Context Configuration Mode Commands A-D

Command Modes

This section includes the commands **aaa accounting** through **domain** 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).

aaa accounting

This command enables/disables accounting for subscribers and context-level administrative users 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

```
aaa accounting { administrator radius-diameter | subscriber [
radius-diameter ] }
default aaa accounting { administrator | subscriber }
no aaa accounting { administrator | subscriber } [ radius-diameter ]
```

default

Configures the default setting.

Default: RADIUS

no

Disables AAA accounting per the options specified.

radius-diameter

Enables AAA accounting for context-level administrative users.

subscriber

Enables AAA accounting for subscribers.

radius-diameter

Enables RADIUS or Diameter accounting for subscribers.

Usage Guidelines

Use this command to enable/disable accounting for subscribers and context-level administrative users for the current context.

To enable or disable accounting for individual local subscriber configurations refer to the **accounting-mode** command in the *Subscriber Configuration Mode Commands* chapter.

Important The accounting parameters in the APN Configuration Mode take precedence over this command for subscriber sessions. Therefore, if accounting is disabled using this command but enabled within the APN configuration, accounting is performed for subscriber sessions.

Example

The following command disables AAA accounting for context-level administrative users:

```
no aaa accounting administrator
```

The following command enables AAA accounting for context-level administrative users:

```
aaa accounting administrator radius-diameter
```

aaa authentication

This command enables/disables authentication for subscribers and context-level administrative users 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

```
[ no ] aaa authentication { administrator | subscriber } { local | none
| radius-diameter }
default aaa authentication { administrator | subscriber }
```

default

Configures the default setting for the specified parameter.

- **administrator**: local+RADIUS
- **subscriber**: RADIUS

no

Disables AAA authentication for administrator(s)/subscribers as specified.

- **local**: Disables local authentication for current context.
- **none**: Disables NULL authentication for current context, which enables both local and RADIUS-based authentication.
- **radius-diameter**: Disables RADIUS or Diameter-based authentication.

administrator | subscriber

- **administrator**: Enables authentication for administrative users.
- **subscriber**: Enables authentication for subscribers.

local | none | radius-diameter

Enables AAA authentication for administrator(s)/subscribers as specified.

- **local**: Enables local authentication for the current context.
- **none**: Disables authentication for the current context.
- **radius-diameter**: Enables RADIUS or Diameter-based authentication.

Usage Guidelines

Use this command to enable/disable AAA authentication during specific maintenance activities or during test periods. The authentication can then be enabled again for the entire context as needed.

Example

The following command disables RADIUS or Diameter-based authentication for subscribers for the current context:

```
no aaa authentication subscriber radius-diameter
```

The following command enables RADIUS or Diameter-based authentication for subscribers for the current context:

```
aaa authentication subscriber radius-diameter
```

aaa constructed-nai

This command configures the password used during authentication for sessions using a Constructed Network Access Identifier (NAI) or an APN-specified user name.

Product

PDSN

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

```
aaa constructed-nai authentication [ [ encrypted ] password user_password |
 use-shared-secret-password ]
no aaa constructed-nai authentication
```

no

Disables authentication based upon the constructed NAI.

[encrypted] password *user_password*

encrypted: Specifies that the user password should be encrypted.

password *user_password*: Specifies an authentication password for the NAI-constructed user.

In 12.1 and earlier releases, the *user_password* must be an alphanumeric string of 0 through 63 characters with or without encryption.

In 12.2 and later releases, the *user_password* must be an alphanumeric string of 0 through 63 characters without encryption, or 1 through 132 characters with encryption.

use-shared-secret-password

Specifies using RADIUS shared secret as the password. Default: No password

Usage Guidelines

This command configures passwords for user sessions that utilize a constructed NAI assigned via a PDSN service or a user name assigned via the APN configuration.

For simple IP sessions facilitated by PDSN services in which the **authentication allow-noauth** and **aaa constructed-nai** commands are configured, this command provides a password used for the duration of the session.

For PDP contexts using an APN in which the outbound user name is configured with no password, this command is used to provide the password.Additionally, this command is also used to provide a password for situations in which an outbound username and password are configured and the **authentication imsi-auth** command has been specified.

The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

If a password is configured with this keyword, then the specified password is used. Otherwise, an empty user-password attribute is sent.

Note that this configuration works in a different way for GGSN services. If a password is configured with this keyword for GGSN service, the specified password is used.Otherwise, if an outbound password is configured, that password is used. If no outbound password is configured, the RADIUS server secret is used as the user-password string to compute the user-password RADIUS attribute.

The NAI-construction consists of the subscriber's MSID, a separator character, and a domain. The domain that is used is either the domain name supplied as part of the subscriber's user name or a domain alias.

Important The domain alias can be set with the **nai-construction domain** command in the PDSN Service Configuration mode, or the **aaa default-domain subscriber** command in the Global Configuration mode for other core network services.

The domain alias is determined according to the following rules:

- If the domain alias is set by **nai-construction domain**, that value is always used and the **aaa default-domain subscriber** value is disregarded, if set. The NAI is of the form **<msid><symbol><nai-construction domain>**.
- If the domain alias is not set by **nai-construction domain**, and the domain alias is set by **aaa default-domain subscriber**, the **aaa default-domain subscriber** value is used. The NAI is of the form **<msid><symbol><aaa default-domain subscriber>**.
- If the domain alias is not set by **nai-construction domain** or **aaa default-domain subscriber**, the domain name alias is the name of the source context for the PDSN service. The NAI is of the form **<msid><symbol><source context of PDSN Service>**.

The special separator character can be one of the following six: @, -, %, \,-, /

The subscriber's MSID is constructed in one of the formats displayed in the following figure.

Example

The following command configures the authentication password for the NAI-constructed user.

```
aaa constructed-nai authentication
```

aaa filter-id rulebase mapping

This command configures the system to use the value of the Filter-Id AVP as the ACS rulebase name.

Product

ACS

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 | default ] aaa filter-id rulebase mapping`

no

Disables the mapping of Filter-Id AVP and ACS rulebase name.

default

Configures the default setting. Default: Disabled

Usage Guidelines

Use this command to enable the mapping of Filter-Id attribute's value returned during RADIUS authentication as the ACS rulebase name.

This feature provides the flexibility for operator to transact between multi-charging-service support for postpaid and prepaid subscribers through Access Control Lists (ACLs) entered in AAA profiles in RADIUS server to single-charging-service system based on rulebase configuration for postpaid and prepaid subscribers.

This feature internally maps the received ACL in to rulebase name and configures subscriber for postpaid or prepaid services accordingly.

When this feature is enabled and ACS rulebase attribute is not received from RADIUS or not configured in local default subscriber template system copies the filter-id attribute value to ACS rulebase attribute.

This copying happens only if the filter-id is configured and received from RADIUS server and ACS rulebase is not configured in ACS or not received from RADIUS.

Example

The following command enables the mapping value of the Filter-Id attribute to ACS rulebase name:

```
aaa filter-id rulebase mapping
```

aaa group

This command enables/disables the creation, configuration or deletion of AAA server groups in 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

aaa group *group_name* **[-noconfirm]**
no aaa group *group_name*

no

Deletes the specified AAA group.

group_name

Specifies name of the AAA group.

If the specified AAA group does not exist, it is created, and the prompt changes to the AAA Server Group Configuration Mode, wherein the AAA group can be configured.

If the specified AAA group already exists, the prompt changes to the AAA Server Group Configuration Mode, wherein the AAA group can be configured.

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

-noconfirm

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

Usage Guidelines

Use this command to create/configure/delete AAA server groups within the context.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-aaa-group)#

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

Example

The following command enters the AAA Server Group Configuration Mode for a AAA group named *test321*:

aaa group test321

aaa nai-policy

This command sets policies on how Network Access Identifiers (NAIs) are handled during the authentication process.

Product

GGSN

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

`[ default | no ] aaa nai-policy reformat-alg-hex-0-9`

default

Sets the NAI policy back to its default setting which is to remap hexadecimal digits in NAIs and accept calls with embedded 0x00 hexadecimal digits.

no

Disable remapping of hexadecimal digits in the NAI and reject calls that have a 0x00 hexadecimal digit embedded in the NAI.

reformat-alg-hex-0-9

Default: Enabled

Controls remapping of NAIs that consist only of hex digits 0x00 through 0x09 or if a 0x00 hexadecimal digit is embedded in the NAI.

By default, the system remaps NAIs that consist solely of characters 0x00 through 0x09to their ASCII equivalent. For example; 0x00 0x01 0x2 0x03 will get remapped to 123.

Also by default the system accepts an NAI containing one or more 0x00 characters within the NAI ignoring all characters after the first 0x00.

When this keyword is disabled NAIs are processed as follows:

- Remapping of hexadecimal digits 0x00 through 0x09 within the user-provided NAI is disabled.
- When the NAI has an embedded 0x00 character anywhere within it (including if there is an extra 0x00 character at the end) the call is rejected.

Usage Guidelines

Use this command to disable or re-enable remapping of hexadecimal digits in the NAI.

Example

The following command disables the remapping of hexadecimal digits in the NAI:

```
no aaa nai-policy reformat-alg-hex-0-9
```

aaa tacacs+

Enables and disables TACACS+ AAA services for this 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

```
[ default | no ] aaa tacacs+
```

default

Enables TACSCS+ services for this context.

no

Disables TACACS+ services for this context.

Usage Guidelines

Use this command to disable or re-enable TACACS+ AAA services for this context.

Important You must first enable TACACS+ services using the Global Configuration mode **aaa tacacs+** command. This command enables TACACS+ services for all contexts. You can then use the Context Configuration mode **no aaa tacacs+** command to selectively disable TACACS+ per context.

Example

The following command disables TACACS+ AAA services for this context:

```
no aaa tacacs+
```

access-list undefined

Configures the behavior of access control for the current context when an undefined access control list is specified.

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

`access-list undefined { deny-all | permit-all }`
`{ default | no } access-list undefined`

default

Configures the default setting.

no

Disables handling undefined access lists.

deny-all

Specifies to drop all packets when an undefined ACL is specified.

permit-all

Specifies to forward all packets when an undefined ACL is specified.

Usage Guidelines

Use this command to specify the default behavior when an ACL specified does not exist.

When the security policies require strict access control the **deny-all** handling should be configured.

Example

The following command sets the packet handling to ignore (drop) all packets when an undefined ACL is specified.

`access-list undefined deny-all`

administrator

Configures a user with Security Administrator privileges in the current context.

Product

All

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

administrator *user_name* **[encrypted] [nopassword] password** *password* **| [ecs] [expiry-date** *date_time* **] [ftp [sftp-server** *sftp_name* **]] [li-administration] [nocli] [noconsole] [noecs] [timeout-absolute** *timeout_absolute* **] [timeout-min-absolute** *timeout_min_absolute* **] [timeout-idle** *timeout_idle* **][timeout-min-idle** *timeout_min_idle* **]**
no administrator *user_name*

no

Removes Security Administrator privileges for the specified user name.

user_name

Specifies the username for which Security Administrator privileges must be enabled in the current context. *user_name* must be an alphanumeric string of 1 through 32 characters.

[encrypted] password *password*

Specifies password for the user name. Optionally, the **encrypted** keyword can be used to specify the password uses encryption.

password must be an alphanumeric string of 1 through 63 characters without encryption, and 1 through 132 characters with encryption.

The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

[nopassword]

This option allows you to create an administrator without an associated password. Enable this option when using ssh public keys (**authorized key** command in SSH Configuration mode) as a sole means of authentication. When enabled this option prevents someone from using an administrator password to gain access to the user account.

ecs

Permits the user to use ACS-specific configuration commands. Default: Permitted

expiry-date *date_time*

Specifies the date and time that this login account expires.

Enter the date and time in the YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss format. Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

ftp

Permits the user to use FTP and SFTP. Default: Not permitted

[sftp-server *sftp_name*]

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

li-administration

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

nocli

Prevents the user from using the command line interface. Default: Permitted

noconsole

Disables user access to a Console line.

Note The Global Configuration mode **local-user allow-aaa-authentication noconsole** command takes precedence in a normal (non-Trusted) StarOS build. In this case, all AAA-based users cannot access a Console line.

noecs

Prevents the user from accessing ACS-specific commands.

timeout-absolute *timeout_absolute*

Important This keyword is obsolete. It has been left in place for backward compatibility. If used, a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum time, in seconds, the Security Administrator may have a session active before the session is forcibly terminated. *timeout_absolute* must be an integer from 0 through 300000000.

The value 0 disables this timeout configuration.

Default: 0

timeout-min-absolute *timeout_min_absolute*

Specifies the maximum time (in minutes) the Security Administrator may have a session active before the session is forcibly terminated. *timeout_min_absolute* must be an integer from 0 through 525600. The value 0 disables this timeout configuration. Default: 0

timeout-idle *timeout_idle*

Important This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum time, in seconds, the Security Administrator may have a session active before the session is terminated. *timeout_idle* must be an integer from 0 through 300000000.

The value 0 disables the idle timeout configuration.

Default: 0

timeout-min-idle *timeout_min_idle*

Specifies the maximum time, in minutes, the Security Administrator may have a session active before the session is terminated. *timeout_min_idle* must be an integer from 0 through 525600. The value 0 disables the idle timeout configuration. Default: 0

Usage Guidelines

Use this command to create new Security Administrators or modify existing user's settings.

Security Administrator users have read-write privileges and full access to all contexts and command modes. Refer to the *Command Line Interface Overview* chapter for more information.

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

Example

The following command creates a Security Administrator account named *user1* with access to ACS configuration commands:

```
administrator user1 password secretPassword
```

The following removes the Security Administrator account named *user1*:

```
no administrator user1
```

apn

Creates or deletes Access Point Name (APN) templates and enters the APN Configuration Mode within the current context.

Product

GGSN

P-GW

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] apn *apn_name* **[-noconfirm]**

no

Deletes a previously configured APN template.

apn_name

Specifies a name for the APN template as an alphanumeric string of 1 through 62 characters that is case insensitive. It may also contain dots (.) and/or dashes (-).

-noconfirm

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

⚠

Caution If this keyword option is used with the **no apn** *apn_name* command, the APN named *apn_name* will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines

This command creates an APN within the system and causes the CLI to enter the APN Configuration Mode.

The APN is a logical name for a packet data network and/or a service to which the system supports access. When a create PDP context request is received by the system, it examines the APN information element within the packet. The system determines if an APN with the identical name is configured. If so, the system uses the configuration parameters associated with that APN as a template for processing the request. If the names do not match, the request is rejected with a cause code of 219 (DBH, Missing or unknown APN).

APN templates should be created/configured within destination contexts on the system.

- Up to 1000 APNs can be configured in the GGSN.
- In StarOS v12.x and earlier, up to 1024 APNs can be configured in the P-GW.
- In StarOS v14.0 and later, up to 2048 APNs can be configured in the P-GW (SAEGW).

Example

The following command creates an APN template called *isp1*:

```
apn isp1
```

asn-qos-descriptor

Creates, deletes or manages the Quality of Service (QoS) descriptor table identifier for Access Service Node Gateway (ASN-GW) service and enters the ASN QoS Descriptor Table Identifier Configuration mode within the source context.

Product

ASN-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

```
asn-qos-descriptor id qos_table_id [ default ] dscp [ be | af11 | af12 |
af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af 43 |
ef ] [ -noconfirm ]
no asn-qos-descriptor qos_table_id [ default ] dscp [ be | af11 | af12 |
af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af 43 |
ef ] [ -noconfirm ]
```

no

Deletes a preciously configured ASN QoS descriptor table identifier.

id *qos_table_id*

Specifies a unique identifier for ASN QoS descriptor table to create/configure. *qos_table_id* must be an integer from 1 through 65535.

[default] dscp

Specifies DSCP marking for this QoS descriptor.

[be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af 43 | ef]

The DSCP marking for this QoS descriptor. Default value is be (best effort).

-noconfirm

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

Caution If this keyword option is used with **no asn-qos-descriptor id** *qos_table_id* command, the ASN QoS descriptor table with identifier *qos_table_id* will be deleted with all active/inactive configurations without prompting any warning or confirmation.

Usage Guidelines

Use this command to configure a QoS description table to manage QoS functionality for an ASN-GW service subscriber. This command creates and allows the configuration of QoS tables with in a context. This command is also used to remove previously configured ASN-GW services QoS descriptor table.

A maximum of 16 QoS Descriptor Tables can be configured per system.

Refer to the *ASN QoS Descriptor Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates a QoS descriptor table with identifier *1234* for the ASN-GW service subscribers:

```
asn-qos-descriptor id 1234
```

asn-service-profile

Creates, deletes or manages the Service Profiles Identifier for Access Service Node Gateway (ASN-GW) service subscribers and enters the ASN Service Profile Configuration mode within the current context.

Product

ASN-GW

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

```
asn-service-profile id asn_profile_id direction { bi-directional | downlink
 | uplink } [ activation-trigger { activate | admit | dynamic-reservation
 | provisioned } [ -noconfirm ]
no asn-service-profile id asn_profile_id [ -noconfirm ]
```

no

Deletes a preciously configured ASN service profile identifier.

id *asn-profile_id*

Specifies a unique identifier for ASN profile to create/configure.

direction { bi-directional | downlink | uplink }

Specifies the direction of data traffic to apply this service profile.

bi-directional: Enables this service profile in both direction of uplink and downlink.

downlink: Enables this service profile in downlink direction, towards the subscriber.

uplink: Enables this service profile in uplink direction, towards the system.

activation-trigger { activate | admit | dynamic-reservation | provisioned

Use this option to configure the activation-trigger for the asn-service-profile. Default: provisioned | admit | activate

-noconfirm

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

Caution If this keyword option is used with **no asn-service-profile id** *asn_profile_id* command, the ASN service profile with identifier *asn_profile_id* will be deleted with all active/inactive configurations without prompting any warning or confirmation.

Usage Guidelines Use this command to configure a service profile to apply the ASN-GW service subscribers. This command creates and allows the configuration of service profiles with in a context. This command is also used to remove previously configured ASN-GW services profiles.

A maximum of 32 ASN Service Profiles can be configured per context.

Refer to the *ASN Service Profile Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates an ASN Service Profile with identifier *1234* for the ASN-GW service subscribers:

```
asn-service-profile id 1234 direction uplink
```

asngw-service

Creates, deletes or manages an Access Service Node Gateway (ASN-GW) service and enters the ASN Gateway Service Configuration Mode within the current context.

Product ASN-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

```
asngw-service asngw_name [ -noconfirm ]
no asn-service asngw_name
```

no

Deletes a previously configured ASN-GW service.

asngw_name

Specifies the name of the ASN-GW service to create/configure as an alphanumeric string of 1 through 63 characters that is case sensitive.

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.

Caution If this keyword option is used with **no asn-service** *asngw_name* command, the ASN-GW service named *asngw_name* will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines

Services are configured within a context and enable certain functionality. This command creates and allows the configuration of services enabling the system to function as an ASN Gateway in a WiMAX network. This command is also used to remove previously configured ASN-GW services.

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 (i.e. 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.

Refer to the *ASN Gateway Service Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates an ASN-GW service name *asn-gw1*:

```
asngw-service asn-gw1
```

asnpc-service

Creates, deletes or manages an ASN Paging Controller service to manage the ASN paging controller service and enters the ASN Paging Controller Configuration mode within the current context.

Product

ASN-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

[no] asnpc-service *asn_pc_svc_name* **[-noconfirm]**

no

Deletes a preciously configured ASN paging controller service.

asnpc-service *asn_pc_svc_name*

Specifies the name of the ASN Paging Controller Service to create and enable as an alphanumeric string of 1 through 63 characters that is case sensitive.

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.

Caution If this keyword option is used with **no asnpc-service** *asn_pc_svc_name* command, the ASN Paging Controller service named *asn_pc_svc_name* will be deleted and disabled with all active/inactive paging groups and paging agents configured in a context for ASN paging controller service without prompting any warning or confirmation.

Usage Guidelines

Use this command to create and enable the ASN paging controller services in the system to provide functionality of an ASN Paging Controller service within a context. Additionally this command provides the access to the ASN Paging Controller Service Configuration mode and also used to remove previously configured ASN Paging Controller services.

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 (i.e. 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.

Refer to the *ASN Paging Controller Service Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates an ASN paging controller service name *asnpc_1*:

```
asnpc-service asnpc_1
```

associate

Associate a global QoS Level 2 mapping table to a VPN context.

Product

ePDG

HSGW

P-GW

SAEGW

S-GW

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)#
```

Syntax Description

```
associate l2-mapping-table name map_table_name
 default associate l2-mapping-table
```

default

Associates the system-default table with this context.

name*map_table_name*

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

map_table_name is an alphanumeric string of 0 through 80 characters.

Usage Guidelines

This command is used to associate an internal QoS L2 mapping table to a VPN context. If no explicit association is created/configured, the system-default mapping table is used.

Important

If an l2-mapping-table association is made at both the VRF and VPN level, the VRF level takes precedence.

The mapping table is configured via the Global Configuration mode **qos l2-mapping-table** command.

Example

The following command associates an internal QoS L2 mapping table to a VPN context:

```
associate l2-mapping-table qostable1
```

bfd-protocol

Enables or disables Bidirectional Forwarding Detection (BFD) protocol and enters the BFD Configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
[ no ] bfd-protocol
```

no

If previously configured, disables BFD protocol.

Usage Guidelines Use this command to set configuration parameters for detecting faults in paths established with BFD-enabled routers.

Refer to the *BFD Configuration Mode Commands* chapter for additional information.

Example

The following command enables BFD Configuration mode:

```
bfd-protocol
```

bgp extended-asn-cap

Enables or disables the router to send 4-octet ASN capabilities.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
[ no ] bgp extended-asn-cap
```

no

Disables the ability of the router to send 4-octet ASN capabilities.

Example

The following command enables the router to send 4-octet ASN Capabilities:

```
bgp extended-asn-cap
```

bmsc-profile

Creates or deletes Broadcast Multicast Service Center (BM-SC) profiles and enters the BMSC Profile Configuration Mode within the current context.

Product

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

`[ no ] bmsc-profile name` *`bmsc_profile_name`* **`[ -noconfirm ]`**

no

Deletes a previously configured BM-SC profile.

name *bmsc_profile_name*

Specifies a name for the BM-SC profile as an alphanumeric string of 1 through 62 characters that is case insensitive. It may also contain dots (.) and/or dashes (-).

-noconfirm

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

Caution If this keyword option is used with **no bmsc-profile name** *bmsc_profile_name* command, the BM-SC profile named *bmsc_profile_name* is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines

Use this command to create a BM-SC profile within the context and take the user to enter the BMSC Profile Configuration Mode.

The BM-SC profile is a logical name for a Broadcast Multicast Service Center in Multimedia Broadcast and Multicast service.

BM-SC profile should be created/configured within contexts on the system. Up to four BM-SC profiles can be configured.

Example

The following command creates a BM-SC Profile called *mbms_sc_1*:

bmsc-profile name mbms_sc_1

busyout ip

Makes addresses from an IPv4 pool in the current context unavailable once they are free.

Product

GGSN

HA

NAT

PDSN

P-GW

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] busyout ip pool { all | all-dynamic | all-static | name *pool_name* **} [address-range** *start_address end_address* **| lower-percentage** *percent* **| upper-percentage** *percent* **]**

no

Disables the busyout command specified.

ip

Configure IPv4 busyout information.

pool

Configure IPv4 pool busyout information.

all

Applies to all IPv4 pools in the current context.

all-dynamic

Applies to all dynamic IPv4 pools in the current context.

all-static

Applies to all static IPv4 pools in the current context.

name *pool_name*

Applies the named IP pool or IP pool group in the current context. *pool_name* must be the name of an existing IP pool or IP pool group in the current context.

address-range *start_address end_address*

Busyout all addresses from *start_address* through *end_address*. *start_address*: The beginning IP address of the range of addresses to busyout entered in IPv4 dotted-decimal notation.

end_address: The ending IP address of the range of addresses to busyout. This IP address must exist in the pool specified and entered in IPv4 dotted-decimal notation.

lower-percentage *percent*

Busyout the percentage of IPv4 addresses specified, beginning at the lowest numbered IP address. This is a percentage of all of the IP addresses in the specified IP pool. *percent* must be an integer from 1 through 100.

upper-percentage *percent*

Busyout the percentage of IPv4 addresses specified, beginning at the highest numbered IP address. This is a percentage of all of the IPv4 addresses in the specified IP pool. *percent* must be an integer from 1 through 100.

Usage Guidelines

Use this command to busyout IPv4 addresses when resizing an IPv4 pool.

Up to 32 instances of this command can be executed per context.

A single instance of this command can busy-out multiple IPv4 address pools in the context through the use of the **all**, **all-static**, or **all-dynamic** keywords.

Example

Assume an IPv4 pool named *Pool10* with addresses from *192.168.100.1* through *192.168.100.254*. To busy out the addresses from *192.168.100.50* through *192.169.100.100*, enter the following command:

```
busyout ip pool name Pool10 address-range 192.168.100.50 192.169.100.100
```

To restore the IPv4 addresses from the previous example and make them accessible again, enter the following command:

```
no busyout ip pool name Pool10 address-range 192.168.100.50 192.169.100.100
```

busyout ipv6

Makes addresses from an IPv6 pool in the current context unavailable once they are free.

Product

GGSN

HA

NAT

PDSN

P-GW

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] busyout ipv6 pool { all | all-dynamic | all-static | name *pool_name* **} [address-range** *start_address end_address* **| lower-percentage** *percent* **| upper-percentage** *percent* **]**

no

Disables the busyout command specified.

ipv6

Configure IPv6 busyout information.

pool

Configure IPv6 pool busyout information.

all

Applies to all IPv6 pools in the current context.

all-dynamic

Applies to all dynamic IPv6 pools in the current context.

all-static

Applies to all static IPv6 pools in the current context.

name *pool_name*

Applies the named IPv6 pool or IPv6 pool group in the current context. *pool_name* must be the name of an existing IPv6 pool or IPv6 pool group in the current context.

address-range *start_address end_address*

Busyout all addresses from *start_address* through *end_address*. *start_address*: The beginning IP address of the range of addresses to busyout entered in IPv6 colon-separated-hexadecimal notation.

end_address: The ending IP address of the range of addresses to busyout. This IP address must exist in the pool specified and entered in IPv6 colon-separated-hexadecimal notation.

lower-percentage *percent*

Busyout the percentage of IP addresses specified, beginning at the lowest numbered IPv6 address. This is a percentage of all of the IP addresses in the specified IP pool. *percent* must be an integer from 1 through 100.

upper-percentage *percent*

Busyout the percentage of IP addresses specified, beginning at the highest numbered IPv6 address. This is a percentage of all of the IP addresses in the specified IP pool. *percent* must be an integer from 1 through 100.

Usage Guidelines

Use this command to busyout IPv6 addresses when resizing an IPv6 pool.

Up to 32 instances of this command can be executed per context.

A single instance of this command can busy-out multiple IP address pools in the context through the use of the **all**, **all-static**, or **all-dynamic** keywords.

Example

Assume an IP pool named *Pool12*. To busy out the addresses from *2700:2010:8003::* through *2700:2010:8003::*, enter the following command:

```
busyout ipv6 pool name Pool12 address-range 2700:2010:8003::
2700:2010:8003::
```

To restore the IPv6 addresses from the previous example and make them accessible again, enter the following command:

```
no busyout ipv6 pool name Pool10 address-range 2700:2010:8003::
2700:2010:8003::
```

cae-group

Creates a CAE group, which is a CAE server cluster that services TCP video requests from the Mobile Video Gateway. The Mobile Video Gateway uses the configured CAE group for CAE load balancing. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape.

Important In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product MVG

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 ] cae-group`** *`cae_group_name`* **`[ -noconfirm ]`**

no*cae_group_name*

Deletes the CAE group if previously configured.

cae_group_name

Creates the specified CAE group and enters the Video Group Configuration Mode. *cae_group_name* is an alphanumeric string of 1 through 79 characters.

-noconfirm

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

Usage Guidelines Use this command to create a CAE group and enter the Video Group Configuration Mode. This command gets issued from the Context Configuration Mode.

Example

The following command creates a CAE group named *group_1* and enters the Video Group Configuration Mode:

```
cae-group group_!
```

camel-service

Creates an instance of the Customized Applications for Mobile Enhanced Logic (CAMEL) service and enters the CAMEL service configuration mode. This mode configures or edits the configuration for the parameters which control the CAMEL functionality on the SGSN.

Important For details about the commands and parameters, check the *CAMEL 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 ] camel-service` *`srvc_name`*

no

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

srvc_name

Creates a CAMEL service instance having a unique name expressed 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 create, edit, or remove an CAMEL service

Example

The following command creates an CAMEL service named *camel1* in the current context:

```
camel-service camel1
```

The following command removes the CAMEL service named *camel2* from the configuration for the current context:

```
no camel-service camel2
```

cbs-service

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

Creates a new Cell Broadcasting Service (CBS) or specifies an existing CBS and enters the CBS Configuration Mode.

Product HNB-GW

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] cbs-service *name*

no

Removes the specified CBS service from the context.

name

Specifies the name of a new or existing CBS service as an alphanumeric string of 1 through 63 characters that must be unique within the same context and across all contexts.

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

Usage Guidelines

Use this command to create a new CBS service or modify an existing one.

CBS Configuration Mode commands are defined in the *CBS Configuration Mode Commands* chapter of this guide.

Example

Following command creates a new CBS service names *test-cbs* in the context configuration mode:

cbs-service*test-cbs*

cipher-suite

Creates a new SSL cipher suite or specifies an existing cipher suite and enters the Cipher Suite 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] cipher-suite *name*

no

Removes the specified SSL cipher suite from the context.

name

Specifies the name of a new or existing SSL cipher suite as n alphanumeric string of 1 through 127 characters that must be unique across all CSCF services within the same context and across all contexts.

Usage Guidelines

Use this command to create a new SSL cipher suite or modify an existing one.

Important One SSL cipher suite can be created per SSL template.

A cipher suite contains the cryptographic algorithms supported by the client, and defines a key exchange and a cipher spec, which specifies the encryption and hash algorithms used during authentication. SSL cipher suites allow operators to select levels of security and to enable communication between devices with different security requirements.

Entering this command results in the following prompt:

```
[context_name]hostname(cfg-ctx-cipher-suite)#
```

Cipher Suite Configuration Mode commands are defined in the *Cipher Suite Configuration Mode Commands* chapter.

Example

The following command specifies the SSL cipher suite *cipher_suite_1* and enters the Cipher Suite Configuration Mode:

```
cipher-suite cipher_suite_1
```

class-map

Creates or deletes a class map. If the class-map is newly created, the system enters the Class-Map Configuration Mode within the current destination context to configure the match rules for packet classification to flow-based traffic policing for a subscriber session flow.

Product

ASN-GW

HA

HSGW

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

`[ no ] class-map name` *`class_name`* **`[ match-all | match-any ]`**

no

Deletes configured Class-Map within the context.

class_name

Specifies the name of Class-Map rule as an alphanumeric string of 1 through 15 characters and is case sensitive.

match-all

Default: Enabled.

Enables AND logic for all matching parameters configured in specific Class-Map to classify traffic flow/packets. It indicates to match all classification rules in specific Class-Map to consider the specified Class-Map as a match.

match-any

Default: Disabled.

Enables OR logic for matching parameters configured in specific Class-Map to classify traffic flow/packets. It indicates to match any of the classification rule in specific Class-Map to consider the specified Class-Map as a match.

Usage Guidelines

Use this command to enter in Class-Map Configuration Mode to set classification parameters or filters in traffic policy for a subscriber session flow.

Important

In this mode classification rules added sequentially with **match** command to form a Class-Map. To change and/or delete or re-add a particular rule entire Class-Map is required to delete.

Example

Following command configures classification map *class_map1* with option to match any condition in match rule.

```
class-map name class_map1 match-any
```

closedrp-rp handoff

Enables or disables session handoff between Closed-RP and RP connections. Default: Disabled

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 **[default | no] closedrp-rp handoff**

default

Resets the command to its default setting of disabled.

no

Disables Closed-RP to RP session handoff.

Usage Guidelines Use this command to enable a PDSN service to handoff sessions between Closed-RP and RP connections.

Example

To enable Closed-RP to RP handoffs, use the following command:

closedrp-rp handoff

To disable Closed-RP to RP handoffs, use the following command:

no closedrp-rp handoff

config-administrator

Configures a context-level configuration administrator account within the current context.

Product All

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

config-administrator *user_name* **[encrypted] [nopassword] password***password* **[ecs] [expiry-date** *date_time* **] [ftp [sftp-server** *sftp_name* **] }] [li-administration] [noconsole] [nocli] [noecs] [timeout-absolute** *abs_seconds* **] [timeout-min-absolute** *abs_minutes* **] [timeout-idle** *timeout_duration* **] [timeout-min-idle** *idle_minutes* **]**
no config-administrator *user_name*

no

Removes a previously configured context-level configuration administrator account.

user_name

Specifies the name for the account as an alphanumeric string of 1 through 32 characters.

[encrypted] password *password*

Specifies the password to use for the user which is being given context-level administrator privileges within the current context. The encrypted keyword indicates the password specified uses encryption.

password is an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 characters with encryption.

The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

[nopassword]

This option allows you to create a configuration administrator without an associated password. Enable this option when using ssh public keys (**authorized key** command in SSH Configuration mode) as a sole means of authentication. When enabled this option prevents someone from using a configuration administrator password to gain access to the user account.

ecs

Permits the user access to ACS-specific configuration commands. Default: Enhanced Charging Service (ECS / ACS) specific configuration commands allowed.

expiry-date *date_time*

Specifies the date and time that this account expires in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.

Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

ftp

Indicates the user gains FTP and SFTP access with the administrator privileges. Default: FTP and SFTP are not allowed.

[sftp-server *sftp_name*]

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

li-administration

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

nocli

Indicates the user is not allowed to access the command line interface. Default: CLI access allowed.

noconsole

Disables user access to a Console line.

Note The Global Configuration mode **local-user allow-aaa-authentication noconsole** command takes precedence in a normal (non-Trusted) StarOS build. In this case, all AAA-based users cannot access a Console line.

noecs

Prevents the specific user from accessing ACS-specific configuration commands.

timeout-absolute *abs_seconds*

Important This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of time (in seconds) that the administrator may have a session active before the session is forcibly terminated. *abs_seconds* must be an integer from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

timeout-min-absolute *abs_minutes*

Specifies the maximum amount of time (in minutes) the context-level administrator may have a session active before the session is forcibly terminated. *abs_minutes* must be an integer from 0 through 525600 (365 days). The value 0 disables the absolute timeout. Default: 0

timeout-idle *timeout_duration*

Important This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of idle time, in seconds, the context-level administrator may have a session active before the session is terminated. *timeout_duration* must be a value in the range from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

timeout-min-idle *idle_minutes*

Specifies the maximum amount of idle time, in minutes, the context-level administrator may have a session active before the session is terminated. *idle_minutes* must be a value in the range from 0 through 525600 (365 days). The value0 disables the idle timeout. Default: 0

Usage Guidelines

Create new context-level configuration administrators or modify existing administrator's options, in particular, the timeout values.

Configuration administrator users have read-write privileges and full access to all contexts and command modes except for security functions. Refer to the *Command Line Interface Overview* chapter of this guide for more information.

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

Example

The following configures a context-level administration named *user1* with ACS parameter control:

```
config-administrator user1 password secretPassword ecs
```

The following command removes a context-level administrator named *user1*:

```
no config-administrator user1
```

content-filtering

Enables or disables the creation, configuration or deletion of Content Filtering Server Groups (CFSG).

Product CF

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

```
content-filtering server-group cf_server_group_name [ -noconfirm ]
no content-filtering server-group cf_server_group_name
```

no

Removes the specified CFSG previously configured in this context.

server-group *cf_server_group_name*

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

-noconfirm

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

Usage Guidelines Use this command to create/configure/delete a CFSG.

Example

The following command creates a CFSG named *CF_Server1*:

```
content-filtering server-group CF_Server1
```

credit-control-service

Enables or disables the creation, configuration or deletion of credit-control services.

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

credit-control-service *service_name* **[-noconfirm]**
no credit-control-service *service_name*

no

Deletes the specified credit-control service.

service_name

Specifies name of the credit-control service as an alphanumeric string of 1 through 63 characters.

If the named credit-control service does not exist, it is created, and the CLI mode changes to the Credit Control Service Configuration Mode wherein the service can be configured.

If the named credit-control service already exists, the CLI mode changes to the Credit Control Service Configuration Mode wherein the service can be configured.

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, configure or delete credit-control services.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-credit-control-service)

Credit control Service Configuration commands are described in the *Credit Control Service Configuration Mode Commands* chapter.

Example

The following command enters the Credit Control Service Configuration Mode for a credit-control service named *test159*:

```
credit-control-service test159
```

crypto dns-nameresolver

Enables or disables the reverse DNS query from a Security Gateway to DNS.

Product

All IPsec security gateway products

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 > 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] crypto dns-nameresolver

no

Disables the Reverse DNS query.

Usage Guidelines

Use this command to enable or disable the reverse DNS query from a WSG to DNS.

Important

You must configure the DNS client prior to enabling the Reverse DNS query.

Example

The following command enables the reverse DNS query:

```
crypto dns-nameresolver
```

crypto group

Creates or deletes a crypto group and enters the Crypto Configuration Mode allowing the configuration of crypto group parameters.

Product

HA

GGSN

PDIF

PDSN

SCM

Privilege

Administrator, Config-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 ] crypto group` *`group_name`*

no

Deletes a previously configured crypto group.

group_name

Specifies the name of the crypto group as an alphanumeric string of 1 through 127 characters that is case sensitive.

Important

A maximum of 32 crypto groups per context can be configured.

Usage Guidelines

Use this command to enter the configuration mode allowing the configuration of crypto group parameters.

Crypto (tunnel) groups are used to support the Redundant IPSec Tunnel Fail-over feature and consist of two configured ISAKMP crypto maps. Each crypto map defines the IPSec policy for a tunnel. In the crypto group, one tunnel serves as the primary, the other as the secondary (redundant).

Example

The following command configures a crypto group called *group1*:

```
crypto group group1
```

crypto ipsec transform-set

Configures transform-sets on the system and enters the Crypto IPSec Transform Set Configuration Mode.

Product

PDSN

PDIF

HA

GGSN

SCM

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

```
crypto ipsec transform-set transform_name [ ah { hmac { md5-96 | none |
sha1-96 } { esp { hmac { { md5-96 | sha1-96 } { cipher { 3des-cbc |
aes-cbc-128 | aes-cbc-256 | des-cbc } } | none } } } } ]
no crypto ipsec transform-set transform_name
```

no

Removes a previously configured transform set

transform_name

Specifies the name of the transform set as an alphanumeric string of 1 through 127 characters that is case sensitive.

ah hmac

Configures the Authentication Header (AH) hash message authentication codes (HMAC) parameter for the transform set to one of the following:

- **md5-96**:Message Digest 5 truncated to 96 bits
- **sha1-96**:Secure Hash Algorithm-1 truncated to 96 bits

esp hmac

Configures the Encapsulating Security Payload (ESP) hash message authentication codes (HMAC) parameter for the transform set to one of the following:

- **md5-96**:Message Digest 5 truncated to 96 bits
- **none**: Disables the use of the AH protocol for the transform set.
- **sha1-96**:Secure Hash Algorithm-1 truncated to 96 bits

cipher

If ESP is enabled, this option must be used to set the encapsulation cipher protocol to one of the following:

- **3des-cbc**: Triple Data Encryption Standard (3DES) in chain block (CBC) mode.
- **aes-cbc-128**: Advanced Encryption Standard (AES) in CBC mode with a 128-bit key.
- **aes-cbc-256**: Advanced Encryption Standard (AES) in CBC mode with a 256-bit key.
- **des-cbc**: DES in CBC mode.

Usage Guidelines

Use this command to create a transform set on the system.

Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.

Transform sets are used during Phase 2 of IPSec establishment. In this phase, the system and a peer security gateway negotiate one or more transform sets (IPSec SAs) containing the rules for protecting packets. This negotiation ensures that both peers can properly protect and process the packets.

Example

Create a transform set that has the name *tset1*, no authentication header, an encapsulating security protocol header hash message authentication code of **md5**, and a bulk payload encryption algorithm of **des-cbc** with the following command:

```
crypto ipsec transform-set tset1 ah hmac none esp hmac md5 cipher des-cbc
```

crypto map

Configures the name of the policy and enters the specified Crypto Map Configuration mode.

Product

PDSN

HA

GGSN

SCM

P-GW

PDIF

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

crypto map *name* **[ikev2-ipv6 | ipsec-dynamic | ipsec-ikev1 | ipsec-manual]**
no crypto map *name*

no

Removes a previously configured crypto map.

name

Specifies the name of the crypto map as an alphanumeric string of 1 through 127 characters that is case sensitive.

ikev2-ipv6

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

ipsec-dynamic

Creates a dynamic crypto map and/or enters the Crypto Map Dynamic Configuration Mode.

ipsec-ikev1

Creates an IKEv1 crypto map and/or enters the Crypto Map IKEv1 Configuration Mode.

ipsec-manual

Creates a manual crypto map and/or enters the Crypto Map Manual Configuration Mode.

Usage Guidelines

Crypto Maps define the policies that determine how IPSec is implemented for subscriber data packets. There are several types of crypto maps supported by the system. They are:

- **Manual crypto maps**: These are static tunnels that use pre-configured information (including security keys) for establishment. Because they rely on statically configured information, once created, the tunnels never expire; they exist until their configuration is deleted.

Important Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, it is recommended that they only be configured and used for testing purposes.

- **IKEv1 crypto maps**: These tunnels are similar to manual crypto maps in that they require some statically configured information such as the IP address of a peer security gateway and that they are applied to specific system interfaces. However, IKEv1 crypto maps offer greater security because they rely on dynamically generated security associations through the use of the Internet Key Exchange (IKE) protocol.
- **IKEv2-IPv6 cryptomaps**: Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.
- **Dynamic crypto maps:** These tunnels are used for protecting L2TP-encapsulated data between the system and an LNS/security gateway or Mobile IP data between an FA service configured on one system and an HA service configured on another.

Important The crypto map type (dynamic, IKEv1, IKEv2-IPv6, or manual) is specified when the map is first created using this command.

Example

Create a dynamic crypto map named *map1* and enter the Crypto Map Dynamic Configuration Mode by entering the following command:

```
crypto map map1 ipsec-dynamic
```

crypto template

Creates a new or specifies an existing crypto template or crypto vendor template and enters the Crypto Template Configuration Mode or Crypto Template IKEv2-Vendor Configuration Mode.

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

Product

ePDG

HeNBGW

PDIF

SAEGW

S-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

```
crypto template name { ikev2-dynamic | ikev2-vendor }
no crypto template name
```

no

Removes a previously configured crypto template.

name ikev2-pdif

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

ikev2-dynamic

Configures the Crypto Template to be used for IPSec functionalities.

ikev2-vendor

Configures the Crypto Vendor Template to be used for IPSec functionalities.

Usage Guidelines

Use this command to create a new or enter an existing crypto template or crypto vendor template.

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

The Crypto Template IKEv2-Vendor Configuration Mode commands are defined in the *Crypto Template IKEv2-Vendor Configuration Mode Commands* chapter.

Example

The following command configures a IKEv2 dynamic crypto template called *crypto1* and enters the Crypto Template Configuration Mode:

```
crypto template crypto1 ikev2-dynamic
```

crypto vendor-policy

Creates a new or specifies an existing crypto vendor policy and enters the Crypto Vendor Policy Configuration Mode.

Product

ePDG

HeNBGW

PDIF

SAEGW

S-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

`[ no ] crypto vendor-policy` *`policy_name`*

no

Removes the previously configured vendor policy.

policy_name

policy_name must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to Creates a new or specifies an existing crypto vendor policy and enters the Crypto Vendor Policy Configuration Mode. A maximum of 32 vendor policies can be configured.

The Crypto Vendor Policy Configuration Mode commands are defined in the *Crypto Vendor Policy Configuration Mode Commands* chapter.

Example

The following command configures a crypto vendor policy called *vodvp1* and enters the Crypto Vendor Policy Configuration Mode:

```
crypto vendor-policy vodvp1
```

css server

In StarOS 9.0 and later releases, this command is obsolete. And, in earlier releases, this command is restricted.

description

Allows you to enter descriptive text for this configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
description text
no description
```

no

Clears the description for this configuration.

text

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines

The description should provide useful information about this configuration.

dhcp-client-profile

Adds a specified Dynamic Host Control Protocol (DHCP) client profile name to allow configuration of DHCP client profile to the current context and enters the configuration mode for that profile.

Product

GGSN

P-GW

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]dhcp-client-profile *clnt_profile_name* **[-noconfirm]**

no

Removes a previously configured DHCP client profile from the current context.

clnt_profile_name

Specifies the name of the DHCP client profile as an alphanumeric string of 1 through 63 characters that is case sensitive.

-noconfirm

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

⚠

Caution If this keyword option is used with **no dhcp-client-profile** *clnt_profile_name* command the DHCP client profile named *clnt_profile_name* is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines

Use this command to add a DHCP client profile to a context configured on the system and enter the DHCP Client Profile Configuration Mode.

Entering this command results in the following prompt:

```
[context_name]hostname(config-dhcp-client-profile)#
```

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

Example

The following command creates a DHCP client profile called *test_profile* :

dhcp-client-profile *test_profile*

dhcp-server-profile

Adds a specified Dynamic Host Control Protocol (DHCP) server profile name to allow configuration of DHCP server profile to the current context and enters the configuration mode for that profile.

Product

GGSN

P-GW

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]dhcp-server-profile *srvr_profile_name* **[-noconfirm]**

no

Removes a previously configured DHCP server profile from the current context.

srvr_profile_name

Specifies the name of the DHCP server profile as an alphanumeric string of 1 through 63 characters that is case sensitive.

-noconfirm

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

Caution If this keyword option is used with **no dhcp-server-profile** *srvr_profile_name* command the DHCP server profile named *srvr_profile_name* is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines

Use this command to add a DHCP server profile to a context configured on the system and enter the DHCP Server Profile Configuration Mode.

Entering this command results in the following prompt:

```
[context_name]hostname(config-dhcp-server-profile)#
```

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

Example

The following command creates a DHCP server profile called *test_server_profile* :

dhcp-server-profile *test_server_profile*

dhcp-service

Adds a Dynamic Host Control Protocol (DHCP) service instance to the current context and enters the DHCP Service Configuration mode for that service.

Product

ASN-GW

eWAG

GGSN

HA

P-GW

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

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

no

Removes a previously configured DHCP service from the current context.

service_name

Specifies the name of the DHCP service as an alphanumeric string of 1 through 63 characters that is case sensitive.

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 add a DHCP service to a context configured on the system and enter the DHCP Service Configuration Mode. A DHCP service is a logical grouping of external DHCP servers.

The DHCP Configuration Mode provides parameters that dictate the system's communication with one or more of these DHCP servers.

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 (i.e. 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.

Refer to the *DHCP Service Configuration Mode* chapter of this reference for additional information.

Example

The following command creates a DHCP service called *dhcp1* and enters the DHCP Service Configuration Mode:

```
dhcp-service dhcp1
```

dhcpv6-service

Creates a specified DHCPv6 service name to allow configuration of DHCPv6 service to the current context and enters the configuration mode for that service.

Product

GGSN

P-GW

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 ]dhcpv6-service` *`service_name`* **`[ -noconfirm ]`**

no

Removes a previously configured DHCPv6 service from the current context.

service_name

Specifies the name of the DHCPv6 service as an alphanumeric string of 1 through 63 characters that is case sensitive.

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.

Caution If this keyword option is used with **no dhcpv6-service** *service_name* command the DHCPv6 service named *service_name* is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines

Use this command to add a DHCPv6 service to a context configured on the system and enter the DHCPv6 Service Configuration Mode.

The DHCPv6 Service Configuration Mode provides parameters that dictate the system's communication with one or more of these DHCPv6 servers.

Entering this command results in the following prompt:

```
[context_name]hostname(config-dhcpv6-service)#
```

DHCPv6 Service Configuration Mode commands are defined in the *DHCPv6 Service Configuration Mode Commands* chapter.

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

Example

The following command creates a DHCPv6 service called *dhcpv6* and enter the DHCPv6 Service Configuration Mode:

```
dhcpv6-service dhcpv6
```

diameter accounting

This command configures Diameter accounting related settings.

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

diameter accounting { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus } | endpoint *endpoint_name* **| hd-mode fall-back-to-local | hd-storage-policy** *hd_policy* **| max-retries** *max_retries* **| max-transmissions** *transmissions* **| request-timeout**

duration **| server** *host_name* **priority** *priority* **}**
default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions | request-timeout }
no diameter accounting { endpoint | hd-mode | hd-storage-policy | max-retries | max-transmissions | server *host_name* **}**

no diameter accounting { endpoint | hd-mode | hd-storage-policy | max-retries | max-transmissions | server *host_name* }

endpoint: Removes the currently configured accounting endpoint. The default accounting server configured in the default AAA group will be used.

hd-mode:Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.

hd-storage-policy: Disables use of the specified HD storage policy.

max-retries: Disables the retry attempts for Diameter accounting in this AAA group.

max-transmissions: Disables the maximum number of transmission attempts for Diameter accounting in this AAA group.

server *host_name*: Removes the Diameter host *host_name* from this AAA server group for Diameter accounting.

default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions | request-timeout }

dictionary: Sets the context's dictionary to the default.

hd-mode:Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.

max-retries:0 (disabled)

max-transmissions:0 (disabled)

request-timeout:20 seconds

dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus }

Specifies the Diameter accounting dictionary.

aaa-custom1 ... aaa-custom10:Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used.

dynamic-load:Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters.For more information on dynamic loading of Diameter dictionaries, see the **diameter dynamic-dictionary** in the *Global Configuration Mode Commands* chapter of this guide.

nasreq: nasreq dictionary—the dictionary defined by RFC 3588.

rf-plus:RF Plus dictionary.

endpoint *endpoint_name*

Enables Diameter to be used for accounting, and specifies which Diameter endpoint to use.

endpoint_name is an alphanumeric string of 1 through 63 characters.

hd-mode fall-back-to-local

Specifies that records be copied to the local HDD if the Diameter server is down or unreachable. CDF/CGF will pull the records through SFTP.

hd-storage-policy *hd_policy*

Specifies the HD Storage policy name.

hd_policy must be the name of a configured HD Storage policy, expressed as an alphanumeric string of 1 through 63 characters.

HD storage policies are configured through the Global Configuration Mode.

This and the **hd-mode** command are used to enable the storage of Rf Diameter Messages to HDD incase all Diameter Servers are down or unreachable.

max-retries *max_retries*

Specifies how many times a Diameter request should be retried with the same server, if the server fails to respond to a request.

max_retries specifies the maximum number of retry attempts. The value must be an integer from 1 through 1000.

Default: 0

max-transmissions *transmissions*

Specifies the maximum number of transmission attempts for a Diameter request. Use this in conjunction with the "**max-retries** *max_retries*" option to control how many servers will be attempted to communicate with.

transmissions specifies the maximum number of transmission attempts for a Diameter request. The value must be an integer from 1 through 1000. Default: 0

request-timeout *duration*

Specifies how long the system will wait for a response from a Diameter server before re-transmitting the request.

duration specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request. This value must be an integer from 1 through 3600. Default: 20

server *host_name* priority *priority*

Specifies the current context Diameter accounting server's host name and priority.

host_name specifies the Diameter host name, expressed as an alphanumeric string of 1 through 63 characters.

priority specifies the relative priority of this Diameter host. The priority is used in server selection. The priority must be an integer from 1 through 1000.

Usage Guidelines

Use this command to manage the Diameter accounting options according to the Diameter server used for the context.

Example

The following command configures the Diameter accounting dictionary as **aaa-custom4**:

```
diameter accounting dictionary aaa-custom4
```

The following command configures the Diameter endpoint named *aaaa_test*:

```
diameter accounting endpoint aaaa_test
```

diameter authentication

This command configures Diameter authentication related settings.

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

diameter authentication { allow any-host | dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq } | endpoint *endpoint_name* **| max-retries** *max_retries* **| max-transmissions** *transmissions* **| redirect-host-avp { just-primary | primary-then-secondary } | request-timeout** *duration* **| server** *host_name* **priority** *priority* **}**
default diameter authentication { dictionary | max-retries | max-transmissions | redirect-host-avp | request-timeout }
no diameter authentication { endpoint | max-retries | max-transmissions | server *host_name* **}**

no diameter authentication { allow any-host | endpoint | max-retries | max-transmissions | server *host_name* }

- **allow any-host**: Accept the response from any-host.
- **endpoint**: Removes the authentication endpoint. The default server configured in default AAA group will be used.
- **max-retries**: Disables the retry attempts for Diameter authentication in this AAA group.
- **max-transmissions**: Disables the maximum transmission attempts for Diameter authentication in this AAA group.

- **server** *host_name*: Removes the Diameter host *host_name* from this AAA server group for Diameter authentication.

default diameter authentication { dictionary | max-retries | max-transmissions | redirect-host-avp | request-timeout }

Configures default setting for specified parameter.

- **allow any-host**: Sets the default behaviour.
- **dictionary**: Sets the context's dictionary to the default.
- **max-retries**: Sets the retry attempts for Diameter authentication requests in this AAA group to default 0 (disable).
- **max-transmissions**: Sets the configured maximum transmission attempts for Diameter authentication in this AAA group to default 0 (disable).
- **redirect-host-avp**: Sets the redirect choice to default (just-primary).
- **request-timeout**: Sets the timeout duration, in seconds, for Diameter authentication requests in this AAA group to default (20).

dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq }

Specifies the Diameter authentication dictionary.

aaa-custom1 ... aaa-custom8,aaa-custom10 ... aaa-custom20: Configures the custom dictionaries.Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used.

Important **aaa-custom11** dictionary is only available in Release 8.1 and later. **aaa-custom12** to **aaa-custom20** dictionaries are only available in Release 9.0 and later releases.

aaa-custom9: Configures the STa standard dictionary.

dynamic-load: Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters.For more information on dynamic loading of Diameter dictionaries, see the **diameter dynamic-dictionary** in the *Global Configuration Mode Commands* chapter of this guide.

nasreq: nasreq dictionary—the dictionary defined by RFC 3588.

endpoint *endpoint_name*

Enables Diameter to be used for authentication, and specifies which Diameter endpoint to use.

endpoint_name is an alphanumeric string of 1 through 63 characters.

max-retries *max_retries*

Specifies how many times a Diameter authentication request should be retried with the same server, if the server fails to respond to a request.

max_retries specifies the maximum number of retry attempts, and must be an integer from 1 through 1000. Default: 0

max-transmissions *transmissions*

Specifies the maximum number of transmission attempts for a Diameter authentication request. Use this in conjunction with the "**max-retries** *max_retries*" option to control how many servers will be attempted to communicate with.

transmissions specifies the maximum number of transmission attempts, and must be an integer from 1 through 1000. Default: 0

diameter authentication redirect-host-avp { just-primary | primary-then-secondary }

Specifies whether to use just one returned AVP, or use the first returned AVP as selecting the primary host and the second returned AVP as selecting the secondary host.

just-primary:Redirect only to primary host.

primary-then-secondary:Redirect to primary host, if fails then redirect to the secondary host.

Default: **just-primary**

request-timeout *duration*

Specifies how long the system will wait for a response from a Diameter server before re-transmitting the request.

duration specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request, and must bean integer from 1 through 3600. Default: 20

server *host_name* priority *priority*

Specifies the current context Diameter authentication server's host name and priority.

host_name specifies the Diameter host name, expressed as an alphanumeric string of 1 through 63 characters.

priority specifies the relative priority of this Diameter host, and must be an integer from 1 through 1000. The priority is used in server selection.

Usage Guidelines

Use this command to manage the Diameter authentication configurations according to the Diameter server used for the context.

Example

The following command configures the Diameter authentication dictionary *aaa-custom14*:

```
diameter authentication dictionary aaa-custom14
```

The following command configures the Diameter endpoint named *aaau1*:

```
diameter authentication endpoint aaau1
```

diameter authentication failure-handling

This command configures error handling for Diameter EAP requests.

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

diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } { request-timeout action { continue | retry-and-terminate | terminate } | result-code *result_code* **{ [to** *end_result_code* **] action { continue | retry-and-terminate | terminate } } }**
no diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } result-code *result_code* **[to** *end_result_code* **]**
default diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } request-timeout action

no

Disables Diameter authentication failure handling.

default

Configures the default Diameter authentication failure handling setting.

authorization-request

Specifies that failure handling is to be performed on Diameter authorization request messages (AAR/AAA).

eap-request

Specifies configuring failure handling for EAP requests.

eap-termination-request

Specifies configuring failure handling for EAP termination requests.

request-timeout action { continue | retry-and-terminate | terminate }

Specifies the action to be taken for failures:

- **continue**:Continues the session
- **retry-and-terminate**:First retries, if it fails then terminates the session

- **terminate**: Terminates the session

result-code *result_code* { [to *end_result_code*] action { continue | retry-and-terminate | terminate } }

result_code: Specifies the result code, must be an integer from 1 through 65535.

to *end_result_code*: Specifies the upper limit of a range of result codes. *end_result_code* must be greater than *result_code*.

action { continue | retry-and-terminate | terminate }: Specifies action to be taken for failures:

- **continue**:Continues the session
- **retry-and-terminate**:First retries, if it fails then terminates the session
- **terminate**: Terminates the session

Important For any failure encountered, the "continue" option terminates the call as with the "terminate" option for all Diameter dictionaries except aaa-custom15 dictionary. This behavior is true in releases prior to 20. In 20 and later releases, the "continue" option is applicable for all S6b dictionaries including aaa-custom15 dictionary.

Usage Guidelines Use this command to configure error handling for Diameter EAP, EAP-termination, and authorization requests.Specific actions (continue, retry-and-terminate, or terminate) can be associated with each possible result-code. Ranges of result codes can be defined with the same action, or actions can be specific on a per-result code basis.

Example

The following commands configure result codes 5001, 5002, 5004, and 5005 to use **action continue** and result code 5003 to use **action terminate**:

```
diameter authentication failure-handling eap-request result-code 5002 to
 5005 action continue
diameter authentication failure-handling eap-request result-code 5003
action terminate
```

diameter dictionary

This command is deprecated and is replaced by the **diameter accounting dictionary** and **diameter authentication dictionary** commands. See **diameter accounting** and **diameter authentication** commands respectively.

diameter endpoint

This command enables the creation, configuration or deletion of a Diameter endpoint.

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 ] diameter endpoint` *`endpoint_name`* **`[ -noconfirm ]`**

no

Removes the specified Diameter endpoint.

Important

In 19.5, 21.0 and later releases, deleting the endpoint using the "no diameter endpoint" command throws the following warning message and prompts for user's confirmation:

```
Warning: It is not recommended to remove the diameter endpoint when there are active calls
 on the system. Hence, please adhere to the 'Method of Procedure' to remove the endpoint.
Otherwise, the system behavior would be undefined.

Are you sure? [Yes|No]:
```

Method of Procedure: The following two steps should be performed in the same order to remove the Diameter endpoint:

1. To disable/breakdown the link/transport connections:
    1. Disable all the peers in the endpoint using the **diameter disable endpoint** *endpoint_name* **peer** *peer-name* CLI command. Repeat this command for all the peers in the endpoint. This will trigger the Disconnect-Peer-Request (DPR) towards the peers with the configured disconnection cause, that is to indicate, graceful shut down.
    2. Remove the endpoint in the respective context, under Diameter configuration, by using the **no endpoint** *endpoint-name* CLI command.
2. To enable/bring up the transport connections, follow the standard procedure of adding the endpoints and corresponding peers in it.
    1. Add the endpoints with "use diamproxy" option. Else, the links will be established from Session Manager via diabase library.
    2. Add the corresponding peers in the endpoints.

endpoint_name

Specifies name of the Diameter endpoint as an alphanumeric string of 1 through 63 characters that should be unique within the system.

If the named endpoint does not exist, it is created, and the CLI mode changes to the Diameter Endpoint Configuration Mode wherein the endpoint can be configured.

If the named endpoint already exists, the CLI mode changes to the Diameter Endpoint Configuration Mode wherein the endpoint can be reconfigured.

-noconfirm

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

Usage Guidelines

Use this command to create/configure/delete a Diameter origin endpoint.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-ctx-diameter)

Diameter origin endpoint configuration commands are described in the *Diameter Endpoint Configuration Mode Commands* chapter.

Example(s)

The following command changes to the Diameter Endpoint Configuration CLI mode for Diameter origin endpoint named *test13*:

```
diameter endpoint test13
```

The following command will throw the warning message and prompt for user's confirmation to remove the Diameter endpoint named *test13*. **Yes** will remove the endpoint *test13*. **No** will abort the action and the endpoint *test13* will not be removed:

```
no diameter endpoint test13
Warning: It is not recommended to remove the diameter endpoint when there are active calls
 on the system. Hence, please adhere to the 'Method of Procedure' to remove the endpoint.
Otherwise, the system behavior would be undefined.
Are you sure? [Yes|No]: No
Action aborted
```

The following command will remove the endpoint *test13* without any additional prompt and confirmation from the user:

```
no diameter endpoint test13 -noconfirm
```

diameter-hdd-module

This command enables/disables the creation, configuration or deletion of the Hard Disk Drive (HDD) module in the context.

Important This command is license dependent. For more information, contact your Cisco account representative.

Product

HA

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

[no] diameter-hdd-module

no

Deletes the HDD module from the context.

Usage Guidelines

In cases where the Assume-Positive interim-quota is allocated, and CCR-T message is not reported/answered, the failed CCR-T message is written to a local file, and saved in the HDD. This local file and directory information can be passed to the customer, and can be fetched and parsed to account for the lost bytes/usage. The retrieval of the file can be done with the PULL mechanism.

Important This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information on the licensing requirements.

The **diameter-hdd-module** CLI command is used to create the HDD module for the context, and configure the HDD module for storing the failed CCR-T messages.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-diameter-hdd)#

Diameter HDD Module Configuration Mode commands are defined in the *Diameter HDD Module Configuration Mode commands* chapter.

Important This feature is applicable only when Assume Positive feature is enabled.

This feature is controlled through the **diameter hdd** CLI command introduced in the Credit Control Group configuration mode. For more information on the command, see the *Credit Control Configuration Mode Commands* chapter.

Example

The following command configures the Diameter HDD module in a context:

diameter hdd-module

diameter sctp

This command configures Diameter SCTP parameters for all Diameter endpoints within the context. In 12.2 and later releases, this command is obsolete and replaced with **associate sctp-parameters-template** command in the Diameter Endpoint 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

diameter sctp { hearbeat-interval *interval* **| path max-retransmissions** *retransmissions* **}**
default diameter sctp { heartbeat-interval | path max-retransmissions }

default

Configures this command with the default settings.

- **heartbeat-interval**: Sets the heartbeat interval to the default value.
- **path max-retransmissions**: Sets the SCTP path maximum retransmissions to the default value.

hearbeat-interval *interval*

Specifies the time interval between heartbeat chunks sent to a destination transport address in seconds.

interval must be an integer from 1 through 255.

Default: 30 seconds

path max-retransmissions *retransmissions*

Specifies the maximum number of consecutive retransmissions over a destination transport address of a peer endpoint before it is marked as inactive.

retransmissions must be an integer from 1 through 10.

Default: 10

Usage Guidelines

Use this command to configure Diameter SCTP parameters for all Diameter endpoints within the context.

Example

The following command configures the heartbeat interval to *60* seconds:

```
diameter sctp hearbeat-interval 60
```

The following command configures the maximum number of consecutive retransmissions to *6*, after which the endpoint is marked as inactive:

```
diameter sctp path max-retransmissions 6
```

diameter origin

This command is deprecated and is replaced by the **diameter endpoint** command.

dns-client

Creates a DNS client and/or enters the DNS Client Configuration Mode.

Product

ePDG

MME

P-GW

SAEGW

SCM

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 ] dns-client` *`name`* **`[ -noconfirm ]`**

no

Removes the specified DNS client from the context.

dns-client *name*

Specifies a name for the DNS client as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to create a new DNS client and enter the DNS Client Configuration Mode or enter the mode for an existing client.

Entering this command results in the following prompt:

```
[context_name]hostname(config-dns-client)#
```

DNS Client Configuration Mode commands are defined in the *DNS Client Configuration Mode Commands* chapter.

Example

The following command enters the DNS Client Configuration Mode for a DNS client named *dns1*:

```
dns-client dns1
```

domain

Configures a domain alias for the current context.

Product

HA

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

domain [*]*domain_name* **[default subscriber** *subscriber_template_name* **]**
no domain [*]*domain_name*

no

Indicates the domain specified is to be removed as an alias to the current context.

[*]*domain_name*

domain_name specifies the domain alias to create/remove from the current context. If the domain portion of a subscribers user name matches this value, the current context is used for that subscriber.

domain_name must be an alphanumeric string of 1 through 79 characters. The domain name can contain all special characters, however note that the character * (wildcard character) is only allowed at the beginning of the domain name.

If the domain name is prefixed with * (wildcard character), and an exact match is not found for the domain portion of a subscriber's username, subdomains of the domain name are matched. For example, if the domain portion of a subscriber's user name is abc.xyz.com and you use the domain command **domain** **xyz.com* it matches. But if you do not use the wildcard (**domain** *xyz.com*) it does not match.

Important The domain alias specified must not conflict with the name of any existing context or domain names.

default subscriber *subscriber_template_name*

Specifies the name of the subscriber template to apply to subscribers using this domain alias.

subscriber_template_name must be an alphanumeric string of 1 through 127 characters. If this keyword is not specified the default subscriber configuration in the current context is used.

Usage Guidelines

Use this command to configure a domain alias when a single context may be used to support multiple domains via aliasing.

Example

```
domain sampleDomain.net
no domain sampleDomain.net
```