Context Configuration Mode Commands S-Z

Command Modes

This section includes the commands **s102-service** through **wsg-service** service.

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

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

- s102-service, on page 2
- saegw-service, on page 3
- sbc-service, on page 4
- server, on page 5
- service-redundancy-protocol, on page 7
- session-event-module, on page 7
- sgsn-service, on page 8
- sgs-service, on page 9
- sgtp-service, on page 10
- sgw-service, on page 11
- sls-service, on page 12
- smsc-service, on page 13
- ssh, on page 15
- ssl, on page 16
- subscriber, on page 17
- sx-service, on page 18
- tac-profile, on page 19
- threshold available-ip-pool-group, on page 19
- threshold ha-service init-rrq-rcvd-rate, on page 21
- threshold ip-pool-free, on page 22
- threshold ip-pool-hold, on page 23
- threshold ip-pool-release, on page 24

- threshold ip-pool-used, on page 26
- threshold ip-pool-usable, on page 27
- threshold ip-pool-usable-final, on page 28
- threshold monitoring, on page 29
- threshold pdsn-service init-rrq-rcvd-rate, on page 30
- twan-profile, on page 31
- udr-module active-charging-service, on page 32
- udr-module charging-service, on page 33
- uidh-server, on page 33
- user-plane-service, on page 34
- uut-profile name, on page 34
- wsg-service, on page 35

s102-service

Creates and configures an S102 service instance to manage an S102 interface. The S102 interface is used in support of the CSFB for CDMA 1xRTT feature and the SRVCC for CDMA 1xRTT feature.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] s102-service` *`service_name`*

no

Remove the configuration for the specified S102 service from the configuration of the current context.

service_name

Specifies the name of the S102 service as a unique alphanumeric string from 1 through 63 characters in length.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to create, edit, or remove an S102 service. The S102 service configuration is used to configure and manage the S102 interface.

An unlimited number of S102 service configurations can be created. However, for the S102 interface associated with the S102 service configuration to function, the S102 service/interface must be associated with an MME service, using the **associate** command in the MME service configuration mode. This requirement effectively limits the MME to supporting a maximum of 8 'associated' S102 service configurations at one time.

For details on the configuration and use of an S102 service/interface, refer to either the CSFB for 1xRTT or SRVCC for 1xRTT feature chapter in the *MME Administration Guide*.

Example

The following command creates an S102 service named *S102intf-1* in the current context:

```
s102-service s102intf-1
```

saegw-service

Creates a System Architecture Evolution Gateway (SAEGW) service or specifies an existing SAEGW service and enters the SAEGW Service Configuration Mode for the current context.

Product

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

saegw-service *service_name* **[-noconfirm]**
no saegw-service *service_name*

no

Removes the specified SAEGW service from the context.

service_name

Specifies the name of the SAEGW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the SAEGW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

Important An S-GW and/or P-GW created in the same context must be associated with this SAEGW service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-saegw-service)#
```

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

Use this command when configuring the following SAE components: SAEGW.

Example

The following command enters the existing SAEGW Service Configuration Mode (or creates it if it does not already exist) for the service named *saegw-service1*:

```
saegw-service saegw-service1
```

The following command will remove *pgw-service1* from the system:

```
no saegw-service saegw-service1
```

sbc-service

Creates or removes an SBc service and enters the SBc Service Configuration mode. This mode configures or edits the configuration for an SBc service which controls the interface between the MME and E-SMLC.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] sbc-service** *sbc_svc_name*

no

Remove the configuration for the specified SBc service from the configuration of the current context.

sbc_svc_name

Specifies the name of the SBc service as a unique alphanumeric string from 1 to 63 characters.

The SBc service name must be unique across all contexts.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to create, edit, or remove an SBc service.

Up to 8 SGs + MME + SBc + SLs Services can be configured on the system.

Example

The following command creates an SBc service named *sbc1* in the current context:

```
sbc-service sbc1
```

server

Configures remote server access protocols for the current context. This command is used to enter the specified protocols configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
server { confd | ftpd | named | sshd | telnetd | tftpd }
no server { confd | ftpd | named | sshd | telnetd | tftpd } [ kill ]
```

no

Disables the specified service.

confd

Enables ConfD-NETCONF protocol that supports a YANG model for transferring configuration and operations data with the Cisco Network Service Orchestrator (NSO). This command is restricted to the local context only. Enabling this command moves you to the NETCONF Protocol Configuration mode.

Important ConfD-NETCONF support requires that a V2-RSA SSH key be configured on the local context. If an SSH key is not available, StarOS generates an error message.

ftpd

Enters the FTP Server Configuration Mode.

Important The FTPD server can only be configured in the local context. FTP is not available in Trusted builds.

Caution For maximum system security, you should not enable FTP functionality. SFTP is the recommended file transfer protocol.

named

Starts the named server.

sshd

Enters the SSH Server Configuration Mode. SSH is the recommended remote access protocol. SSH must be configured to support SFTP.

Important The SSHD server allows only three unsuccessful login attempts before closing a login session attempt.

telnetd

Enters the Telnet Server Configuration Mode. Telnet is not available in Trusted builds.

Important The TELNET server allows only three unsuccessful login attempts before closing a login session attempt.

Caution For maximum system security, you should not enable telnet functionality. SSH is the recommended remote access protocol.

tftpd

Enters the TFTP Server Configuration Mode.

Important The TFTPD server can only be configured in the local context.

kill

Indicates all instances of the server are to be stopped.

This option only works with the **ftpd**, **sshd**, **telnetd**, and **tftpd** commands.

Usage Guidelines Enter the Context Configuration Mode for the appropriate, previously defined context, to set the server option(s). Repeat the command as needed to enable/disable more than one option server daemon.

Example

The following command sequence enables SSH login:

```
server sshd
```

service-redundancy-protocol

Configures Interchassis Session Recovery (ICSR) services for the current context. This command is used to enter the Service Redundancy Protocol Configuration Mode.

Product All products supporting ICSR

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **service-redundancy-protocol**

Usage Guidelines Enter the Configuration Mode to set the service redundancy protocol options.

Example

The following command enters Service Redundancy Protocol Configuration Mode.

```
service-redundancy-protocol
```

session-event-module

Enables the event module, enters the Session Event Module Configuration Mode where the sending of P-GW or S-GW subscriber-specific event files to an external server can be configured. From release 15.0 onwards, the session-event module is used by SGSN for event logging. By default, EDR files are generated at the location: /hd-raid/records/edr. After upgrading to release R15.0, if this CLI is configured, the path for EDR files changes to: /hd-raid/records/event.

Product P-GW

SAEGW (Pure-S calls)

S-GW

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] session-event-module

no

Disables the event module configuration.

Usage Guidelines

Enter the Session Event Module Configuration Mode where the sending of P-GW or S-GW subscriber-specific event files to an external server can be configured.

Entering this command results in the following prompt:

```
[context_name]hostname(config-event)#
```

Session Event Module Configuration Mode commands are defined in the *Session Event Module Configuration Mode Commands* chapter.

sgsn-service

Creates an SGSN service instance and enters the SGSN Service Configuration mode. This mode configures or edits the configuration for an SGSN service which controls the SGSN functionality.

An SGSN mediates access to GPRS/UMTS network resources on behalf of user equipment (UE) and implements the packet scheduling policy between different QoS classes. It is responsible for establishing the packet data protocol (PDP) context with the GGSN.

Important For details about the commands and parameters, check the *SGSN Service Configuration Mode* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] sgsn-service *srvc_name*

no

Remove the configuration for the specified SGSN service from the configuration of the current context.

srvc_name

Specifies the name of the SGSN service as a unique alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines Use this command to create, edit, or remove an SGSN service.

Example

The following command creates an SGSN service named *sgsn1* in the current context:

```
sgsn-service sgsn1
```

The following command removes the sgsn service named *sgsn1* from the configuration for the current context:

```
no sgsn-service sgsn1
```

sgs-service

Creates an SGs service instance and enters the SGS Service Configuration mode.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] sgs-service** *name*

no

Remove the configuration for the specified SGs service from the configuration of the current context.

name

Specifies a name for an SGs service as a unique alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the SGS Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following CLI prompt:

```
[context_name]hostname(config-sgs-service)#
```

SGS Service Configuration Mode commands are defined in the *MME SGS Service Configuration Mode Commands* chapter.

Example

The following command creates an SGS service named *sgs1* in the current context:

```
sgs-service sgs1
```

The following command removes the SGS service named *sgs1* from the configuration for the current context:

```
no sgs-service sgs1
```

sgtp-service

Creates an SGTP service instance and enters the SGTP Service Configuration mode. This mode configures the GPRS Tunneling Protocol (GTP) related settings required by the SGSN and eWAG to support GTP-C (control plane) messaging and GTP-U (user data plane) messaging.

Product

eWAG

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] sgtp-service *sgtp_service_name*

no

If previously configured, removes the specified SGTP service configuration in the current context.

sgtp_service_name

Specifies name of the SGTP service.

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

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to create, edit, or remove an SGTP service.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-sgtp-service)#

Example

The following command creates an SGTP service named *sgtp1* in the current context:

```
sgtp-service sgtp1
```

The following command removes, if previously configured, the SGTP service named *sgtp1* from the current context:

```
no sgtp-service sgtp1
```

sgw-service

Creates an S-GW service or specifies an existing S-GW service and enters the S-GW Service Configuration Mode for the current context.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
sgw-service service_name [ -noconfirm ]
no sgw-service service_name
```

service_name

Specifies the name of the S-GW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no sgw-service *service_name*

Removes the specified S-GW service from the context.

Usage Guidelines

Enter the S-GW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-sgw-service)#
```

S-GW Service Configuration Mode commands are defined in the *S-GW Service Configuration Mode Commands* chapter.

Use this command when configuring the following SAE components: S-GW.

Example

The following command enters the existing S-GW Service Configuration Mode (or creates it if it does not already exist) for the service named *sgw-service1*:

```
sgw-service sgw-service1
```

The following command will remove *spgw-service1* from the system:

```
no sgw-service sgw-service1
```

sls-service

Creates an SLs service or configures an existing SLs service and enters the SLs Service Configuration Mode in the current context.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SLs Service Configuration

configure > context *context_name* **> sls-service** *service_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

sls-service *service_name* **[-noconfirm]**
[no] sls-service *service_name*

no

Removes the specified SLs service from the context.

service_name

Specifies the name of the SLs service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 64 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Enter the SLs Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

Up to 4 SLs services can be configured on the system.

The SLs service name must be unique across all contexts.

Entering this command results in the following prompt:

```
[context_name]hostname(config-sls-service)#
```

SLs Service Configuration Mode commands are defined in the SLs Service Configuration Mode Commands chapter.

Example

The following command enters the existing SLs Service Configuration Mode (or creates it if it does not already exist) for the service named *sls1*.

```
sls-service sls1
```

smsc-service

Creates and configures an SMSC peer service to allow communication with SMSC peer.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] smsc-service *smsc_svc_name* **[-noconfirm]**

no

Removes the specified SMSC service from the current context.

smsc_svc_name

Specifies the name of the SMSC service. *smsc_svc_name* is an alphanumeric string of 1 through 63 characters. If *smsc_svc_name* does not refer to an existing service, the new service is created if resources allow.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create and configure an SMSC peer service to allow communication with SMSC peer.

Entering this command results in the following prompt:

```
[context_name]hostname(config-smsc-service)#
```

SMSC Service Configuration Mode commands are defined in the *MME SMSC Service Configuration Mode Commands* chapter.

Example

The following command creates an SMSC service named *sm1* in the current context (or enters the existing SMSC Service Configuration Mode if it already exists):

```
smsc-service sm1
```

The following command will remove the configured SMSC service named *sm1* from the current context:

```
no smsc-service sm1
```

ssh

Generates public/private key pairs for use with the configured Secure Shell (SSH) server and sets the public/private key pair to specified values.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ssh { generate key | key *data* **length** *octets* **} [type { v1-rsa | v2-rsa | v2-dsa }]**
no ssh key [type { v1-rsa | v2-rsa | v2-dsa }]

no ssh key [type { v1-rsa | v2-rsa | v2-dsa }]

This command clears configured SSH keys. If type is not specified, all SSH keys are cleared.

generate key

Generates a public/private key pair which is to be used by the SSH server. The generated key pair is in use until the command is issued again.

Important In Release 19.2 and higher, the **v2-dsa** keyword is removed in tthe **ssh generate key type** syntax.

key *data* length *octets*

Sets the public/private key pair to be used by the system where *data* is the encrypted key and *length* is the length of the encrypted key in octets. *data* must be an alphanumeric string of 1 through 1023 characters and *octets* must be a value in the range of 0 through 65535.

Important In Release 19.2 and higher, the **v2-dsa** keyword is cconcealed in the **ssh key** *name* **length** *key_length* **type v2-rsa** syntax.

[type { v1-rsa | v2-rsa | v2-dsa }]

Specifies the type of SSH key to generate. If type is not specified, all three key types are generated.

- **v1-rsa**: SSHv1 RSA host key only (obsolete)
- **v2-dsa**: SSHv2 DSA host key only (deprecated)

- **v2-rsa**: SSHv2 RSA host key only

Important For maximum security, it is recommended that only SSH v2 be used. **v2-rsa** is the recommended key type.

Usage Guidelines Generate secure shell keys for use in public key authentication.

Example

The following command generates SSH key pairs for all supported types:

```
ssh generate key
```

The following command generates an SSH key pair of a specified length using an encrypted key:

```
ssh key g6j93fw59cx length 128
```

ssl

Creates a new Secure Sockets Layer (SSL) template or specifies an existing one and enters the SSL Template Configuration Mode.

Product SCM

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] ssl template** *name* **{ ssl-subscriber }**

no

Removes the specified SSL template from the context.

template *name*

Specifies the name of a new or existing SSL template as an alphanumeric string of 1 through 127 alphanumeric characters.

ssl-subscriber

Specifies that the SSL template is an SSL subscriber template.

Usage Guidelines Use this command to create a new SSL template or modify an existing one.

Entering this command results in the following prompt:

`[context_name]hostname(cfg-ctx-ssl-subscriber-template)#`

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

Example

The following command specifies the SSL template *ssl_template_1* and enters the SSL Template Configuration Mode:

```
ssl template ssl_template_1 ssl-subscriber
```

subscriber

Configures the specified subscriber for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
subscriber { default | name user_name } asn-service-info mobility [ ipv4 |
 ipv6 | ipv6-ipv4 ]
no subscriber { default | name user_name }
```

no

Indicates the subscriber specified is to be removed from the list of allowed users for the current context.

default | name *user_name*

default: Enters the Subscriber Configuration Mode for the context's default subscriber settings.

name *user_name*: Specifies the user which is to be allowed to use the services of the current context. *user_name* must be an alphanumeric string of 1 through 127 characters.

asn-service-info mobility:Indicates the type of mobility supported and enabled in the Autonomous System Number (ASN).

Usage Guidelines

Enter the Subscriber Configuration Mode for actual users as well as for a default subscriber for the current context.

Entering this command results in the following prompt:

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

Subscriber Configuration Mode commands are defined in the *Subscriber Configuration Mode Commands* chapter.

NAS uses the specified parameter for asn-service-info mobility to indicate and pack the mobility support field for IPv4, IPv6, or both, in the Service-Info attribute in the Access-request. RADIUS sends back this attribute in the Access-accept message by indicating respective bits to authorize the service indicated by NAS.

Important A maximum of 128 subscribers and/or administrative users may be locally configured per context.

Example

Following command configures the default subscriber in a context:

```
subscriber default
```

Following command removes the default subscriber from a context:

```
no subscriber default
```

Following command configures a subscriber named *user1* in a context:

```
subscriber name user1
```

Following command removes a subscriber named *user1* from a context:

```
no subscriber name user1
```

sx-service

Configures Sx service for the current context. This command is used to enter the Sx Service Configuration Mode.

Product CUPS

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
sx-service
```

Usage Guidelines Enter the Configuration Mode to set the Sx service options.

Example

The following command enters Sx Service Configuration Mode.

```
sx-service
```

tac-profile

Configures Tracking Area Code (TAC) profile for the current context. This command is used to enter the TAC Profile Configuration Mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

tac-profile *profile_name*

tac-profile *profile_name*

Specifies the name of TAC profile. *profile_name* is an alphanumeric string of 1 through 31 characters. If *profile_name* does not refer to an existing profile, the new profile is created if resources allow.

Usage Guidelines

Enter the Configuration Mode to set the TAC profile options.

Entering this command results in the following prompt:

```
[context_name]hostname(config-tac-profile)#
```

Example

The following command creates a TAC profile named *tp1* in the current context (or enters the existing TAC Profile Configuration Mode if it already exists):

```
tac-profile tp1
```

threshold available-ip-pool-group

Configures context-level thresholds for IP pool utilization for the system.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold available-ip-pool-group *low_thresh* **[clear** *high_thresh* **]**
default threshold available-ip-pool-group

default

Configures the default setting.

low_thresh

The low threshold IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. *low_thresh* can be configured as an integer from 0 through 100. Default: 10

clear *high_thresh*

Specifies the high threshold IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. *high_thresh* can be configured as an integer from 0 through 100. Default: 10

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage Guidelines

When IP address pools are configured on the system, they can be assigned to a group. IP address pool utilization thresholds generate alerts or alarms based on the utilization percentage of all IP address contained in the pool group during the specified polling interval.

All configured public IP address pools that were not assigned to a group are treated as belonging to the same group. Individual configured static or private pools are each treated as their own group.

Alerts or alarms are triggered for IP address pool utilization based on the following rules:

- **Enter Condition**: Actual IP address utilization percentage per pool group ≤ Low Threshold
- **Clear Condition**: Actual IP address utilization percentage per pool group > High Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

The following table describes the possible methods for configuring IP pool utilization thresholds:

Table 1: IP Pool Utilization Thresholds - Configuration Methods

Method	Description
Context-level	A single IP pool utilization threshold can be configured for all IP pool groups with given system context. If a single threshold is configured for all pool groups, separa alerts or alarms can be generated for each group. This command configures that threshold.

Method	Description
IP address pool-level	Each individual IP address pool can be configured with its own threshold. Thre configured for individual pools take precedence over the context-level threshol would otherwise be applied (if configured). In the event that two IP address pools belonging to the same pool group are co with different thresholds, the system uses the pool configuration that has the gr low threshold for that group.

Example

The following command configures a context-level IP pool utilization low threshold percentage of *10* and a high threshold of *35* for an system using the Alarm thresholding model:

```
threshold available-ip-pool-group 10 clear 35
```

threshold ha-service init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for an HA service.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold ha-service init-rrq-rcvd-rate *high_thresh* **[clear** *low_thresh* **]**
no threshold ha-service init-rrq-rcvd-rate

no

Deletes the alert or alarm.

high_thresh

Sets the high threshold average number of calls setup per second that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 1000000. Default: 0

clear *low_thresh*

Sets the low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured as an integer from 0 through 1000000. Default: 0

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines Use this command to set an alert or an alarm when the average number of calls set upper second is equal to or less than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter Condition**: Actual number of calls setup per second > High Threshold
- **Clear Condition**: Actual number of calls setup per second ≤ Low Threshold

Example

The following command configures a number of calls setup per second threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold ha-service init-rrq-rcvd-rate 1000 clear 500
```

threshold ip-pool-free

Sets an alarm or alert based on the percentage of IP addresses that are unassigned in an IP pool. This command affects all IP pools in the current context.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
threshold ip-pool-free low_thresh [ clear high_thresh ]
default threshold ip-pool-free
```

default

Configures the default setting.

low_thresh

Sets the low threshold percentage of addresses available in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 100. Default:0

clear *high_thresh*

Sets the high threshold percentage of addresses available in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer between 0 and 100. Default: 0

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage Guidelines Use this command to set an alert or an alarm when the number of unassigned IP addresses in any pool is equal to or less than a specified percentage of the total number of addresses in the pool.

Alerts or alarms are triggered for percentage of IP address pool free based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses free per pool ≤ Low Threshold
- **Clear Condition**: Actual percentage of IP addresses free per pool > High Threshold

Important This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are unused low threshold percentage of *10* and a high threshold of *35* for an system using the Alarm thresholding model:

```
threshold ip-pool-free 10 clear 35
```

threshold ip-pool-hold

Sets an alert based on the percentage of IP addresses from an IP pool that are on hold. This command affects all IP pools in the current context.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
threshold ip-pool-hold high_thresh [ clear low_thresh ]
default threshold ip-pool-hold
```

default

Configures the default setting.

high_thresh

Sets the high threshold percentage of addresses on hold in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default: 0

clear *low_thresh*

Sets the low threshold percentage of addresses on hold in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises below the low threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer from 0 through 100. Default: 0

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the percentage of IP addresses on hold in any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.

Alerts or alarms are triggered for percentage of IP address pool addresses on hold based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses on hold per pool > High Threshold
- **Clear Condition**: Actual percentage of IP addresses on hold per pool ≤ Low Threshold

Important This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are on high threshold percentage of *35* and a low threshold of *10* for an system using the Alarm thresholding model:

```
threshold ip-pool-hold 35 clear 10
```

threshold ip-pool-release

Sets an alert based on the percentage of IP addresses from an IP pool that are in the release state. This command affects all IP pools in the current context.

Product All

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold ip-pool-release *high_thresh* **[clear** *low_thresh* **]**
default threshold ip-pool-release

default

Configures the default setting.

high_thresh

Sets the high threshold percentage of addresses in the release state in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default: 0

clear *low_thresh*

Sets the low threshold percentage of addresses in the release state in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises below the low threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer from 0 through 100. Default:0

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of IP addresses the release state in any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.

Alerts or alarms are triggered for percentage of IP address pool addresses in the release state based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses in the release state per pool> High Threshold
- **Clear Condition**: Actual percentage of IP addresses in the release state per pool ≤ Low Threshold

Important This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are in the release state high threshold percentage of *35* and a low threshold of *10* for an system using the Alarm thresholding model:

```
threshold ip-pool-release 35 clear 10
```

threshold ip-pool-used

Sets an alert based on the percentage of IP addresses that have been assigned from an IP pool. This command affects all IP pools in the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold ip-pool-used *high_thresh* **[clear** *low_thresh* **]**
default threshold ip-pool-used

default

Configures the default setting.

high_thresh

Sets the high threshold percentage of addresses assigned from an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default:0

clear *low_thresh*

Sets the low threshold percentage of addresses assigned from an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. It may be configured to any integer between0 and 100. Default: 0

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of IP addresses assigned from any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.

Alerts or alarms are triggered for percentage of IP address pool addresses used based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses used per pool > High Threshold
- **Clear Condition**: Actual percentage of IP addresses used per pool ≤ Low Threshold

Important This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are used high threshold percentage of *35* and a low threshold of *10* for an system using the Alarm thresholding model:

```
threshold ip-pool-used 35 clear 10
```

threshold ip-pool-usable

Enable the **ip-pool-usable** threshold for ip pool usable of IPs, which are in either FREE or RELEASE states.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold ip-pool-usable *low_thresh* **[clear** *high_thresh* **]interval** *time*

ip-pool-usable*low_thresh*clear *high_thresh*

Configures the IP pool usable pre threshold state as either free or release. The trap is raised if the ip pool usable is less than or equal to the configured ip-pool-usable low threshold value.

The **PreThreshClearIPPoolUsable** trap gets triggered if the pool usable value is greater than a clear high threshold value.

Usage Guidelines

Use this command to set an alert or an alarm when the number of IP addresses assigned from any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.

These are the types of Pre and final threshold SNMP alarms generated based on the configured thresholds:

- PreThreshIPPoolUsable alarm for entering condition
- PreThreshClearIPPoolUsable alarm for clearing condition
- FinalThreshIPPoolUsable alarm for entering condition
- FinalThreshClearIPPoolUsable alarm for clearing condition

Example

The following command configures a context-level IP pool percentage of IP addresses that are used high threshold percentage of *50* and a low threshold of *40* for an system using the Alarm thresholding model:

```
threshold ip-pool-usable 40 clear 50
```

threshold ip-pool-usable-final

Enable the **ip-pool-usable-final** threshold for ip pool usable of IPs, which are in either FREE or RELEASE states.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold ip-pool-usable-final *low_thresh* **[clear** *high_thresh* **]interval** *time*

ip-pool-usable-final*low_thresh*clear *high_thresh*

Configures Configure the IP pool usable final threshold state in either free or release state.

The **FinalThreshIPPoolUsable** alarm is raised when the measured pool usable value is less than or equal to the **ip-pool-usable-final** value.

The FinalThreshClearIPPoolUsable trap clears when the ip-pool-usable-final clear value is greater than a clear threshold.

Usage Guidelines

Use this command to Configure the IP pool usable final threshold state in either free or release state.

These are the types of Pre and final threshold SNMP alarms generated based on the configured thresholds:

- PreThreshIPPoolUsable alarm for entering condition
- PreThreshClearIPPoolUsable alarm for clearing condition
- FinalThreshIPPoolUsable alarm for entering condition
- FinalThreshClearIPPoolUsable alarm for clearing condition

Example

The following command configures a context-level IP pool percentage of IP addresses that are used high threshold percentage of *36* and a low threshold of *35* for an system using the Alarm thresholding model:

```
threshold ip-pool-usable-final 35 clear 36
```

threshold monitoring

Enables or disables thresholds alerting for a group of thresholds.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] threshold monitoring available-ip-pool-group

default

Configures the default setting.

no

Disables threshold monitoring for the specified value.

available-ip-pool-group

Enables threshold monitoring for IP pool thresholds at the context level and the IP address pool-level.

Refer to the **threshold available-ip-pool-group** command, the **threshold ip-pool-x** commands and the **alert-threshold** keyword of the **ip pool** command for additional information on these values.

Usage Guidelines

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2)section of the *SNMPMIB Reference*.

The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

- **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists and/or a condition clear alarm is generated.

"Outstanding" alarms are reported to through the system's alarm subsystem and are viewable through the CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

Table 2: Thresholding Reporting Mechanisms by Model

Model	SNMP Traps	Logs	Alarm System
Alert	X	X	
Alarm	X	X	X

Refer to the **threshold poll** command in Global Configuration Mode Commands for information on configuring the polling interval over which IP address pool utilization is monitored.

Example

the following command enables threshold monitoring for IP pool thresholds at the context level and the IP address pool-level:

```
threshold monitoring available-ip-pool-group
```

threshold pdsn-service init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for a PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
threshold pdsn-service init-rrq-rcvd-rate high_thresh [ clear low_thresh ]
no threshold pdsn-service init-rrq-rcvd-rate
```

no

Deletes the alert or alarm.

high_thresh

Sets the high threshold average number of calls setup per second that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 1000000. Default: 0

clear *low_thresh*

Sets the low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured as an integer between 0 and 1000000. Default: 0

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines Use this command to set an alert or an alarm when the average number of calls set upper second is equal to or less than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter Condition**: Actual number of calls setup per second > High Threshold
- **Clear Condition**: Actual number of calls setup per second ≤ Low Threshold

Example

The following command configures a number of calls setup per second threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold pdsn-service init-rrq-rcvd-rate 1000 clear 500
```

twan-profile

Creates a Trusted Wireless Access Network (TWAN) profile and enters the TWAN Profile Configuration Mode for the current context. The TWAN profile contains information on the RADIUS client addresses (WLC) and access-type corresponding to the RADIUS clients.

Product SaMOG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] twan-profile** *twan_profile_name*

no

Deletes the TWAN profile configuration for the current context.

twan_profile_name

Specifies the name of the TWAN profile. If a *twan_profile_name* does not already exist, a new profile is created.

In Release 17 and earlier, *twan_profile_name* must be an alphanumeric string of 1 through 64 characters.

In Release 18 and later, *twan_profile_name* must be an alphanumeric string of 1 through 48 characters.

Usage Guidelines

Use this command to create a Trusted Wireless Access Network (TWAN) profile and enter the TWAN Profile Configuration Mode for the current context.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-twan-profile)#

TWAN Profile Configuration Mode commands are defined in the *TWAN Profile Configuration Mode Commands* chapter.

udr-module active-charging-service

Enables creation, configuration and deletion of the User Data Record (UDR) module for the context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] udr-module active-charging-service`

no

Deletes the UDR module configuration for the current context.

Usage Guidelines

Use this command to create the UDR module for the context, and configure the UDR module for active charging service records. You must be in a non-local context when specifying this command, and you must use the same context when specifying the EDR module command.

On entering this command, the CLI prompt changes to:

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

Example

The following command creates the UDR module for the context, and enters the UDR Module Configuration Mode:

`udr-module active-charging-service`

udr-module charging-service

Enters the UDR Charging Service Configuration Mode.

Product

PDSN

HA

LNS

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

udr-module charging-service

Usage Guidelines

Use this command to enter the UDR Charging Service Configuration Mode.

Example

The following command enters the UDR Charging Service Configuration Mode:

udr-module charging-service

uidh-server

Use this command to enter the UIDH Server Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

uidh-server *uidh_server_name*

uidh_server_name

Is a string of size ranging from 1 to 63 characters.

user-plane-service

Creates User Plane Service. Minimum or critical parameters to start a user-plane service is to have one Sx interface and thre GTPU services of the interface type PGW-ingress, SGW-ingress, and SGW-egress. The associated services must also be in the running mode. Stopping of associated services result in stopping of user-plane service. If any of the critical parameters are removed or changed from the user-plane service, it results in user-plane service being stopped. By default, this CLI command is disabled.

Product

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] user-plane-service` *<userplane_service_name>*

no

Removes the user-plane service from the particular context.

user-plane-service

Creates specified User Plane service name to allow configuration of User Plane service.

userplane_service_name

Assigns a service name to the user-plane service.

Usage Guidelines

Use this command to create the user plane service for the context and configure it.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-user-plane-service)#

Example

The following command creates the user plane service "UPLte" for the context, and enters the User Plane Service Configuration Mode:

```
user-plane-service UPLte
```

uut-profile name

Configures UE Usage Type (UUT) profile name for the current context. This command is used to enter the UUT Profile Name Configuration Mode.

Product CUPS

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] uut-profile name** *profile_name*

uut-profile name *profile_name*

Specifies the name of UUT profile. *profile_name* is an alphanumeric string of 1 to 63 characters.

Usage Guidelines Enter the Configuration Mode to set the UUT profile options.

Entering this command results in the following prompt:

```
[context_name]hostname(config-uut-profile)#
```

Example

The following command disables the UUT profile with the name *prof1*.

```
no uut-profile name prof1
```

wsg-service

Enables or disables Wireless Security Gateway (WSG) service. When enabled you are in WSG Service Configuration mode. (VPC only)

Product SecGW (WSG)

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **wsg-service** *service_name*
no wsg-service *service_name*

no

Disables the specified WSG service.

service_name

Specifies the name of the WSG service as an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to enter the WSG Service Configuration Mode. For additional information, see the *WSG Service Configuration Mode Commands* chapter.

Example

The following command enters the WSG Service Configuration Mode:

```
wsg-service wsg01
```