# Global Configuration Mode Commands (A-K)

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

## Command Modes

This section includes the commands **aaa accounting-overload-protection** through **imei-profile**.

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).

# aaa accounting-overload-protection

This command configures Overload Protection Policy for accounting requests.

**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**

**`aaa accounting-overload-protection prioritize-gtpp`**
**`{ default | no } aaa accounting-overload-protection`**

**default**

Configures the default setting.

Default: no priority assigned

**no**

Disables the Overload Protection configuration.

**prioritize-gtpp**

Gives higher priority to GTPP requests among the other outstanding requests. So while purging the lower priority requests will be selected first.

**Usage Guidelines**

Use this command to configure Overload Protection Policy for accounting requests.

**Example**

The following command prioritizes GTPP requests among the other outstanding requests:

**`aaa accounting-overload-protection prioritize-gtpp`**

# aaa default-domain

Configure global accounting and authentication default domain for subscriber and context-level administrative user sessions.

**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**

**aaa default-domain { administrator | subscriber }** *domain_name*
**no aaa default-domain { administrator | subscriber }**

**no**

Removes all or only the specified configured domain.

**administrator | subscriber**

**administrator**: Configures the default domain for context-level administrative users.

**subscriber**: Configures the default domain for subscribers.

***domain_name***

Sets the default context.

*domain_name* must be an alphanumeric string of 1 through 79 characters.

**Usage Guidelines** This command configures the default domain which is used when accounting and authentication services are required for context-level administrative user and subscriber sessions whose user name does not include a domain.

**Example**

The following commands configure the default domains for context-level administrative users and subscribers, respectively:

```
aaa default-domain administrator sampleAdministratorDomain
aaa default-domain subscriber sampleSubscriberDomain
```

# aaa domain-matching ignore-case

This command disables case sensitivity when performing domain matching. When this command is enabled, the system disregard case when matching domains.

**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 ] aaa domain-matching ignore-case`**
**`default aaa domain-matching`**

**default**

Configures ignore-case as the domain matching method.

**no**

Specifies that the system consider case when domain matching.

**Usage Guidelines**

Use this command to configure the system to ignore case when matching domains.

**Example**

The following command configures the system to ignore case when matching domains:

**`aaa domain-matching ignore-case`**

# aaa domain-matching imsi-prefix

Enables domain lookup for session based on the International Mobile Subscriber Identity (IMSI) prefix length. Default: Disabled

**Important** This command is only available in 8.3 and later releases.

**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**

**`aaa domain-matching imsi-prefix prefix-length`** *`prefix_length`*
**`no aaa domain-matching imsi-prefix`**
**`default aaa domain-matching`**

**no**

Specifies the system must not consider imsi-prefix domain matching method.

***prefix-length***

Specifies the IMSI length to be matched with the domain.

*prefix_length* must be an integer from 1 through 15.

**Usage Guidelines**

Use this command to configure the IMSI-prefix method of domain matching. This command enables domain lookup for the session based on the IMSI prefix length. If there is a domain configured with the matching IMSI prefix, the associated configuration is used.

This feature does not support partial matches.

**Example**

The following command configures the IMSI prefix method for domain matching setting the prefix length to *10*.

```
aaa domain-matching imsi-prefix prefix-length 10
```

# aaa large-configuration

This command enables or disables the system to accept a large number of RADIUS configurations to be defined and stored.

When aaa large-configuration is disabled, the following restrictions are in place:

- Only one (1) NAS IP address can be defined per context with the **radius attribute** command.
- The RADIUS attribute **nas-ip-address** can only be configured if the RADIUS group is **default**.
- Only 320 RADIUS servers can be configured system-wide.
- Only 64 RADIUS groups can be configured system-wide.

**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 ] aaa large-configuration
```

**no**

Disables AAA large configuration support.

**Usage Guidelines**

When aaa large-configuration is enabled, the system provides the ability to configure multiple NAS IP addresses in a single context to used with different radius groups. As well, the command allows support for up to 1,600

RADIUS server configurations and for a PDSN a maximum of 400 or for a GGSN a maximum of 800 RADIUS server group configurations system-wide.

**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

To enable the definition of a large number of RADIUS configurations, enter the following commands in the following order:

In APN Configuration mode, enter:

```
default aaa group
```

In Global Configuration mode, enter:

```
aaa large-configuration
```

In Exec mode, use the **save configuration** command and then the **reload** command.

# aaa last-resort

Configure global accounting and authentication last resort domain for subscriber and context-level administrative user sessions.

**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**

```
aaa last-resort context { administrator | subscriber context_name }
no aaa last-resort context { administrator | subscriber }
```

**no**

Removes all or only the specified previously configured authentication last resort domain name.

**administrator | subscriber**

**administrator**: Configures the last resort domain for context-level administrative.

**subscriber**: Configures the last resort domain for the subscribers.

***context_name***

Specifies the context which is to be set as the last resort. *context_name* must be an alphanumeric string of 1 to 79 characters.

**Usage Guidelines**

Set the last resort context which is used when there is no applicable default domain (context) and there is no domain provided with the subscriber's or context-level administrative user's name for use in the AAA functions.

**Example**

The following commands configure the last resort domains for context-level administrative user and subscribers, respectively:

```
aaa last-resort administrator sampleAdministratorDomain
aaa last-resort subscriber sampleSubscriberDomain
```

The following command removes the previously configured domain called *sampleAdministratorDomain*:

```
no aaa last-resort administrator sampleAdministratorDomain
```

# aaa tacacs+

Enables or disables system-wide TACACS+ AAA (authentication, authorization and accounting) services for administrative users. This command is valid only if TACACS+ servers and related services have been configured in TACACS 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**

```
[ no ] aaa tacacs+ [ noconsole ]
```

**no**

Disables TACACS+ AAA authentication.

**noconsole**

Disables TACACS+ authentication on the Console line only. By default this option is disabled; TACACS+ server authentication is performed for login via SSH or telnet (vty line) and a connection to the Console port.

With **noconsole** enabled, TACACS+ authentication is bypassed; the authentication request goes directly to the local database. Effectively TACACS+ authentication on the Console port is disabled. However, TACACS+ authentication remains enabled via vty lines.

**Important** When **aaa tacacs+ noconsole** is configured, a local user with valid credentials can log into a Console port even if **on-authen-fail stop** and **on-unknown-user stop** are enabled via the TACACS+ Configuration mode. If the user is not a TACACS+ user, he/she cannot login on a vty line.

**Usage Guidelines** Enables or disables the use of TACACS+ AAA services for administrative users.

**Example**

```
aaa tacacs+
no aaa tacacs+
```

# aaa username-format

Configure global accounting and authentication user name formats for AAA (authentication, authorization and accounting) functions. Up to six formats may be configured.

**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 ] aaa username-format { domain | username } separator
default aaa username-format
```

**no**

Removes the specified user name format from the configuration.

**domain | username**

Default: username @

**domain**: indicates the left side of the string from the separator character is a domain name and the right side is the user name.

**username**: indicates the left side of the string from the separator character is a user name and the right side is the domain name.



**Important** The user name string is always searched from right to left for the first occurrence of the separator character.

***separator***

Specifies the character to use to delimit the domain from the user name for global AAA functions.Permitted characters include: @, %, -, \, #, or /. To specify a back slash ('\') as the separator, you must enter a double back slash ('\\') on the command line.

**Usage Guidelines** Define the formats for user name delimiting if certain domains or groups of users are to be authenticated based upon their user name versus domain name.

**Example**

```
aaa username-format domain @
aaa username-format username %
no aaa username-format username %
```

# access-policy

This command allows you to create/configure/delete the access-policy.

**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**

```
access-policy policy_name [ -noconfirm ]
no access-policy policy_name
```

**no**

Deletes the configured access-policy.

**access-policy *policy_name***

Specifies the name of the access-policy.

*policy_name* must be an alphanumeric string of 1 through 64 characters.

If the named access-policy does not exist, it is created, and the CLI mode changes to the Access Policy Configuration Mode. If the named access-policy already exists, the CLI mode changes to the Access Policy Configuration Mode.

**-noconfirm**

Specifies that the command must execute without any additional prompt and confirmation from the user.

**Usage Guidelines** Use this command to create/configure/delete an access-policy in the system.

A maximum of four access-policies can be configured. One access-policy can contain upto 16 entries of precedence pointing to 16 different access-profiles.

On entering this command, the CLI prompt changes to:

[*context_name*]*host_name*(access-policy-*policy_name*)#

### Example

The following command creates an access-policy named *ap1*:

**access-policy ap1**

# access-profile

This command allows you to create/configure/delete the access-profile.

**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**

**access-profile** *profile_name* **[ -noconfirm ]**
**no access-profile** *profile_name*

#### no

Deletes the configured access-profile.

#### access-profile *profile_name*

Specifies the name of the access-profile.

*profile_name* must be an alphanumeric string of 1 through 64 characters.

If the named access-profile does not exist, it is created, and the CLI mode changes to the Access Profile Configuration Mode. If the named access-profile already exists, the CLI mode changes to the Access Profile Configuration Mode.

#### -noconfirm

Specifies that the command must execute without any additional prompt and confirmation from the user.

**Usage Guidelines**

Use this command to create/configure/delete an access-profile in the system.

A maximum number of 16 access-profiles can be configured in the system.

To use the access-profiles, the access-policies must be created under the Global Configuration mode and associated under mme-service or call-control-profile.

One access-policy can contain upto 16 entries of precedence along with access-profile, device type, and RAT type. When the precedence is lower, the priority is higher.

On entering this command, the CLI prompt changes to:

[*context_name*]*host_name*(access-profile-*profile_name*)#

### Example

The following command creates an access-profile named *apr3*:

**access-profile apr3**

# active-charging service

This command allows you to create/configure/delete the Active Charging Service (ACS)/Enhanced Charging Service (ECS).

**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**

**active-charging service** *acs_service_name* **[ -noconfirm ]**
**no active-charging service** *acs_service_name*

#### no

Deletes the specified Active Charging Service.

#### *acs_service_name*

Specifies name of the Active Charging Service.

*acs_service_name* must be the name of an Active Charging Service, and must be an alphanumeric string of 1 through 15 characters.

If the named Active Charging Service does not exist, it is created, and the CLI mode changes to the ACS Configuration Mode wherein the service can be configured. If the named Active Charging Service already exists, the CLI mode changes to the ACS Configuration Mode.

#### -noconfirm

Specifies that the command must execute without any additional prompt and confirmation from the user.

**Usage Guidelines**

Use this command to create/configure/delete an Active Charging Service in the system. Note that, in this release, only one Active Charging Service can be created in the system.

Use this command after enabling ACS using the **require active-charging** command. This command allows administrative users to configure the ACS functionality.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-acs)#

**Example**

The following command creates an ACS service named *test*:

```
active-charging service test
```

# alarm

Enables or disables alarming options for the SSC internal alarm and the central-office external alarms. To verify the state of the alarms, refer to the **show alarm** command.

**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 ] alarm { audible | central-office }
```

**no**

Disables the option specified.

**audible**

Enables the internal audible alarm on ASR 5500 SSCs.

**central-office**

Enables the central office (external relay) alarms.

**Usage Guidelines**

Use this command to enable or disable audible and external relay alarms on ASR 5500 SSCs.

**Example**

The following command enables the internal audible alarm:

```
alarm audible
```

# apn-profile

Creates an instance of an Access Point Name (APN) profile.

**Product**

MME

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 ] apn-profile`** *`apn_profile_name`*

**no**

Deletes the APN profile instance from the configuration.

***apn_profile_name***

Specifies the name of the APN profile. Enter an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Use this command to create an instance of an APN profile and to enter the APN profile configuration mode. An APN profile is a template which groups a set of APN-specific commands that may be applicable to one or more APNs. See the *APN Profile Configuration Mode Commands* chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

**Important**

An APN profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what APN profiles have already been created, return to the Exec mode and enter the **show apn-profile all** command.

**Example**

The following command creates a configuration instance of an APN profile:

```
apn-profile apnprof27
```

# apn-remap-table

Creates an instance of an Access Point Name (APN) remap table.

**Product**

MME

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 ] apn-remap-table** *apn_remap_table_name*

**no**

Deletes the APN remap table instance from the configuration.

***apn_remap_table_name***

Specifies the name of the APN remap table. Enter an alphanumeric string of 1 through 65 characters.

**Usage Guidelines**

Use this command to create an instance of an APN remap table and to enter the APN remap table configuration mode. An APN remap table includes entries that define how an incoming APN, or the lack on one, will be handled. See the *APN Remap Table Configuration Mode Commands* chapter for information regarding the definition of the entries contained within the table and the use of the table.

**Important** An APN remap table is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what APN remap tables have already been created, return to the Exec mode and enter the **show apn-remap-table all** command.

**Example**

The following command creates a configuration instance of an APN remap table:

```
apn-remap-table pnremap-USorigins-table1
```

# arp

Configures a system-wide time interval for performing Address Resolution Protocol (ARP) refresh.

**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**

**arp base-reachable-time** *time*
**default arp base-reachable-time**

**default**

Restores the parameter to its default setting.

***time***

Default: 30

Specifies the ARP refresh interval (in seconds) as an integer from 30 through 86400.

**Usage Guidelines**

Use this command to configure a system-wide ARP refresh interval. Once a neighbor is found, the entry is considered valid for at least a random value between the *time*/2 and the *time**1.5.

**Example**

The following command configures an ARP refresh interval of 1 hour:

```
arp base-reachable-time 3600
```

# autoconfirm

This command disables or enables confirmation for certain commands. This command affects all future CLI sessions and users.

**Important** To change the behavior for the current CLI session only, use the **autoconfirm** command in the Exec Mode.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] autoconfirm**

**no**

Disables the autoconfirm feature.

**Usage Guidelines**

When autoconfirm is enabled, certain commands ask you to answer yes or no to confirm that you want to execute the command. When autoconfirm is disabled the confirmation prompts never appear. Disabling autoconfirm disables command confirmation for all future CLI sessions.

By default **autoconfirm** is enabled.

**Important** If autoconfirm is enabled, commandguard will not take effect until autoconfirm is disabled in both Exec and Global Configuration modes.

**Example**

The following command enables command confirmation for all future CLI sessions and users:

```
autoconfirm
```

# autoless

This command is obsolete. It is included in the CLI for backward compatibility with older configuration files. When executed, this command issues a warning and performs no function.

# banner

Configures the CLI banner which is displayed upon the start of a CLI session.

**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**

```
banner { charging-service | lawful-intercept | motd | pre-login } string
no banner { charging-service | lawful-intercept | motd | pre-login }
```

**no**

Removes the banner message by setting it to be a string of zero length.

**charging-service**

Specifies the Active Charging Service banner message. The banner is displayed upon initialization of an SSH CLI session with ACS-admin privileges (whenever anyone with the CLI privilege bit for ACS logs on).

**lawful-intercept**

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

**motd**

Configures the CLI banner message of the day which is displayed upon the initialization of any CLI session.

**pre-login**

Configures the CLI banner displayed before a CLI user logs in.

**Important** This banner is displayed only for serial port and telnet log ins. It is not supported in ssh and, therefore, will not be displayed before ssh log ins.

***string***

Specifies the banner or message to be displayed at session initialization. *string* may be an alphanumeric string of 0 through 2048 characters. The string must be enclosed in double quotation marks if the banner or message is to include spaces.

**Usage Guidelines** Set the message of the day banner when an important system wide message is needed. For example, in preparation for removing a chassis from service, set the banner 1 or more days in advance to notify administrative users of the pending maintenance.

**Example**

The following command creates a message of the day with the text *Have a nice day.*

```
banner motd "Have a nice day."
```

# bearer-control-profile

This command creates an instance of a Bearer Control profile, a key element of the MME QoS Profile feature.

**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 ] bearer-control-profile** *bcprofile_name*

**no**

Including this command prefix causes the MME to delete the named instance of the bearer control profile from the MME's configuration.

***bcprofile_name***

Enter an alphanumeric string of 1 through 64 characters to identify a specific bearer control profile.

**Usage Guidelines**

Entering this command provides access to the configuration commands of the Bearer Control Profile Configuration Mode to configure QoS parameters for dedicated-bearers and for default-bearers. Bearer level parameters such as ARP-PL, ARP-PVI, ARP-PCI, MBR, GBR, remap QCI value can be configured here independently for default/dedicated bearer along with the action to be taken, such as prefer-as-cap or pgw-upgrade. Bearer Control profile can be applied for specific QCIs or range of QCIs.

**Example**

The following sample command creates an instance of a bearer control profile named *BCProf*:

**bearer-control-profile BCProf**

# boot delay

Configures the delay period, in seconds, before attempting to boot the system from a software image file residing on an external network server.

**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**

**boot delay** *time*
**no boot delay**

**no**

Deletes the setting for the boot delay. The boot process executes immediately.

**time**

Specifies the amount of time (in seconds) to delay prior to requesting the software image from the external network server as an integer from 1 through 300.

**Usage Guidelines**

Useful when booting from the network when connection delays may cause timeouts. Such as when the Spanning Tree Protocol is used on network equipment.

**Important**

The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Example**

The following sets the boot delay to *10* seconds:

```
boot delay 10
```

# boot interface

Configures Ethernet network interfaces for obtaining a system software image during the system boot process.

**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**

**boot interface { local-eth1 | local-eth2 } [ medium { auto | speed** *medium_speed* **duplex** *medium_duplex* **} [ media** *medium_media* **] ]**
**no boot interface**

**no**

Removes the boot interface configuration from the boot.sys file. Only files from the local file system can be loaded.

**local-eth1 | local-eth2**

Specifies the network interface to be configured where **local-eth1** is the primary ethernet interface and **local-eth2** is the secondary ethernet interface.

For the ASR 5500, the primary interface is port 1 (1000Base-T) on the MIO and the secondary interface is port 2 (1000Base-T) on the MIO.

**medium { auto | speed *medium_speed* duplex *medium_duplex* }**

Default: auto

**auto**: Configures the interface to auto-negotiate the interface speed. and duplex.

**speed** *medium_speed* **duplex** *medium_duplex*: Specifies the speed to use at all times where *medium_speed* must be one of:

- 10
- 100
- 1000

The keyword **duplex** is used to set the communication mode of the interface where *medium_duplex* must be one of:

- full
- half

**media *medium_media***

Default: rj45

Optionally sets the physical interface where *medium_media* must be either **rj45** or **sfp**.

**Usage Guidelines**

Modify the boot interface settings to ensure that the system is able to obtain a software image from an external network server.

**Important** The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Example**

The following command configures the primary interface to auto-negotiate the speed:

```
boot interface local-eth1 medium auto
```

The following command configures the secondary interface to a fixed gigabit speed at full duplex using RJ45 connectors for the physical interface:

```
boot interface local-eth2 medium speed 1000 duplex full media rj45
```

The following command restores the defaults for the boot interface:

```
no boot interface
```

# boot nameserver

Configures the IP address of the DNS (Domain Name Service) server to use when looking up hostnames in URLs for network booting.

**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**

**boot nameserver** *ip_address*
**no boot nameserver**

**no**

Removes the network boot nameserver information from the boot.sys file.

***ip_address***

IPv4 dotted-decimal address of the DNS server the system uses to lookup hostnames in URLs for a software image from the network during the system boot process.

**Usage Guidelines** Use this command to identify the DNS server to use to lookup hostnames in a software image URL.

**Important** The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Example**

The following configures the system to communicate with a DNS nameserver with the IP address of 10.2.3.4:

```
boot nameserver 10.2.3.4
```

# boot networkconfig

Configures the networking parameters for the Switch Processor I/O card network interfaces to use when obtaining a software image from an external network server during the system boot process.

**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

```
boot networkconfig { dhcp | { { dhcp-static-fallback | static } ip address
 spio24 ip_address [ spio25 ip_address ] netmask ip_mask [ gateway gw_address ]
 } }
no boot networkconfig
```

### no

Removes the network configuration information from the boot.sys file.

### dhcp

Indicates that a Dynamic Host Control Protocol (DHCP) server is used for communicating with the external network server.

### dhcp-static-fallback | static

**dhcp-static-fallback**: provides static IP address fallback network option when a DHCP server is unavailable.

**static**: specifies a fixed network IP address for the external network server that hosts the software image.

### spio24 *ip_address* [ spio25 *ip_address* ] netmask *ip_mask* [ gateway *gw_address* ]

**spio24** *ip_address* [ **spio25** *ip_address* ]: the IP address to use for the SPIO in slot 24 and optionally the SPIO in slot 25 for network booting. *ip_address* must be specified using IPv4 dotted-decimal notation.

**netmask** *ip_mask*: the network mask to use in conjunction with the IP address(es) specified for network booting. *ip_mask* must be specified using IPv4 dotted-decimal notation.

**gateway** *gw_address*: the IP address of a network gateway to use in conjunction with the IP address(es) specified for network booting. *gw_address* must be entered using IPv4 dotted-decimal notation.

**Important** If *gw_address* is not specified, the network server must be on the same LAN as the system. Since both SPIOs must be in the same network, the netmask and gateway settings are shared.

## Usage Guidelines

Configure the network parameters for the ports on the SPIO cards to use to communicate with an external network server that hosts software images.

**Important** The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Important** When configuring static addresses both SPIOs must have different IP addresses. Neither address can be the same as the local context IP address.

### Example

The following configures the system to communicate with the external network server via DHCP with a fallback to IP address *192.168.100.10*, respectively.

```
boot networkconfig dhcp-static-fallback ip address spio24 192.168.100.10
 netmask 255.255.255.0
```

The following command configures the system to communicate with an external network server using the fixed (static) IP address *192.168.100.10* with a network mask of *255.255.255.0*.

```
boot networkconfig static ip address spio24 192.168.100.10 netmask
255.255.255.0
```

The following restores the system default for the network boot configuration options.

```
no boot networkconfig
```

# boot system priority

Specifies the priority of a boot stack entry to use when the system first initializes or restarts. Up to 10 boot system priorities (entries in the boot.sys file located in the /flash device in the SPC, SMC or MIO) can be configured.

**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**

**boot system priority** *number* **image** *image_url* **config** *config_path*
**no boot system priority** *number*

**no**

Remove a boot stack entry at the priority specified from the boot stack when it is no longer used.

**priority *number***

Specifies the priority for the file group (consisting of an image (.bin) and its corresponding configuration (.cfg) file) specified in the boot stack. The value must be in the range from 1 through 100 where a priority of 1 is the highest. Up to 10 boot system priorities (boot stack entries) can be configured.

**Important**

When performing a software upgrade it is important that the new file group have the highest priority (lowest number) configured.

**Important** To ensure that higher priority numbers remain open, use an "N-1" priority numbering methodology, where "N" is the first priority in the current boot stack.

**image *image_url***

Specifies the location of a image file to use for system startup. The URL may refer to a local or a remote file. The URL must be formatted according to the following format:

For the ASR 5000:

- **[ file: ]{ /flash | /pcmcia1 | /hd }[** */directory* **]**/*filename*
- **[ http: | tftp: ]**//*host***[ :***port* **][** */directory* **]**/*filename*

**Important** Use of the SMC hard drive is not supported in this release.

For the ASR 5500:

- **[ file: ]{ /flash | /usb1 | /hd }[** */directory* **]**/*filename*
- **[ http: | tftp: ]**//*host***[ :***port* **][**/*directory* **]**/*filename*

**Important** Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

*directory* is the directory name.

*filename* is the actual file of interest.

*host* is the IP address or host name of the server.

*port#* is the logical port number that the communication protocol is to use.

**Important** A file intended for use on an ASR 5000 uses the convention xxxxx.asr5000.bin, where xxxxx is the software build number.

**Important** A file intended for use on an ASR 5500 uses the convention xxxxx.asr5500.bin, where xxxxx is the software build number.

**Important** When using the TFTP, it is advisable to use a server that supports large blocks, per RFC 2348. This can be implemented by using the "block size option" to ensure that the TFTP service does not restrict the file size of the transfer to 32MB.

**config *config_path***

Specifies the location of a configuration file to use for system startup. This must be formatted according to the following format:

For the ASR 5000:

- **[ file: ]{ /flash | /pcmcia1 | /hd }[** */path* **]***/filename*

**Important** Use of the SMC hard drive is not supported in this release.

For the ASR 5500:

- **[ file: ]{ /flash | /usb1 | /hd }[** */path* **]***/filename*

Where *path* is the directory structure to the file of interest, and *filename* is the name of the configuration file. This file typically has a **.cfg** extension.

## Usage Guidelines

This command is useful in prioritizing boot stack entries in the boot.sys file, typically located on the /flash device of the Active SPC, SMC, or MIO, for automatic recovery in case of a failure of a primary boot file group.

**Important** The configuration file must reside on the SPC's, SMC's, or MIO's local filesystem, stored on one of its local devices (/flash, or /pcmcia1, or /hd-raid/pcmcia1, or /pcmcia2, or /usb1, or /hd-raid). Attempts to load the configuration file from an external network server will result in a failure to load that image and configuration file group, causing the system to load the image and configuration file group with the next highest priority in the boot stack.

**Important** Configuration changes do not take effect until the system is reloaded.

**Important** The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

### Example

The following commands set up two locations from which to obtain a boot file group.

```
boot system priority 1 image tftp: //remoteABC/pub/2012jan.bin config
/flash/pub/data/2012feb.cfg
boot system priority 2 image /flash /pub/data/2002jun.bin config
/pcmcia1/pub/data/2012feb.cfg
```

The following removes the current priority **1** boot entry from the boot.sys file.

```
no boot system priority 1
```

# bulkstats

Enables the collection of bulk statistics and/or enters the bulk statistics 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**

```
bulkstats { collection | config [ schema | supplement ] | historical
collection | mode | ssd-samples { 1 | 2 } }
no bulkstats { collection | historical | ssd-samples }
default bulkstats { historical collection | ssd-samples }
```

**no**

Disables the collection of bulk statistics.

**default**

Restores the bulkstats configuration to its default value.

**ssd-samples**: Disabled

**collection**

Enables the statistics collection process. Collects a periodic snapshot of activity and performance data as configured via the Bulk Statistics Configuration mode.

**config [ schema | supplement ] *url***

Enables bulkstats configuration replacement with contents of file if present. If no file is present, bulkstats mode configuration will be saved in the file of the given name when issuing a **save configuration** *url* command.

**schema**: This keyword takes a local URL keyword as a parameter. It will perform a full bulkstats schema configuration replacement with the contents of the file provided. If the file exists, no schema will be saved when issuing a **save configuration** *url* command.

**supplemental**: This keyword takes a local URL keyword as a parameter. It will supplement running bulkstats configuration with the contents of the configuration file provided.

*url*: Specifices the URL where the **[file:]{/flash | /hd-raid | /usb1 | /usb2 | /usb3 | /rmm1 | /cdrom1 | /sftp}[/directory]**/*filename*

The system will allow configuration of only 1 of these options. They are mutually exclusive.

### historical collection

Enables the collection of historical bulk statistics.

If enabled, StarOS tracks activities that require the storing of more data, such as "the highest value that's been seen over the last 24 hours".

### mode

Enters the Bulk Statistics Configuration mode. The resulting command-line prompt will look similar to:

```
[<context-name>]host_name(config-bulkstats)#
```

### ssd-samples { 1 | 2 }

Enables the collection of bulk statistics samples in the SSD archive. In the current release, a maximum of two bulkstats samples can be collected in the SSD archive. Each sample contains all the bulkstats collected during the configured transfer interval.

Also see the **show support details** command under the *Exec Mode Commands* for more information on excluding the bulkstats samples from the SSD archive.

**Usage Guidelines**

The Bulk Statistics Configuration mode consists of commands for configuring bulk statistic properties, such as the periodicity of collection. Detailed command descriptions appear in the *Bulk Statistics Configuration Mode Commands* chapter.

The collected bulk statistics are sent to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group or schema, for example, system statistics, port statistics, RADIUS statistics.

Once the receiver, schema, and collection properties are configured, the **bulkstats collection** command enables or disables the collection of the data.

To collect a sample that will provide an average, for example, an average of CPU counters, the "historical" features must be enabled with the **bulkstats historical collection** command.

Since bulk statistics are collected at regular, user-defined intervals, the Exec mode **bulkstats force** command can be used to manually initiate the immediate collection of statistics.

### Example

The following command enables the collection of bulk statistics:

```
bulkstats collection
```

The following command performs a full bulkstats schema configuration replacement with the contents of the file provided:

```
bulkstats config schema /tmp/bsutscm2.cfg
```

# ca-certificate-list

**Product**

ePDG

**Privilege**

Administrator, Security Administrator, Operator

**Command Modes** Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description** **ca-certificate-list** *ca_certificate_list_name* [**ca-cert-name** *ca-cert-name_1* ] [ **ca-cert-name** *ca-cert-name_2* ] [**ca-cert-name** *ca-cert-name_3* ] [**ca-cert-name** *ca-cert-name_4* ]

**no ca-certificate-list name** *ca_certificate_list_name*

**name *ca_certificate_list_name***

Specifies the CA certificate list as an alphanumeric string of 1 through 128 characters.

**ca-cert-name *ca-cert-name_1* to *ca-cert-name_4***

Specifies the the CA certificate name as an string of size 1 through 128.

Configuring atleat one ca-cert-name is mandatory.

**Usage Guidelines** Use this command to configure CA certificate list name 10 and four certificates ca-cert-name_1, ca-cert-name_2, ca-cert-name_3, ca-cert-name_4:

**ca-certificate-list name** *10* **ca-cert-name** *ca-cert-name_1* **ca-cert-name** *ca-cert-name_2* **ca-cert-name** *ca-cert-name_3* **ca-cert-name** *ca-cert-name_4*

# ca-certificate

Configures and selects an X.509 CA certificate to enable a security gateway to perform certificate-based peer (client) authentication. StarOS supports a maximum of 16 certificates and 16 CA (Certificate Authrority) root certificates. A maximum of four CA root certificates can be bound to a crypto or SSL (Secure Sockets Layer) template.

**Product** All IPSec-related products

**Privilege** Administrator, Security Administrator, Operator

**Command Modes** Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description** **ca-certificate name** *name* **{ der url** *url_format* **| pem { data** *pemdata* **| url** *url_format* **[ cert-enc ] [ cert-hash-url url** *url_format* **] } }**
**no ca-certificate name** *name*

**no**

Disables ca-certificate.

**Note** If the CA-CERT is mandatory for the service to be up and running, then the removal of that CA-CERT is not allowed.

**name *name***

Specifies the name the CA certificate as an alphanumeric string of 1 through 128 characters.

**der url**

Specifies the use of the Distinguished Encoding Rules (DER) binary format.

**url** is the Universal Reosurce Locator of the file containing certificate in der format.

**pem**

Specifies that the Privacy-enhanced Electronic Mail (PEM) format is to be used.

**data *pemdata***

ndicates that the CA certificate data will be in PEM format. *pemdata* must be an alphanumeric string of 1 through 4095 characters.

**cert-enc**

Specifiesa certificate encoding type other than default encoding type.

**cert-hash-url**

Specifies a hash of X.509 Certificate.

**url**

Specifes the Universal Resource Locator of the file containing the CA certificate.

***url_format***

Specifies an existing URL expressed in one of the following formats:

- [file:]{/flash | /pcmcia1 | /hd-raid}[/directory]/<filename
- tftp://<host>[:<port>][/<directory>]/<filename
- ftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename
- sftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename
- http://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename

When read via a file, note that **show configuration** will not contain the URL reference, but will instead output the data via **data pemdata**, such that the configuration file is self-contained.

## Usage Guidelines

Use this command to configure and select an X.509 CA certificate to enable a security gateway or SCM to perform certificate-based peer (client) authentication.

### Example

Use the following command to remove a certificate named *fap1*:

```
no ca-certificate fap1
```

# ca-crl

Configures the name and URL path of a Certificate Authority-Certificate Revocation List (CA-CRL).

**Product**

All IPSec-related products

**Privilege**

Operator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**ca-crl name** *name* **{ der | pem } { url** *url* **}**
**no ca-crl name** *name*

**no**

Removes the named CA-CRL.

***name***

Provides a name of the CA-CRL. *name* must be an alphanumeric string of 1 through 128 characters.

**der**

Specifies that Distinguished Encoding Rules (DER) format is to be used for the source format.

**pem**

Specifies that Privacy-enhanced Electronic Mail (PEM) format is to be used for the source format.

**url *url***

Specifies the URL where the CA-CRL is to be fetched. *url* must be an existing URL expressed as an alphanumeric string of 1 through 1023 characters in one of the following formats:

- [file:]{/flash | /pcmcia1 | /hd-raid}[/directory]/<filename
- tftp://<host>[:<port>][/<directory>]/<filename
- ftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename
- sftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename

- http://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename
- ldap://<host>[:<port>][/<dn>][?<attributes>][?<scope>][?<filter>][?<extensions>]

**Usage Guidelines**

Use this command to name and fetch a CA-CRL from a specified location.

Without additional information from the CA, an issued certificate remains valid to any verifier until it expires. To revoke certificates, the CA publishes a CRL periodically to provide an updated list of certificates revoked, but not yet expired. Like a certificate, a CRL is a digital document signed by the CA. In addition to a list of serial numbers of revoked certificates, the CRL includes attributes such as issuer name (same as the issuer name in the certificate), signature (signed by the issuer using the same key that signs certificates), last update (the time this CRL was issued), and next update (the time next CRL will be available).

### Example

The following command fetches a CA-CRL named *list1.pem* from a *host.com/CRLs* location and names the list *CRL5*:

```
ca-crl name CRL5 pem url http://host.com/CRLs/list1.pem
```

# call-control-profile

Creates an instance of a call-control profile.

**Product**

MME

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 ] call-control-profile`** *`cc_profile_name`*

**no**

Deletes the Call-Control Profile instance from the configuration.

***cc_profile_name***

Specifies the name of the call-control profile. Enter an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Use this command to create an instance of a call-control profile and to enter the call-control profile configuration mode. A call-control profile is a template which groups a set of call-handling instructions that may be applicable to one or more incoming calls. See the *Call-Control Profile Configuration Mode Commands* chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

**Important** A call-control profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what call-control profiles have already been created, return to the Exec mode and enter the **show call-control-profile all** command.

### Example

The following command creates a configuration instance of an call-control profile:

```
call-control-profile ccprof1
```

# card

Enters the Card Configuration mode for the specified card.

**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**

```
card slot_number
```

***slot_number***

Specifies the slot number of the card for which the card configuration mode is to be entered. *slot_number* must be an integer from 1 to 20.

**Usage Guidelines** Enter the configuration mode for a specific card when changes are required.

**Important** This command is not supported on virtual platforms.

### Example

The following command enters Card Configuration mode for the card in slot *8* of the chassis:

```
card 8
```

# card-standby-priority

Configures the redundancy priorities for packet processing cards by specifying the slot number search order for a standby card when needed.

**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**

**`card-standby-priority`** *`slot_num`* **`+`**

***slot_num***

Specifies the slot of the card for the order of the standby cards. *slot_num* must be in the range from 1 through 10 excluding slots 5 and 6 (on the ASR 5500).

**+**

Indicates that you may enter as many slot numbers (separated by a space) as necessary to indicate the complete search order.

**Usage Guidelines**

Set the standby order of the redundant cards when multiple standby cards are available.

Questionable hardware should be placed lower in the priority list.

**Important** This command replaces the **pac-standby-priority** command.

**Important** This command is not supported on all platforms.

### Example

The following command configures the redundancy priority to use the standby cards in slots 2, 4, and 7 in that order:

```
card-standby-priority 2 4 7
```

# cdr-multi-mode

This command enables multiple instances of CDRMOD, one per packet processing card.

**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**

```
[ default ] cdr-multi-mode
```

**default**

Configures this command with its default setting.

Default: Single-CDRMOD mode

**Usage Guidelines**

Use this command to enable the multi-CDRMOD mode, wherein there will be one instance of CDRMOD per packet processing card. All the SessMgr instances that are running on a packet processing card will send the records to the CDRMOD instance running on that card.

By default, CDRMOD runs in single mode, wherein there will be only one instance of CDRMOD running for the entire chassis. All the SessMgr instances that are running on a packet processing card will send the records to the CDRMOD instance.

**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** In multi-CDRMOD mode, you should enable hard-disk usage.

# certificate

Configures and selects an X.509 Trusted Author certificate.

**Product**

All IPSec-related products

**Privilege**

Administrator, Security Administrator, Operator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

## Syntax Description

```
certificate name name { der url url  | pem { data pemdata | url url }
private-key pem { [ encrypted ] data pemdata | url url [cert-enc]
[cert-hash-url url  url ] } }
no certificate name name
```

**no**

Disables certificate.

**name *name***

Names the certificate. *name* must be from 1 to 128 alphanumeric characters.

**der url**

Specifies that the Distinguished Encoding Rules (DER) binary format is to be used.

**pem**

Specifies that the Privacy-enhanced Electronic Mail (PEM) format is to be used.

**data *pemdata***

Certificate/private key data in PEM format. *pemdata* must be an alphanumeric string of 1 through 4095 (if private key is not implmented) or 1 through 8191 (if private key is implemented) characters.

**cert-enc**

Specifies a certificate encoding type other than default encoding type.

**cert-hash-url**

Specifes a hash and URL of the X.509 Certificate.

**url *url***

Specifies the Universal Resource Locator (URL) of the file containing certificate/private key.

***url_format***

Sepcifies an existing URL expressed in one of the following formats:

- [file:]{/flash | /pcmcia1 | /hd-raid}[/directory]/<filename
- tftp://<host>[:<port>][/<directory>]/<filename
- ftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename
- sftp://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename
- http://[<username>[:<password>]@]<host>[:<port>][/<directory>]/<filename

When read via a file, **show configuration** will not contain the URL reference, but instead outputs the data via **data** *pemdata*, such that the configuration file is self-contained.

**private-key pem**

Specifies use of private key PEM data.

**encrypted**

Specifs the use of encrypted private key data.

**Usage Guidelines** Use this command to Configures and selects an X.509 Trusted Author certificate.

**Example**

Use the following command to remove a certificate named *box1*:

```
no certificate data box1
```

# cli

Configures global Command Line Interface (CLI) parameters.

**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**

```
cli { access { monitor-protocol | monitor-subscriber | show-configuration
 } { administrator | operator } } | configuration-monitor | hidden |
login-failure-delay number | max-sessions number | operator
clear-subscriber-one-only | test-commands [encrypted] password password |
trap config-mode }
no cli { configuration-monitor | hidden | login-failure-delay number |
max-sessions | operator clear-subscriber-one-only | trap config-mode }
default cli { access { monitor-protocol | monitor-subscriber |
show-configuration } | configuration-monitor | login-failure-delay |
max-sessions | operator clear-subscriber-one-only | trap config-mode }
```

**no**

Removes the specified option.

**default**

Resets the keywords to their default values.

**access { monitor-protocol | monitor-subscriber | show-configuration }{ operator | administrator }**

Sets access privileges on the **monitor protocol** and **monitor subscriber** commands:

**monitor-protocol**: Selects privileges for the **monitor protocol** command.

**monitor-subscriber**: Selects privileges for the **monitor subscriber** command.

**show-configuration**: Selects privileges for the **show-configuration**command. However the default access level for this command is the user with operator privileges.

**operator**: Sets the privileges for the selected command to allow use by users with operator privileges.

**administrator**: Restricts use of the selected command to administrators only.

**configuration-monitor**

When this keyword is enabled, the system executes a **show configuration checksum** command every 15-minutes. The resulting checksum is compared with the previous checksum.

When a configuration change is detected, a log message and SNMP notification are generated. The SNMP notification only indicates that a change has occurred without identifying what change had been made.

The 15-minute interval is fixed and cannot be configured. By default configuration monitoring is disabled.

**Note** When enabled, the system's Shared Configuration Task (SCT) process may experience CPU spikes when the underlying **show configuration checksum** command is executed. This is most noticable with large StarOS configurations.

**hidden**

Allows a Security Administrator to enable access to hidden cli test-commands command.

The **no cli hidden** command disables access to the **cli test-commands** command. This is the default mode. Refer to the description of the **test-commands** keyword below for additional information.

**login-failure-delay *number***

Specifies the time to wait before a login failure is returned and another login may be attempted. Default is five seconds.

**max-sessions *number***

Sets the number of allowed simultaneous CLI sessions on the system. If this value is set to a number below the current number of open CLI sessions, the open sessions will continue until closed. *number* must be an integer from 2 through 100.

**Caution** Use caution when setting this command. Limiting simultaneous CLI sessions prevents authorized users from accessing the system if the maximum number allowed has been reached. The system already limits CLI sessions based on available resources. Additional limitation could have adverse effects.

### operator clear-subscriber-one-only

Restricts Operator to clearing only one subscriber session at a time.

### test-commands [encrypted] password *password_string*

Enables access to the CLI test-commands. The commands and keywords made available under this mode are for internal testing and debugging.

**Caution** CLI test-commands are intended for diagnostic use only. Access to these commands is not required during normal system operation. These command are intended for use only by Cisco TAC personnel. Some of these commands can slow system performance, drop subscribers, and/or render the system inoperable

**Important** An SNMP trap is generated when a user enables **cli test-commands** (starTestModeEntered). Refer to the *SNMP MIB Reference* for additional information.

**encrypted**: Specifies that the system will save the password in an encrypted format in the configuration file. The system displays the encrypted keyword in the configuration file as a flag indicating that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

**password** *password_string*: Prompts for the password required to access CLI test-commands. This password must have been previously configured by a Security Administrator via the **tech-suport test-commands password** command. The password is an alphanumeric string of 1 through 64 characters (plain text password) or 1 through 524 characters (encrypted password).

If the **password** keyword is not entered, the user is prompted (no-echo) to enter the password. If **tech-support test-commands password** has not been enabled, you will be unable to execute **cli test-commands**.

Once this test mode is entered under Global Configuration mode, CLI test-commands become part of the current configuration. Therefore, any generated configuration file will contain the **cli test-commands** command as the first configuration command.

**Caution** Use of CLI test-commands may cause significant service interruption. Contact Cisco TAC before executing any commands while in this mode.

The **no cli test-commands** command disables access to the CLI test-commands mode.

### trap config-mode

Enables sending an SNMP trap (starCLIConfigMode) when a CLI user enters the configuration mode.

**Usage Guidelines**

This command sets access parameters and enables several operational parameters for the system's command line interface.

**Important**

The maximum number of multiple CLI sessions that can be supported is based on the amount of available memory. A minimum of 15 CLI sessions are supported on the ASR 5500. One of the CLI sessions is reserved for use exclusively by a CLI session on a serial console interface. Additional CLI sessions beyond the pre-reserved set are permitted if sufficient management card resources are available. If the Resource Manager is unable to reserve resources for a CLI session beyond those that are pre-reserved, administrative users are prompted as to whether or not the system should attempt to create the new CLI session even without reserved resources.

**Example**

The following command sets the number of allowed simultaneous CLI sessions to *5*:

```
cli max-sessions 5
```

The following command sets the command **monitor protocol** to administrator-only:

```
cli access monitor-protocol administrator
```

# cli-encrypt-algorithm

Specifies the type of encryption algorithm to be used for passwords and secrets.

**Product**

All

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
cli-encrypt-algorithm { A | B | C }
default cli-encrypt-algorithm
```

**default**

Resets the encryption algorithm to "A" (prior to release 21.0) or "B" (release 21.0 and higher).

**A**

Specifies MD5-based cipher encryption algorithm. This is the default for StarOS releases prior to 21.0. Passwords encrypted with this key will have "+A" prefixes in the configuration file.

**B**

Specifies the AES-CTR-128 cipher algorithm for encryption and the HMAC-SHA1 cipher algorithm for authentication. Passwords encrypted with this key will have "+B" prefixes in the configuration file. Algorithm B is the default for release 21.0 and higher.

**C**

Specifies HMAC-SHA512 cipher algorithm for encryption and authentication. Passwords encrypted with this key will have "+C" prefixes in the configuration file.

**Usage Guidelines**

Use this command to specify the types of cipher algorithm(s) to be used as encryption and authentication keys for passwords.

The encryption key protects the confidentiality of passwords, while the authentication key protects their integrity.

**Important** For release 20.0 and higher Trusted builds, option **A** is not available.

**Example**

The following command sets the encryption key to **C**:

```
cli-encrypt-algorithm C
```

# client ssh

Enters the SSH Client 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**

```
[ no ] client ssh
```

**no**

Removes the SSH client key pair configuration.

**Usage Guidelines**

Use this command to enter the SSH Client Configuration mode. The CLI commands in that mode allow you to create an SSH key pair and push the private key to external servers for SSH access between the StarOS gateway and external servers.

### Example

The following command moves you to the SSH Client Configuration mode:

```
client ssh
```

# clock

Configures system clock timezone and what local time zone to use.

**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**

```
clock timezone tz [ local ]
no clock timezone
```

**no**

Resets the system timezone to the system default UTC.

***tz***

Specifies the system time zone to use as one of:

- america-buenos-aires (GMT-3:00; Buenos Aires)
- america-caracas (GMT-4:00) Caracas
- america-guatemala (GMT-6:00; Guatemala, Guatemala)
- america-la_paz (GMT-4:00; La Paz)
- america-lima (GMT-5:00; Lima, Peru)
- america-puerto-rico (GMT-4:00; Puerto Rico)
- america-sao-paulo (GMT -3:00; Brazil)
- america-tijuana (GMT-8:00; Tijuana)
- asia-almaty (GMT+6.00; Almaty, Kazakhstan)
- asia-baghdad (GMT+3:00; Baghdad, Russia Zone 2, Kuwait, Nairobi, Riyadh, Moscow, Tehran)
- asia-bangkok (GMT+7:00; Bangkok)
- asia-calcutta (GMT+5:30; Calcutta, Mumbai, New Delhi)

- asia-dhaka (GMT+6:00; Dhaka)
- asia-hong-kong (GMT+8:00; Hong_Kong)
- asia-irkutsk (GMT+9:30; Irkutsk)
- asia-kabul (GMT+4:30; Kabul)
- asia-karachi (GMT+5:00; Karachi)
- asia-katmandu (GMT+5:45; Kathmandu)
- asia-magadan (GMT+11:00; Magadan)
- asia-muscat (GMT+4:00; Abu Dhabi, UAE, Muscat, Tblisi, Volgograd, Kabul)
- asia-rangoon (GMT+6:30; Rangoon)
- asia-seoul (GMT+9:00) Seoul
- asia-tehran (GMT+3:30; Tehran)
- asia-tokyo (GMT+9:00; Tokyo, Russia Zone 8)
- atlantic-azores (GMT-2:00; Azores)
- atlantic-cape-verde (GMT-1:00; Cape Verde Islands)
- australia-perth (GMT+8:00) Perth
- australia-darwin (GMT+9:30) Northern Territory - Alice Springs, Darwin, Uluru
- australia-adelaide (GMT+9:30) Southern Territory - Adelaide
- australia-melbourne (GMT+10:00) Victoria - Ballarat, Melbourne
- australia-sydney (GMT+10:00) New South Wales - Newcastle, Sydney, Wollongong
- australia-hobart (GMT+10:00) Tasmania - Hobart, Launceston
- australia-brisbane (GMT+10:00) Queensland - Brisbane, Cairns, Toowoomba, Townsville
- australia-lordhowe (GMT+10:30) Lord Howe Island
- canada-newfoundland (GMT-3:30; Newfoundland)
- canada-saskatchewan (GMT-6:00; Saskatchewan)
- europe-central (GMT+1:00; Paris, Berlin, Amsterdam, Brussels, Vienna, Madrid, Rome, Bern, Stockholm, Oslo)
- europe-dublin (GMT+0:00) Dublin, Ireland
- europe-eastern (GMT+2:00; Russia Zone 1, Athens, Helsinki, Istanbul, Jerusalem, Harare)
- newzealand-auckland (GMT +12:00; Auckland, Willington)
- newzealand-chatham (GMT +12:45; Chatham)
- nuku (GMT-13:00; Nuku'alofa)
- pacific-fiji (GMT+12:00; Wellington, Fiji, Marshall Islands)

- pacific-guam (GMT+10:00; Brisbane, Cairns, Sydney, Guam)
- pacific-kwajalein (GMT-12:00; Kwajalein)
- pacific-norfolk - (GMT+11:30) Norfolk Island
- pacific-samoa (GMT-11:00; Samoa)
- us-alaska (GMT-9:00; Alaska)
- us-arizona (GMT-7:00; Arizona)
- us-central (GMT-6:00; Chicago, Mexico City, Saint Louis)
- us-eastern (GMT-5:00; Bogota, Lima, New York City)
- us-hawaii (GMT-10:00; Hawaii)
- us-indiana (GMT-6:00; Indiana)
- us-mountain (GMT-7:00; Cheyenne, Denver, Las Vegas)
- us-pacific (GMT-8:00) San Francisco, LA, Seattle
- utc (GMT; Universal Time Coordinated: London, Dublin, Edinburgh, Lisbon, Reykjavik, Casablanca)

### local

Indicates the timezone specified by *tz* is to be considered the local time zone for local time display and conversion.

**Usage Guidelines**

Clock and timezone management is necessary for proper accounting records. The chassis may be set to display a different local time than that of the system clock which allows accounting records to use the system time but to display the proper local time for users.

### Example

The following command sets the clock time zone to UTC (Universal Time Coordinated):

```
clock timezone utc
```

# cmp auto-fetch

Use this command to add a fetch configuration for each certificate for which automatic update is required. This is a Certificate Management Protocol v2 command.

**Product**

All products supporting IPSec CMPv2 features

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**cmp auto-fetch current-name** *cert_name* **ca-root** *ca_name* **time** *days*
**no auto-fetch current-name** *cert_name*

**no**

Removes auto-fetch configuration for a certificate.

**current-name *cert-name***

Specifies a valid security gateway certificate as an alphanumeric string of 1 through 129 characters.

**ca-root *ca_name***

Specifies the filename of the root certificate of the CA server. *ca_name* is an alphanumeric string of 1 through 129 characters.

**time *days***

Specifies the number of days before the certificate expires as the time when the auto fetch should be triggered. *days* is specified as an integer from 1 through 256.

**Usage Guidelines**

Use this command to specify when a current certificate should be automatically fetched.

**Example**

The following command automatically fetches the current certificate (*aqaw12345*) 10 days before it is to expire:

```
cmp fetch current-name aqaw12345 ca-root ca001 time 10
```

# cmp cert-store location

Use this command to add a file location on /flash disk where the certificates and private keys will be stored. This is a Certificate Management Protocol v2 command.

**Product**

All products supporting IPSec CMPv2 features

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**cmp cert-store location** *pathname* **[ key reuse ]**
**no cmp cert-store**

**no**

Removes the certificate storage location configuration.

***pathname***

Specifies the storage location of the certificates and key files in the following formats:

- **[file:]{ /flash | /usb1 | /hd-raid }[**/<*directory*>**]**/<*filename*>
- **tftp:**//<*host*>**[:**<*port*>**]|[**/<*directory*>**]**/<*filename*>
- **ftp:**//**[**<*username*>**[:**<*password*>]**@]**<*host*>**[:**<*port*>**]|[**/<*directory*>**]**/<*filename*>
- **sftp:**//**[**<*username*>**[:**<*password*>**]@]**<*host*>**[:**<*port*>**]|[**/<*directory*>**]**/<*filename*>
- **http:**//**[**<*username*>**[:**<*password*>**]@]**<*host*>**[:**<*port*>**]|[**/<*directory*>**]**/<*filename*>

**Usage Guidelines**

Use this command to specify where certificates and key files should be stored.

**Example**

The following command stores certificates and key files in a location different from the default location:

```
cmp  cert-store location file://certificates
```

# cmp cert-trap time

Defines when an SNMP MIB certificate expiry trap should be sent as the number of hours before expiration.

**Product**

All products supporting IPSec CMPv2 features

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**cmp cert-trap time** *hours*
**no cmp cert-trap time**

**no**

Removes the certificate expiry MIB trap notification.

**time *hours***

Specifies the number of hours before certificate expiry when a MIB trap should be sent. *hours* is an integer from 1 through 1024.

**Usage Guidelines**

Use this command to set when an SNMP MIB certificate expiry trap should be sent.

**Example**

The following command specifies that an SNMP MIB certificate expiry trap should be sent 48 hours prior to expiration:

```
cmp  cert-trap time 48
```

# commandguard

Forces mandatory confirmation prompting for the **autoconfirm** (Exec mode and Global Configuration mode) and **configure** (Exec mode).

**Product**

All products

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] commandguard [ exec-command** *exec_mode_category* **]**

**no**

Disables commandguard functionality if enabled.

**exec-command *exec_mode_category***

Applies mandatory prompting for specified categories of Exec mode configuration commands, even when **autoconfirm** is enabled.

*exec_mode_category* specifies one of the following categories of Exec mode configuration commands.

- card
- clear
- copy
- debug
- delete
- filesystem
- hd
- reload
- rename
- shutdown
- task
- upgrade

You can enter multiple **commandguard exec-command** *exec_mode_category* commands.

## Usage Guidelines

Use this command to force mandatory confirmation prompting for the **autoconfirm** (Exec mode and Global Configuration mode) and **configure** (Exec mode). This command prevents users from accidentally entering Global Configuration mode, or to prevent file replay (most commonly caused by a cut and paste error in the configuration file). By default this command is disabled.

The status of **commandguard** is output in **show configuration** commands.

**Important** If autoconfirm is enabled, commandguard will not take effect until autoconfirm is disabled in both Exec and Global Configuration modes.

Use the **commandguard** command to apply mandatory prompting for specified categories of Exec mode configuration commands, even when autoconfirm is enabled.

- All Exec mode commands beginning with the specified category word will prompt for confirmation, regardless if **autoconfirm** is enabled.
- You can turn off confirmation prompting for a specific category using **no commandguard exec-command** *exec_mode_category*.
- If autoconfirm is overridden by **commandguard exec-command** for an Exec mode command, StarOS displays an informational message indicating why autoconfirm is being overridden when you attempt to execute the command.
- Users may selectively override confirmation prompting for any Exec mode configuration command that supports the **-noconfirm** keyword.

### Example

The following command enables confirmation prompting for all configuration commands:

**commandguard**

# congestion-control

This command enables and disables the congestion control functionality 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**

**`[ default | no ] congestion-control`**

**default**

Sets the congestion control to its default value.

**no**

Disables the congestion control functionality. This is the default behavior.

**Usage Guidelines**

Congestion control on the system is used to monitor the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (i.e high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may impact the system's ability to service subscriber sessions. The purpose of congestion control is to aid in the identification of such conditions and invoke policies for addressing the situation.

Congestion control operation is based on the configuration of the following:

- **Call disconnections on overload**: With this functionality, the system enables and disables the policy for disconnecting passive calls (chassis-wide) during an overload situation. It also configures and fine-tunes the overload-disconnect congestion control policy for an entire chassis.
- **Congestion condition thresholds**: Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a similar fashion to the operation thresholds that can be configured for the system (as described in later in this chapter). The primary difference is that when these thresholds are reached, not only is an SNMP trap generated (starCongestion), but a service congestion policy is invoked as well.

  A threshold tolerance is configured to dictate the percentage under the configured threshold that must be reached in order for the condition to be considered "cleared". An SNMP trap (starCongestionClear) is then triggered.

- **Service congestion policies**: Congestion policies are configurable for each service (e.g., PDSN, GGSN, P-GW, SGSN, etc.). These policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

Since the congestion control functionality on the system is disabled by default, this command should be executed once congestion-control thresholds and policies have been configured. (Refer to the other congestion-control related commands for more information.)

### Example

The following command enables the congestion control functionality on the system.

```
congestion-control
```

# congestion-control overload-disconnect

This command enables and disables the policy for disconnecting passive calls (chassis-wide) during an overload situation. It also configures and fine-tunes the overload-disconnect congestion control policy for an entire chassis.

**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**

```
congestion-control overload-disconnect [ iterations-per-stage integer |
percent percentage_value | threshold { license-utilization percentage_value |
max-sessions-per-service-utilization percentage_value | tolerance number } ]
default congestion-control overload-disconnect [ iterations-per-stage |
percent | threshold { license-utilization |
max-sessions-per-service-utilization | tolerance } ]
no congestion-control overload-disconnect
```

#### default

When "default" and one of the keywords is added to the command, the policy remains in its current state and the value for the specified keyword is reset to its default value.

When "default" and the command are entered without keywords, the overload-disconnect policy for congestion control is disabled.

#### no

Disables the overload-disconnect policy for congestion control.

#### iterations-per-stage *integer*

Specifies the number of calls to be disconnected during the defined number of seconds. *integer* is a value from 2 through 8. The default value is 8.

#### percent *percentage_value*

Specifies the percentage of calls to be disconnected, in stages, during an overload situation. *percentage_value* is an integer from 1 through 100. The default value is 5.

#### threshold

**license-utilization:** Specifies the license-utilization percentage threshold for overload situations. If candidates are available, passive calls are disconnected when this threshold is exceeded. *percentage_value* is an integer from 1 through 100. The default value is 80.

**max-sessions-per-service-utilization:** Specifies a percentage of the maximum sessions per service. If candidates are available, passive calls are disconnected when this threshold is exceeded. *percentage_value* is an integer from 1 through 100. The default value is 80.

**tolerance:**Specifies the percentage of calls the system disconnects below the values set for the other two thresholds. In either case, a Clear Traps message is sent after the number of calls goes below the corresponding threshold value. *number* is an integer from 1 through 25. The default value is 10.

### Usage Guidelines

Use this command to set the policy for call disconnects when the chassis experiences call overload.

To verify the congestion-control configuration use **show congestion-control configuration** from the Exec mode.

To set overload-disconnect policies for individual subscribers., see **overload-disconnect** in Subscriber Configuration Mode Commands.

#### Example

The following command sets an overload-disconnect policy for the chassis in which 5 calls would be disconnected very 5 seconds during an overload situation.

```
congestion-control overload-disconnect interations-per-stage 5
```

Both of the following commands disable the overload-disconnect policy without changing the policy configuration.

```
default congestion-control overload-disconnect
```

or

```
no congestion-control overload-disconnect
```

To instruct the system to stop call disconnects when the number of calls goes down 85% of the total allowed calls for that service, enter both of the following commands to set the max-sessions-per-service-utilization value to 90% and the tolerance value to 5%:

```
congestion-control overload-disconnect threshold
max-sessions-per-service-utilization 90
congestion-control overload-disconnect threshold tolerance 5
```

# congestion-control policy

Configures congestion control policies.

**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**

**congestion-control policy { asngw-service | asnpc-service | epdg-service fng-service | ggsn-service | ha-service | hnbgw-service | hsgw-service | ipsg-service | lma-service | lns-service | mipv6ha-service | pcc-af-service | pcc-policy-service | pdg-service | pdif-service | pdsn-service | pdsnclosedrp-service | pgw-service | phsgw-service | phspc-service | saegw-service | samog-service | sgsn-service | sgw-service | wsg-service } action { drop | none | redirect | reject }**
**congestion-control policy mme-service action { drop | none | reject | report-overload { permit-emergency-sessions | reject-new-sessions | reject-non-emergency-sessions } enodeb-percentage** *percentage* **}**
**congestion-control policy { critical mme-service action-profile** *action_profile_name* **| major mme-service action-profile** *action_profile_name* **| minor mme-service action-profile** *action_profile_name* **}**
**congestion-control policy { critical | major | minor } sgsn-service action-profile** *action_profile_name*
**no congestion-control policy { critical | major | minor } sgsn-service**
**default congestion-control policy { asngw-service | asnpc-service | epdg-service | fng-service | ggsn-service | ha-service | hnbgw-service | hsgw-service | ipsg-service | lma-service | lns-service | mipv6ha-service | mme-service | pcc-af-service | pcc-policy-service | pdg-service | pdif-service | pdsn-service | pdsnclosedrp-service | pgw-service | phsgw-service | phspc-service | saegw-service samog-service | | sgsn-service | sgw-service | wsg-service }**

**default**

Specifies the Congestion Control policy action for the selected service to its default value.

**asngw-service**

Specifies the Congestion Control policy action for the ASN-GW service.

**asnpc-service**

Specifies the Congestion Control policy action for the ASN PC-LR service.

**critical**

For MME (starting with Release 14.0), or ePDG (starting with Release 14.1), or for SGSN (starting with Release 17.0), this keyword associates the action-profile to be used for critical congestion thresholds for the MME or SGSN's service.

### epdg-service action

Specifies the Congestion Control policy action for the ePDG service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

For ePDG type of session/calls, **redirect** action is not supported.

### fng-service

Specifies the Congestion Control policy action for the FNG service.

### ggsn-service

Specifies the Congestion Control policy action for the GGSN service.

### ha-service

Specifies the Congestion Control policy action for the HA service.

### hnbgw-service

**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.

Specifies the Congestion Control policy action for the HNB-GW service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

### hsgw-service

Specifies the Congestion Control policy action for the HSGW service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **redirect**: Specifies that the system should redirect new session requests to an alternate device.

**Important** If this option is used, the IP address of the alternate device must be configured using the **policy overload redirect** command that is part of the HSGW service configuration.

- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

### ipsg-service

Specifies the Congestion Control Policy action for the IPSG service. The policy specifies how the IPSG service will respond when the system detects that a congestion condition threshold has been crossed.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.

**Default**: **none**

### lma-service

Specifies the Congestion Control policy action for the LMA service

### lns-service

Specifies the Congestion Control policy action for the LNS service.

### mipv6ha-service

Specifies the Congestion Control policy action for the MIPv6-HA service.

### major

For MME (starting with Release 14.0), or ePDG (starting with Release 14.1), or for SGSN (starting with Release 17.0), this keyword associates the action-profile to be used for major congestion thresholds for the MME or SGSN's service.

### minor

For MME (starting with Release 14.0), or ePDG (starting with Release 14.1), or for SGSN (starting with Release 17.0), this keyword associates the action-profile to be used for minor congestion thresholds for the MME or SGSN's service.

### mme-service

Sets the congestion control policy for action to take when subscriber sessions exceeds the defined threshold limit.

For MME type of session/calls, **redirect** action is not supported.

**Important** The **mme-service** keyword option is available only in releases prior to 14.0. In 14.0 and higher, you must first select either the critical, major or minor policy level first. Refer to the **congestion-action-profile** command in the LTE Policy Configuration mode to create action-profiles which in turn define the actions to be taken when thresholds are exceeded in Release 14.0 and higher for MME.

### pcc-af-service

Specifies the Congestion Control policy action for the PCC Application Function (AF) service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

### pcc-policy-service

Specifies the Congestion Control policy action for the PCC Policy service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

### pcc-quota-service

Specifies the Congestion Control policy action for the PCC Quota service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

### pdg-service

Specifies the Congestion Control policy action for the PDG service.

### pdif-service

Specifies the Congestion Control policy action for the PDIF service.

### pdsn-service

Specifies the Congestion Control policy action for the PDSN service.

### pdsnclosedrp-service

Specifies the Congestion Control policy action for the PDSN Closed R-P service.

### pgw-service

Specifies the Congestion Control policy action for the P-GW service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

  For P-GW sessions/calls, **redirect** action is not supported.

### saegw-service

Specifies the Congestion Control policy action for the SAEGW service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

  For SAEGW sessions/calls, **redirect** action is not supported.

### samog-service

Specifies the Congestion Control policy action for the SaMOG service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

### sgsn-service

Specifies the Congestion Control policy - the congestion response actions for the SGSN service.

Prior to Release 17.0, the supported policy actions in this command are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.

- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

With Release 17.0 and higher, to define a policy you must first select one of the three congestion levels: critical, major or minor. Next select the service with the **sgsn-service** keyword and then associate a congestion-action-profile. Refer to the **congestion-action-profile** command in the SGSN-Global Configuration mode to create the congestion-action-profiles which define the congestion response actions to be taken when thresholds are exceeded for the SGSN.

### sgw-service

Specifies the Congestion Control policy action for the S-GW service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

  For S-GW sessions/calls, **redirect** action is not supported.

### wsg-service

Specifies the Congestion Control policy action for the WSG service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

### action { drop | none | redirect | reject }

Specifies the policy action:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action. This is the default for PDIF-service.
- **redirect**: Specifies that the system should redirect new session requests to an alternate device. (HA, HSGW, and PDSN only)

  

  **Important** If this option is used, the IP address of the alternate device must be configured using the **policy overload redirect** command that is part of the service configuration. Note that this option can not be used in conjunction with GGSN, MME, P-GW, SAEGW, or S-GW services.

- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

(For PDSN and HA, the reply code is 130, "insufficient resources". For the GGSN, the reply code is 199, "no resources available".)

**report-overload { permit-emergency-sessions | reject-new-sessions | reject-non-emergency-sessions } enodeb-percentage *percentage***

**Important** This set of keywords is supported only by the MME.

Enables the MME to report overload conditions to eNodeBs and take additional action to alleviate congestion situations.

**permit-emergency-sessions**: Specifies that only emergency sessions are allowed to access the MME during the overload period.

**reject-new-sessions**: Specifies that all new sessions destined for the MME will be rejected during the overload period.

**reject-non-emergency-sessions**: Specifies that all non-emergency sessions will be rejected during the overload period.

**enodeb-percentage** *percentage*: Configures the percentage of known eNodeBs that will receive the overload report. *percentage* must be an integer from 1 to 100.

**Usage Guidelines** Congestion policies can be configured for each service. When congestion control functionality is enabled, these policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

### Example

The following command configures a congestion control policy of reject for PDSN services:

```
congestion-control policy pdsn-service action reject
```

The following command configures a congestion control policy of reject for MME services:

```
congestion-control policy mme-service action reject
```

# congestion-control threshold

Configures the congestion control threshold values that are to be monitored.

**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

**congestion-control threshold { license-utilization** *percent* **|**
**max-sessions-per-service-utilization** *percent* **| message-queue-utilization** *percent* **| message-queue-wait-time** *time* **| port-rx-utilization** *percent* **|**
**port-specific {** *slot/port* **| all } [ tx-utilization** *percent* **] [ rx-utilization** *percent* **] port-specific-rx-utilization critical |**
**port-specific-tx-utilization critical | port-tx-utilization** *percent* **|**
**service-control-cpu-utilization** *percent* **| system-cpu-utilization** *percent* **|**
**system-memory-utilization** *percent* **| tolerance** *percent* **}**
**default congestion-control threshold { license-utilization |**
**max-sessions-per-service-utilization | message-queue-utilization |**
**message-queue-wait-time | port-rx-utilization | port-specific |**
**tx-utilization | rx-utilization | port-tx-utilization |**
**service-control-cpu-utilization | system-cpu-utilization |**
**system-memory-utilization | tolerance }**
**no congestion-control threshold port-specific {** *slot/port* **| all }**
**no congestion-control threshold port-specific {** *slot/port* **| all } [**
**rx-utilization** *percent* **] [ tx-utilization** *percent* **]**
**no congestion-control threshold port-specific-rx-utilization critical**
**no congestion-control threshold port-specific-tx-utilization critical**
**no congestion-control threshold { message-queue-utilization |**
**message-queue-wait-time | port-rx-utilization** *percent* **| port-tx-utilization**
**percent | service-control-cpu-utilization | system-cpu-utilization |**
**system-memory-utilization }**

### default congestion-control threshold *keyword*

Sets the threshold keyword to its default value.

### no congestion-control threshold port-specific { slot/port | all }

This command disables port specific threshold monitoring on the specified port or on all ports.

*slot/port*: Specifies the port for which port specific threshold monitoring is being configured. The slot and port must refer to an installed card and port.

**all**: Set port specific threshold monitoring for all ports on all cards.

### no congestion-control threshold port-specific-rx-utilization critical

This command disables specific receive port utilization.

### no congestion-control threshold port-specific-tx-utilization critical

This command disables specific transmit port utilization.

### license-utilization *percent*

Default: 100

The percent utilization of licensed session capacity as measured in 10 second intervals.

*percent* can be configured to any integer value from 0 to 100.

**max-sessions-per-service-utilization *percent***

Default: 80

The percent utilization of the maximum sessions allowed per service as measured in real-time. This threshold is based on the maximum number of sessions or PDP contexts configured for the a particular service. (Refer to the **bind** command for the PDSN, GGSN, SGSN, or HA services.)

*percent* can be an integer from 0 through 100.

**message-queue-utilization *percent***

Default: 80

The percent utilization of the Demux Manager software task's message queue as measured in 10 second intervals. The queue is capable of storing a maximum of 10000 messages.

*percent* can be an integer from 0 through 100.

**message-queue-wait-time *time***

Default: 5

The maximum time (in seconds) messages can be held in queue as measured by packet time stamps.

*time* is measured in seconds and can be an integer from 1 through 30.

**Important** In the event that this threshold is crossed, an SNMP trap is not triggered. The service congestion policy invocation resulting from the crossing of this threshold is enforced only for the packet that triggered the action.

**[ no ] port-rx-utilization *percent***

Default: 80

The average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

*percent* can be an integer from 0 through 100.

**[ no ] port-specific { *slot/port* | all } [ rx-utilization *percent* ] [ tx-utilization *percent*]**

Default: Disabled

Sets port-specific thresholds. If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is applied system-wide.

*slot/port*: Specifies the port for which port-specific threshold monitoring is being configured. The slot and port must refer to an installed card and port.

**all**: Set port specific threshold monitoring for all ports on all cards.

**rx-utilization** *percent*: Default 80%. The average percent utilization of port resources for the specified port by received data as measured in 5-minute intervals. *percent* must an integer from 0 through 100.

**tx-utilization** *percent*: Default 80%. The average percent utilization of port resources for the specified port by transmitted data as measured in 5-minute intervals. *percent* must be an integer from 0 through 100.

**[ no ] port-tx-utilization *percent***

Default: 80

The average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

*percent* can be an integer from 0 through 100.

**service-control-cpu-utilization *percent***

Default: 80

The average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

*percent* can be an integer from 0 through 100.

**system-cpu-utilization *percent***

Default: 80

The average percent utilization for all PAC/PSC/PSC2 CPUs available to the system as measured in 10-second intervals.

*percent* can be an integer from 0 through 100.

This threshold setting can be disabled with **no congestion-control threshold system-cpu-utilization** command. In case later you want to enable the same threshold setting **congestion-control threshold system-cpu-utilization** command will enable the CPU utilization threshold to preconfigured level.

**system-memory-utilization *percent***

Default: 80

The average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

*percent* can be an integer from 0 through 100.

**tolerance *percent***

Default: 10

The percentage under a configured threshold that dictates the point at which the condition is cleared.

*percent* can be an integer from 0 through 100.

## Usage Guidelines

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a similar fashion to the operation thresholds that can be configured for the system (as described in later in this chapter). The primary difference is that when these thresholds are reached, not only is an SNMP trap generated (starCongestion), but a service congestion policy is invoked as well.

The tolerance parameter establishes the threshold at which the condition is cleared. An SNMP trap (starCongestionClear) is generated for the clear condition, as well.

**Important** The MME (version 14.0 and higher) supports three levels of thresholds – critical, major and minor – for each condition. Refer to the **congestion-control threshold** commands immediately following this command for information specific to the MME.

### Example

The following command configures a system CPU utilization threshold of 75%.

```
congestion-control threshold system-cpu-utilization 75
```

This setting will remain in configuration unless you specify another threshold value in place of 75. This threshold setting can be disabled with **no congestion-control threshold system-cpu-utilization** command but cannot be removed from configuration. Later if you want to enable the previously configured threshold value of *75* percent, you only need to enter the **congestion-control threshold system-cpu-utilization** command without specifying any threshold value. It will enable the CPU utilization threshold to preconfigured level of *75* percent.

For example, **no congestion-control threshold system-cpu-utilization** disables the configured threshold setting and **congestion-control threshold system-cpu-utilization** again enables the threshold setting of 75%.

The following command configures a threshold tolerance of 5%:

```
congestion-control threshold license-utilization tolerance 5
```

In the above examples, the starCongestion trap gets triggered if the license utilization goes above 75% and the starCongestionClear trap gets triggered if it reaches or goes below 70%.

# congestion-control threshold connected-sessions-utilization

Supports congestion based on the total number of utilized connected sessions.

**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**

```
   congestion-control threshold connected-sessions-utilization{ critical
 percent | major percent | minor }
   [ default | no ] congestion-control threshold
connected-sessions-utilization { critical | major
| minor }
```

**default congestion-control threshold connected-sessions-utilization**

Sets all connected-sessions-utilization thresholds to the default values.

**critical *percent***

Default: 80

The critical threshold value of utilized connected sessions.

*percent* can be configured to any integer value from 0 to 100.

**major *percent***

Default: 0

The major threshold value of utilized connected sessions.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value of utilized connected sessions.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of utilized connected sessions.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Important** The **major** and **minor** keywords in this command are product dependent. PGW, SGW and SAE-GW products only allow critical configuration threshold levels.

**Example**

The following command configures a minor threshold level of 25%.

```
congestion-control threshold connected-sessions-utilitization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

# congestion-control threshold demuxmgr-cpu-utilization

Configures a demux manager facility type to be monitored for an average CPU utilization along with the threshold values.

**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**

**congestion-control threshold demuxmgr-cpu utilization facility { *egtpegmgr* { critical *percent* | major *percent* | minor *percent* } | *egtpinmgr* { critical *percent* | major *percent* | minor *percent* } | *gtpumgr* { critical *percent* | major *percent* | minor *percent* }}**

**[ default | no ] congestion-control threshold demuxmgr-cpu utilization { facility *egtpegmgr* { critical | major | minor } | *egtpinmgr* { critical | major | minor } | *gtpumgr* { critical | major | minor }}**

**default congestion-control threshold demuxmgr-cpu-utilization**

Sets all demuxmgr-cpu-utilization thresholds to the default values.

**facility**

Specifies the specific facility.

**egtpegmgr**

Specifies the EGTP egress demux manager.

**egtpinmgr**

Specifies the EGTP ingress demux manager.

**gtpumgr**

Specifies the GTPUMGR demux manager.

**critical *percent***

Default: 0

The critical threshold value for average percent CPU utilization to trigger the congestion control based on the configured congestion control policy.

*percent* can be configured to any integer value from 0 to 100.

**Important** The recommended critical threshold value *percent* is 80.

**major *percent***

Default: 0

The major threshold value for average percent CPU utilization to trigger the congestion control based on the configured congestion control policy.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value for average percent CPU utilization to trigger the congestion control based on the configured congestion control policy.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent CPU utilization to trigger the congestion control based on the configured congestion control policy.

The demux manager facility average cpu utilization is the average of all the demux manager instances cpu utilization of same facility type that are currently running in the chassis. If the demux manager facility average cpu utilization exceeds the configuration threshold value, then congestion is notified to all services and the appropriate action begins based on the congestion policy configured.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Important** **congestion-control threshold demuxmgr-cpu-utilization** is visible for all products but configuration is only applicable for PGW, SGW and SAE-GW.

The **major** and **minor** keywords in this command are product dependent. PGW, SGW and SAE-GW products only allow critical configuration threshold levels.

**Example**

The following command configures a minor threshold level of 25%.

```
congestion-control threshold demuxmgr-cpu-utilitization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold demuxmgr-cpu-utilization
```

# congestion-control threshold license-utilization

Configures the congestion threshold levels for license utilization on the system.

**Important** This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**

MME

ePDG

**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**

**congestion-control threshold license-utilization { critical** *percent* **| major** *percent* **| minor** *percent* **}**
**default congestion-control threshold license-utilization**

**default congestion-control threshold license-utilization**

Sets all license-utilization thresholds to the default values.

**critical *percent***

Default: 100

The critical threshold value for percent utilization of licensed session capacity, measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**major *percent***

Default: 0

The major threshold value for percent utilization of licensed session capacity, measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value for percent utilization of licensed session capacity, measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of licensed session capacity as a percentage as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

### Example

The following command configures a minor threshold level for license utilization of 25%.

```
congestion-control threshold license-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold license-utilization
```

# congestion-control threshold max-sessions-per-service-utilization

Configures the congestion thresholds for the maximum sessions allowed per service.

**Important** This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**

MME

ePDG

**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**

```
congestion-control threshold max-sessions-per-service-utilization {
critical percent | major percent | minor percent }
default congestion-control threshold max-sessions-per-service-utilization
```

#### default congestion-control threshold max-sessions-per-service-utilization

Sets all max-sessions-per-service-utilization thresholds to the default values.

#### critical *percent*

Default: 80

The critical threshold value for percent utilization of the maximum sessions allowed per service.

*percent* can be configured to any integer value from 0 to 100.

**major *percent***

Default: 0

The major threshold value for percent utilization of the maximum sessions allowed per service.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value for percent utilization of the maximum sessions allowed per service.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of maximum sessions per service as a percentage measured in real-time. This threshold is based on the maximum number of sessions or PDP contexts configured for the a particular service. (Refer to the **bind** command for the PDSN, GGSN, SGSN, or HA services.)

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Example**

The following command configures a minor threshold level of 25%.

```
congestion-control threshold max-sessions-per-service-utilization minor
25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold max-sessions-per-service-utilization
```

# congestion-control threshold message-queue-utilization

Configures the congestion thresholds for the percent utilization of the Demux Manager software task's message queue.

**Important** This command applies to ePDG (version 14.1 and higher).

**Product** ePDG

**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

**congestion-control threshold message-queue-utilization { critical** *percent* **| major** *percent* **| minor** *percent* **}**
**default congestion-control threshold message-queue-utilization**

### default congestion-control threshold message-queue-utilization

Sets all max-sessions-per-service-utilization thresholds to the default values.

### critical *percent*

Default: 80

The critical threshold value for percent utilization of the Demux Manager software task's message queue as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

### major *percent*

Default: 0

The major threshold value for percent utilization of the Demux Manager software task's message queue as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

### minor *percent*

Default: 0

The minor threshold value for percent utilization of the Demux Manager software task's message queue as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

## Usage Guidelines

Use this command to set the critical, major and minor threshold levels of percent utilization of the Demux Manager software task's message queue as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

### Example

The following command configures a minor threshold level of 25%.

```
congestion-control threshold message-queue-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

**default congestion-control threshold message-queue-utilization**

# congestion-control threshold message-queue-wait-time

Configures the congestion thresholds for the maximum time (in seconds) messages can be held in queue as measured by packet time stamps.

**Important** This command applies to ePDG (version 14.1 and higher).

**Product**

ePDG

**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**

**congestion-control threshold message-queue-wait-time { critical** *time* **| major** *time* **| minor** *time* **}**
**default congestion-control threshold message-queue-wait-time**

**default congestion-control threshold message-queue-wait-time**

Sets all max-queue-wait-time thresholds to the default values.

**critical *time***

Default: 5

The critical threshold value for the maximum time (in seconds) that messages can be held in queue as measured by packet time stamps.

*time* is measured in seconds and can be an integer from 1 through 30.

**major *time***

Default: 0

The major threshold value for the maximum time (in seconds) that messages can be held in queue as measured by packet time stamps.

*time* is measured in seconds and can be an integer from 1 through 30.

**minor *time***

Default: 0

The minor threshold value for the maximum time (in seconds) that messages can be held in queue as measured by packet time stamps.

*time* is measured in seconds and can be an integer from 1 through 30.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels for the maximum time (in seconds) messages can be held in queue.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed a congestion action-profile is invoked, if configured.

This command requires a valid product license.

**Example**

The following command configures a major threshold level of 4 seconds.

```
congestion-control threshold message-queue-wait-time major 4
```

This setting will remain in configuration unless you specify another minor threshold level in place of 4.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold message-queue-wait-time
```

# congestion-control threshold mmemgr-average-cpu-utilization

Configures MMEMgr-specific thresholds to monitor the MMEMgrs' average CPU utilization.

**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**

```
congestion-control threshold mmemgr-average-cpu-utilization { critical
percent | major percent | minor percent }
[ default | no ] congestion-control threshold
mmemgr-average-cpu-utilization { critical | major |  minor }
```

**default**

Resets the configured thresholds to the system defaults.

**no**

Disables the configured thresholds and removes them from the MME's configuration.

**critical *percent***

Default: 80

The critical threshold value for the average percent utilization of all the CPU memory available to the MMEMgr measured in 10-second intervals.

*percent* can be configured to any integer value from 1 to 100.

**major *percent***

Default: 0

The major threshold value for the average percent utilization of all the CPU memory available to the MMEMgr measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value for the average percent utilization of the all the CPU memory available to the MMEMgr measured in 10-second intervals.

*percent* can be configured to any integer value from 1 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent utilization of all CPU memory available to the MMEMgrs as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked.

The most commonly recommended threshold for the MMEMgr is the service CPU utilization. This is reflective of the MMEMgr's CPU usage since all MMEmgrs are located on demux cards.

**Example**

Use a command similar to the following to set a critical threshold of 89% for MMEMgr CPU usage:

```
congestion-control threshold mmemgr-average-cpu-utilization critical 89
```

# congestion-control threshold port-rx-utilization

Configures the congestion thresholds for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

**Important** This command applies to ePDG (version 14.1 and higher).

**Product**

ePDG

**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**

**congestion-control threshold port-rx-utilization { critical** *percent* **| major** *percent* **| minor** *percent* **}**
**default congestion-control threshold port-rx-utilization**

**default congestion-control threshold port-rx-utilization**

Sets all port-rx-utilization thresholds to the default values.

**critical *percent***

Default: 80

The critical threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**major *percent***

Default: 0

The major threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

### Example

The following command configures a minor threshold level of 25%.

```
congestion-control threshold port-rx-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold port-rx-utilization
```

# congestion-control threshold port-specific

Configures the congestion thresholds for specific port utilization.

**Important** This command applies to ePDG (version 14.1 and higher).

**Product**

ePDG

**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**

**congestion-control threshold port-specific { *slot/port* [ tx-utilization { critical *percent* | major *percent* | minor *percent* ] [ rx-utilization { critical *percent* | major *percent* | minor *percent* } | all { critical *percent* | major *percent* | minor *percent* } }**
**no congestion-control threshold port-specific { *slot/port* { critical | major | minor } | all { critical | major | minor } }**

**no congestion-control threshold port-specific { *slot/port* { critical | major | minor } | all { critical | major | minor } }**

Sets all port-specific utilization thresholds to the default values.

***slot/port***

Default: Disabled

Specifies the port for which port specific threshold monitoring is being configured. The slot and port must refer to an installed card and port. If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is applied system-wide.

**all**

Set threshold monitoring for all ports on all cards.

**rx-utilization**

Set threshold monitoring for received data only.

**tx-utilization**

Set threshold monitoring for transmitted data only.

**critical *percent***

Default: 80

The critical threshold value for average percent utilization of the specified port resources as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**major *percent***

Default: 0

The major threshold value for average percent utilization of the specified port resources as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value for average percent utilization of the specified port resources as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

## Usage Guidelines

Use this command to set the critical, major and minor threshold levels of average percent utilization of specified resources for all ports by transmitted data as measured in 5-minute intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

### Example

The following command configures a minor threshold level of 5% for received data on port 1 of the card in slot 17.

```
congestion-control threshold port-specific 17/1 rx-utilization minor 5
```

This setting will remain in configuration unless you specify another minor threshold level in place of 5.

# congestion-control threshold port-rx-utilization

Configures the congestion thresholds for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

**Important** This command applies to ePDG (version 14.1 and higher).

**Product**

ePDG

**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**

```
congestion-control threshold port-rx-utilization { critical percent | major
 percent | minor percent }
default congestion-control threshold port-rx-utilization
```

**default congestion-control threshold port-rx-utilization**

Sets all port-rx-utilization thresholds to the default values.

**critical *percent***

Default: 80

The critical threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**major *percent***

Default: 0

The major threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Example**

The following command configures a minor threshold level of 25%.

```
congestion-control threshold port-rx-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold port-rx-utilization
```

# congestion-control threshold port-tx-utilization

Configures the congestion thresholds for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

**Important** This command applies to ePDG (version 14.1 and higher).

**Product**

ePDG

**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**

```
congestion-control threshold port-tx-utilization { critical percent | major
 percent | minor percent }
default congestion-control threshold port-tx-utilization
```

**default congestion-control threshold port-tx-utilization**

Sets all port-tx-utilization thresholds to the default values.

**critical *percent***

Default: 80

The critical threshold value for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**major *percent***

Default: 0

The major threshold value for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Example**

The following command configures a minor threshold level of 25%.

```
congestion-control threshold port-tx-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold port-tx-utilization
```

# congestion-control threshold service-control-cpu-utilization

Configures the congestion thresholds for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

**Important** This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**

MME

ePDG

**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**

**congestion-control threshold service-control-cpu-utilization { critical** *percent* **| major** *percent* **| minor** *percent* **}**
**default congestion-control threshold service-control-cpu-utilization**

**default congestion-control threshold service-control-cpu-utilization**

Sets all service-control-cpu-utilization thresholds to the default values.

**critical *percent***

Default: 80

The critical threshold value for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**major *percent***

Default: 0

The major threshold value for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

When the service-control-cpu-utilization critical threshold setting is exceeded, ipsecmgrs running in the congested CPU are notified of the congestion. The ipsecmgrs raise traps for service-congestion exceeded and update the NPU so that no new calls are sent to those ipsecmgrs. The NPU does not send any new calls to the

congested ipsecmgrs. However, if all ipsecmgrs are congested the action is always drop regardless of the setting for congestion policy action. The packet drops are silently done by the NPU.

When ipsecmgrs are congested and an NPU receives a packet whose Security Parameter Index, Initiator (SPIi) in IKE_SA_INIT matches that of a currently established session, the packet is classified as belonging to the existing session. Since congestion action is applied only on new sessions, such IKE_SA_INIT packets are allowed to create sessions. If the IKE_SA_INIT uses an SPIi which does not match any of the existing sessions, it is processed according to the congestion policy action.

This command requires a valid product license.

### Example

The following command configures a minor threshold level of 25%.

```
congestion-control threshold service-control-cpu-utilitization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold service-control-cpu-utilization
```

# congestion-control threshold system-cpu-utilization

Configures the congestion thresholds for average percent CPU utilization of all packet processing cards available to the system as measured in 10-second intervals.

**Important** This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**

MME

ePDG

**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**

```
congestion-control threshold system-cpu-utilization { critical percent |
major percent | minor percent | exclude demux }
default congestion-control threshold system-cpu-utilization
```

#### default congestion-control threshold system-cpu-utilization

Sets all system-cpu-utilization thresholds to the default values.

**critical *percent***

Default: 80

The critical threshold value for average percent CPU utilization of all packet processing cards available to the system.

*percent* can be configured to any integer value from 0 to 100.

**major *percent***

Default: 0

The major threshold value for average percent CPU utilization of all packet processing cards available to the system.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value for average percent CPU utilization of all packet processing cards available to the system.

*percent* can be configured to any integer value from 0 to 100.

**exclude *demux***

Configures exclusion from the system CPU utilization calculation.

If **exclude** *demux* is not configured, then the demux CPU will be included while calculating the system CPU utilization. It is recommended to use this keyword to ensure accurate values of system CPU utilization.

*demux* Removes the demux DPC from the system CPU utilization calculation.

## Usage Guidelines

Use this command to set the critical, major and minor threshold levels of average percent CPU utilization of all packet processing cards available to the system as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Important** The **major** and **minor** keywords in this command are product dependent. PGW, SGW and SAE-GW products only allow critical configuration threshold levels.

### Example

The following command configures a minor threshold level of 25%.

```
congestion-control threshold system-cpu-utilitization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

**default congestion-control threshold system-cpu-utilization**

# congestion-control threshold system-memory-utilization

Configures the congestion thresholds for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

**Important** This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**

MME

ePDG

**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**

**congestion-control threshold system-memory-utilization { critical** *percent* **| major** *percent* **| minor** *percent* **| exclude** *demux* **}**
**default congestion-control threshold system-memory-utilization**

**default congestion-control threshold system-memory-utilization**

Sets all system-memory-utilization thresholds to the default values.

**critical *percent***

Default: 80

The critical threshold value for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**major *percent***

Default: 0

The major threshold value for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The minor threshold value for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**exclude *demux***

Configures exclusion from the system CPU utilization calculation.

If **exclude** *demux* is not configured, then the demux CPU will be included while calculating the system CPU utilization. It is recommend to use this keyword to ensure accurate values of system memory utilization.

*demux* Removes the demux DPC from the system CPU utilization calculation.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Important** The **major** and **minor** keywords in this command are product dependent. PGW, SGW and SAE-GW products only allow critical configuration threshold levels.

**Example**

The following command configures a minor threshold level of 25%.

```
congestion-control threshold system-memory-utilitization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold system-memory-utilization
```

# congestion-control threshold tolerance

Configures the percentage under a configured threshold value that dictates the point at which the condition is cleared.

**Important** This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**

MME

ePDG

**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**

**congestion-control threshold tolerance { critical** *percent* **| major** *percent* **| minor** *percent* **}**
**default congestion-control threshold system-cpu-utilization**

**default congestion-control threshold tolerance**

Sets all threshold tolerances to the default values.

**critical *percent***

Default: 10

The tolerance percentage for critical thresholds. When a critical threshold drops below this level, the condition is cleared.

*percent* can be configured to any integer value from 0 to 100.

**major *percent***

Default: 0

The tolerance percentage for major thresholds. When a major threshold drops below this level, the condition is cleared.

*percent* can be configured to any integer value from 0 to 100.

**minor *percent***

Default: 0

The tolerance percentage for minor thresholds. When a minor threshold drops below this level, the condition is cleared.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the tolerance limits for critical, major and minor thresholds.

The tolerance parameter establishes the threshold at which the condition is cleared. An SNMP trap (starCongestionClear) is generated for the clear condition.

This command requires a valid product license.

### Example

The following command configures the tolerance level of 5% for minor thresholds.

```
congestion-control threshold tolerance minor 5
```

This setting will remain in configuration unless you specify another tolerance for minor thresholds in place of 5.

The following command returns the critical, major, and minor threshold tolerance levels to their default values:

```
default congestion-control threshold tolerance
```

# connectedapps

Enables the configuration of Connected Apps (CA) client communication with the IOS-XR CA server on an ASR 9000. This command sends you to the Connected Apps Configuration mode.

**Product** SecGW (WSG)

**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** **connectedapps**

**Usage Guidelines** Use this command to go to the Connected Apps Configuration mode. In this mode you can set CA client session parameters and ASR 9000 VSM High Availability (HA) chassis and network modes.

### Example

The following command sends you to the Connected Apps Configuration mode:

```
connnectedapps
```

# content-filtering category database directory

This command configures the base directory to be used for storing all content-rating databases that are required for Category-based Content Filtering application.

**Product** CF

**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**

**content-filtering category database directory path** *directory_path*
**default content-filtering category database directory path**

**default**

Specifies the default base directory and directory path for Category-based Content Filtering application.

***directory_path***

Default: /pcmcia1/cf

Specifies the base directory and its path to store all of the full or incremental content rating databases for the Category-based Content Filtering application.

*directory_path* must be an alphanumeric string of 1 through 255 characters.

**Usage Guidelines**

Use this command to specify the directory and its path to download all full or incremental category-rating databases to be used for the Category-based Content Filtering application.

Merging of incremental database can be done as part of the database upgrade process preformed with **upgrade content-filtering category database** command in the Executive Mode.

**Example**

The following command configures the */flash/cf_temp/DB* as the base directory to download all full and incremental content-rating databases for content filtering application.

```
content-filtering category database directory path /flash/cf_temp/DB
```

# content-filtering category database max-versions

This command configures the number of full content-rating databases to maintain/archive in the base directory for category-based content filtering application.

**Product**

CF

**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**

**content-filtering category database max-versions** *num_archive*
**default content-filtering category database max-versions**

**default**

Sets the default number of full databases for specified directory path/location.

***num_archive***

Default: 2

Specifies the maximum number of database to be archived or maintained in the specific location.

*num_archive* must be an integer from 1 through 3.

**Usage Guidelines**

Use this command to set the number of full content-rating database to be maintained in the specified directory path with the base file name specified using the **content-filtering database override file** command. The specified directory path is the location specified using the **content-filtering category database directory path** command.

**Example**

The following command configures the system to maintain *3* full content-rating databases for category-based content filtering application.

```
content-filtering category database max-versions 3
```

# content-filtering category database override

This command specifies the name of a file to be used by the category-rating database load process for category-based content filtering application.

**Product**

CF

**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**

**content-filtering category database override file** *file_name.extension*
**default content-filtering category database override file**

**default**

Sets the default content rating database file name; for example, optcmd.bin.

**file *file_name.extension***

Specifies the header of the file in the database directory path location to determine the newest full database.

*file_name* must be an alphanumeric string of up to 10 characters with an extension of 3 characters after a period (.) as *extension*.

**Usage Guidelines**

Use this command to configure the category-rating database file name to determine the newest version of full database. A process called "**LOAD_DATABASE**" invokes during the system startup or the database upgrade process by **upgrade content-filtering category database** command in Executive Mode. This process examines the header of each of the files in the database folder specified by **content-filtering category directory path** command in this mode.

Note that by default system examines the header of those files only which begins with the string "OPTCMDB" and having extension ".bin".

**Example**

The following command configures the system to examine the header of files that begins with *CF_sta.DB* only for content filtering application.

```
content-filtering category database override file CF_sta.DB
```

# context

Creates or specifies an existing StarOS context and enters the Context 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**

```
context context_name [ -noconfirm ]
no context context_name
```

**no**

Removes the specified context from the configuration.

***name***

Specifies the name of a context to enter, add, or remove. When creating a new context, the context name must be unique.

**Important** When creating a new context, the *context_name* specified must not conflict with the name of any existing context or domain names.

**-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 remove a specified context and enter the COntext configuration mode.

**Important** You can create a maximum of 64 contexts.

**Example**

The following command creates a context named *sampleContext*:

```
context sampleContext
```

# crash enable

Enables or disables the copying of crash data to a specified location.

**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**

```
crash enable { async-core-transfer | critical-task-core | [ encrypted ]
url crash_url [ filename-pattern pattern ] [ restrict mbyte ] [ rotate num_cores
 ] }
```

```
no crash enable { async-core-transfer | critical-task-core | url }
```

**no**

Disables the specified option.

**Important** System crash information is generated and stored in the crash list even when the **no** keyword is specified. The information maintained in the crash lists is minimal crash information when the **no** keyword has been specified.

**async-core-transfer**

Maintains the transfer of the core dump to the management card while asynchronously beginning proclet recovery which can reduce the total outage. This feature is enabled by default.

**Important** When a proclet crashes, a minimum 10% of the available total memory must be free in the CPU to start a new or rename the standby proclet.

**critical-task-core**

Limits core collections from critical task on the active management card. This feature is enabled by default.

**encrypted**

Indicates that the URL is encrypted for security reasons.

**filename-pattern *pattern***

Specifies an alphanumeric string containing any or all of the following variables:

- *%hostname%* - The system hostname
- *%ip%* - A SPIO IP address
- *%cpu%* - CPU number
- *%card%* - Card number
- *%time%* - POSIX timestamp in hexadecimal notation
- *%filename%* - Alias for *crash-%card%-%cpu%-%time-core%*
- *%%* - A single *%* sign

If no pattern is specified, the result is the same as the pattern *filename*.

Use '/' characters in the filename pattern part to store crashes in per-system subdirectories.

**url *crash_url***

Specifies the location to store crash files. *crash_url* may refer to a local or a remote file. *crash_url* must be entered using the following format:

For the ASR 5500:

- **[ file: ]{/flash|/usb1|/hd}[***/directory***]/**
- **tftp://{***host***[:***port#***]}[***/directory***]/**
- **[ ftp:| sftp: ]//[***username***[:***password***]@] {***host***}[***:port#***][/***directory***]/**

**Important** Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

**Important** Support for FTP is disabled in release 20 and higher Trusted builds.

*directory* is the directory name.

*filename* is the actual file of interest.

*username* is the user to be authenticated.

*password* is the password to use for authentication.

*host* is the IP address or host name of the server.

*port#* is the logical port number that the communication protocol is to use.

**restrict *mbyte***

Specifies a maximum amount of memory (in megabytes) to use for storing crash files as an integer from 1 to 128.

The **restrict** keyword is only applicable to local URLs.

Default: 128

**rotate *num_cores***

Specifies the number of core dumps to retain on the local storage. *num_cores* must be an integer from 1 to 256.

Default: 15

**Usage Guidelines** Enable crashes if there are systems that are not stable and the crash information will be useful for trouble shooting. The remote storage of the crash file reduces the memory utilized on the chassis.

**Example**

The following command saves a maximum of 64 megabytes of crash data to the /flash drive:

```
crash enable url /flash/pub/data/crash.dmp restrict 64
```

# crypto blacklist file

Configures a blacklist (access denied) file to be used by a Wireless Security Gateway (WSG).

**Product** All products supporting IPSec blacklisting

**Important** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege** Security Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**crypto blacklist file** *pathname*
**no crypto blackilist file**

**no**

Removes the blacklist file from the system.

***pathname***

Specifies the location of the blacklist file as:

- **[ file: ]{/flash|/usb1|/hd-raid}[***/directory***]/***<filename>*
- **tftp://{***host***[:***port#***]}[***/directory***]/***<filename>*
- **[ ftp: | sftp: ]//[***username***[:***password***]@] {***host***}[***:port#***][***/directory***]/***<filename>*
- **http://[***<username>***[:***<password>***]@]***<host>***[:***<port>***][***/<directory>***]/***<filename>*

**Usage Guidelines**

Use this command to configure the location of the blacklist file to be used by a WSG.

A blacklist is a list or register of entities that are being denied a particular privilege, service, mobility, access or recognition. With blacklisting, any peer is allowed to connect as long as it does not appear in the list.

Each entry in the blacklist file should contain the ID type so that the validation is performed for that ID type. In every entry, the ID type and ID value should be separated by a space. Only DOS and UNIX file formatting are supported. For additional information, refer to the *System Administration Guide*.

**Important** Either a blacklist, a whitelist or none is configured. Both listing techniques cannot be used simultaneously on the system.

**Example**

The following command specifies the use of a crypto backlist file on the /flash drive:

```
crypto blacklist file /flash/pub/data/blacklist.txt
```

# crypto peer-list

Enables an SecGW to initiate an IKEv2 session setup request when the peer does not initiate a setup request within a specified time interval. Executing this command moves you to the Peer List Configuration mode. This functionality is only applicable for site-to-site (S2S) based tunnels within a WSG service. For remote access tunnels the peer is always the initiator. (VPC-VSM only)

**Product**

SecGW (WSG)

**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 ] crypto peer-list { ipv4 | ipv6 }`** *`peer_list_name`*

**no**

Disables the specified crypto peer list.

***peer_list_name***

Specifies the name of the peer list as an alphanumeric string of one through 32 characters.

**Usage Guidelines**

Use this command to enable an SecGW to initiate an IKEv2 session setup request when the peer does not initiate a setup request within a specified time interval. Executing this command moves you to the Peer List Configuration mode. This functionality is only applicable for site-to-site (S2S) based tunnels within a WSG service. For remote access tunnels the peer is always the initiator. (VPC-VSM only)

The following restrictions apply when configuring an SecGW as an Initiator:

- The **peer-list** *peer_list_name* command is only executed if the deployment mode for WSG service is **site-to-site**, and the bind address type matches with the peer list address type (IPv4 or IPv6).
- You cannot change the WSG service deployment-mode if **peer-list** *peer_list_name* is enabled under the service. You will be prompted to remove the peer list before changing the mode.
- A maximum of 1,000 peer IP addresses can be added to the peer list via the Peer List Configuration mode **address** command.
- WSG service address binding is not allowed if a peer list is configured and both address types do not match. An error message is generated if they do not match.
- An IPv4 or IPv6 peer list cannot be modified if **peer-list** *peer_list_name* is enabled under the WSG service.

When a peer list has been configured in the WSG service, the initiator and responder mode timer intervals each default to 10 seconds. The SecGW will wait for 10 seconds in the responder mode for a peer session initiation request before switching to the initiator mode and waiting 10 seconds for a peer response.

You can change the default settings for the initiator and/or responder mode intervals using the WSG Service Configuration mode **initiator-mode-duration** and **responder-mode-duration** commands.

For additional information, refer to the *Peer List Configuration Mode Commands* and *WSG Service Configuration Mode Commands* chapters of this guide. Also see the *Security Gateway as Initiator* chapter in the *IPSec Reference*.

### Example

The following command enables SecGW as an Initiator functionality and creates an IPv4 peer list named *peer1*.

```
crypto peer-list ipv4 peer1
```

# crypto remote-secret-list

Specifies the remote secret list for storing remote secrets based on the ID type. This command sends you to the Remote Secret List Configuration mode. Only one active remote-secret-list is supported per system.

**Product**

All products supporting IPSec remote secrets

**Important** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

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 ] crypto remote-secret-list`** *`listname`*

**no**

Deletes the remote-secret-list file from the system.

**Important** You must unbind the remote-secret-list from any crypto maps or templates before it can be deleted.

***listname***

Specifies the name of the remote secret list as an alphanumeric string from 1 to 127 characters.

**Usage Guidelines**

Use this command to specify the remote secret list for storing remote secrets based on the ID type. Only one remote-secret-list can be configured per system. Executing this command places you in the Remote Secret List Configuration mode.

This list of remote pre-shared keys is based on the remote ID type. The remote secret list can contain up to 1000 entries.

For additional information, refer to the *Remote Secret List Configuration Commands* chapter and the *System Administration Guide*.

**Example**

The following command creates a remote-secret-list named *rs-list*:

```
crypto remote-secret-list rs-list
```

# crypto whitelist file

Configures a whitelist (access permitted) file to be used by a Wireless Security Gateway (WSG).

**Product**

All products supporting IPSec whitelisting

**Important** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

**Syntax Description**

**crypto whitelist file** *pathname* **[ -noconfirm ]**
**no crypto whitelist file**

**no**

Removes the blacklist file from the system.

***pathname***

Specifies the location of the whitelist file as:

- **[ file: ]{/flash|/usb1|/hd-raid}[**/*directory*]/<*filename*>
- **tftp:**//{*host*[**:***port#*]}[/*directory*]/<*filename*>
- **[ ftp: | sftp: ]**//[*username*[**:***password*]**@]** {*host*}[*:port#*]**[**/*directory*]/<*filename*>
- **http://[**<*username*>**[:**<*password*>**]@]**<*host*>**[:**<*port*>**]**[/<*directory*>]/<*filename*>

**Usage Guidelines**

Use this command to configure the location of the white file to be used by a WSG.

A whitelist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With whitelisting, no peer is allowed to connect unless it appears in the list.

Each entry in the whitelist file should contain the ID type so that the validation is performed for that ID type. In every entry, the ID type and ID value should be separated by a space. Only DOS and UNIX file formatting are supported. For additional information, refer to the *System Administration Guide*.

**Important** Usually either a blacklist, a whitelist or none is configured. Both listing techniques cannot be used simultaneously on the system.

### Example

The following command specifies the use of a crypto whitelist stored on the /flash drive.

```
crypto whitelist file /flash/pub/data/whitelist.txt
```

# cs-network

**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.

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

**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**

**cs-network** *cs_instance* **[ -noconfirm ]**
**no cs-network** *cs_instance*

**no**

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

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

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

***cs_instance***

Specifies the name of the Circuit Switched Core Networks instance which needs to be associated with the HNB Radio Network PLMN via the HNB RN-PLMN Configuration mode. If *cs_instance* does not refer to an existing HNB-PS network instance, the new HNB-CS network instance is created.

*cs_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-CS Network Configuration mode for an existing CS network instance or for a newly defined HNB-CS network instance. This command is also used to remove an existing HNB-CS network instance.

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

A maximum of one HNB-CS network instance per HNB-GW service 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 cannot access MSC(s) in CS core network without this configuration. Any change to this configuration would lead to disruption in HNB access to CS core network.

Entering this command results in the following prompt:

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

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

**Example**

The following command enters the existing HNB-CS Network configuration mode (or creates it if it does not already exist) for the instance named *hnb-cs1*:

```
cs-network hnb-cs1
```

The following command will remove HNB-CS network instance *hnb-cs1* from the system without any warning to operator:

```
no cs-network hnb-cs1
```

# css acsmgr-selection-attempts

This is a restricted command. In 9.0 and later releases this command is obsolete.

# css delivery-sequence

This is a restricted command. In 9.0 and later releases this command is obsolete.

# css service

This is a restricted command. In 9.0 and later releases this command is obsolete.

# decor-profile

This command allows you to create a DECOR profile, which represents a Dedicated Core Network (DCN) deployed by the operator.

**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**

**`[ no ] decor-profile`** *`profile_name`* **`[ -noconfirm ]`**

**no**

Removes the specified DECOR profile from the Global Configuration.

**decor-profile *profile_name***

**decor-profile** *profile_name*: Configures the Dedicated Core Network as deployed by operator. *profile_name* must be an alphanumeric string of 1 through 63 characters.

If the named decor-profile does not exist, it is created, and the CLI mode changes to the Decor Profile Configuration Mode. If the named decor-profile already exists, the CLI mode changes to the Decor Profile Configuration Mode.

**-noconfirm**

Specifies that the command must execute without any additional prompt and confirmation from the user.

**Usage Guidelines**

Use this configuration to configure a DECOR profile. A decor-profile without any ue-usage-types configuration is treated as a Common Core Network.

On entering the **decor-profile** *profile_name* command, the CLI prompt changes to:

[*context_name*]*host_name*(config-decor-profile-*profile_name*)#

**Example**

The following command creates a DECOR profile named *dp1*:

**`decor-profile dp1`**

# dedicated-li context

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

# default transaction-rate

Sets the **transaction-rate bucket-interval** and **nw-initiated-setup-teardown-events qci** commands to their default settings.

**Product**

ePDG

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**

**default transaction-rate**

**default transaction-rate**

Sets the transaction rate key performance indicator (KPI) settings to their default settings. These settings include **transaction-rate bucket-interval** and **nw-initiated-setup-teardown-events qci**.

The default setting for **transaction-rate bucket-interval** is 2 minutes.

The default setting for **nw-initiated-setup-teardown-events qci** specifies that all qci values are to be tracked for network initiated setup/tear down events.

**Usage Guidelines**

Use this command to return transaction rate KPI settings to their default value.

The **transaction-rate bucket-interval** setting configures the transaction rate KPI session events per second value. These KPIs have been implemented to assist operators in measuring the signaling load on the P-GW. These KPIs include total session events per second, successful session events per second, and unsuccessful session events per second.

The **nw-initiated-setup-teardown-events qci** setting assists operators in measuring the Voice-over-LTE (VoLTE) call setup and tear down events rate at the P-GW/ePDG. Both Create Bearer Requests (CBReqs) and Delete Bearer Requests (DBReqs) originally initiated by the P-GW and CBReqs and DBReqs initiated by the P-GW as a result of Home Subscriber Server (HSS)- and User Equipment (UE)- initiated events are accounted for in these KPIs.

For more information, refer to the descriptions for the **transaction-rate bucket-interval** and **nw-initiated-setup-teardown-events qci** commands in the *Global Configuration Mode Commands* section of this CLI Reference.

### Example

The following command returns the transaction rate KPI settings to their default values.

```
default transaction-rate
```

# diameter dynamic-dictionary

This command allows configuring a Diameter dictionary dynamically at run time, and then loading the dynamic dictionary in to the system.

**Important** The maximum number of dynamic dictionaries that can be loaded in to the system is 10.

**Product**

GGSN

HA

HSGW

IPSG

PDSN

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**

```
diameter dynamic-dictionary name url
no diameter dynamic-dictionary name
```

**no**

Unloads the specified dynamic Diameter dictionary from the system.

***name***

Specifies the name of the dynamic Diameter dictionary as an alphanumeric string of 1 through 15 characters.

***url***

Specifies the URL of the Diameter dictionary to be loaded in to the system. The input must be an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

This command is used to define a new Diameter dictionary on the fly, and load the dynamic dictionary in to the system.

To perform this configuration, you should first create a text file in ABNF format and configure all the required Diameter AVPs and command codes in the file. Then, save the file in flash or some URL that will be accessible by the system.

Now, configure a dynamic dictionary with an unique name and map it to the URL of the file to be loaded dynamically in to the system at the global configuration level.

When the names of the dynamic dictionaries and their URLs are configured, the corresponding files at the respective URLs are parsed and populated in all SessMgr and AAAmgr facilities as new dictionaries and kept available to be used when these dictionary names are configured under any Diameter application level or AAA group.

When a dynamic dictionary name is configured under an application such as IMS authorization service or in a AAA group, the corresponding dictionary (which is already loaded in SessMgrs and AAAMgrs) entry will be used.

There will be only one instance of a dynamic dictionary loaded in to a task for one dynamic dictionary name even if the same dictionary name is configured in multiple AAA groups or multiple application configurations. That is, even if the same dictionary name is configured in several applications or several AAA groups, all these applications and AAA groups will refer to the same dynamic dictionary instance.

**Example**

The following command configures a Diameter dictionary named *dyn1* and loads this dictionary to */flash/diameter_custom1.sndd* path:

```
diameter dynamic-dictionary dyn1 /flash/diameter_custom1.sndd
```

# diameter-host-template

Specifies the name of a Diameter host template and enters the Diameter Host Select mode. A Diameter host template is a table of peer servers that can be shared by multiple services.

**Product**

GGSN

HA

HSGW

IPSG

PDSN

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**

**diameter-host-template** *name* **[ -noconfirm ]**
**no diameter-host-template** *name*

**no**

Removes the specified Diameter host template from the Global Configuration.

***name***

Specifies the name of the template as an alphanumeric string of 1 through 63 characters.

**[ -noconfirm ]**

Executes the command without prompting for further input from the user.

**Usage Guidelines**

Specifies the name of a new or existing Diameter host template and opens the Diameter Host Select mode. You can configure up to 256 templates on the system.

To use the template, Diameter applications must be associated with the template. When an association is made to the template, the system selects the Diameter peer to be contacted based on rows configured in the table and the algorithm configured for selecting rows in the table.

**Important** Currently, only Gx service can be associated with the template.

If more than one service is using the same set of **peer-select** commands, then it is better to define all the peer selection CLIs in the template and associate the services to the template.

Entering this command results in the following prompt:

```
[context_name]hostname(config-host-template)#
```

Diameter host select configuration commands are defined in the *Diameter Host Select Configuration Mode Commands* chapter.

**Example**

The following command specifies a Diameter host template named *diamtemplate*:

**diameter-host-template diamtemplate**

# diameter-proxy conn-audit

This command enables the Diameter proxy Peer Connection Status Audit with Diabase clients.

**Product**

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**

**diameter-proxy conn-audit interval** *1-10*
**default diameter-proxy conn-audit**

**default**

Configures the default setting.

By default, Diameter proxy Peer Connection Status Audit with Diabase clients is disabled.

**diameter-proxy**

Specifies the Diameter proxy related configurations.

**conn-audit**

Specifies the periodic connection status audit processes. Disabled by default.

**interval *1-10***

Specifies the connection status audit interval in minutes, in the range of 1 through 10. Recommended value is 2 minutes.

**Usage Guidelines**

Enabling Diamproxy Peer Connection Status Audit with Diabase clients might affect performance of the services using Diameter interface. Service is impacted only when auto-correction happens (due to mismatch) and the cases are:

1. When Diabase state is IDLE and Diameter proxy is OPEN.
2. When Diabase state is OPEN and Diameter proxy is IDLE.

In both these cases, Diabase corrects the connection status based on information received in audit message. Diameter messaging failures is avoided once Diabase corrects the connection status.

**Example**

The following command specifies that the connection status audit interval is *2*minutes:

**diameter-proxy conn-audit interval 2**

# diameter-proxy ram-disk

This command configures the amount of extra RAM disk space in MB to be allocated to Diamproxy task when local storage (hard disk) is enabled.

**Product**

HSGW

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**

**diameter-proxy ram-disk mb** *space_mb*
**default diameter-proxy ram-disk mb**

**default**

Configures the default setting.

Default: 32 MB

**mb space_mb**

Specifies the storage space in MB.

*space_mb* must be an integer from 10 through 256.

**Usage Guidelines**

Specifies the additional storage space to be allocated to Diamproxy for file write, in MB. The specified memory in MB is added to the existing memory allocated to Diamproxy only if HDD storage is enabled. By default, 32 MB is additionally allocated.

**Example**

The following command specifies that *100* MB of additional storage space be allocated to the Diamproxy task:

**diameter-proxy ram-disk mb 100**

# do show

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

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

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

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

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

# ecmp-lag hash

**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.

This command provides the configuration to select source Boxer Internal Address (SBIA) as the input to the hashing function for ECMP-LAG distribution.

**Product** 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**

```
[no] ecmp-lag hash use-sbia-only
```

**no**

Disables the hashing function selection and sets the system to use IP Source Address, IP Destination Address, IP Protocol and Source BIA as inputs to the hashing algorithm for ECMP-LAG distribution.

**Usage Guidelines** Use this command to allow the operator to change the way hashing works in deciding which link to use for ECMP and Link Aggregation. In the default hashing algorithm the IP Source Address, IP Destination Address, IP Protocol and Source BIA are used in the hashing function. When "use-sbia-only" option is selected, only the Source BIA is used in the hashing function.

**Caution** When using ECMP-LAG on a HNB-GW, this configuration is **mandatory** for standalone HNB-GW deployment and highly recommended in other deployment scenarios where HNB-GW is used in combination with other services.

### Example

The following command enables the SBIA as input to hash function for ECMP-LAG on the HNB-GW:

```
ecmp-lag hash use-sbia-only
```

The following commands sets the hashing function to use standard inputs for ECMP-LAG on HNB-GW:

```
no ecmp-lag hash use-sbia-only
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

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

# enforce imsi-min equivalence

Enables the PDSN/HA to treat IMSI and MIN as the same for identifying the PDSN/HA session.

**Product** PDSN

HA

**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 ] enforce imsi-min equivalence
```

**default**

Returns the command to its default setting of disabled.

**no**

Disables the PDSN/HA from treating IMSI and MIN as the same for identifying the PDSN/HA session.

**Usage Guidelines**

Generally on an HA, the IMSI and MIN are treated as different and hence the RRQs with 1x and DO PDSNs are processed as different sessions. You can use this feature to treat the IMSI and MIN with the matching lower 10-digit as the same for identifying a session. The 10-digit MIN and the 15-digit IMSI are treated as equivalent for the purpose of matching sessions if the lower 10 digits are the same. Any handoff from 1x to DO or vice-versa is treated as the same session if the NAI and HoA also match. If the NAI and/or HoA do not match, then the duplicate IMSI session detect and terminate feature is applicable.

Generally on a PDSN, the IMSI and MIN are treated as different and hence RP messages from 1x and DO PDSNs are processed as different sessions. You can use this feature to treat the IMSI and MIN with the matching lower 10-digit as the same for identifying a session. The 10-digit MIN and the 15-digit IMSI are treated as equivalent for the purpose of matching PDSN sessions if the lower 10 digits are the same. Any handoff from 1x to DO or vice-versa is treated as the same session.

**Example**

To monitor or clear subscriber session information filtered by on IMSI/MIN refer to the **show subscribers msid** command.

**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 the treatment of the IMSI and MIN as the same for identifying the session:

```
enforce imsi-min equivalence
```

Either of the following commands disables the treatment of the IMSI and MIN as the same for identifying sessions:

```
no enforce imsi-min equivalence
default enforce imsi-min equivalence
```

# enforce spof

Disables XGLC SPOF alarms when port redundancy is supported at Layer 2 via a Link Aggregation Group (LAG) on an ASR 5000.

**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 ] enforce spof suppress-xglc-lag**

**no**

Enables XGLC SPOF alarms if they have previously been disabled.

**suppress-xglc-lag**

Disables XGLC SPOF alarms if redundancy is configured via LAG.

**Usage Guidelines**

An XGLC that has not been configured for horizontal port redundancy with an adjacent XGLC constitutes a Single Point of Failure (SPOF). If the card or a port fails, service is disrupted and data is lost until the card is replaced.

Link-aggregation can be configured to support port redundancy across non-redundant XGLCs by combining multiple physical ports together to create a single high-bandwidth data path. Sharing load across the member ports enhances connection reliability.

When XGLC ports are part of a LAG group, failure of a single port in the group will not result in data outage; the data will be rerouted through other available links. An individual port that is part of a LAG group does not constitute a SPOF.

**enforce spof suppress-xglc-lag** disables XGLC SPOF alarms if redundancy is configured via LAG.

**no enforce spof suppress-xglc-lag** enables XGLC SPOF alarms if they have been previously suppressed.

**Important** With SPOF alarming suppressed, a port in a LAG group will trigger a SPOF alarm if it is the only available distributing port in the LAG group.

**Example**

To disable XGLC SPOF alarming for Layer 2 LAG redundancy enter the following command:

```
enforce spof suppress-xglc-lag
```

# exit

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description** **exit**

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

# fa-spi-list

Replaces a duplicate Foreign Agent- Security Parameter Index (FA-SPI) remote address list applied to multiple FA services with a list name.

**Product** PDSN

FA

**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 ] fa-spi-list** *fa_spi_list*

**no**

Disables this feature.

***fa_spi_list***

Remote address list name expressed as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines** Use this command to Replace duplicate FA-SPI remote address list applied to multiple FA or HA services with a list name.

**Example**

The following command configures the list FA SPI list to *fa-list2*:

**fa-spi-list fa-list2**

# fabric egress drop-threshold

Enables or disables the generation of a syslog event message when the number of egress Fabric Access Processor (FAP) packet drops exceeds a set threshold within a window of time on an ASR 5500.

**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**

**fabric egress drop-threshold { disable | enable count** *number* **interval-secs** *seconds* **}**

**disable**

Disables the egress dropped-packet threshold settings. Settings are disabled by default.

**enable**

Enables the specified egress dropped-packet threshold settings. Settings are disabled by default.

**count *number***

Specifies the maximum number of egress traffic packets that can be dropped before a syslog event message is generated. The count is specified as an integer from 10 to 5000.

**interval-secs *seconds***

Specifies the time interval (window) within which the maximum egress packet drop count can be exceeded. The interval is specified in seconds as an integer from 30 to 600.

**Usage Guidelines**

Use this command to enable or disable the generation of a syslog event message when the number of egress FAP packet drops exceeds a set threshold within a window of time on an ASR 5500.

When the threshold is exceed, the syslog event message is generated once, until the condition clears. Only then will it be generated again.

By default this feature is disabled.

**Example**

The following command sets the egress FAP dropped-packet threshold at 2000 packets within a 60-second window:

```
fabric egress drop-threshold enable count 2000 interval-secs 60
```

# fabric fsc-auto-recovery

Enables or disables Fabric Storage Card (FSC) fabric recovery via automatic resets on the ASR 5500.

**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**

**fabric fsc-auto-recovery { disable | enable } [ max-attempts [** *number_attempts* **| unlimited ] ]**

**{ disable | enable }**

**Disable** turns off the automatic FSC recovery feature.

**Enable** turns on the automatic FSC recovery feature. When enabled the FSC will initiate auto recovery/reset upon detecting an excessive number of discarded fabric egress (EGQ) packets.

**[ max-attempts [** ***number_attempts*** **| unlimited ]**

Specifies how many times StarOS will attempt to reset each FSC as an integer from 1 to 99 or unlimited (will not stop until FSC is reset). Default is 1.

**Usage Guidelines**

Use this command to enable or disable automatic FSC auto recovery/reset in the ASR 5500 upon detecting an excessive number of discarded egress packets. You can optionally specify the maximum number of reset attempts; the default is 1.

**Important** To enable this feature, you must first configure the Fabric Egress Drop Threshold via the Global Configuration mode **fabric egress drop-threshold** command.

**Example**

The following command enables FSC automatic recovery with a maximum of 50 attempts.

```
fabric fsc-auto-recovery enable max-attempts 50
```

# failure-handling-template

This command allows the user to create/modify/delete a Diameter failure handling template at the global configuration level. This command specifies the name of failure handling template and enters the Failure Handling Template mode. The users can define the failure handling configurations within this template.

**Important** A maximum of 64 templates can be configured on the system.

**Product**

GGSN

HA

HSGW

IPSG

PDSN

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**

**failure-handling-template** *name* **[ -noconfirm ]**
**no failure-handling-template** *name*

**no**

Removes the specified failure handling template from the Global Configuration.

***name***

Specifies the name of the failure handling template as an alphanumeric string of 1 through 63 characters.

**[ -noconfirm ]**

Executes the command without prompting for further input from the user.

**Usage Guidelines**

Specifies the name of a new or existing failure handling template and opens the Failure Handling Template mode. Depending on which application is using the failure handling template, some of the syntactically possible configurations within the template are not applicable.

To use the template, Diameter applications must be associated with the template. When an association is made to the template, in the event of a failure, the system takes the action as defined in the failure handling template. Both IMS Authorization (Gx) and Diameter Credit Control Application (DCCA) (Gy) services can be associated with the template.

Entering this command results in the following prompt:

```
[context_name]hostname(config-fh-template)#
```

Failure handling template configuration commands are defined in the *Diameter Failure Handling Template Configuration Mode Commands* chapter.

**Example**

The following command specifies a failure handling template named *FHtemplate*:

```
failure-handling-template FHtemplate
```

# fast-data-plane-convergence

Enables and disables fast MIO failure detection and switchover for existing sessions.

**Product**

All (ASR 5500 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**

**[ no ] fast-data-plane-convergence**

**no**

Disables this feature.

**Usage Guidelines**

You can enable this feature to minimize traffic disruption for existing sessions during MIO/UMIO failover.

For maximum benefit, this feature assumes deployment of an Active-Active LAG configuration with aggressive MicroBFD timers. This feature can be enabled with an Active-Standby LAG configuration, however, reduced switchover time cannot be guaranteed.

**Important** Active-Active LAG groups must be configured, along with aggressive microBFD timers (such as 150*3). During MIO card recovery BGP Sessions might flap based on the configuration. To avoid traffic loss during these events, BGP graceful restart must be configured with proper hold/keepalive and restart timers. See the description of the **bgp graceful-restart** command in the *BGP Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

### Example

The following command enables faster recovery of existing sessions during MIO/UMIO failover:

**fast-data-plane-convergence**

# global-title-translation address-map

Creates an instance of a Global Title Translation (GTT) address-map, a database, for global titles (ISDN-type address) used for SCCP routing. Upon creating the instance, the system enters global title translation address-map configuration mode. For the commands to configure the database, go to the *Global Title Translation Address-Map Configuration Mode Commands* chapter.

**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 ] global-title-translation address-map instance`** *`instance`*

**no**

Removes the specified GTT address-map database from the SCCP portion of the configuration.

***instance***

This value uniquely identifies a specific instance of a GTT address-map.

*instance* must be an integer from 1 through 4096.

**Usage Guidelines**

Create a GTT address map with a unique identifier and enter the GTT address-map configuration mode.

**Example**

The following command creates a GTT address map identified as *324*:

**`global-title-translation address-map instance 324`**

# global-title-translation association

Creates an instance of a Global Title Translation (GTT) association which defines the rules for handling global title translation. Upon creating the instance, the system enters global title translation association configuration mode. For the commands to configure the rules, go to the *Global Title Translation Association Configuration Mode Commands* chapter.

**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**

**`global-title-translation association instance`** *`instance`*
**`no global-title-translation association instance`** *`instance`*

**no**

Removes the specified instance of a GTT association from the SCCP portion of the configuration.

***instance***

This value uniquely identifies a specific instance of a GTT association.

*instance* must be an integer from 1 through 16.

**Usage Guidelines** Create a GTT association with a unique identifier and enter the GTT association configuration mode.

**Example**

The following command creates a GTT association identified as *2*:

```
global-title-translation association instance 2
```

# gtpc-load-control-profile

Creates a GTP-C Load Control Profile and enters GTP-C Load Control Configuration Mode.

**Product** P-GW

SAEGW

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** **`[ no ] gtpc-load-control-profile`** *profile_name*

**no**

Removes specified GTP-C Load Control Profile.

**gtpc-load-control-profile**

Creates a GTP-C Load Control Profile and enters GTP-C Load Control Profile Configuration Mode.

***profile_name***

Must be an alphanumeric string from 1 to 64 characters in length.

**Usage Guidelines** Use this command to create a GTP-C Load Control Profile and enter GTP-C Load Control Profile Configuration Mode

### Example

The following example creates a GTP-C Load Control Profile named LOADCTRL.

```
gtpc-load-control-profile  LOADCTRL
```

# gtpc-overload-control-profile

Creates a GTP-C Overload Control Profile and enters GTP-C Overload Control Profile Configuration Mode.

**Product**

P-GW

SAEGW

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**

**`[ no ] gtpc-overload-control-profile`** *`profile_name`*

**no**

Removes specified GTP-C Overload Control Profile.

**gtpc-overload-control-profile**

Creates a GTP-C Overload Control Profile with the specified profile name.

***profile_name***

Must be an alphanumeric string from 1 to 64 characters in length.

**Usage Guidelines**

Use this command to create a GTP-C Overload Control Profile and enter GTP-C Overload Control Profile Configuration Mode.

### Example

This example creates a GTP-C Overload Control Profile named OVERLOADCTRL

```
gtpc-overload-control-profile  OVERLOADCTRL
```

# gtpp compression-process

This command configures the maximum number of child compression processes that AAA proxy can have.

**Product**

GGSN

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**

**gtpp compression-process** *max_number*
**default gtpp compression-process**

**default**

Restores the system to the default settings for the number of child compression processes allowed.

***max_number***

Specifies the maximum number of child processes. The default is 1

*max_number:* must be an integer from 1 through 4.

**Usage Guidelines**

This command configures the maximum number of child compression processes that AAA proxy can have only if hard disk storage is enabled.

**Example**

```
gtpp compression-process 3
```

# gtpp push-to-active

This command enables/disables Push-To-Active feature to automatically transfer CDR files from new standby chassis to new active chassis when the ICSR switchover occurs.

**Product**

**Important** This CLI command is applicable only to GTPP groups having streaming mode.

GGSN

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**

**gtpp push-to-active [ encrypted ] url** *url* **via-context** *context_name*
**no gtpp push-to-active**

**no**

Disables Push-To-Active feature to automatically transfer CDR files from new standby chassis to new active chassis.

**[ encrypted ] url *url***

Specifies the peer chassis URL where the CDR files are to be transferred when the chassis becomes standby.

This keyword denotes the peer chassis URL in this format: sftp://user:password@host:[port]/hd-raid/records/cdr/. It accepts a string of size 1 through 1024.

**[ encrypted ]** - Indicates that the URL is encrypted for security reasons.

**via-context *context_name***

Specifies the name of the context through which the active chassis is reachable. *context name* must be an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**

During an ICSR switchover, the GTPP charging interface between the active chassis and CGF server goes down and all pending CDRs are written to internal hard disk. Once the chassis becomes standby, the CDRs will remain on HDD until the chassis becomes active.

This feature provides a way to move the stranded CDRs from the new standby chassis to the new active chassis and stream them to the OCG. This CLI command enables/disables the Push-To-Active feature to automatically transfer CDR files from new standby chassis to new active chassis.

Releases prior to 16.0, CDRs from current standby chassis were manually transferred to current active chassis using the CLI command "**gtpp storage-server streaming start**". Once the transfer is complete, a CLI command in the Exec mode is configured to stream the CDRs to CGF.

In 16.0 and later releases, the stranded CDRs in the standby ICSR node (moved from active to standby) are automatically transferred to the newly active ICSR node. This automation process is achieved through the use of "**gtpp push-to-active**" CLI command in the global configuration mode.

This feature could lead to duplicate CDRs. When streaming is in progress and ICSR switchover happens, the current file being streamed, will not complete the streaming as interface with CGF went down. This file will be transferred to new active chassis and streamed from beginning from new chassis.

In case AAAProxy restarts during file transfer, the file transfer statistics will not be accurate. The accounting contexts should be in same order in both the chassis. The directory names are created using vpn-id. If the accounting contexts are in different order, vpn-id will be different and the sub-directories in HDD will be different in both the chassis for same GTPP group.

### Example

The following command enables the Push-To-Active feature to automatically transfer CDR files from new standby chassis to new active chassis.:

```
gtpp push-to-active url sftp://user:password@host:5000 via-context aaa
```

# gtpp ram-disk-limit

This command configures additional storage space to be allocated for writing files.

**Product**

GGSN

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**

```
gtpp ram-disk-limit mb mega_bytes
default gtpp ram-disk-limit
```

#### default

Restores the system to the default settings of 32 MB of storage.

#### mb *mega_bytes*

Specifies the number of megabytes of storage allocated for files.

*mega_bytes:* must be an integer from 10 through 256. The default is 32 MB.

**Usage Guidelines**

The memory specified with this command would be added to the existing memory allocated to the AAA proxy only if hard disk storage is enabled.

### Example

```
gtpp ram-disk-limit mb 256
```

# gtpp single-source

Configures the system to reserve a CPU for performing a proxy function for accounting.

**Product**

ePDG

GGSN

SGSN

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**

```
gtpp single-source [ centralized-lrsn-creation | private-extensions ]
no gtpp single-source
```

#### centralized-lrsn-creation

Defines Log Record Sequence Number (LRSN) generation at proxy. The AAA proxy will generate the LRSN for all CDR types generated by either the GGSN or the SGSN.

Default: disabled

**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.

#### private-extensions

This optional keyword enables the proprietary use of customer-specific GTPP extensions.

If **private-extensions** is not configured, all customer specific private extensions related to GTPP message transfer with CGF and recovery through GSS are disabled.

**Important** In order for the customer-specific extensions to work properly, the **gtpp max-pdu-size** command in the Context Configuration Mode should be set to 65400 and the **gtpp server** command's **max** value should be set to "1".

**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.

**no**

Disables GTPP single-sourcing. This is the default setting.

**Caution** Entering this command while PDP contexts are in process could cause the loss of pending CDRs. The configuration must be saved and the chassis reloaded for this option to take effect.

## Usage Guidelines

When GTPP single-sourcing is enabled, the system's AAA proxy function generates requests to the accounting server using a single UDP source port number, instead of having each AAA Manager generate independent requests with unique UDP source port numbers. This is accomplished by the AAA Managers forwarding their GTPP PDUs to the AAA Proxy function that runs on a reserved packet processing card CPU. Since a packet processing card CPU is being reserved, fewer Session Managers and AAA Managers will be started on that card.

**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.

**Caution** This command must be entered prior to the configuration of other services. Specifying it later may return an error due to a lack of CPU availability.

### Example

The following command enables GTPP single-sourcing with the use of private GTPP extensions:

```
gtpp single-source private-extensions
```

The following command disables GTPP single-sourcing:

```
no gtpp single-source
```

# ha-spi-list

Replaces a duplicate Home Agent-Security Parameters Index (HA-SPI) remote address list applied to multiple HA services with a list name.

**Product**

PDSN

HA

**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**

**ha-spi-list** *ha_spi_list*

***ha_spi_list***

Remote address list name expressed as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Use this command to Replace duplicate HA-SPI remote address list applied to multiple HA services with a list name.

**Example**

The following command configures the list HA SPI list to *ha-list2*:

```
ha-spi-list ha-list2
```

# hd raid

Enters the HD RAID configuration mode, and performs RAID management operations on the platform's hard disk drives.

**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**

**hd raid**

**Usage Guidelines**

Use this command to configure RAID parameters. All HD RAID commands need confirmation unless the **-noconfirm** is included in the command.

RAID commands are needed to intervene in the following situations:

- The hard disk controller task cannot determine the correct operation.
- Administrative action is required by policy.
- The administrator wants to wipe an unused disk.

In an automated system, the policies created with this CLI address the possibility of a manually partitioned disk, a disk resulting from a different version of software, a partially constructed disk, or the case of two unrelated disks in the system.

To reduce administrator intervention, a set of policies can be configured to set the default action using the commands in the HD RAID configuration mode. These commands are described in the *HD Storage Policy Configuration Mode Commands* chapter of this guide.

**Caution** Use of the **hd raid** commands and keywords has the potential for deleting the contents of hard disk drives without the possibility of recovery. You should only use these commands under guidance from the Cisco Technical Assistance Center (TAC).

Entering this command results in the following prompt:

```
[context_name]hostname(config-hd-raid)#
```

HD RAID Configuration Mode commands are defined in the HD RAID Configuration Mode Commands chapter.

# hd storage-policy

Provides access to the local hard drive configuration mode in order to manage parameters supporting local storage of records.

**Product**

GGSN

SGSN

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**

**`[ no ] hd storage-policy`** *`name`*

**no**

Removes a configured HD storage policy from the system.

**storage-policy *name***

Specifies a name for an HD storage policy and then enters the HD Storage Policy Configuration Mode. *name* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Creates a new policy or specifies an existing policy and enters the HD Storage Policy Configuration Mode.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-hd-storage-policy)#

HD Storage Policy Configuration Mode commands are defined in the HD Storage Policy Configuration Mode Commands chapter.

**Example**

The following command creates an HD storage policy named *policy3* and enters the HD Storage Policy Configuration Mode:

**`hd storage-policy policy3`**

# health-monitoring

Configures Health Monitoring of Crypto Chip.

**Product**

ePDG

**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**

**`health-monitoring crypto-chip failure-threshold`** *`failure_threshold`*

**`nohealth-monitoring crypto-chip`**

***failure_threshold***

Configures the failure threshold of health-monitoring crypto-chip. This is failure packet threshold count between 100 and 4294967295. Default is 10000.

# high-availability

Configures the speed for detection of packet processing card task failures before switchover occurs.

**Product**

PDSN

GGSN

ASN-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**

*Releases prior to 21.8*

```
high-availability fault-detection speed { aggressive | normal }
default high-availability fault-detection speed
```

**Syntax Description**

*Release 21.8 and higher*

```
high-availability fault-detection [ speed { aggressive | normal } ] | [
card { dp-outage seconds | hb-loss value} ]
default high-availability fault-detection [ speed ] | [ card [ dp-outage
 |  hb-loss ] ]
```

**default**

- **speed**: Resets fault detection speed to normal.
- **card dp-outage**: Restores the default dp-outage value. The default value is 2 seconds.
- **card hb-loss**: Restores the heartbeat value only between the management and packet processing cards to the default value. The default value is 2 heartbeats.

**speed aggressive**

Specifies packet processing card failover should occur without performing additional checks.

**speed normal**

Specifies that packet processing card failover will only occur after additional checks have been performed performed. This is the default setting.

**card**

Specifies the packet processing card.

**dp-outage *seconds***

Configures the secondary card fault detection criteria in "seconds". The value of this parameter can range from 0 to 20 seconds. The default value is 2 seconds.

**hb-loss *value***

Configures the consecutive heartbeat loss threshold at which the non-responsive card (packet processing card) may be declared as failed. The supported value ranges from 2 to 20. The default value is 2 heartbeats.

## Usage Guidelines

Use the **high-availability fault-detection speed { aggressive | normal }** command to increase the fault detection speed for faster switchovers after a packet processing card task failure.

Setting fault detection speed to aggressive will trigger packet processing card failover as soon as possible if a potential failure is detected. Aggressive mode will reduce the duration of subscriber outages caused by a failed packet processing card if session recovery is enabled.

Aggressive mode also bypasses most information gathering steps and logs that can be used to determine the root cause of the failure.

In normal mode, additional checks are performed before triggering a packet processing card failover to ensure that the card has actually failed. In aggressive mode these checks are bypassed so that session recovery can start as soon as possible. These additional checks reduce the likelihood of a false positive failure.

Use the **high-availability fault-detection dp-outage** *seconds* command to configure configure a secondary fault detection criteria to be used with hb-loss. If Data Plane monitor packets from the packet processing card have arrived at the managment card within the most recent dp-outage seconds when the hb-loss threshold has been met, then card failure is deferred. This criteria is used to defer card failure for up to 5 additonal heartbeat losses. This command parameter is restricted to the Administrator access on the VPC- DI platform.

Use the **high-availability fault-detection card hb-loss** *value* command to define the number of consecutive one second heartbeat losses between the management card and a packet processing card at which the packet processing card is assumed to have failed. If not configured, the default for this parameter is 2. This command is supported for all products.

### Examples

The following command sets the fault detection speed for packet processing card tasks to **aggressive**:

```
high-availability fault-detection speed aggressive
```

The following command sets the secondary card fault detection criteria at 2 seconds:

```
high-availability fault-detection card dp-outage 2
```

The following command sets the fault detection for packet processing card tasks to 3 seconds:

```
high-availability fault-detection card hb-loss 3
```

# iftask boot-options

Enables or disables iftask boot-options configuration.

**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 ] iftask boot-options`**

**no**

If previously configured, disables the iftask boot-options configuration.

**Usage Guidelines** Use this commnad to enable or disable iftask boot-options configuration.

Entering this command results in the following prompt:

[local]hostname(config-iftask-boot-options)#

Refer to the *IFTask Boot-Options Configuration Mode Commands* chapter for additional information.

**Example**

The following command enables iftask boot-options configuration:

**`iftask boot-options`**

# iftask di-net-encrypt-rss

Configures Receive Side Scaling (RSS) for Distributed Instance Network (DI-net) encrypted traffic. This command applies only to VPC-DI.

**Product** All

**Privilege** Operator

**Command Modes** Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

**Syntax Description** **`[ no ] iftask di-net-encrypt-rss`**

**no**

Disables RSS for DI network encrypted traffic, which is the default setting.

**Usage Guidelines**

In releases prior to 21.7, RSS was enabled by default and could not be disabled. In 21.7 and later releases, this command can be used to enable RSS for DI network encrypted traffic. In 21.7 and later releases, RSS is disabled by default for DI network encrypted traffic.

The following example enabled RSS for DI network encrypted traffic:

```
iftask di-net-encrypt-rss
```

# iftask fullcore-enable

Configures iftask to collect full core dump with huge pages in the event of an iftask process failure. This command applies only to StarOS on virtualized platforms.

**Product**

All

**Privilege**

Operator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] iftask fullcore-enable
```

**no**

Disables collection of huge pages upon iftask process failure. When disabled, only the core dump is collected.

**Usage Guidelines**

In the event of an iftask process fault, the system dumps its core to /var/crash. The core file is then compressed and transferred to to the configured location [/flash/fullcores].

When this command is enabled, the core dump will include the huge pages.

This functionality is disabled by default.

**Note**

When this option is enabled, faulted iftask processes take approximately 2 minutes to dump the core. This will affect back-to-back iftask restart.

# iftask mcdmatxbatch

Configures multi-channel direct memory access (MCDMA) transmit batching. The MCDMA is the path from the IFTASK to the SESSMGR. This command applies only to StarOS on virtualized platforms.

**Product**

All

**Privilege**

Operator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] iftask mcdmatxbatch { burstsize`** *number_of_packets* **`| latency`** *milliseconds* **`}`**

**no**

Deletes the setting for iftask mcdmatxbatch.

**burstsize *number_of_packets***

Maximum packets per burst from 1 through 1024.

**latency *milliseconds***

Not currently supported.

**Usage Guidelines**

The following example sets the maximum number of packets per burst for MCDMA to 512:

```
iftask mcdmatxbatch burstsize 512
```

# iftask restart-enable

Configures iftask to restart automatically in case of iftask process failure. This command applies only to StarOS on virtualized platforms.

**Product**

All

**Privilege**

Operator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] iftask restart-enable`**

**no**

Disables automatic iftask restart

**Usage Guidelines**

This functionality is enabled by default (iftask will restart automatically if a failure occurs). It should only be disabled if iftask restart behavior is not operating as expected.

Refer to the **iftask fullcore-enable** command for more information about the steps taken in the event that the iftask process fails.

The following example disabled automatic iftask restart

```
no iftask restart-enable
```

# iftask sw-rss

Configures receive side scaling (RSS) so that the VPC distributes traffic flows across the available vCPU cores. This command applies only to StarOS on virtualized platforms.

**Product**

All

**Privilege**

Operator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
iftask sw-rss { comprehensive | supplemental }
```

**no**

Deletes the setting for iftask sw-rss. All traffic is routed to a single core, unless HW RSS is available on the hardware device.

**comprehensive**

Distributes all traffic received by the DPDK in the VPC. Use this option where the hardware does not support RSS.

In Release 21.6 and higher, L4 information is added to hash inputs for packet filtering (PF) with the following limitations:

For IPv4:

- TCP: IP source/destination and TCP ports source/destination are supported.
- TCP/UDP fragmented: only IP source/destination are supported.
- UDP non-fragmented and not GTPU (any port which does not equal 2152): IP source/destination and UDP port source/destination.
- UDP non-fragmented and GTPU (port 2152): IP source/destination and UDP port source/destination and GTP tunnel ID.
- Any other protocol: Default back to IP source/destination.

For IPv6, only L3 (IP source and destination) based hashing is supported.

**Note** The system automatically detects if packets belong to GTPU (port 2152) and hashes on the GTP tunnel ID.

**supplemental**

Distributes the traffic flow for protocols not supported by the hardware RSS. The traffic distribution is performed in addition to the distribution performed by the hardware device.

**Usage Guidelines**

The Cisco USC NIC supports hardware-based RSS; however RSS is only supported on IP traffic. For other network protocols, such as MPLS, GTP, L2TP, GRE and IPv6, all the traffic is routed into a single queue. The **iftask sw-rss** command enables the software to distribute the traffic to the available vCPU cores for processing, thus increasing resource utilization and providing improved throughput.

By default, RSS is disabled.

The following example enables RSS in addition to the supported hardware RSS functionality on the device:

```
iftask sw-rss supplemental
```

# iftask txbatch

Configures transmit batching. This command applies only to StarOS on virtualized platforms.

**Product**

All

**Privilege**

Operator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] iftask txbatch { burstsize** *number_of_packets* **| flush_latency | latency** *milliseconds* **}**

**no**

Deletes the setting for iftask txbatch.

**burstsize *number_of_packets***

Specifies the maximum number of packets from 1 through 1024 to accumulate in a vector before sending to the ethernet interface.

**latency *milliseconds***

Not currently supported.

**Usage Guidelines** Use this command to configure the transmit batching parameters for system-wide IFTASK operation.

The following example sets the maximum number of packets per burst for MCDMA to *512*:

```
iftask txbatch burstsize 512
```

The following example sets the maximum wait time to *1000* milliseconds to flush the bytes on the control port:

```
iftask txbatch flush_latency 1000
```

# ikesa delete on-mismatch

Enables IPSec to automatically remove existing IKEv1 and IKEv2 ACL tunnels when critical parameters are changed in the crypto map.

**Product** All products that support IPSec

**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** **ikesa delete on-mismatch**

**Usage Guidelines** Use this command to enable IPSec to automatically remove existing IKEv1 and IKEv2 ACL tunnels when critical parameters are changed in the crypto map. For more information, see the *IPSec Reference* guide.

**Important** As per ANSSI standards, this command cannot be removed once enabled. The configuration can be removed only by rebooting.

**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** Use this configuration only on Trusted builds.

### Example

The following command enables automatic removal of existing IKEv1 and IKEv2 ACL modes:

```
ikesa delete on-mismatch
```

# imei-profile

Creates an instance of an International Mobile Equipment Identity (IMEI) profile.

**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 ] imei-profile`** *imei_profile_name*

**no**

Deletes the IMEI profile instance from the configuration.

***imei_profile_name***

Specifies the name of the IMEI profile as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Use this command to create an instance of an IMEI profile and to enter the IMEI Profile Configuration mode. An IMEI profile is a template which groups a set of device instructions, such as blacklisting, that may be applicable to one or more calling devices. See the *IMEI Profile Configuration Mode Commands* chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

**Important**

An IMEI profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what IMEI profiles have already been created, return to the Exec mode and enter the **show imei-profile all** command.

### Example

The following command creates a configuration instance of an IMEI profile:

```
imei-profile imeiprof1
```

# imsi-group

This command configures the International Mobile Subscriber Identity (IMSI) 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**

**imsi-group** *group_name*

**imsi-group *group_name***

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

**Usage Guidelines**

Use this command to create the IMSI group. An IMSI group can contain up to 500 elements of either individual IMSI or range of IMSI numbers. Once an IMSI group is created, each group can be configured with up to 500 unique IMSI values. Multiple lines of IMSI and IMSI-range can be up to 20 lines per group.

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

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-imsi-group)#

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