

- af11 through af13: DSCP values 5 through 7 respectively
- af21 through af23: DSCP values 9 through 11 respectively
- af31 through af33: DSCP values 13 through 15 respectively
- af41 through af43: DSCP values 17 through 19 respectively

be

Assigns the Best Effort forwarding PHB which has a corresponding DSCP value of 0.

ef

Assigns the Expedited Forwarding PHB which has a corresponding DSCP value of 23.

dscp_num

Specifies a specific DSCP value as an integer from 0 through 31.

Usage Guidelines

The differentiated services (DS) field of a packet contains six bits (0-5) that represent the differentiated service code point (DSCP) value.

Five of the bits (1-5) represent the DSCP. Therefore, up to 32 (25) DSCPs can be assigned to the various priorities. By default, they're all assigned to the lowest priority (best-effort).

For additional information on the NPU QoS functionality, refer to the *System Administration Guide*.

Important This functionality is not supported for use with the PDSN at this time.

Example

The following command maps the ef DSCP to the gold priority queue:

```
qos npu inter-subscriber traffic priority gold assigned-to dscp ef
```

quality-of-service-profile

This command creates an instance of a quality of service QoS profile and causes the system to enter the QoS Profile Configuration Mode for commands to configure the QoS parameters.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ no ] quality-of-service-profile` *`qos_profile_name`* **`[ -noconfirm ]`**

no

Including the **no** command filter causes the system to delete the QoS profile instance from the system configuration.

noconfirm

Do not prompt for additional verification when executing this command.

qos_profile_name

Enter 1 to 64 alphanumeric characters to uniquely name a quality of service (QoS) profile.

Usage Guidelines

This command creates a quality of service profile and provides access to the QoS profile configuration mode to use the commands to configure the QoS parameters, refer to the *QoS Profile* section of the *Command Line Interface Reference* for command information. The parameters configured in the QoS profile will override the QoS parameters configured using the APN profile configuration commands if configured for the APN profile.

Important

The MME's QoS profile does not become valid until it is associated with an APN profile with access type "eps". For more information, refer to the *APN Profile Configuration Mode* section in the *Command Line Interface Reference*

Example

Create a QoS profile named *QoStest*:

```
quality-of-service-profile QoStest
```

ran-peer-map

Creates a Radio Access Network (RAN) Peer Map and enters the RAN Peer Map Configuration Mode.

Product

ASN-GW

PHSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ no ] ran-peer-map` *`name`* `[ -noconfirm ]`

no

Removes the RAN Peer Map from the system.

name

Specifies the name of the RAN Peer Map. *name* must be an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Use this command to create a new RAN Peer Map or edit an existing one. RAN peer maps reconcile base station MAC addresses received in R6 protocol messages to the base station's IP address.

Entering this command results in the following prompt:

```
[context_name]hostname(config-ran-peer-map)#
```

See the *RAN Peer Map Configuration Mode* chapter for descriptions of the commands supported in this mode.

Example

The following command creates a RAN peer map named *ran12*:

```
ran-peer-map ran12
```

require active-charging

This command enables/disables Active Charging Service (ACS) with or without the Category-based Content Filtering application.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
require active-charging [ content-filtering category [ static-and-dynamic
 ] ]  [ traffic-optimization ]
no require active-charging
```

no

Disables ACS on the system.

content-filtering category [static-and-dynamic]

Enables the Category-based Content Filtering application with ACS support and creates the necessary Static Rating Database (SRDB) tasks to utilize the internal database of static/dynamic URLs.

For Dynamic Content Filtering support, the **static-and-dynamic** keyword must be configured to specify that the Dynamic Rater Package (model and feature files) must be distributed to rating modules on startup, recovery, etc. If not configured, by default, the static-only mode is enabled.

traffic-optimization

Enables loading of Cisco Ultra Traffic Optimization solution.

Important Enabling or disabling the Traffic Optimization can be done through Service-scheme framework.

Important After you configure this keyword, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Important In 21.5 and later releases, the **require active-charging traffic-optimization** CLI command has been deprecated as dependency on the chassis reboot is not valid anymore. The Cisco Ultra Traffic Optimization engine is loaded by default. The Cisco Ultra Traffic Optimization configuration CLIs are available when the license is enabled.

Usage Guidelines Use this command to enable/disable ACS with or without Category-based Content Filtering application on the chassis.

Important This command triggers the resource subsystem to switch to ACS-enabled mode and start ACS-related tasks. This CLI command must be configured before any services are configured, so that the resource subsystem can appropriately reserve adequate memory for the ACS-related tasks. After configuring this command, the configuration must be saved and the system rebooted in order to allocate the resources for ACS upon system startup.

require aes-ni

Enables or disables a aes-ni related Requirements.

Product

ePDG

PDIF

SecGw

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
[ no | default ] require aes-ni { capability | transform-set }
```

default

Sets / Restores default value assigned for aes-ni requirement.

no

Disables aes-ni requirement.

capability

Enables AES NI capability.

transform-set

Enables AES NI Restricted Transform Set Mode.

Usage Guidelines

Enabling this command allows the resource manager (RM) task to enables or disables a aes-ni related Requirements.

Important

After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Example

The following command enables AES NI capability:

```
require aes-ni capability
```

require crypto

This command enables IPSec Software Data Path for IKEv1/IKEv2 Maps.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
[ no ] require crypto [ ikev1-acl software | ikev2-acl software ]
```

no

- **require crypto** : Enables Crypto related parameters.
- **ikev1-acl**: Configures IKEv1-ACL IPSec sessions.
- **ikev2-acl**: Configures IKEv2-ACL IPSec sessions.
- **software**: IPSec Manager performs encryption, decryption and DH calculations.
- **no**: Disables IPSec Manager from encryption, decryption and DH calculations.
- By default this command is disabled.

Usage Guidelines

When enabled, this command configures IPSec Software Data Path for IKEv1/IKEv2 Maps.

Important This command must be enabled for IPSec encryption.

Example

The following command enables IPSec Software Data Path for IKEv1 Maps:

```
require crypto ikev1-acl software
```

require demux

Enables or disables demux capabilities on an ASR 5500. When demux tasks are enabled on a management card, the Active and Standby MIOs will host and migrate all demux tasks.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
[ default | no ] require demux { management-card | processing-card |
smgr-suspension interval seconds }
```

default

Demux functions will be run on a processing card.

no

Disables the demux capabilities except when session recovery is enabled.

Important On a system with session recovery licensed and enabled, a processing or management card must be designated to run demux functions.

management-card

Enables demux functionality on a management (ASR 5500 MIO) card.

Note After you configure this keyword, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

processing-card

Enables demux functionality on a processing card (default).

smgr-suspension interval *seconds*

Used to address some specific failure scenarios, where either the sessmgr or the corresponding aaa manager restarts, and the PGW service/sessmgr is unable to bring new calls up or establish a connection with all other dependent services. In these failure scenarios if a call landed on this particular P-GW service/sessmgr, the call establishment is significantly delayed and would fail until all the dependent services come up. This resulted in the possibility that the S-GW might time out and report that the peer P-GW is not responding to the Create Session Request (CSReq) message. Although the issue is usually self-correcting and takes between 10 to 25 seconds, if operators see too many call rejects due to a peer not responding to the Create Session Response (CSResp) message, and this is happening after a aaa manager restart or a sessmgr restart, this feature can be configured to temporarily stop seeing the peer not responding error.

The variable seconds must be an integer from 5 to 30 seconds.

There is no default setting.

Usage Guidelines

Use this command to configure the system to direct demux task placement.

The following restrictions apply when enabling an MIO/UMIO as a demux card:

- The require **demux management-card** command must be configured before any service or contexts have been created on the system. The command will not execute after a mode of operation has been selected for the chassis.
- Only the following services currently support the designation of an MIO/UMIO card for demux functions: GGSN, S-GW, P-GW, HA and SAEGW.
- Ex-GW, L2TP, MME, NEMO and SGSN are not supported.
- After the ASR 5500 has booted with demux functions running on an MIO/UMIO, you cannot configure non-supported services. A maximum of eight Demux Managers are supported. Any attempt to add more than eight Demux Managers will be blocked.
- Service/products requiring a large number of VPN Managers, VRFs and/or Demux Managers must not enable demux functions on an MIO.
- With demux functions running on an MIO, the ASR 5500 supports a maximum of 10 contexts, 64 interfaces per context and 250 VRFs per system.

Implementation of this feature assumes that CEPS (Call Events Per Second) and the number of subscribers will remain constant, and only the data rate will increase. This ensures that the CPU demand will not increase on the MIO/UMIO.

Caution Enabling the Demux on MIO/UMIO feature changes resource allocations within the system. This directly impacts an upgrade or downgrade between StarOS versions in ICSR configurations. Contact Cisco TAC for procedural assistance prior to upgrading or downgrading your ICSR deployment.

Important Contact Cisco TAC for additional assistance when assessing the impact to system configurations when enabling the Demux on MIO/UMIO feature.

Example

The following command configures a DPC/UDPC as a demux card:

```
require demux processing-card
```

The following command configures an MIO/UMIO as a demux card:

```
require demux management-card
```

require detailed-rohc-stats

Enables or disables context-specific Robust Header Compression (RoHC) statistics.

Product

HSGW

PDSN

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
[ no ] require detailed-rohc-stats
```

no

Disables statistics for RoHC calls. This is the default condition.

Usage Guidelines

Enables context-specific statistics for RoHC calls.

Example

Enter the following command to enable context specific statistics for RoHC calls:

```
require detailed-rohc-stats
```

require diameter origin-host-abbreviation

This command controls the truncation of Diameter origin-host name used in the system.

Product

HA

HSGW

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
require diameter origin-host-abbreviation
no require diameter origin-host-abbreviation
```

no

This keyword does not allow truncation of the origin-host name but enables to construct the origin-host name with the full proclet name. This is the default configuration.

diameter origin-host-abbreviation

Truncates the Diameter origin-host name to a single character prefix according to the proclet name.

Usage Guidelines

Typically, Diameter host name is too long for the customer network to handle and process. The host name cannot be changed as it remains constant throughout the lifecycle of client application. So, this CLI command is used to control the truncation of Diameter origin-host name.

Important

This CLI configuration is applicable only at the time of system boot. If the CLI command is configured during run time, the following warning message is displayed "Warning: System already has running services, save config and reboot to take effect".

The Diameter origin-host name is represented as <*instance-number*>-<*procletname*>.<*name*>, where the proclet name can be sessmgr, diamproxy or aaamgr.

The **require diameter origin-host-abbreviation** CLI command aids in reducing the length of Diameter origin-host names by using "d" instead of "diamproxy", "s" instead of "sessmgr", and "a" instead of "aaamgr". If this CLI command is configured then the Diameter origin-host name value is constructed with the corresponding proclet name abbreviations.

For example, if a Diameter proxy is used to connect to a peer then the origin host will be *0001-diamproxy.endpoint* without the CLI configuration. When the **require diameter origin-host-abbreviation** CLI is enabled, the origin host will be *0001-d.endpoint*.

Important This CLI option does not take effect during ICSR upgrade and downgrade. When this CLI command is configured and **require diameter-proxy single** is used there will not be any changes in host name.

Example

The following command configures origin host name with "a" as the prefix when AAA manager communicates with the peer:

```
require diameter origin-host-abbreviation
```

require diameter-proxy

This command enables or disables Diameter Proxy mode.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
require diameter-proxy { master-slave |max count| multiple | single } [
diamproxy-per-card 2 ] [ algorithm { facility | round-robin } ]
no require diameter-proxy
```

no

Disables Diameter Proxy mode. This is the default configuration.

master-slave

Sets the Diameter-Proxy to Master-Slave mode.

In Master-Slave mode, multiple Diameter proxies are running, one on each packet processing card. One proxy serves as the Master and the other proxies are Slaves. The Master proxy relays the traffic across multiple Slave Diameter proxies.

Important After you configure this keyword, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

max *count*

This keyword configures the maximum number of Diameter proxies to be spawned in the system. *count* specifies the number Diameter proxies to be spawned in the system. The range of allowed Diameter proxies in the system is an integer from 1 to 48.

If the *count* values is specified as 1, only one Diameter proxy is spawned in the VPC-DI/SCALE environment for all SF cards. A single Diameter proxy is started on the active non-DEMUX card. Spawning of one Diameter proxy in this configuration is different than the **require diameter-proxy single** configuration, which spawns a Diameter proxy on a DEMUX card.

The variable *count* with value as 48 is similar to the **require diameter-proxy multiple** configuration.

multiple [diamproxy-per-card 2] [algorithm { facility | round-robin }]

Configures one Diameter proxy for each active packet processing card.

Important After you configure this keyword, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Important The **[diamproxy-per-card 2] [algorithm { facility | round-robin }]** options are primarily applicable for ASR 5500 DPC2 hardware. Multiple Diamproxies per card is the default behavior for the DPC2. This functionality can be extended to the DPC with a maximum of 2 instances of Diamproxies.

- **diamproxy-per-card**: Configure the number of Diameter proxies per card. By default, two Diamproxies are spawned for each DPC2. This allows the DPC2 to handle more transactions per proxy.
- **algorithm**: Configures the algorithm to be used to distribute the load to Diamproxies. The algorithm determines how the endpoints are distributed. Whenever an endpoint is associated with a service, the session controller sends an Allocate-Request message specifying the endpoint name with the facility type. The framework allocates a CPU based on the algorithm that has been configured.
  - **facility**: This algorithm specifies that the Diameter proxy (endpoint) will be selected based on the facility type. This is the default option. In this algorithm, all AAA endpoints will be present in CPU 0 and all session manager endpoints will be present in CPU 1.
  - **round-robin**: This algorithm specifies that the Diameter proxy selection will be in Round Robin fashion. For example, if the number of proclets running per card is 2, the first endpoint configured is associated with CPU 0 (proxy running in CPU 0 of the same card) and the next endpoint configured will be associated with CPU 1, the third one with CPU 0 and fourth one with CPU1.

single [diamproxy-per-card 2] [algorithm { facility | round-robin }]

Configures one Diameter proxy for the entire chassis.

Important After you configure this keyword, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Important The **[diamproxy-per-card 2] [algorithm { facility | round-robin }]** options are primarily applicable for ASR 5500 DPC2 hardware. Multiple Diamproxies per card is the default behavior for the DPC2. This functionality can be extended to the DPC with a maximum of 2 instances of Diamproxies.

- **diamproxy-per-card**: Configures the number of Diameter proxies per card. By default, two Diamproxies are spawned for each DPC2. This allows the DPC2 to handle more transactions per proxy.
- **algorithm**: Configures the algorithm to be used to distribute the load to Diamproxies. The algorithm determines how the endpoints are distributed. Whenever an endpoint is associated with a service, the session controller sends an Allocate-Request message specifying the endpoint name with the facility type. The framework allocates a CPU based on the algorithm that has been configured.
  - **facility**: This algorithm specifies that the Diameter proxy (endpoint) will be selected based on the facility type. This is the default option. In this algorithm, all AAA endpoints will be present in CPU 0 and all session manager endpoints will be present in CPU 1.
  - **round-robin**: This algorithm specifies that the Diameter proxy selection will be in Round Robin fashion. For example, if the number of proclets running per card is 2, the first endpoint configured is associated with CPU 0 (proxy running in CPU 0 of the same card) and the next endpoint configured will be associated with CPU 1, the third one with CPU 0 and fourth one with CPU1.

Usage Guidelines

When the Diameter Proxy mode is enabled, each proxy process is a Diameter host, instead of requiring every Diameter application user (such as, every ACSMgr and/or every SessMgr, depending on the application) to be a host.

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

In Master-Slave mode, multiple Diameter proxies are running, one on each packet processing card. One proxy serves as the Master and the other proxies are Slaves. The Master relays the traffic from an incoming connection to a specific Slave Diameter proxy.

In releases prior to 18, when the chassis is in standby state, all the Diameter proxies are stopped. In 18 and later releases, all the Diameter proxies will be running even when the chassis is in standby mode. Any change in ICSR grouping mask will lead to stopping and restarting of all the diamproxies on the standby chassis.

Example

The following command configures a Diameter proxy for each active packet processing card:

```
require diameter-proxy multiple
```

The following command configures a single Diameter proxy for the entire chassis:

require diameter-proxy single

The following command configures a maximum of 20 diameter proxies that can be spawned in the system:

require diameter-proxy max 20

require ecs credit-control

This command configures the Diameter Credit-Control Application (DCCA) to work in per subscriber-PDN level Gy mode.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config)#`

Syntax Description

In 14.0 and earlier releases:

[no] require ecs credit-control subscriber-mode

In 14.1 and later releases:

[no] require ecs credit-control session-mode per-subscriber

no

Creates DCCA/Gy sessions per bearer/PDP-context.

Usage Guidelines

In 14.0 and earlier releases:

This command is applicable to all products using the Gy interface. Use this command to configure DCCA/Gy to work in per subscriber-PDN level Gy mode, wherein one Diameter session is created per subscriber PDN rather than per bearer, and only one DCCA/Gy session is created for multi-bearer PDNs.

If this command is not configured, or the **no require ecs credit-control subscriber-mode** command is configured, DCCA/Gy sessions are created per bearer/PDP-context, and as a result when there are multiple PDP contexts or multiple bearers in a PDN as many DCCA/Gy sessions are created.

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Important This command is independent of the **require active-charging** command. The **ecs** keyword in this command is license dependent.

In 14.1 and later releases:

This CLI command is made configurable on the fly, that means, the credit control mode can be seamlessly changed from subscriber (PDN) to sub-session and vice-versa without requiring a system reboot.

This change is done to align with the new CLI commands "**credit-control-client override session-mode { per-sub-session | per-subscriber }**" introduced in APN and Subscriber Group configuration modes.

This will be the default mode for all subscribers unless overwritten by APN/Subscriber configuration mode CLI commands.

Releases prior to 14.1, subscriber mode Gy and bearer mode Gy were implemented based on the configuration of CLI command **require ecs credit-control subscriber-mode**. This CLI is used as a chassis level configuration which mandates that all subscribers anchored to this chassis should always be running in only one of these two modes. Enabling and disabling the CLI requires system reboot. ICSR switchover between two chassis running in two different modes will not work.

Release 14.1 and later, the Subscriber/Bearer mode Gy is selected based on APN/Subscriber mode instead of chassis wide configuration. This will provide the following:

- Flexibility to configure different modes for different subscriber.
- Flexibility to switch between modes without system reboot.
- Flexibility to switchover between two chassis working in different modes.

require graceful-cleanup-during-audit-failure

Enables or disables graceful cleanup of dropped calls during ICSR audit failures.

Product

ICSR

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
require graceful-cleanup-during-audit-failure [ del-cause non-ims-apn {
none | system-failure } ]
[ default | no ] graceful-cleanup-during-audit-failure
```

default

By default, the Cause IE will be omitted from the Delete Bearer Request for Non-IMS/Custom1 APNs.

no

The Cause IE will be omitted from the Delete Bearer Request for Non-IMS/Custom1 APNs.

del-cause

For P-GW, specifies the Cause Code to be sent in the Delete Bearer Request resulting from the graceful cleanup for Audit Failure.

non-ims-apn { none | system-failure }]

For Non IMS/Custom1 APNs, specifies the Cause Code to be sent in Delete Bearer Request from the P-GW resulting from the graceful cleanup for Audit Failure. By default the Cause IE will be omitted from the Delete Bearer Request for Non-IMS/Custom1 APNs.

- **none**: Omits the GTP Cause IE from the Delete Bearer Request resulting from the graceful cleanup for Audit Failure.
- **system-failure**: Sends the GTP Cause Code SYSTEM FAILURE.

Usage Guidelines

Use this command to enable or disable graceful cleanup of dropped calls during ICSR audit failures.

During an audit on the gateways (P-GW/S-GW/GGSN/SAEGW) after Session Recovery or an ICSR event, if any critical information, internally or externally related to a subscriber session seems inconsistent, ICSR will locally purge the associated session information.

Since external gateways (peer nodes) are unaware of the purging of this session, the UE session may be maintained at other nodes. This leads to unnecessary hogging of resources external to the gateway and an unreachable UE for VoLTE calls.

When this feature is enabled, graceful cleanup for an ICSR audit of failed calls occurs. External signaling notifies peers of session termination before purging the session. The gateway will attempt to notify external peers of the removal of the session. External nodes to the local gateway include: S-GW, P-GW, SGSN, MME, AAA, PCRF, and IMSA.

Audit failure can occur because of missing or incomplete session information. Therefore, only the peers for which the information is available will be notified.

Example

The following command sequence enables graceful cleanup and sends a Cause IE for non-IMS/Custom1 APNs of SYSTEM FAILURE.

```
require graceful-cleanup-during-audit-failure del-caus non-ims-apn
system-failure
```

require ipsec-large

Enables or disables a boost in IPSec crypto processing performance.

Product

ePDG

PDIF

SecGw

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
[ no ] require ipsec-large
```

no

Disables this feature.

Usage Guidelines

Enabling this command allows the resource manager (RM) task to assign additional IPSec managers to packet processing cards with sufficient processing capacity.

Important

After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Example

The following command assigns additional IPSec managers to packet processing:

```
require ipsec-large
```

require segregated li-configuration

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

require session ipsecmgr-per-vcpu

Configures the number of IP Security Manager (ipsecmgr) processes per vCPU.

Product ePDG (VPC-DI platform only)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description **`[ default ] require session ipsecmgr-per-vcpu`** *`count`* **`}`**

default

Returns the number of ipsecmgrs per vCPU to the default of 1.

Note The default value can be adjusted as needed per your call model deployment requirements. Please contact your Sales or Support representative for more information.

count

Sets the number from 1 through 2 of the ipsecmgr processes to be created for each vCPU. Default: 1.

Usage Guidelines Enables multiple IP Security Manager (ipsecmgr) processes per vCPU.

Example

The following command configures the system to create 2 ipsecmgrs per vCPU:

```
require session ipsecmgr-per-vcpu 2
```

require session recovery

Enables session recovery when hardware or software fault occurs within system.

Product ePDG

GGSN

ASN-GW

HA

HSGW

MME

PDG/TTG

PDIF

PDSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ default | no ] require session recovery [ optimized-checkpointing ]`

default

Disables session recovery if enabled; requires a system restart via the **reload** command.

no

Disables session recovery feature after the configuration file is saved and the system is restarted via a **reload** command.

optimized-checkpointing

Disables variable time interval full checkpoints on an Active chassis based on the number of sessions in a sessmgr. Enabling or disabling this option takes effect immediately, even for existing connected calls. By default optimized checkpointing is disabled.

Important

For release 20.0 and higher, periodic full checkpointing is performed for AAA manager every 12 minutes. The setting is fixed and cannot be disabled by the new keyword.

Usage Guidelines

When this feature is enabled, the system attempts to recover any home agent-based Mobile IP sessions that would normally be lost due to a hardware or software fault within the system.

This functionality is available for the following call types:

- ASN-GW services supporting simple IP, Mobile IP, and Proxy Mobile IP
- PDSN services supporting simple IP, Mobile IP, and Proxy Mobile IP
- Closed RP PDSN services supporting simple IP, Mobile IP, and Proxy Mobile IP
- HA services supporting Mobile IP and/or Proxy Mobile IP session types with or without per-user Layer 3 tunnels
- GGSN services for IPv4 and PPP PDP contexts
- SGSN services for all attached and/or activated subscribers

- LNS session types
- PDIF services supporting Simple-IP, Mobile-IP and Proxy Mobile-P
- MME services

The default setting for this command is disabled.

The **no** option of this command disables this feature.

This command only works when the Session Recovery feature is enabled through a valid Session and Feature Use License Key.

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Example

The following command enables session recovery:

```
require session recovery
```

require session sessmgr-per-vcpu

Configures the number of Session Manager (sessmgr) processes per vCPU.

Product All (VPC-DI platform only)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **`[ default ] require session sessmgr-per-vcpu`** *`count`* **`}`**

default

Returns the number of sessmgrs per vCPU to the default of 1.

Caution The default value can be adjusted as needed per your call model deployment requirements. However, the recommendation is to use the default value. To change or adjust the default value, contact your Sales or Support representative.

count

Sets the number the sessmgr processes to be created for each vCPU. The valid values are 1 and 2 . The default value is 1.

Only for MME/SGSN, the count can go up to 2 for the number of sessmgrs per vCPU.

All other values are reserved.

Usage Guidelines

For applications that are light on CPU usage but heavy on RAM usage, such as Internet of Things (IoT) Gateway, it is more efficient to have multiple session manager (sessmgr) processes per vCPU.

Table 2: vCPU Support per Platform

Platform	vCPU Support
Gateway	• For 1 sessmgr process per vCPU, 16 sessmgr processes per Service Function (SF) VM are supported. • For 2 sessmgr processes per vCPU, 32 sessmgr processes per SF VM are supported.
MME/SGSN	For 2 sessmgr processes per vCPU, 56 sessmgr processes per SF VM are supported.

Example

The following command configures the system to create 2 sessmgrs per vCPU:

```
require session sessmgr-per-vcpu 2
```

reveal disabled commands

Enables the input of commands for features that do not have license keys installed. The output of the command **show cli** indicates when this is enabled. This command effects all future CLI sessions. This is disabled by default.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
[ no ] reveal disabled commands
```

no

Do not show disabled commands.

Usage Guidelines

When this is enabled and a disabled command is entered, a message is displayed that informs you that the required feature is not enabled and also lists the name of the feature that you need to support the command.

When this is disabled and a disabled command is entered, the CLI does not acknowledge the existence of the command and displays a message that the keyword is unrecognized.

Example

Set the CLI to accept disabled commands and display the required feature for all future CLI sessions with the following command:

```
reveal disabled commands
```

Set the CLI to reject disabled commands and return an error message for all future CLI sessions:

```
no reveal disabled commands
```

rlf-template

This command enters the Rate Limiting Function (RLF) Template Configuration Mode. This mode is used to configure the RLF template to control the throttling parameters.

Important RLF template cannot be deleted if it is bound to any application (peers/endpoints).

Product

GGSN

P-GW

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ no ] rlf-template` *`rlf_template_name`*

no

Remove the specified RLF template from global configuration.

rlf_template_name

The name of the RLF template to create or remove. *rlf_template_name* must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to enter the RLF Template Configuration mode. The users can define the rate limiting configurations within this template.

Important Rate Limiting Function (RLF) is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

This feature implements a generic framework that can be used by multiple interfaces and products for rate-limiting/throttling outgoing messages like Diameter messages on Gx, Gy interface towards PCRF.

When applications send messages to peers at a high rate, (e.g. when a large number of sessions goes down at the same time, accounting stop messages for all the sessions are generated at the same time) the peer may not be able to handle the messages at such high rates. To overcome this situation, the Rate Limiting Function (RLF) framework is developed so that the application sends messages at an optimal rate such that peer is capable of receiving all the messages and does not enter an overload condition.

When RLF feature is enabled, all the messages from the application are pushed to the RLF module for throttling and rate control, and depending on the message-rate configured the RLF module sends the messages to the peer. Once the rate or a threshold value is reached, the RLF module notifies the application to slow down or stop sending messages. RLF module also notifies the application when it is capable of accepting more messages to be sent to the peer. RLF module typically uses a Token Bucket Algorithm to achieve rate limiting.

Currently in the deployment of the Diameter applications (Gx, Gy, etc.), many operators make use of "**max-outstanding** <*number*>" as a means of achieving some rate-limiting on the outgoing control traffic. With RLF in place, this is no longer required since RLF takes care of rate-limiting in all cases. If RLF is used and **max-outstanding** is also used, there might be undesirable results.

Important If RLF is being used with an "**diameter endpoint**", then set the **max-outstanding** value of the peer to be 255.

To use the template, Diameter or any other applications must be associated with the template. The RLF provides only the framework to perform the rate limiting at the configured Transactions Per Second (TPS). The applications (like Diameter) should perform the configuration specific to each application.

Entering this command results in the following prompt:

```
[context_name]host_name(cfg-rlf-template)#
```

RLF Template Configuration Mode commands are defined in the *RLF Template Configuration Mode Commands* chapter.

Example

The following command creates an RLF template named *rlf_1* and enters the RLF Template Configuration mode:

```
rlf-template rlf_1
```

rohc-profile

This command allows you to create an RoHC (Robust Header Compression) profile and enter the RoHC Profile Configuration Mode. This mode is used to configure RoHC Compressor and Decompressor parameters. RoHC profiles can then be assigned to specific subscriber sessions when RoHC header compression is configured.

Product

HSGW

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

rohc-profile profile-name *name* **[-noconfirm] [common-options | compression-options | decompression-options]**
no rohc-profile profile-name *name*

common-options

Configures common parameters for compressor and decompressor.

compression-options

Configures ROHC compression options.

decompression-options

Configures ROHC decompression options.

no

Remove the specified RoHC profile.

name

The name of the RoHC profile to create or remove. *name* must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Do not prompt for additional verification when executing this command.

Usage Guidelines

Use this command to enter the RoHC Profile Configuration mode.

Entering this command results in the following prompt:

```
[context_name]host(config-rohcprofile-<profile_name>)#
```

RoHC Profile Configuration Mode commands are defined in the *RoHC Profile Configuration Mode Commands* chapter.

Example

Enter the following command to create an RoHC profile named *HomeUsers* and enter the RoHC Configuration mode without prompting for verification:

```
rohc-profile profile-name HomeUsers
```

The following command removes the RoHC profile named *HomeUsers*:

```
no rohc-profile profile-name HomeUsers
```

sccp-network

This command creates or removes a Signaling Connection Control Part (SCCP) network instance which is used to define the SS7 end-to-end routing in a UMTS network. As well, this command enters the SCCP network configuration mode. The SGSN supports up to 12 SCCP network instances at one time.

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

Product

SGSN

HNBGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
sccp-network sccp_net_id [ -noconfirm ]
no sccp-network sccp_net_id
```

no

Remove the SCCP network configuration with the specified index number from the system configuration.

sccp_net_id

This number identifies a specific SCCP network configuration.

sccp_net_id: must be an integer from 1 through 12.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create or modify an SCCP network and enter the SCCP network configuration mode.

The SCCP network is not a standard SS7 or UMTS concept - this concept is specific to this platform.

For details about the commands and parameters needed to create and edit the SCCP Network configuration, check the *SCCP Network Configuration Mode* chapter.

Example

The following command creates an SCCP network with the index number of *1*:

```
sccp-network 1
```

The following command creates an SCCP network with the index number of *2* to associate with HNB-GW service for HNB access network users without any prompt.:

```
sccp-network 2 -noconfirm
```

sctp-param-template

This command allows you to create an SCTP parameter template and enter the SCTP Parameter Template Configuration Mode. This mode is used to configure parameters for SCTP associations.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ no ] sctp-param-template` *`name`*

no

Removes the specified SCTP parameter template from the system.

name

Specifies the name of the SCTP parameter template being created or accessed. *name* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to enter the SCTP Parameter Template Configuration mode.

Entering this command results in the following prompt:

```
[context_name]host(sctp-param-template)#
```

SCTP Parameter Template Configuration Mode commands are defined in the *SCTP Parameter Template Configuration Mode Commands* chapter.

Important The SCTP parameters will be activated in a service only if the corresponding service restarts or if the SCTP parameter template is re-associated with its corresponding service. The SCTP parameters will not be active if the SCTP template is changed.

Example

The following command creates a new SCTP parameter template or enters an existing template named *sctp-tmpl2*:

```
sctp-param-template sctp-tmpl2
```

security

Enters the Security configuration mode. Commands for configuration of security features are available in the *Security Configuration Mode Commands* chapter.

Important This is a license-controlled feature. For more information, contact your Cisco account or support representative.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
security
no security
```

no

Removes all configuration within the Security configuration mode.

Usage Guidelines Use this command to enter the Security configuration mode to define or modify the connection with the Talos content-filtering server and configure URL categorization parameters.

service-chain

This command enters the Service Chain Configuration Mode. This command gives service-chain definition.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

service-chain *<service_chain_name>*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-service-chain)#
```

service-chain

Defines service chain association.

service_chain_name

Specifies name of the service chain. This is entered as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to give service-chain definition.

Example

The following command associates nsh-format with service-chain:

```
service-chain SC1
```

session disconnect-reasons bucket-interval

Configures an interval in minutes for displaying disconnect reasons.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

session disconnect-reasons bucket-interval *interval_minutes*
no session disconnect-reasons bucket-interval *interval_minutes*

no

Removes the specified bucket-interval.

interval_minutes

Configures interval "x" in minutes to display disconnect reasons for additional historical time intervals. The interval is specified as an integer from 1 through 20.

Usage Guidelines

Use this command to configure an interval in minutes for displaying historical disconnect reasons.

Example

The following command specifies a bucket-interval of 5 minutes.

```
session disconnect-reasons bucket-interval 5
```

session trace

This command configures the type of network elements, file transfer protocol, and Trace collection entity mode to be used for the transportation of trace files collected for the subscriber session tracing on the UMTS/EPC network element(s) along with network connection parameters and timers.

Product

GGSN

MME

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
session trace network-element { all | enb | mme | pgw | sgw | ggsn | saegw
 } [ collection-timer sec ] [ file-type { a-type | b-type } ] [ tce-mode
{ none | push transport sftp path string username name { encrypted password
 enc_pw | password password } } ]
no session trace network-element { all | enb | mme | pgw | sgw | ggsn
saegw }
```

no

Removes the entire session trace configuration from the system or a specific network element trace configuration.

Important To modify the session trace network-element configuration, you must first enter the **no session trace network-element** form of the command to remove the session trace configuration and then entire an entirely new configuration.

network-element { all | enb | mme | pgw | sgw | ggsn saegw }

Identifies the type of service to the session trace application in order to determine the applicable interfaces.

all: Specifies that all network elements and their associated interfaces are to be made available to the session trace application.

enb: Specifies that the eNodeB and its associated interfaces is to be made available to the session trace application. With this option, the allocated Trace Recording Session Reference and the Trace Reference is sent to MME over S1AP, which looks up the IMSI/IMEI associated with the corresponding S1 session and forwards the two references and UE ID to the TCE.

ggsn: Specifies that the GGSN and its associated interfaces is to be made available to the session trace application.

mme: Specifies that the MME and its associated interfaces is to be made available to the session trace application.

pgw: Specifies that the P-GW and its associated interfaces is to be made available to the session trace application.

sgw: Specifies that the S-GW and its associated interfaces is to be made available to the session trace application.

saegw: Specifies that the SAEGW and its associated interfaces is to be made available to the session trace application.

collection-timer *sec*

Specifies the amount of time (in seconds) to wait from initial activation/data collection before data is reported to the Trace Collection Entity (TCE). *sec* must be an integer from 0 through 255.

file-type { a-type | b-type }

Specifies which type of XML file is generated by the session trace. Options include an A-type file and B-type file. When B-type XML files are used, multiple trace recording session elements will be encoded in a single XML file. It should be noted that different trace recording sessions may be associated with different TCEs, according to the TCE IP address specified during activation. As expected, each Type-B XML file will contain traceRecSession elements that pertain only to the same target TCE. There will be different XML Type-B files created for different TCEs and they will be placed in different tce_x directories for transmission to the target TCEs.

Default: a-type

Important If using the file-type keyword, it must be entered in the command before entering either of the other optional keywords.

tce-mode none

Specifies that session trace files are to be stored locally and must be pulled by the TCE.

tce-mode push transport sftp path *string* username *name* { encrypted password *enc_pw* | password *password* }

Specifies that session trace files are to be pushed to the Trace Collection Entity (TCE).

sftp: Specifies that Secure FTP is used to push session trace files to the TCE.

path *string*: Specifies the directory path on the TCE where files will be placed.

username *name*: Specifies the username to be used when pushing files to the TCE.

encrypted password *enc_pw*: Specifies the encrypted password to be used when pushing files to the TCE.

password *password*: Specifies the password to be used when pushing files to the TCE.

Usage Guidelines

Use this command to configure the file transfer methods and modes for subscriber session trace functionality and to how and where session trace files are sent after collection.

This configuration contains collection timer, UMTS/EPC network element, type of file transfer, and user credentials setting to send the collected trace files to the TCE.

Example

The following command configures the collection time for session traces to *30* seconds, identifies the network element as all elements (GGSN, MME, S-GW, SAEGW, and P-GW), and pushes session trace files to a TCE via SFTP into a directory named */trace/agw* using a username *admin* and a password of *pw123*:

```
session trace network-element all collection-timer 30 tce-mode push
transport sftp path /trace/agw username admin password pw123
```

The following command configures the collection time for session traces to *30* seconds, identifies the network element as an MME, and pushes session trace files to a TCE via SFTP into a directory named */trace/sgw* using a username *admin* and a password of *pw123*:

```
session trace network-element mme collection-timer 30 tce-mode push
transport sftp path /trace/mme username admin password pw123
```

The following command configures the collection time for session traces to *30* seconds, identifies the network element as GGSN, and pushes session trace files to a TCE via SFTP into a directory named */trace/ggsn* using a username *admin* and a password of *pw123*:

```
session trace network-element ggsn collection-timer 30 tce-mode push
transport sftp path /trace/ggsn username admin password pw123
```

sgsn-global

This command gives access to the SGSN Global configuration mode to set parameters relevant to the SGSN and HNB-GW as a whole.

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

Product

SGSN

HNBGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

sgsn-global

Usage Guidelines

Using this command moves into SGSN Global Configuration mode. In this mode, you can set system-wide parameters on SGSN and HNB-GW to perform the following tasks:

On SGSN:

- monitoring and managing TLLIs in the BSSGP layer.
- defining IMSI ranges used as filters in the operator policy selection process.

On HNB-GW:

- setting system-wide IPC message aggregation parameters

Example

Enter the SGSN Global configuration mode with the following:

sgsn-global

sgsn-operator-policy

This command creates an SGSN Operator Policy and enters the SGSN operator policy configuration mode. Commands for configuration of the policies are available in the SGSN Operator Policy Configuration Mode chapter elsewhere in this Command Line Interface Reference.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
sgsn-operator-policy ( default | name name } [ -noconfirm ]
no sgsn-operator-policy ( default | name name }
```

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

no

Removes the specified SGSN operator policy from the system configuration.

default

In this case, default is the name of a specific operator policy. This default policy is used when no other defined operator policy matches the incoming IMSI.

Important You should configure this default operator policy so that is it available to handle IMSIs that are not matched with other defined policies.

name *name*

Usage Guidelines

Use this command to create an SGSN operator policy and to enter the SGSN operator policy configuration mode to define or modify policies.

The SGSN Operator Policy specifies rules governing the services, facilities and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements such as DNS servers and HLRs.

The system supports up to 1000 operator policies, including the default operator policy.

Important Once the instance of an operator policy is defined, to use the policy it is necessary to go into the SGSN Operator Policy Configuration Mode to define the IMSI range with the MCC command - this requirement does not hold if you are using a default operator policy.

Example

The following command accesses the default SGSN operator policy and enters the SGSN operator policy configuration mode to view or modify the specified policy:

```
sgsn-operator-policy default
```

snmp authentication-failure-trap

Enables or disables the SNMP traps for authentication failures.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ no ] snmp authentication-failure-trap`

no

Disables SNMP traps for authentication failures. When omitted, SNMP traps for authentication failures will be generated.

Usage Guidelines

Disables authentication failure traps if they are not of interest. At this time the option may be changed to support trouble shooting.

By default SNMP authentication failure traps are disabled.

Example

The following command enables SNMP authentication failure traps:

`snmp authentication-failure-trap`

snmp community

Configures the SNMP v1 and v2 community strings.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

In StarOS 12.3 and later releases:

snmp community [encrypted] name *string* **[context** *context_name* **| read-only | read-write | view** *view_name* **]**
no snmp community [encrypted] name *string*

In StarOS 12.2:

snmp community [encrypted] name *string* **[read-only | read-write]**
no snmp community [encrypted] name *string*

In StarOS 12.1 and earlier releases:

snmp community *string* **[read-only | read-write]**
no snmp community *string*

no

The specified community string is removed from the configuration.

encrypted

Specifies the use of an encrypted string when entering the community name. Without the encrypted option, the plain-text community name must be provided.

name *string*

Specifies a community string whose options are to be modified. An unencrytpted string must be an alphanumeric string of 1 through 31 characters. An encrypted string is an alphanumeric string of 1 through 80 characters.

context *context_name*

Default: community string applies to all contexts.

Specifies a the context to which the community string shall be applied. *context_name* must be an alphanumeric string of 1 through 31 characters.

read-only | read-write

Default: read-only

Specifies if access rights for the community string.

read-only: the configuration may only be viewed.

read-write: the configuration may be viewed and edited.

view *view_name*

Default: community string applies to all views.

Specifies the view to which the community string shall be applied. *view_name* must be an alphanumeric string of 1 through 31 characters.

Usage Guidelines

The community strings define the privileges of SNMP users. It may be desirable to give read-only access to front line operators.

Example

The following command configures an SNMP community name of *BxB102*:

```
snmp community name BxB102
```

snmp discard-snmpv3-pdu

Configures the system to discard all SNMPv3 protocol data units (PDUs) received.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

[no] snmp discard-snmpv3-pdu

no

Returns the command to the default setting, where SNMPv3 messages are processed.

discard-snmpv3-pdu

Configures the system to discard all SNMPv3 PDUs received.

Usage Guidelines

Use this command to configure the system to discard all SNMPv3 messages received. By default, the system processes SNMPv3 PDUs.

Example

The following command configures the system to discard all SNMPv3 messages received.

snmp discard-snmpv3-pdu

snmp engine-id

Configures the SNMP engine to use for SNMP requests when SNMPv3 agents are utilized.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

snmp engine-id local *id*

id

Specifies the SNMPv3 engine to employ. *id* must be an alphanumeric string of 1 through 31 characters.

Usage Guidelines

When SNMPv3 is used for SNMP access to the chassis the engine ID can be used to quickly change which schema is used for SNMP access.

Important

The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must not configure this command to use.

Example

The following command configures an SNMP engine ID of *secure23*.

```
snmp engine-id local secure23
```

snmp heartbeat

Enables the sending of periodic "heartbeat" notifications (traps).

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

snmp heartbeat { interval *minutes* **| second-interval** *seconds* **}**
[default | no] snmp heartbeat

default

Resets the SNMP heartbeat to 60 minutes.

no

Disables the feature.

interval *minutes*

Specifies the interval time in minutes between notificationsas an integer from 1 through 1440. Default: 60

second-interval *seconds*

Default: 30

Specifies the interval time in seconds between notificationsas an integer from 10 through 50.

Usage Guidelines

Use this command to enable the sending of a heartbeat notification periodically to confirm a system is up and communicating.

Example

The following command sets the SNMP heartbeat notification interval to 2 hours, 15 minutes.

```
snmp heartbeat interval 135
```

snmp history heartbeat

Enables the recording of heartbeat notifications in SNMP history.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
[ default | no ] snmp history heartbeat
```

default

Returns the command to the default setting of enabled.

no

Disables the history recording feature.

Usage Guidelines

Use this command to enable the recording of SNMP heartbeat notifications in SNMP history files.

Example

The following command enables the recording of heartbeat notifications in SNMP history:

```
snmp history heartbeat
```

snmp mib

Enables or disables a specified SNMP Management Information Base (MIB).

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

[no] snmp mib *mib_name*

no

Disables the specified MIB.

mib_name

Specifies a MIB by its name. You can find the currently supported MIBs by running the Exec mode **show snmp server** command. Enter the MIB name as a text string exactly as displayed under "SNMP Agent Mib Configuration",

By default the STARENT-MIB is enabled.

Usage Guidelines

Use this command to enable or disable system support for an SNMP MIB.

Example

The following command enables the SNMP MIB entitled "CISCO-MOBILE-WIRELESS-SERVICE-MIB".

```
snmp mib CISCO-MOBILE-WIRELESS-SERVICE-MIB
```

snmp notif-threshold

Configures the number of SNMP notification that need to be generated for a given event before it is propagated to the SNMP users.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

snmp notif-threshold *count* **[low** *low_count* **] [period** *seconds* **]**
[default | no] snmp notif-threshold

default

Resets the threshold to 100.

no

Removes all SNMP notification thresholds. All notifications will be broadcast to SNMP users.

count

The traps creation rate will be monitored periodically (as configured by the **period** field). If the number of traps created over one period cycle exceeds the count value configured, then the trap creation will be disabled. *count* must be an integer from 1 through 10000. Default: 100 for release 18.0 and earlier Default: 300 for release 19.0 and forward

low *low_count*

The traps creation rate will be monitored periodically (as configured by the **period** field). The trap creation will be enabled again only if the number of trap creation drops below the *low_count* value configured. Otherwise, trap creation remains disabled. *low_count* must be an integer from 1 through 10000. Default: 20

period *seconds*

Specifies the number of seconds of the monitoring window size before any subsequent notification may be broadcast to users. *seconds* must be an integer from 10 through 3600. Default: 300

Usage Guidelines

Set the notification threshold to avoid a flood of events which may be the result of a single failure or maintenance activity.

Example

The following command sets the SNMP notification threshold to 100 traps:

```
snmp notif-threshold 100
```

snmp runtime-debug

Enables or disables runtime SNMP debugging. When enabled (the default), this feature consumes CPU time with event logging. Disabling runtime debugging controls CPU usage and mitigates potential security threats when external bogus packets keep hitting SNMP.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

snmp runtime-debug [debug-tokens *token_id* **+**
no snmp runtime-debug

no

Disables SNMP runtime debugging.

debug-tokens *token_id* +

Enables DEBUGMSG tokens from the list of supported tokens appearing below. **+** indicates that multiple token IDs can be specified separated by spaces.

- **agentx** – agentx(12) token
- **disman** – disman(11) token
- **dumph** – dumph(13) token
- **dumpv** – dumpv token
- **init_mib** – init_mib(14) token
- **mib_init** – mib_init(1) token
- **parse-file** – parse-file(2) token
- **parse-mibs** – parse-mibs(3) token
- **read_config** – read_config(4) token
- **snmp** – snmp(5) token
- **snmpd** – snmpd(6) token
- **snmptrapd** – snmptrapd(7) token
- **transport** – transport(9) token
- **trap** – trap(8) token
- **usm** – usm(10) token

The numbers appearing in parentheses above will appear in the output of the **show snmp server** command for "Runtime Debug Token."

Usage Guidelines

Use this command to enable and disable SNMP runtime debugging. When enabled (the default), this feature consumes CPU time with event logging. Disabling runtime debugging controls CPU usage and mitigates potential security threats when external bogus packets keep hitting SNMP.

This command also supports optional DEBUGMSG MIB tokens that represent textual MIB files that are to be found and parsed. The list of supported tokens is limited to those that appear in the CLI.

Example

The following command disables SNMP runtime debugging:

```
no snmp runtime-debug
```

snmp server

Enables the SNMP server as well the configuration of the SNMP server port.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
snmp server [ port number ]
no snmp server
```

no

Restores the default SNMP port assignment of 161.

port *number*

Specifies the port number to use for SNMP communications. *number* must be an integer from 1 to 65535. Default: 161

Usage Guidelines

Set the SNMP port for communications when SNMP is enabled.

Important

This will result in restarting the SNMP agent when the **no** keyword is omitted. SNMP queries as well as notifications/traps will be blocked until the agent has restarted.

Example

The following command sets the SNMP server to communicate on port 100:

```
snmp server port 100
```

snmp target

Configures remote receivers for SNMP notifications.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

snmp target *name ip_address* **[port** *number* **] [non-default] [security-name** *string* **] [version { 1 | 2c | 3 | view] [security-level { noauth | { auth | priv-auth privacy [encrypted] des** *privpassword* **} authentication [encrypted] { md5 | sha }** *authpassword* **} } [informs | traps]**
no snmp target *name*

no

Removes the specified target as a receiver of unsolicited SNMP messages (traps).

authentication { md5 | sha } ***authpassword***

Reads the authentication type and password if the security level of the SNMP messages is set to **auth** or **priv-auth**. Authentication types are:

- **md5**: Configures the hash-algorithm to implement MD5 per RFC 1321.
- **sha**: Specifies that the hash protocol is Secure Hash Algorithm.

security-level **{ noauth | { auth | priv-auth privacy [encrypted] des** ***privpassword*** **}**

Sets the security level of the SNMPv3 messages, as follows:

- **noauth**: No authentication and encryption is used.
- **auth**: Only authentication will be used.
- **priv-auth**: Both authentication and encryption will be used.
- **privacy des** *privpassword*: Reads the privacy type and password.

name

Specifies a logical name to use to refer to the remote receiver. *name* must be an alphanumeric string of 1 through 31 characters.

ip_address

Specifies the IP address of the receiver. *ip_address* must be specified using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

non-default

Specifies that this destination is only used for SNMP traps which have been specifically identified.

port *number*

Default: 162

Specifies the port which is to be used in communicating with the remote receivers. *number* must be an integer from 0 through 65535.

security-name *string*

Default: no community string included

Specifies the community string to use in the unsolicited messages. *string* must be an alphanumeric string of 1 through 31 characters.

version { 1 | 2c | 3 } | view

Default: 1

Specifies the SNMP version the target supports and consequently the version of the SNMP protocol to use for communications.

Important The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices.However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must configure this command to use version 1 or version 2c.

informs | traps

Default: traps

Specifies the type of SNMP event to use to send notifications to SNPM targets. **traps** are unacknowledged (fire and forget) whereas **informs** require a response from the SNMP target.

If the notification type is set to **informs**, the notification is resent if no response is received within 5 seconds. The notification is resent at most two times.

Usage Guidelines

The target manages the list of remote receivers to which unsolicited messages are sent. Use this command to add /remove a monitoring system to/from a network.

Example

The following command configuures a target named *rcvr021* at IP address 10.1.1.1 to accept version 2c traps

```
snmp target rcvr021 10.1.1.1 version 2c traps
```

snmp trap

This command enables or disables generation of specific or all SNMP traps.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

Releases prior to Release 21.9

snmp trap { enable | suppress } {*trap_name* **+ | all | target** *target_name* **}| }**

From Release 21.9

snmp trap { { enable | suppress } { *trap_name* **+ | MMEManagerBusy | MMEManagerNormal| all | target** *target_name* **}] | { { snmp trap chassis-throughput-warn-threshold** *percentage* **trap-interval** *time_in_seconds* **} }**

enable

Enables or allows the generation of one or more SNMP traps by the system.

suppress

Disables the generation of one or more SNMP traps by the system.

***trap_name* +**

The name of the specific SNMP trap to enable or disable. + indicates that multiple traps separated by a space can be listed for a single instance of this command.

Important

The system disregards character case (case insensitive) when entering trap names.

MMEManagerBusy

Trap Number 1405.

MMEManagerNormal

Trap Number 1406.

all

Specifies that all SNMP traps will be affected by the specified operation (enable or suppress). Default: Enable All

target *target_name*

Specifies that these SNMP traps should be sent to the specified target name. *target_name* is the name of an eisitng SNMP target specified as an alphanumeric string of 1 through 31 characters.

chassis-throughput-warn-threshold*percentage*

Sets the chassis-throughput percentage at which a trap is raised to indicate that warning level is reached. The default value is 70%.

trap-interval*time_in_seconds*

Specifies the interval (in seconds) between the warn traps. The default value is 3600 seconds.

Usage Guidelines

SNMP traps are used by the system to indicate that certain events have occurred. A complete listing of the traps supported by the system and their descriptions can be found in the *SNMP MIB Reference*. Additionally, a trap listing can be viewed using the following command:

snmp trap { enable | suppress } ?

By default, the system enables the generation of all traps. However, individual traps can be disabled allowing only traps of a certain type or alarm level to be generated. This command can be used to disable un-desired traps and/or re-enable previously suppressed traps.

The **snmp trap chassis-throughput-warn-threshold** *percentage* **trap-interval***time in seconds* keywords are added to the **snmp trap** command to configure the following:

- Raise SNMP traps when the served throughput crosses the warning threshold levels (70%, 80%, and so on) of the committed throughput and the frequency.
- Specify the trap interval (in seconds) between each successive warn traps such that the second warn trap is raised only after the trap interval has lapsed.

A license is required to enable the Rate Limiting System Throughput Support feature. If the license for rate-limiting-throughput is not present, chassis-throughput cannot be calculated, rate limiting cannot be enforced, and SNMP traps cannot be raised.

When the rate-limiting-throughput per chassis license is applied but this CLI is not configured, it assumes the default values for the chassis throughput warn threshold trap interval.

Example

The following command suppresses the LogMessage trap:

```
snmp trap suppress logmessage
```

Example

The following command configures the warn level threshold and trap interval:

```
snmp trap chassis-throughput-warn-level 90 trap-interval 3000
```

snmp trap-pdu-v1tov2

Converts responses received from a SNMPv1 entity acting in an agent role into responses sent to a SNMPv2 entity acting in a manager role. This command inserts an extra zero in the outgoing trap PDU as required by RFC 1908 section 3.1.2.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

`[ no ] snmp trap-pdu-v1tov2`

no

Disables the adding of the extra zero in the outgoing trap PDU.

Usage Guidelines

Use this command to enable SNMPv2 support as defined in RFC 1908, section 3.1.2. By default, StarOS does not add the extra zero because Cisco Prime Network does not support the extra zero.

Example

The following command adds the extra zero to support of SNMPv2:

`snmp trap-pdu-v1tov2`

snmp trap-timestamps

Adds an additional system-time varbind to generated traps.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

```
[ no ] snmp trap-timestamps
```

no

Disables the adding of timestamps to generated traps.

Usage Guidelines

The timestamp added to the generated trap reflects the current system time. The timestamp is proprietary. This functionality is disabled by default.

Important

If the Web Element Manager application is used as your alarm server, the application relies on the timestamp provided by enabling this command to identify duplicate traps. As a result, it is recommended that this parameter be enabled for this case.

Example

The following command enables the inclusion of a timestamp with each generated trap:

```
snmp trap-timestamps
```

snmp user

Configures an SNMPv3 user for secure SNMP access.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
snmp user user_name [ [ encrypted ] password password | engine id | group
grp_name | security-model model  auth authentication { md5 [ [ encrypted ]
password password ] | sha [ [ encrypted ] password password  ] } | no auth |
 priv-auth privacy des [ [ encrypted ] password password ] | [ [ encrypted
 ] password password ] ]
no snmp user user_name
```

no

Removes the specified user from the list of valid SNMPv3 users.

user_name

Specifies the user which is to use SNMPv3 interfaces to the system. *user_name* must be an alphanumeric string of 1 through 31 characters.

engine *id*

The SNMP engine ID. **id** must be an alphanumeric string of 1 through 31characters.

group *grp_name*

Default: undefined (not a member of any group)

Specifies the user SNMPv3 group the into which user will be added. *grp_name* must be an alphanumeric string of 1 to 1023 characters.

security-model *model* auth

Default: USM

Specifies the security model used to authenticate the user. *model* must be configured to the following:

- **usm**: Designates the use of the User-based Security Model [RFC 2574].
- **auth**: Only authentication will be used.
- **authentication**: Specifies the SNMP authentication type of the target/user.
- **noauth**: No authentication or encryption is used.
- **priv-auth**: Both authentication and encryption will be used.
- **md5**: Specifies the authentication type as MD5.
- **sha**: Specifies the authentication type as SHA.
- **des**: Specifies the privacy type as DES.
- The **encrypted** keyword indicates the password will be received in an encrypted form. *password* must be an alphanumeric string of 16 through 368 characters.
- *password* must be a case-sensitive alphanumeric string of 8 through 127 characters.

[encrypted] password *password*

Default: undefined

Specifies the password for authenticating the user when the security model is set to User-based Security Model (USM).

The **encrypted** keyword indicates the password will be received in an encrypted form. *password* must be an alphanumeric string of 8 through 31 characters.

In StarOS 21.0 and later, *password* must be an alphanumeric string of 8 through 368 characters.

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

Usage Guidelines

Add and remove SNMPv3 users as operations staff or automated systems are updated. The security model will be user dependant based upon the support the users system provides.

Important The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However prior to StarOS 21.0, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must not configure this command to use.

Example

The following command configures SNMP user *user1*.

```
snmp user user1
```

ss7-routing-domain

This command creates an SS7 routing domain instance and enters the SS7 Routing Domain Configuration mode.

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

Product

SGSN

HNBGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
ss7-routing-domain rd_id variant v_type [ -noconfirm ]
no ss7-routing-domain rd_id
```

no

Removes the specified SS7 routing domain from the system configuration.

rd_id

Identifies a specific SS7 routing domain. Once it has been created, it can be accessed for further configuration and modification by entering the *rd_id* without entering the variant.

rd_id must be an integer from 1 through 12.

variant *v_type*

Identifies the national standard to be used for call setup, routing and control, signaling. Select one of the following:

- **ansi:** American National Standards Institute (U.S.A.)
- **bici:** Broadband Intercarrier Interface standard
- **china:** Chinese standard
- **itu:** International Telecommunication Union (ITU-T) Telecommunication Standardization Sector
- **ntt:** Japanese standard
- **ttc:** Japanese standard

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create an SS7 routing domain configuration instance or to enter the SS7 routing domain configuration mode to edit the configuration.

A routing domain groups configuration items to facilitate the management of the SS7 connection resources for an SGSN service. An Access Gateway supports up to 12 configured SS7 routing domains at one time.

After entering this command, the prompt appears as:

[*context_name*]<hostname>(config-ss7-routing-domain-*routing_domain_id*)#

For details about the commands and parameters used to define or edit an SS7 routing domain, refer *SS7 Routing Domain Configuration Mode* chapter.

Example

The following creates an SS7 routing domain with an index of *1* and the variant selection of Broadcast Intercarrier Interface (*bici*):

```
ss7-routing-domain 1 variant bici
```

The following command creates an SS7 routing domain instance with an index of *2* and the variant selection of Broadcast Intercarrier Interface (*bici*) to be associated with HNB RN-PLMN in an HNB access network:

```
ss7-routing-domain 1 variant bici
```

ssh key-gen wait-time

Specifies the wait time in seconds between the last key generation and when another key generation can be initiated. The default interval is 5 minutes.

Product

All

Privilege

Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **ssh key-gen wait-time** *seconds*

seconds

Specifies the wait interval in seconds as an integer from 0 to 86400. Default = 300.

Usage Guidelines Specifies the wait time in seconds between the last key generation and when another **ssh generate key** command can be initiated. The default interval is 5 minutes.

Example

The following command sets the SSH key generation wait interval as 6 minutes:

```
ssh key-gen wait-time 360
```

ssh key-size

Configures the key size in bits for SSH RSA key generation for all contexts.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **ssh key-size { 2048 | 3072 | 4096 | 5120 | 6144 | 7168 | 9216 }**

Usage Guidelines Configures the SSH key size in bits used to generate RSA key pairs for all contexts.

Example

The following command sets the SSH key size as 4096 bits:

```
ssh key-size 4096
```

statistics-backup

Enables the *Backup and Recovery of Key KPI Statistics* functionality.

Product

GGSN

MME

P-GW

SAEGW

SGSN

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ no ] statistics-backup { ggsn | mme | pgw | saegw | sgsn | sgw }`

no

Disables the backup/recovery of key KPI counters.

ggsn

Enables the backup and recovery of the GGSN's key KPI counters, including session disconnect reason and node-level statistics. If GGSN node is configured to back up, the following dependent services will be considered:

- GGSN service
- eGTP-C ingress
- GTP-U ingress

Important Checkpointing is done at the AAAMgr; therefore, there is a dependency of 1MB memory on AAAMgr for each corresponding SessMgr.

mme

Enables the backup and recovery of the MME's key KPI counters, which are identified in the MME-BK schema.

pgw

Enables the backup and recovery of the P-GW's key KPI counters, including session disconnect reason and node-level statistics. If P-GW node is configured to back up, the following dependent services will be considered:

- P-GW service
- eGTP-C ingress
- GTP-U ingress

s2a, s2b, and s5s8 interfaces are also considered.

Important Checkpointing is done at the AAAMgr; therefore, there is a dependency of 1MB memory on AAAMgr for each corresponding SessMgr.

saegw

Enables the backup and recovery of the SAEGW's key KPI counters, including session disconnect reason and node-level statistics. If SAEGW node is configured to back up, the following dependent services will be considered:

- P-GW service
- S-GW service
- SAEGW service
- P-GW eGTP-C ingress
- P-GW GTP-U ingress
- S-GW eGTP-C ingress/egress
- S-GW GTP-U ingress/egress

Important Checkpointing is done at the AAAMgr; therefore, there is a dependency of 1MB memory on AAAMgr for each corresponding SessMgr.

sgsn

Enables the backup and recoveru of the SGSN's key KPI counters, which are identified in the IuPS-BK schema, the GPRS-BK schema, MAP-BK schema, and the SGTP-BK schema.

sgw

Enables the backup and recovery of the S-GW's key KPI counters, including session disconnect reason and node-level statistics. If S-GW node is configured to back up, the following dependent services will be considered:

- S-GW service

- eGTP-C ingress/egress
- GTP-U ingress/egress

Important Checkpointing is done at the AAAMgr; therefore, there is a dependency of 1MB memory on AAAMgr for each corresponding SessMgr.

backup-interval

Important This keyword has been deprecated in Release 17.1 and replaced by the **statistics-backup-interval** command, also in this Global Configuration mode.

Usage Guidelines

This command enables the backup and recovery of key KPI counters after a crash. The counter values that are backed up and recovered are a subsets of the counters of the GGSN, MME, P-GW, SAEGW, S-GW, or SGSN and SGTP schemas. For additional information about this functionality, we recommend that you check the schema listed above in the *Statistics and Counters Reference* or the *Backup and Recovery of Key KPI Statistics* feature chapters in the associated product *Administration Guide* .

Example

Use a command similar to the following to enable backup of the SGSN or MME's key KPI statistics:

```
statistics-backup mme
```

Use a command similar to the following to disable backup of key KPI statistics for the MME or SGSN:

```
no statistics-backup sgsn
```

stats-profile

Creates a statistics profile and accesses *Stats Profile Configuration Mode*. In *Stats Profile Configuration Mode*, operators can configure per QCI packet drop counters and ARP granularity for QCI level counters.

Important ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

`[ no ] stats-profile` *name*

no

Disables the specified statistics profile.

stats-profile *name*

Specifies the name for the statistics profile.

The name must be an alphanumeric string from 1 to 64 characters in length.

Usage Guidelines

Use this command to create a statistics profile and enter *Stats Profile Configuration Mode*.

Statistics profiles enable operators to monitor QoS statistics that identify multiple services running with the Statistics profiles enable operators to monitor QoS statistics that identify multiple services running with the same QCI value. In addition, packet drop counters have been introduced to provide the specific reason the Enhanced Charging Service (ECS) dropped a packet. The packet drop counters provide output on a per ARP basis. This provides additional information that operators can use to troubleshoot and identify network issues that may be affecting service

For detailed information on this feature, refer to the *Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters* chapter in the *P-GW Administration Guide* or the *SAEGW Administration Guide*.

Example

The following command creates a Stats Profile named STATS:

`stats-profile` *STATS*

statistics-backup-interval

This command defines the time between backups of the service's key KPI statistics.

Product

GGSN

MME

P-GW

SAEGW

SGSN

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

statistics-backup-interval *minutes*
no statistics-backup-interval

no

Disables the interval configuration.

minutes

Enter an integer from 1 to 60 to define the number of minutes for the interval between each backup.

Usage Guidelines

This interval should only be defined after the **statistics-backup** command has been entered to configure the GGSN, MME, P-GW, SAEGW, S-GW, or SGSN to enable backup of statistics. For details on the feature, refer to the *Backup and Recovery of Key KPI Statistics* feature chapter in the associated product *Administration Guide*.

Example

Set the interval between backups to 30 minutes with the following command:

```
statistics-backup-interval 30
```

support collection

Modifies and/or enables the Support Data Collector (SDC) process. If record collection has been previously disabled, this command enables the collection activity. If the record collection is currently enabled, this command may be used to modify the sleep-duration interval and/or the maximum number of Support Data Records (SDRs) that can be collected and stored.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

support collection sleep-duration { hours | minutes }*value* **max-records** *number_records*
[default | no] support collection

default

Resets the sleep duration and maximum number of records to their default values.

no

Removes the settings for support collection and effectively disables the SDC.

support collection

Enables the SDC.

sleep-duration { hours | minutes }*value*

Specifies the hours and/or minutes between record collection activity. *value* must be an integer from 1 through 1000. The default setting is one hour (60 minutes).

Important The period between SDRs is equal to the configured sleep-duration interval + the time taken to collect the previous record.

max-records *number_records*

Specifies the maximum number of records to maintain within the record collection. *number_records* must be an integer from 1 through 1000. When this value is exceeded, a new SDR overwrites the oldest SDR. Default is 168.

Usage Guidelines

Use this command to control the amount of support information that is collected by the Support Data Collector. Increasing the sleep interval for data collection and reducing the number of records to be collected frees system resources for processing calls and storing other data records.

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

Example

The following command sets the collection sleep interval to *30* minutes with a maximum of *100* records being stored:

```
support collection sleep-duration minutes 30 max-records 100
```

support record

Specifies the **show** commands that will be collected and output by the Support Data Collector (SDC) process in the specified record section(s). The order in which the record section commands are specified defines the order in which the collected support data record sections are saved.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

support record section*section_name* **command "***command_string***" [section** *section_name* **command "***command_string***"] +**
no support record { all | section *section_name* **}**
default support record section { all | section *section_name* **}**

no support record { all | section *section_name*

Removes the specified record section or all sections from the output of the SDC. This effectively disables the support data collector mechanism.

default support record section { all | section *section_name* }

Resets all support record sections or the specified section to the default command listing.

section *section_name*

Identifies the record section as an alphanumeric string of 1 through 64 characters.

command "*command_string*"

Identifies a CLI **show** command to be included in the record section as an alphanumeric string of 1 through 256 characters enclosed in double quotation marks.

Important Refer to the *System Administration Guide* for a comprehensive list of command strings that can be entered via this keyword.

+ indicates that you can add command strings to the record section by repeating the **section** *section_name* **command "***command_string***"** keywords.

Usage Guidelines

Use this command to tune the output of the Support Data Collector to meet specific site requirements. Refer to the *System Administration Guide* for a complete description of the SDC feature

Important If the **support record section** command is not explicitly configured by the user, a default set of record section commands are used. These default record section commands are displayed when you run the **show configuration verbose** command. If support record section commands are explicitly configured, they replace the default commands.

Example

The following command creates a record section named *show_ip_ vrf* containing the CLI command **show ip vrf**:

```
support record section vrf command "show ip vrf"
```

suspend local-user

Suspends a local-user administrative account.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

`[ no ] suspend local-user` *`name`*

no

Removes the suspended status for the specified local-user account.

name

The name of the local-user account expressed as an alphanumeric string of 3 through 16 characters that is case sensitive.

Usage Guidelines

This command allows a security administrator to suspend local-user administrative accounts.

A "suspended" user cannot login to the system. The user's account information (passwords, password history, etc.), however, is preserved.

Example

The following command suspends a local-user account called *Inspector1*:

```
suspend local-user Inspector1
```

The following command removes the suspension from a local-user account called *Admin300*:

```
no suspend local-user Admin300
```

system

Configures system information which is accessible via SNMP.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

system { carrier-id mcc *mcc_id* **mnc** *mnc_id* **| contact** *who* **| description** *string* **| hostname** *host_name* **| location** *text* **| serial-number** *ser_number* **| sysdesc-sysoid-style [default | new] }**
default system { contact | location }

default

Removes the configured **system contact** and **system location** form the system.

carrier-id mcc *mcc_id* mnc *mnc_id*

Important This carrier ID is not used by the GGSN.

Specifies a carrier-id that is a unique identifier for the carrier that has installed the system. When the carrier ID values are set, the carrier-id and gmt_offset attributes are included in access-request and accounting packets when using the following RADIUS dictionaries:

- 3gpp2
- 3gpp2-835
- starent
- starent-835
- starent-vsa1
- starent-vsa1-835
- custom9

mcc *mcc_id*: The mobile country code. This must be specified as a 3-digit string from 001 through 999.

mnc *mnc_id*: The mobile network code. This must be specified as a 2- or 3-digit string from 01 through 999.

contact *who*

Specifies the contact information for the chassis. *who* must be an alphanumeric string of 0 through 255 characters. The string must be embedded in double quotes (") if spaces and special punctuation is to be used.

Default: No contact specified.

description *string*

Allows a user to describe the system for identification purposes. The system description can be comprised of a mix of alphanumeric characters, as follows:

- **%version%** - software version

- **%build%** - software build number
- **%chassis%** - chassis type
- **%staros%** - OS type
- **%hostname%** - system name
- **%release%** - release number
- **%kerver%** - kernel version
- **%machine%** - machine hardware name
- *string* - an alphanumeric string of 1 through 255 characters

hostname *host_name*

Configures the chassis host name where *host_name* must be an alphanumeric string of 1 through 63 characters.

Important Please note that changing the chassis host name results in the command prompt changing as well to reflect the new name. This may affect any previously scripted interfaces from an OSS or maintenance facility.

location *text*

Specifies the system location expressed as an alphanumeric string of 0 through 255 characters. The text specified must be embedded in double quotes (") if spaces are to be used.

Default: No location specified.

serial-number *ser_number*

Specifies a system identifier as an alphanumeric string of 1 through 11 characters.

Default: None.

sysdesc-sysoid-style [default | new]

Allows the user to select the SNMP return for the objects sysDescr and sysOId.

- **default** - SNMP returns old style system description and old style system OID string.
- **new** - SNMP returns Cisco style system description and Cisco style OID string.

Usage Guidelines

Specify system basic information which is useful back at a network operations center which uses the SNMP interfaces for management.

Example

The following commands configure the contact information, system host name, and location text, or remove configured location and system respectively.

```
system contact user1@company.com
system hostname system16
system location "Clark Street Closet\nBasement Rack 4"
```

The following commands remove the configured contact and location from system respectively

```
default system contact
default system location
```