Context Configuration Mode Commands N-R

Command Modes

This section includes the commands **nw-reachability server** through **router** 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).

nw-reachability server

Adds or deletes a reachability-detect server and configures parameters for retrying the failure-detection process. When network reachability is enabled, an ICMP ping request is sent to this device. If there is no response after a specified number of retries, the network is deemed failed. Execute this command multiple times to configure multiple network reachability servers.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

nw-reachability server *server_name* **[interval** *seconds* **] [local-addr** *ip_addr* **] [num-retry** *num* **] [remote-addr** *ip_addr* **] [timeout** *seconds***] [vfr** *name***]**
no nw-reachability server *server_name*

no

Delete the reference to the specified network reachability server.

server_name

Specifies the name for the network device that is sent ping packets to test for network reachability.

interval ***seconds***

Specifies the frequency in seconds for sending ping requests as an integer from 1 through 3600. Default: 60

local-addr ***ip_addr***

Specifies the IP address to be used as the source address of the ping packets; If this is unspecified, an arbitrary IP address that is configured in the context is used. *ip_addr* must be entered using IPv4 dotted-decimal notation.

num-retry ***num***

Specifies the number of retries before deciding that there is a network-failure as an integer from 0 through 100. Default: 5

remote-addr *ip_addr*

Specifies the IP address of a network element to use as the destination to send the ping packets for detecting network failure or reachability. *ip_addr* must be entered using IPv4 dotted-decimal notation.

timeout *seconds*

Specifies how long to wait (in seconds) before retransmitting a ping request to the remote address as an integer from 1 through 1. Default: 3

vrf *name*

Specifies an existing VRF name as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to set up a network device on a destination network that is used ensure that Mobile IP sessions can reach the required network from the P-GW.

Important Refer to the P-GW Configuration Mode command **policy nw-reachability-fail** to configure the action that should be taken when network reachability fails.

Important Refer to the Subscriber Config Mode command **nw-reachability-server** to bind the network reachability to a specific subscriber.

Important Refer to the **nw-reachability server server_name** keyword of the **ip pool** command in this chapter to bind the network reachability server to an IP pool.

Example

To set a network device called Internet Device with the IP address of *192.168.100.10* as the remote address that is pinged to determine network reachability and use the address *192.168.200.10* as the origination address of the ping packets sent, enter the following command:

```
nw-reachability server InternetDevice local-addr 192.168.200.10 remote-addr
 192.168.100.10
```

network-requested-pdp-context activate

Configures the mobile station(s) (MSs) for which network initiated PDP contexts are supported.

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

network-requested-pdp-context activate address *ip_address* **dst-context** *context_name* **imsi** *imsi* **apn** *apn_name*
no network-requested-pdp-context activate address *ip_address* **dst-context** *context_name*

no

Disables the system's ability to accept network-requested PDP contexts on the specified interface.

ip_address

Specifies the static IP address of the MS n IPv4 dotted-decimal notation.

dst-context *context_name*

Specifies the name of the destination context configured on the system containing the static IP address pool in which the MS's IP address is configured. *context_name* is an alphanumeric string of 1 through 79 characters that is case sensitive.

imsi *imsi*

Specifies the International Mobile Subscriber Identity (IMSI) of the MS as a string of 1 through 15 numeric characters

apn *apn_name*

Specifies the Access Point Name (APN) that is passed to the SGSN by the system. *apn_name* is an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage Guidelines

Use this command to specify the MS(s) for which network initiated PDP contexts are supported.

When a packet is received for an MS that does not currently have a PDP context established, the system checks the configuration of this parameter to determine if the destination IP address specified in the packet is specified by this parameter. If the address is not specified, then the system discards the packet. If the address is specified, the system uses the configured IMSI and APN to determine the appropriate SGSN from the Home Location Register (HLR). The system communicates with the HLR through the interworking node configured using the network-requested-pdp-context gsn-map command.

Once the session is established, the destination context specified by this command is used in place of the one either configured within the specified APN template or returned by a RADIUS server during authentication.

This command can be issued multiple times supporting network initiated PDP contexts for up to 1,000 configured addresses per system context.

Example

The following command enables support for network initiated PDP contexts for an MS with a static IP address of *20.13.5.40* from a pool configured in the destination context pdn1 with an IMSI of *3319784450* that uses an APN template called *isp1*:

```
network-requested-pdp-context activate address 20.13.5.40 dst-context
pdn1 imsi 3319784450 apn isp1
```

network-requested-pdp-context gsn-map

Configures the IP address of the interworking node that is used by the system to communicate with the Home Location Register (HLR), and optionally sets the GTP version to use.

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

network-requested-pdp-context gsn-map *ip_address* **[gtp-version { 0 | 1 }]**
no network-requested-pdp-context gsn-map

no

Deletes a previously configured gsn-map node.

ip_address

Specifies the IP address of the gsn-map node in Pv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

gtp-version { 0 | 1 }

Specifies the gtp version used. Default: 1

Usage Guidelines

Communications from the system to the HLR must go through a GSN-map interworking node that performs the protocol conversion from GTPC to SS7.

The UDP port for this communication is 2123.

Support for network requested PDP contexts must be configured within source contexts on the system. Only one gsn-map node can be configured per source context.

The source context also contains the GGSN service configuration that specifies the IP address of the Gn interface. If multiple GGSN services are configured in the source context, one is selected at random for initiating the Network Requested PDP Context Activation procedure.

Communication with the gsn-map node is done over the Gn interface configured for the GGSN service. The IP address of that interface is used as the system's source address.

Example

The following command configures the system to communicate with a gsn-map node having an IP address of *192.168.2.5*:

```
network-requested-pdp-context gsn-map 192.168.2.5
```

network-requested-pdp-context hold-down-time

Configures the time duration to that the system will wait after the SGSN rejects an attempt for a network-requested PDP context creation for the subscriber.

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

```
network-requested-pdp-context hold-down-time time
default network-requested-pdp-context hold-down-time
```

default

Configures the default setting.

Default:60 seconds

time

Specifies the time interval (in seconds) as an integer from 0 through 86400.

Usage Guidelines

Packets received during this time period would be discarded, rather than being used to cause another network-requested PDP context creation attempt for the same subscriber. After the time period has expired, any subsequent packets received would cause another network-requested PDP context creation procedure to begin.

Example

The following command configures a hold-down-time of *120* seconds:

```
network-requested-pdp-context hold-down-time 120
```

network-requested-pdp-context interval

Configures the minimum amount of time that must elapse between the deletion of a network initiated PDP context and the creation of a new one for the same MS.

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

`network-requested-pdp-context interval` *`time`*
`default network-requested-pdp-context interval`

default

Returns the command to its default setting of 60.

time

Specifies the minimum amount of time (in seconds) that must pass before the system allows another network-requested PDP context for a specific MS after the previous context was deleted. *time* is an integer from 0 through 86400. Default: 60

Usage Guidelines

Once an MS deletes a PDP context that initiated from the network, the system automatically waits the amount of time configured by this parameter before allowing another network initiated PDP context for the same MS.

Example

The following command specifies that the system waits *120* seconds before allowing another network requested PDP context for an MS:

`network-requested-pdp-context interval 120`

network-requested-pdp-context sgsn-cache-time

Configures the time duration that the GGSN keeps the SGSN/subscriber pair cached in its local memory.

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

network-requested-pdp-context sgsn-cache-time *time*
default network-requested-pdp-context sgsn-cache-time

default

Configures the default setting.

Default: 300 seconds

time

Specifies the time interval (in seconds) as an integer from 0 through 86400.

Usage Guidelines

For an initial network-requested PDP context creation, the system contacts the HLR (via the GSN-MAP interworking node) to learn which SGSN is currently servicing the subscriber. The system keeps that information in cache memory for the configured time, so that future network-requested PDP context creations for that subscriber can be initiated without having to contact the HLR again.

Example

The following command configures an sgsn-cache-time of *500* seconds:

```
network-requested-pdp-context sgsn-cache-time 500
```

operator

Configures a context-level operator 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

operator *user_name* **[encrypted] [nopassword] password** *password* **[ecs] [expiry-date** *date_time* **] [li-administration] [noconsole] [noecs] [timeout-absolute** *abs_seconds* **] [timeout-min-absolute** *abs_minutes* **] [timeout-idle** *timeout_duration* **] [timeout-min-idle** *idle_minutes* **][exp-grace-interval** *days***][exp-warn-interval** *days***][no-exp-grace-interval][no-exp-warn-interval]**
no operator *user_name*

no

Removes a previously configured context-level operator account.

user_name

Specifies a 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 operator 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 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 operator 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 operator password to gain access to the user account.

ecs

Permits the specific user to access ACS-specific configuration commands from Exec Mode only. Default: ACS-specific configuration commands are not allowed.

expiry-date *date_time*

Specifies the date and time that this account expires. Enter the date and time 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.

li-administration

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

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 configuration commands. Default: Enabled

timeout-absolute *abs_seconds*

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) the context-level operator may have a session active before the session is forcibly terminated. *abs_seconds* must be a value in the range 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 operator may have a session active before the session is forcibly terminated. *abs_minutes* must be an integer from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

timeout-idle *timeout_duration*

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 operator may have a session active before the session is terminated. *timeout_duration* must be an integer 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 operator may have a session active before the session is terminated. *idle_minutes* must be an integer from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

Usage Guidelines

Use this command to create new context-level operator or modify existing operator's options, in particular, the timeout values.

Operators have read-only privileges. They can maneuver across multiple contexts, but cannot perform configuration operations. 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.

[max-age *days*]

Defines the maximum age of a user password before it has to be changed. **max-age** is the replacement for **expiry-date**.

[no-max-age]

This parameter ensures that password never expires (these are non expiring passwords).

exp-warn-interval *days*

Impends password expiry warning interval in days. There is no default value at per user level. If any of the value is specified, Context global values are considered.

For example:

```
operator trexpac111 password pass@1234
```

In the previous example, there are no values for expiry, grace, and warn are provided. In this case, Global values for both of them will be considered.

[no-exp-warn-interval]

Disables impending password expiry warnings .

exp-grace-interval *days*

Specifies password expiry grace interval in days. Default = 3 days after expiry.

[no-exp-grace-interval]

Disables grace period of expired password.

Example

The following command creates a context-level operator account named *user1* with ACS control:

```
operator user1 password secretPassword ecs
```

The following command removes a previously configured context-level operator account named *user1*:

```
no operator user1
```

Example

The following command shows the notifications you will receive if the password is not reset before the expiration date:

operator *user_name* **password** *password* **[max-age** *days*]**[password-exp-grace-interval** *days*]**[password-exp-grace-interval** *days*]

```
login: xxx
password: xxx
1. <Normal>
# <you are logged in>

2. <When in warning period>
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :

3.<when in grace period>
Your password has expired
Current password:
New password:
Repeat new password:
```

```
4. <after the grace period>
Password Expired (even beyond grace period, if configured). Contact Security Administrator
 to reset password
```

optimize pdsn inter-service-handoff

Controls the optimization of the system's handling of inter-PDSN handoffs.

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 ] optimize pdsn inter-service-handoff`

default

Resets the command to its default setting of enabled.

no

Disables the feature.

Usage Guidelines

When more than one PDSN service is defined in a context, each PDSN-Service acts as an independent PDSN. When a Mobile Node (MN) moves from one PDSN service to another PDSN service, by rule, it is an inter-PDSN handoff. This command optimizes PDSN handoffs between PDSN Services that are defined in the same context in the system.

The default for this parameter is enabled. The no keyword disables this functionality.

When enabled, the system treats handoffs happening between two PDSN services in the same context as an inter-PDSN handoff. Existing PPP session states and connection information is reused. If the inter-PDSN handoff requires a PPP restart, then PPP is restarted. The optimized inter-service-handoff may not restart the PPP during handoffs allowing the MN to keep the same IP address for the Simple IP session.

Example

`optimize pdsn inter-service-handoff`

password

Configures password rules (exp-grace-interval, exp-warn-interval, max-age, complexity, and minimum length) to be enforced for all users in this context.

Product All

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

[default] password { [{ [complexity { ansi-t1.276-2003 | none }] } [auto-generate]
[none | password min-length *min_size* **][lockout-password-aging** *days* **][password exp-grace-interval** *days***][password exp-warn-interval** *days* **][password max-age** *days***]**

[default] password {exp-grace-interval | exp-warn-interval | max-age}

[default] no password {exp-grace-interval | exp-warn-interval | max-age}

default

The default password complexity is **ansi-t1.276-2003**.

The default minimum length is **8**.

The default password expiry warning interval is **30** days before expiry.

The default password expiry grace interval is **3** days after expiry.

The default value of max-age parameter is **90** days.

Note For non-default commands, the 3 variables needs *days* as an input

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

Specifies the complexity to be enforced for all context user passwords.

ansi-t1.276-2003 requires that all context user passwords comply with the following rules:

- Passwords may not contain the username or the reverse of the username

  .
- Passwords may contain no more than three of the same characters used consecutively.
- Passwords must contain at least three of the following:
  - uppercase alpha character (A, B,C, D...Z)
  - lowercase alpha character (a, b, c, d ...z)
  - numeric character (0, 1, 2, 3...)
  - special character (see the *Alphanumeric Stirngs* section of the *Command Line Interface Overview* chapter)

none results in only the password length being checked.

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

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

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

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

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

exp-warn-interval *days*

Impends password expiry warning interval in days. Default = 30 days before expiry.

exp-grace-interval *days*

Specifies password expiry grace interval in days. Default = 3 days after expiry.

[lockout-password-aging *days*]

Specifies that the user account gets locked after passoword expiration

[no-lockout-password-aging *days*]

Specifies that the user account doest not get locked out after password expiration

max-age *days*

Defines the max-age of a user password before it has to be changed. Default = 90 days.

Description:

The password expiration notification to Context/AAA/Radius users is enhanced. With the enhancement after password expiry and within the grace period, you can log in and change the password on your own. Beyond the grace period, the security administrator will reset the password for you. The following password change prompt is displayed:

```
WARNING: Your password has expired.
You must change your password now and login again!
(current)  password:
Enter new  password:
Retype new password:
```

For example:

```
login: xxx
password: xxx

Case 1: [Normal]
# {you are logged in}

Case 2: [When in warning period]
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :
```

```
Case 3: [when in grace period]
Your password has expired
Current password:
New password:
Repeat new password:

Case 4: [after the grace period]
Password Expired (even beyond grace period, if configured). Contact Security Administrator
to reset password
```

Usage Guidelines Use this command to specify the complexity and minimum length of all passwords assigned within this context.

Example

The following commands set the password complexity to ANSI-T1.276 requirements and minimum length to 12.

```
password complexity ansi-t1.276-2003
password min-length 12
```

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

```
password auto-generate length 10
```

pcc-af-service

Creates or removes an IPCF Policy and Charging Control (PCC) Application Function (AF) service or configures an existing PCC-AF service. It enters the PCC-AF Service Configuration Mode to link, configure, and manage the Application Function endpoints and associated PCC services over the Rx interface for the IPCF services.

Product IPCF

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

```
pcc-af-service service_name [ -noconfirm ]
no pcc-af-service service_name
```

no

Removes the specified PCC-AF service from the context.

service_name

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

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

-noconfirm

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

Usage Guidelines

Use this command to enter the PCC-AF Service Configuration Mode for an existing service or for a newly defined PCC-AF service. This command is also used to remove an existing service.

The PCC-AF-Service consolidates the provisioning and management required for the PCC-AF services being supported by the network that fall under the PCC regime. The application service handles the **Rx** interface over which the IPCF may receive media information for the application usage from AF.

Important In the absence of an Rx interface, the media information is available in the PCC-AF Service statically.

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

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

Entering this command results in the following prompt:

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

The commands available in this mode are defined in the *PCC -AF Service Configuration Mode Commands* chapter.

Caution This is a critical configuration. The PCC-AF service cannot be configured without this configuration. Any change to this configuration would lead to restarting the PCC-AF service and removing or disabling this configuration will stop the PCC-AF service.

Example

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

```
pcc-af-service af-service1
```

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

```
no pcc-af-service af-service1
```

pcc-policy-service

Creates or removes an IPCF PCC-Policy service or configures an existing PCC-Policy service. It enters the PCC-Policy Service Configuration Mode to link, configure, and manage the Gx interface endpoints for policy authorization where IPCF acts as a policy server.

Product

IPCF

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

pcc-policy-service *service_name* **[-noconfirm]**
no pcc-policy-service *service_name*

no

Removes the specified PCC-Policy service from the context.

service_name

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

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

-noconfirm

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

Usage Guidelines

Use this command to enter the PCC-Policy Service Configuration Mode for an existing service or for a newly defined PCC-Policy service. This command is also used to remove an existing service.

The PCC-Policy-Service is mainly used to provide a mechanism to manage the external Gx or similar interfaces required for policy authorization purpose. It manages Gx and Gx-like interfaces such as Gxc/Gxa between IPCF/PCRF and PCEF or BBERF, which is based on the dictionary used for PCC.

Multiple instances of PCC-Policy-Service may exist in a system which could link with the same PCC-Service that controls the business logic. This service allows for management of configuration for peers as well self related to Gx like functions.

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

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

Entering this command results in the following prompt:

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

The commands available in this mode are defined in the *PCC-Policy Service Configuration Mode Commands* chapter.

Caution This is a critical configuration. The PCC-Policy service cannot be configured without this configuration. Any change to this configuration would lead to restarting the PCC-Policy service and removing or disabling this configuration will stop the PCC-Policy service.

Example

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

```
pcc-policy-service gx-service1
```

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

```
no pcc-policy-service gx-service1
```

pcc-service

Creates or removes an IPCF Policy and Charging Control (PCC) service or configures an existing PCC service. It enters the PCC Service Configuration Mode for IPCF related configurations in the current context.

Product IPCF

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

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

no

Removes the specified PCC service from the context.

service_name

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

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

-noconfirm

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

Usage Guidelines

Use this command to enter the PCC Service Configuration Mode for an existing service or for a newly defined PCC service. This command is also used to remove an existing service.

The IPCF PCC Service Configuration Mode is used to link, consolidate and manage the policy logic for the networks. The authorization of resources for a subscriber's data usage under various conditions and policies are defined in the IPCF PCC service.

Only one PCC service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) configured per system.

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

Entering this command results in the following prompt:

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

The commands available in this mode are defined in the *PCC Service Configuration Mode Commands* chapter.

Caution This is a critical configuration. The PCC service cannot be configured without this configuration. Any change to this configuration would lead to restarting the Policy and Charging Control service and removing or disabling this configuration will stop the PCC service.

Example

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

```
pcc-service ipcf-service1
```

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

```
no pcc-service ipcf-service1
```

pcc-sp-endpoint

Creates or removes a PCC Sp interface endpoint or configures an existing PCC Sp interface client endpoint. It enters the PCC Sp Endpoint Configuration Mode to link, configure, and manage the operational parameters related to its peer.

Product

IPCF

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

```
pcc-sp-endpoint sp_intfc1 [ -noconfirm ]
no pcc-sp-endpoint name sp_intfc1
```

no

Removes the specified PCC Sp interface endpoint from the context.

sp_intfc1

Specifies the name of the PCC Sp interface endpoint. If *sp_intfc_endpoint* does not refer to an existing endpoint, the new endpoint is created if resources allow.

sp_intfc_endpoint is an alphanumeric string of 1 through 63 characters.

-noconfirm

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

Usage Guidelines

Use this command to enter the PCC-Sp-Endpoint Configuration Mode for an existing interface or for a newly defined PCC **Sp** interface endpoint. This command is also used to remove an existing endpoint.

An instance of PCC Sp endpoint represents a client end for SSC/SPR interactions. It is possible to support multiple Sp endpoints each supporting the same or different protocol(s). The PCC Sp endpoint facilitates the configuration of the treatment required of the Sp interface as well as manages the connection and operational parameters related to its peer.

Only one PCC Sp endpoint across a chassis can be configured on a system.

Entering this command results in the following prompt:

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

The commands available in this mode are defined in the *PCC-Sp-Endpoint Configuration Mode Commands* chapter.

Caution This is a critical configuration. The PCC Sp endpoint cannot be configured without this configuration. Any change to this configuration would lead to reset the PCC Sp interface and removing or disabling this configuration also disables the PCC Sp interface.

Example

The following command enters the existing PCC Sp Endpoint Configuration Mode (or creates it if it does not already exist) for the endpoint named *sp_intfc1*:

```
pcc-sp-endpoint sp_intfc1
```

The following command will remove *sp_intfc1* from the system:

```
pcc-sp-endpoint name sp_intfc1
```

pdg-service

Creates a new PDG service or specifies an existing PDG service and enters the PDG Service Configuration Mode. A maximum of 16 PDG services can be created. This limit applies per ASR 5000 chassis and per context.

Product PDG/TTG

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] pdg-service** *name*

no*name*

Deletes the specified PDG service.

name

Specifies the name of a new or existing PDG service as an alphanumeric string 1 through 63 characters that must be unique across all FNG services 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 in Context Configuration Mode to create a new PDG service or modify an existing one. Executing this command enters the PDG Service Configuration Mode.

Example

The following command configures an PDG service named *pdg_service_1* and enters the PDG Service Configuration Mode:

```
pdg-service pdg_service_1
```

pdif-service

Creates a new, or specifies an existing, Packet Data Interworking Function (PDIF) service and enters the PDIF Service Configuration Mode.

Product

PDIF

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 ] pdif-service` *`name`* **`[ -noconfirm ]`**

name

Specifies the name of a new or existing PDIF service as an alphanumeric string of 1 through 63 characters.

Important

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

Usage Guidelines

Use this command to create a new or enter an existing PDIF service.

Entering this command results in the following prompt:

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

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

Example

The following command configures a PDIF service called *pdif2* and enters the PDIF Service Configuration Mode:

```
pdif-service pdif2
```

pdsn-service

Creates or deletes a packet data service or specifies an existing PDSN service for which to enter the Packet Data Service Configuration Mode for the current context.

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

`[ no ] pdsn-service` *name*

no

Indicates the packet data service specified is to be removed.

name

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

Important

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

Usage Guidelines

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

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

Caution

Large numbers of services greatly increase the complexity of management and may impact overall system performance (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 Cisco service representative for more information.

Example

The following command will enter the PDSN Service Configuration Mode creating the service *sampleService*, if necessary.

```
pdsn-service sampleService
```

The following command will remove *sampleService* as being a defined PDSN service.

```
no pdsn-service sampleService
```

pdsnclosedrp-service

Creates or deletes a Closed R-P packet data service or specifies an existing PDSN Closed R-P service for which to enter the Closed R-P Service Configuration Mode for the current context.

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

`[ no ] pdsnclosedrp-service` *`name`*

no

Removes the specified PDSN Closed R-P service.

name

Specifies the name of the Closed R-P PDSN service to configure. If *name* does not refer to an existing service, the new service is created if resources allow. *name* is an alphanumeric string of 1 through 63 characters.

Important

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

Usage Guidelines

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

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

Caution

Large numbers of services greatly increase the complexity of management and may impact overall system performance (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.

Example

The following command enters the Closed R-P Service Configuration Mode creating the service *sampleService*, if necessary:

```
pdsnclosedrp-service sampleService
```

The following command removes *sampleService* as being a defined Closed R-P PDSN service:

no pdsnclosedrp-service sampleService

pgw-service

Creates a PDN-Gateway (P-GW) service or specifies an existing P-GW service and enters the P-GW Service Configuration Mode for the current context.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

service_name

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

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

-noconfirm

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

no pgw-service *service_name*

Removes the specified P-GW service from the context.

Usage Guidelines

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

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

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

Entering this command results in the following prompt:

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

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

Use this command when configuring the following eHRPD and SAE components: P-GW.

Example

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

pgw-service pgw-service1

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

no pgw-service pgw-service1

policy

Enters an existing accounting policy or creates a new one where accounting parameters are configured.

Product

HSGW

P-GW

S-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] policy accounting *name*

no

Removes the specified accounting policy from the context.

name

Specifies the name of the existing or new accounting policy as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to enter the Accounting Policy Configuration mode to edit an existing accounting policy or configure an new policy.

Entering this command results in the following prompt:

```
[context_name]hostname(config-accounting-policy)#
```

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

Example

The following command enters the Accounting Policy Configuration Mode for a policy named *acct5*:

```
policy accounting acct5
```

policy-group

Creates or deletes a policy group. It enters the Policy-Group Configuration Mode within the current destination context for flow-based traffic policing to a subscriber session flow.

Product

PDSN

HA

ASN-GW

HSGW

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] policy-group name *policy_group*

no

Deletes configured policy group within the context.

name *policy_group*

Specifies the name of Policy-Group as an alphanumeric string of 1 through 15 characters that is case sensitive.

Usage Guidelines Use this command to form a policy group from a set of configured Policy-Maps. A policy group supports up to 16 policies for a subscriber session flow.

Example

The following command configures a policy group *policy_group1* for a subscriber session flow:

```
policy-group name policy_group1
```

policy-map

Creates or deletes a policy map. It enters the Traffic Policy-Map Configuration Mode within the current destination context to configure the flow-based traffic policing for a subscriber session flow.

Product

PDSN

HA

ASN-GW

HSGW

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 ] policy-map name` *`policy_name`*

no

Deletes configured Policy-Map within the context.

name *policy_name*

Specifies the name of Policy-Map as an alphanumeric string of 1 through 15 characters that is case sensitive.

Usage Guidelines Use this command to enter Traffic Policy-Map Configuration Mode and to set the Class-Map and corresponding traffic flow treatment to traffic policy for a subscriber session flow.

Example

Following command configures a policy map *policy1* where other flow treatments is configured.

```
policy-map name policy1
```

ppp

Configures point-to-point protocol parameters for the current context.

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

ppp { acfc { receive { allow | deny } | transmit { apply | ignore | reject} } | auth-retry suppress-aaa-auth | chap fixed-challenge-length *length* **| dormant send-lcp-terminate | echo-max-retransmissions** *num_retries* **| echo-retransmit-timeout** *msec* **| first-lcp-retransmit-timeout** *milliseconds* **| lcp-authentication-discard retry-alternate** *num_discard* **| lcp-authentication-reject retry-alternate | lcp-start-delay** *delay* **| lcp-terminate connect-state | lcp-terminate mip-lifetime-expiry | lcp-terminate mip-revocation | max-authentication-attempts** *num* **| max-configuration-nak** *num* **| max-retransmissions** *number* **| max-terminate** *number* **| mru** *packet_size* **| negotiate default-value-options | peer-authentication** *user_name* **[encrypted] password** *password* **] | pfc { receive { allow | deny } | transmit { apply | ignore | reject} } | reject-peer-authentication | renegotiation retain-ip-address | retransmit-timeout** *milliseconds* **}**
no ppp { auth-retry suppress-aaa-auth | chap fixed-challenge-length | dormant send-lcp-terminate | lcp-authentication-descard retry-alternate *num_discard* **| lcp-authentication-reject retry-alternate | lcp-start-delay | lcp-terminate connect-state | reject-peer-authentication | renegotiation retain-ip-address }**
default lcp-authentication-descard retry-alternate *num_discard*

default

Restores the system defaults for the specific command/keyword.

no

Disables, deletes, or resets the specified option.

For **no ppp renegotiation retain-ip-address** the initially allocated IP address will be released and a new IP address will be allocated during PPP renegotiation.

acfc { receive { allow | deny } | transmit { apply | ignore | reject} }

Configures PPP Address and Control Field Compression (ACFC) parameters.

receive { allow | deny }

This keyword specifies whether to allow Address and Control Field Compressed PPP packets received from the Peer. During LCP negotiation, the local PPP side indicates whether it can handle ACFC compressed PPP packets. Default: **allow**

When allow is specified, the local PPP side indicates that it can process ACFC compressed PPP packets and compressed packets are allowed. When deny is specified, the local PPP side indicates that it cannot handle ACFC compressed packets and compressed packets are not allowed.

transmit { apply | ignore | reject }

Specifies how Address and Control Field Compression should be applied for PPP packets transmitted to the Peer. During LCP negotiation, the Peer indicates whether it can handle ACFC compressed PPP packets. Default: **ignore**

When apply is specified, if the peer requests ACFC, the request is accepted and ACFC is applied for transmitted PPP packets. When ignore is specified, if the peer requests ACFC, the request is accepted, but ACFC is not applied for transmitted PPP packets. When reject is specified, if the peer requests ACFC, the request is rejected and ACFC is not applied to transmitted packets.

auth-retry suppress-aaa-auth

This option does not allow PPP authentication retries to the AAA server after the AAA server has already authenticated a session. PPP locally stores the username and password, or challenge response, after a successful PPP authentication. If the Mobile Node retries the PAP request or CHAP-Response packet to the PDSN, PPP locally compares the incoming username, password or Challenge Response with the information stored from the previous successful authentication. If it matches, PAP ACK or CHAP Success is sent back to the Mobile Node, without performing AAA authentication. If the incoming information does not match with what is stored locally, then AAA authentication is attempted. The locally stored PPP authentication information is cleared once the session reaches a connected state.

Default: **no auth-retry suppress-aaa-auth**

Important This option is not supported in conjunction with the GGSN product.

chap fixed-challenge-length *length*

Normally PPP CHAP use sa random challenge length from 17 to 32 bytes. This command allows you to configure a specific fixed challenge length of from 4 through 32 bytes. *length* must be an integer from 4 through 32.

Default: Disabled. PAPCHAP uses a random challenge length.

dormant send-lcp-terminate

Indicates a link control protocol (LCP) terminate message is enabled for dormant sessions.

Important This option is not supported in conjunction with the GGSN product.

echo-max-retransmissions *num_retries*

Configures the maximum number of retransmissions of LCP ECHO_REQ before a session is terminated in an always-on session. *num_retries* must be an integer from 1 through 16. Default: 3

echo-retransmit-timeout *msec*

Configures the timeout (in milliseconds) before trying LCP ECHO_REQ for an always-on session. *msec* must be an integer from 100 through 5000. Default: 3000

first-lcp-retransmit-timeout *milliseconds*

Specifies the number of milliseconds to wait before attempting to retransmit control packets. This value configures the first retry. All subsequent retries are controlled by the value configured for the ppp **retransmit-timeout** keyword.

milliseconds must be an integer from 100 through 5000. Default: 3000

lcp-authentication-discard retry-alternate *num_discard*

Sets the number of discards up to which authentication option is discarded during LCP negotiation and retries starts to allow alternate authentication option. *num_discard* must be an integer from 0 through 5. Recommended value is 2. Default: Disabled.

lcp-authentication-reject retry-alternate

Specifies the action to be taken if the authentication option is rejected during LCP negotiation and retries the allowed alternate authentication option.

Default: Disabled. No alternate authentication option will be retried.

lcp-start-delay *delay*

Specifies the delay (in milliseconds) before link control protocol (LCP) is started. *delay* must be an integer from 0 through 5000. Default: 0

lcp-terminate connect-state

Enables sending an LCP terminate message to the Mobile Node when a PPP session is disconnected if the PPP session was already in a connected state.

Note that if the no keyword is used with this option, the PDSN must still send LCP Terminate in the event of an LCP/PCP negotiation failure or PPP authentication failure, which happens during connecting state.

Important This option is not supported in conjunction with the GGSN product.

lcp-terminate mip-lifetime-expiry

Configures the PDSN to send an LCP Terminate Request when a MIP Session is terminated due to MIP Lifetime expiry (default).

Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when a MIP session is terminated due to MIP Lifetime expiry.

lcp-terminate mip-revocation

Configures the PDSN to send a LCP Terminate Request when a MIP Session is terminated due to a Revocation being received from the HA (default).

Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when a MIP session is terminated due to a Revocation being received from the HA.

max-authentication-attempts *num*

Configures the maximum number of time the PPP authentication attempt is allowed. *num* must be an integer from 1 through 10. Default: 1

max-configuration-nak *num*

This command configures the maximum number of consecutive configuration REJ/NAKs that can be sent during CP negotiations, before the CP is terminated. *num* must be an integer from 1 through 20. Default: 10

max-retransmission *number*

Specifies the maximum number of times control packets will be retransmitted. *number* must be an integer from 1 through 16. Default: 5

max-terminate *number*

Sets the maximum number of PPP LCP Terminate Requests transmitted to the Mobile Node. *number* must be an integer from 0 through 16. Default: 2

Important This option is not supported in conjunction with the GGSN product.

mru *packet_size*

Specifies the maximum packet size that can be received in bytes. *packet_size* must be an integer from 128 through 1500. Default: 1500

negotiate default-value-options

Enables the inclusion of configuration options with default values in PPP configuration requests. Default: Disabled

The PPP standard states that configuration options with default values should not be included in Configuration Request (LCP, IPCP, etc.) packets. If the option is missing in the Configuration Request, the peer PPP assumes the default value for that configuration option.

When **negotiate default-value-options** is enabled, configuration options with default values are included in the PPP configuration Requests.

peer-authenticate *user_name* [[encrypted] password *password*]

Specifies the username and an optional password required for point-to-point protocol peer connection authentications. *user_name* is an alphanumeric string of 1 through 63 characters. The keyword **password** is optional and if specified *password* is an alphanumeric string of 1 through 63 characters. The password specified must be in an encrypted format if the optional keyword **encrypted** was 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.

pfc { receive { allow | deny } | transmit { apply | ignore | reject} }

Configures Protocol Field Compression (PFC) parameters.

receive { allow | deny } Default: **allow**

This keyword specifies whether to allow Protocol Field Compression (PFC) for PPP packets received from the peer. During LCP negotiation, the local PPP side indicates whether it can handle Protocol Field Compressed PPP packets.

When allow is specified, the peer is allowed to request PFC during LCP negotiation. When deny is specified, the Peer is not allowed to request PFC during LCP negotiation.

transmit { apply | ignore | reject } Default: **ignore**

This keyword specifies how Protocol field Compression should be applied for PPP packets transmitted to the Peer. During LCP negotiation, the Peer indicates whether it can handle PFC compressed PPP packets.

When **apply** is specified, if the peer requests PFC, it is accepted and PFC is applied for transmitted PPP packets. When **ignore** is specified, If the peer requests PFC, it is accepted but PFC is not applied for transmitted packets. When **reject** is specified, all requests for PCF from the peer are rejected.

reject-peer-authentication

If disabled, re-enables the system to reject peer requests for authentication. Default: Enabled

renegotiation retain-ip-address

If enabled, retain the currently allocated IP address for the session during PPP renegotiation (SimpleIP) between FA and Mobile node. Default: Enabled

If disabled, the initially allocated IP address will be released and a new IP address will be allocated during PPP renegotiation.

retransmit-timeout *milliseconds*

Specifies the number of milliseconds to wait before attempting to retransmit control packets. *milliseconds* must be an integer from 100 through 5000. Default: 3000

Usage Guidelines

Modify the context PPP options to ensure authentication and communication for PPP sessions have fewer dropped sessions.

Example

The following commands set various PPP options:

```
ppp dormant send-lcp-terminate
ppp max-retransmission 3
ppp peer-authenticate user1 password secretPwd
ppp peer-authenticate user1
ppp retransmit-timeout 1000
```

The following command disables the sending of LCP terminate messages for dormant sessions.

```
no ppp dormant send-lcp-terminate
```

ppp magic-number

Manages magic number checking during LCP Echo message handling. The magic number is a random number chosen to distinguish a peer and detect looped back lines.

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

```
[ no | default ] ppp magic-number receive ignore
```

no

Disables the specified behavior.

default

Restores the system defaults for the specific command/keyword.

receive ignore

Ignores the checking of magic number at the PDSN during LCP Echo message handling. Default: Disabled.

If a valid magic numbers were negotiated for the PPP endpoints during LCP negotiation and LCP Echo Request/Response have invalid magic numbers, enabling this command will cause the system to ignore the checking of magic number during LCP Echo message handling.

Usage Guidelines

Use this command to allow the system to ignore invalid magic number during LCP Echo Request/Response handling.

Example

The following command allows the invalid magic number during LCP Echo Request/Response negotiation:

```
ppp magic-number receive ignore
```

ppp statistics

Changes the manor in which some PPP statistics are calculated.

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

`[ no ] ppp statistics success-sessions { lcp-max-retry | misc-reasons | remote-terminated }`

no

Disable the specified behavior.

ppp statistics success-sessions lcp-max-retry

Alters statistical calculations so that: ppp successful session = successful sessions + lcp-max-retry.

success-sessions misc-reasons

Alters statistical calculations so that: ppp successful session = successful sessions + misc-reasons.

success-sessions remote-terminated

Alters statistical calculations so that: ppp successful session = successful sessions + remote-terminated.

Usage Guidelines

Use this command to alter how certain PPP statistics are calculated.

Caution This command alters the way that some PPP statistics are calculated. Please consult your designated service representative before using this command

Example

The following command alters the statistic "ppp successful session" so that it displays the sum of successful sessions and lcp-max-retry:

`ppp statistics success-sessions lcp-max-retry`

The following command disables the alteration of the statistic ppp successful session:

`no ppp statistics success-sessions lcp-max-retry`

proxy-dns intercept-list

Enters the HA Proxy DNS Configuration Mode and defines a name of a redirect rules list for the domain name servers associated with a particular FA (Foreign Agent) or group of FAs.

Important HA Proxy DNS Intercept is a license-enabled feature.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] proxy-dns intercept-list` *`name`*

no

Removes the intercept list from the system.

name

Defines the rules list and enters the Proxy DNS Configuration Mode. *name* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to define a name for a list of rules pertaining to the IP addresses associated with the foreign network's DNS. Up to 128 rules of any type can be configured per rules list.

Upon entering the command, the system switches to the HA Proxy DNS Configuration Mode where the lists can be defines. Up to 64 separate rules lists can be configured in a single AAA context.

This command and the commands in the HA Proxy DNS Configuration Mode provide a solution to the Mobile IP problem that occurs when a MIP subscriber, with a legacy MN or MN that does not support IS-835D, receives a DNS server address from a foreign network that is unreachable from the home network. The following flow shows the steps that occur when this feature is enabled:

By configuring the Proxy DNS feature on the Home Agent, the foreign DNS address is intercepted and replaced with a home DNS address while the call is being handled by the home network.

Example

The following command creates a proxy DNS rules list named *list1* and places the CLI in the HA Proxy DNS Configuration Mode:

```
proxy-dns intercept-list list1
```

rac-profile

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

rac-profile *profile_name*

rac-profile *profile_name*

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

Usage Guidelines

Enter the Configuration Mode to set the RAC profile options.

Entering this command results in the following prompt:

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

Example

The following command creates a RAC profile named *rp1* in the current context (or enters the existing RAC Profile Configuration Mode if it already exists):

```
rac-profile rp1
```

radius accounting

This command configures RADIUS accounting parameters 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

```
radius accounting { archive [ stop-only ] | deadtime dead_minutes |
detect-dead-server { consecutive-failures consecutive_failures | keepalive |
 response-timeout timeout_duration } | interim interval seconds |
max-outstanding max_messages | max-pdu-size octets | max-retries max_retries |
 max-transmissions max_transmissions | timeout timeout_duration |
unestablished-sessions }
default radius accounting { deadtime | detect-dead-server | interim
interval seconds | max-outstanding | max-pdu-size | max-retries |
max-transmissions | timeout }
no radius accounting { archive | detect-dead-server | interim interval |
 max-transmissions | unestablished-sessions }
```

default

Configures the default settings.

no

Removes earlier configuration for the specified keyword.

archive [stop-only]

Enables archiving of RADIUS Accounting messages in the system after the accounting message has exhausted retries to all available RADIUS Accounting servers. All RADIUS Accounting messages generated by a session are delivered to the RADIUS Accounting server in serial. That is, previous RADIUS Accounting messages from the same call must be delivered and acknowledged by the RADIUS Accounting server before the next RADIUS Accounting message is sent to the RADIUS Accounting server.

stop-only specifies archiving of STOP accounting messages only.

Default: Enabled

deadtime *dead_minutes*

Specifies the number of minutes to wait before attempting to communicate with a server which has been marked as unreachable.

dead_minutes must be an integer from 0 through 65535.

Default: 10

detect-dead-server { consecutive-failures *consecutive_failures* | keepalive | response-timeout *timeout_duration* }

- **consecutive-failures** *consecutive_failures*: Specifies the number of consecutive failures, for each AAA manager, before a server is marked as unreachable.

  consecutive_failures must be an integer from 0 through 1000.

  Default: 4

- **keepalive**: Enables the AAA server alive-dead detect mechanism based on sending keep alive authentication messages to all authentication servers.

  Default: Disabled

- **response-timeout** *timeout_duration*: Specifies the number of seconds for each AAA manager to wait for a response to any message before a server is detected as failed, or in a down state.

  timeout_duration must be an integer from 1 through 65535.

Important If both **consecutive-failures** and **response-timeout** are configured, then both parameters have to be met before a server is considered unreachable, or dead.

interim interval *seconds*

Specifies the time interval (in seconds) for sending accounting INTERIM-UPDATE records. *seconds* must be an integer from 50 through 40000000.

Important If RADIUS is used as the accounting protocol for the GGSN product, other commands are used to trigger periodic accounting updates. However, these commands would cause RADIUS STOP/START packets to be sent as opposed to INTERIM-UPDATE packets. Also note that accounting interim interval settings received from a RADIUS server take precedence over those configured on the system.

Default: Disabled

max-outstanding *max_messages*

Specifies the maximum number of outstanding messages a single AAA manager instance will queue. *max_messages* must be an integer from 1 through 4000. Default: 256

max-pdu-size *octets*

Specifies the maximum sized packet data unit which can be accepted/generated in bytes (octets). *octets* must be an integer from 512 through 4096. Default: 4096

max-retries *max_retries*

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as unreachable and the detect dead servers consecutive failures count is incremented. *max_retries* must be an integer from 0 through 65535. Default: 5

Once the maximum number of retries is reached this is considered a single failure for the consecutive failures count for detecting dead servers.

max-transmissions *max_transmissions*

Sets the maximum number of transmissions for a RADIUS accounting message before the message is declared as failed. *max_transmissions* must be an integer from 1 through 65535. Default: Disabled

timeout *seconds*

Specifies the amount of time to wait for a response from a RADIUS server before retransmitting a request. *seconds* must be an integer from 1 through 65535. Default: 3

unestablished-sessions

Indicates RADIUS STOP events are to be generated for sessions that were initiated but never fully established.

Usage Guidelines Manage the RADIUS accounting options according to the RADIUS server used for the context.

Example

The following commands configure accounting options.

```
radius accounting detect-dead-server consecutive-failures 5
radius accounting max-pdu-size 1024
radius accounting timeout 16
```

radius accounting algorithm

This command specifies the fail-over/load-balancing algorithm to select the RADIUS accounting server(s) to which accounting data must be sent.

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

```
radius accounting algorithm { first-n n | first-server [ fallback ] |
round-robin }
default radius accounting algorithm
```

default

Configures the default setting.

Default: **first-server**

first-n *n*

Specifies that the AGW must send accounting data to *n* (more than one) AAA accounting servers based on their priority. The full set of accounting data is sent to each of the *n* AAA servers. Response from any one of the servers would suffice to proceed with the call. On receiving an ACK from any one of the accounting servers, all retries are stopped.

n is the number of AAA accounting servers to which accounting data will be sent, and must be an integer from 2 through 128. Default: 1 (Disabled)

first-server[fallback]

Specifies that the context must send accounting data to the RADIUS accounting server with the highest configured priority. In the event that this server becomes unreachable, accounting data is sent to the accounting server with the next-highest configured priority. This is the default algorithm.

fallback: This algorithm is an extension of the existing "**first-server**" algorithm. This algorithm specifies that the context must send accounting data to the RADIUS server with the highest configured priority. When the server is unreachable, accounting data is sent to the server with the next highest configured priority. If a higher priority server recovers back, the accounting requests of existing sessions and new sessions are sent to the newly recovered server.

This new algorithm behaves similar to "**first-server**" algorithm, i.e. the accounting data is sent to the highest priority RADIUS/mediation server at any point of time.

If the highest priority server is not reachable, accounting data is sent to the next highest priority server. The difference between "**first-server**" and "**first-server fallback**" is that, with the new algorithm, if a higher priority server recovers, all new RADIUS requests of existing sessions and new accounting sessions are sent to the newly available higher priority server. In the case of "**first-server**" algorithm, the accounting requests of existing sessions continued to be sent to the same server to which the previous accounting requests of those sessions were sent.

The following are the two scenarios during which the requests might be sent to lower priority servers even though a higher priority server is available:

- When **radius max-outstanding** command or **max-rate** is configured, there are chances that the generated requests might be queued and waiting to be sent when bandwidth is available. If a higher priority server recovers, the queued requests will not be switched to the newly available higher priority server.
- When a higher priority server becomes reachable, all existing requests, which are being retried to a lower priority server, will not be switched to the newly available higher priority RADIUS server.

round-robin

Specifies that the context must load balance sending accounting data among all of the defined RADIUS accounting servers. Accounting data is sent in a circular queue fashion on a per Session Manager task basis, where data is sent to the next available accounting server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.

Usage Guidelines

Use this command to specify the algorithm to select the RADIUS accounting server(s) to which accounting data must be sent.

Example

The following command specifies to use the round-robin algorithm to select the RADIUS accounting server:

```
radius accounting algorithm round-robin
```

radius accounting apn-to-be-included

This command configures the Access Point Name (APN) to be included for RADIUS accounting.

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

```
radius accounting apn-to-be-included { gi | gn }
default radius accounting apn-to-be-included
```

default

Configures the default setting.

gi

Specifies the usage of the Gi APN name in the RADIUS accounting request. The Gi APN represents the APN received in the Create PDP context request message from the SGSN.

gn

Specifies the usage of the Gn APN name in the RADIUS accounting request. The Gn APN represents the APN selected by the GGSN.

Usage Guidelines Use this command to configure the APN name for RADIUS Accounting. This can be set to either gi or gn.

Example

The following command specifies the usage of Gn APN name in the RADIUS accounting request:

```
radius accounting apn-to-be-included gn
```

radius accounting billing-version

This command configures the billing-system version of RADIUS accounting servers.

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

radius accounting billing-version *version*
default radius accounting billing-version

default

Configures the default setting. Default: 0

version

Specifies the billing-system version of RADIUS accounting servers as an integer from 0 through 4294967295. Default: 0

Usage Guidelines

Use this command to configure the billing-system version of RADIUS accounting servers.

Example

The following command configures the billing-system version of RADIUS accounting servers as *10*:

```
radius accounting billing-version 10
```

radius accounting gtp trigger-policy

This command configures the RADIUS accounting trigger policy for GTP messages.

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

radius accounting gtp trigger-policy [standard | ggsn-preservation-mode]
default radius accounting gtp trigger-policy

default

Resets the RADIUS accounting trigger policy to standard behavior for GTP session.

standard

Sets the RADIUS accounting trigger policy to standard behavior which is configured for GTP session for GGSN service.

ggsn-preservation-mode

Sends RADIUS Accounting Start when the GTP message with private extension of preservation mode is received from SGSN.

Important This is a customer-specific keyword and needs customer-specific license to use this feature. For more information on GGSN preservation mode, refer to *GGSN Service Configuration Mode Commands* chapter.

Usage Guidelines Use this command to set the trigger policy for the AAA accounting for a GTP session.

Example

The following command sets the RADIUS accounting trigger policy for GTP session to standard:

```
default radius accounting gtp trigger-policy
```

radius accounting ha policy

This command configures the RADIUS accounting policy for HA sessions.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius accounting ha policy { session-start-stop | custom1-aaa-res-mgmt }
default radius accounting ha policy
```

session-start-stop

Specifies to send Accounting Start when the session is connected, and send Accounting Stop when the session is disconnected. This is the default behavior.

custom1-aaa-res-mgmt

Accounting Start/Stop messages are generated to assist special resource management done by AAA servers. It is similar to the session-start-stop accounting policy, except for the following differences:

- Accounting Start is generated when a new call overwrites an existing session. Accounting Start is also generated during MIP session handoffs.
- No Accounting stop is generated when an existing session is overwritten and the new session continues to use the IP address assigned for the old session.

Usage Guidelines Use this command to set the behavior of the AAA accounting for an HA session.

Example

The following command sets the HA accounting policy to **custom1-aaa-res-mgmt**:

```
radius accounting ha policy custom1-aaa-res-mgmt
```

radius accounting interim volume

This command configures the volume of uplink and downlink volume octet counts that triggers RADIUS interim accounting.

Product GGSN

PDSN

HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius accounting interim volume { downlink bytes uplink bytes | total bytes
 | uplink bytes downlink bytes }
no radius accounting interim volume
```

no

Disables volume based RADIUS accounting.

downlink *bytes* uplink *bytes*

Specifies the downlink to uplink volume limit for RADIUS Interim accounting, in bytes. *bytes* must be an integer to 100000 through 4000000000.

total *bytes*

Specifies the total volume limit for RADIUS interim accounting in bytes. *bytes* must be an integer from 100000 through 4000000000.

uplink *bytes*

Specifies the uplink volume limit for RADIUS interim accounting in bytes. *bytes* must be an integer from 100000 through 4000000000.

downlink *bytes*

Specifies the downlink volume limit for RADIUS interim accounting in bytes. *bytes* must be an integer from 100000 through 4000000000.

Usage Guidelines

Use this command to trigger RADIUS interim accounting based on the volume of uplink and downlink bytes.

Example

The following command triggers RADIUS interim accounting when the total volume of uplink and downlink bytes reaches *110000*:

```
radius accounting interim volume total 110000
```

radius accounting ip remote-address

This command configures IP remote address-based RADIUS accounting parameters.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] radius accounting ip remote-address { collection | list` *`list_id`* **`}`**

no

Removes earlier configuration for the specified keyword.

collection

Enables collecting and reporting Remote-Address-Based accounting in RADIUS Accounting. This should be enabled in the AAA Context. It is disabled by default.

list *list_id*

Enters the Remote Address List Configuration Mode. This mode configures a list of remote addresses that can be referenced by the subscriber's profile. *list_id* must be an integer from 1 through 65535.

Usage Guidelines

This command is used as part of the Remote Address-based Accounting feature to both configure remote IP address lists and enable the collection of accounting data for the addresses in those lists on a per-subscriber basis.

Individual subscriber can be associated to remote IP address lists through the configuration/specification of an attribute in their local or RADIUS profile. (Refer to the **radius accounting** command in the Subscriber Configuration mode.) When configured/specified, accounting data is collected pertaining to the subscriber's communication with any of the remote addresses specified in the list.

Once this functionality is configured on the system and in the subscriber profiles, it must be enabled by executing this command with the collection keyword.

Example

The following command enables collecting and reporting Remote-Address-Based accounting in RADIUS Accounting:

```
radius accounting ip remote-address collection
```

radius accounting keepalive

This command configures the keepalive authentication parameters for the RADIUS accounting server.

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

```
radius accounting keepalive { calling-station-id id | consecutive-response
 responses_no_of | framed-ip-address ip_address | interval interval_duration |
retries retries_no_of | timeout timeout_duration | username user_name }
no radius accounting keepalive framed-ip-address
default radius accounting keepalive { calling-station-id |
consecutive-response | interval | retries | timeout | username }
```

no

Removes configuration for the specified keyword.

default

Configures the default settings.

calling-station-id *id*

Configures the Calling-Station ID to be used for the keepalive authentication as an alphanumeric string of size 1 to 15 characters. Default: 000000000000000

consecutive-response *responses_no_of*

Configures the number of consecutive authentication response after which the server is marked as reachable. *responses_no_of* must be an integer from 1 through 5. Default: 1

Important The keepalive request is tried every 0.5 seconds (non-configurable) to mark the server as up.

Important In this case (for keepalive approach) "radius accounting deadtime" parameter is not applicable.

framed-ip-address *ip_address*

Specifies the framed ip-address to be used for the keepalive accounting in IPv4 dotted-decimal notation.

interval *interval_duration*

Configures the time interval (in seconds) between the two keepalive access requests. Default:30

retries *retries_no_of*

Configures the number of times the keepalive access request to be sent before marking the server as unreachable. *retries_no_of* must be an integer from 3 through 10. Default: 3

timeout *timeout_duration*

Configures the time interval between each keepalive access request retries. *timeout_duration* must be an integer from 1 through 30. Default: 3

username *user_name*

Configures the username to be used for the authentication as an alphanumeric string of 1 through 127 characters. Default: Test-Username

Usage Guidelines Configures the keepalive authentication parameters for the RADIUS accounting server.

Example

The following command sets the user name for the RADIUS keepalive access requests to *Test-Username2*:

```
radius accounting keepalive username Test-Username2
```

The following command sets the number of retries to *4*:

```
radius accounting keepalive retries 4
```

radius accounting rp

This command configures the current context's RADIUS accounting R-P originated call options.

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

```
radius accounting rp { handoff-stop { immediate | wait-active-stop } |
tod minute hour | trigger-event { active-handoff | active-start-param-change
 | active-stop } | trigger-policy { airlink-usage [ counter-rollover ] |
 custom [ active-handoff | active-start-param-change | active-stop ] |
standard } | trigger-stop-start }
no radius accounting rp { tod minute hour | trigger-event { active-handoff
 | active-start-param-change | active-stop } | trigger-stop-start }
default radius accounting rp { handoff-stop | trigger-policy }
```

no

Removes earlier configuration for the specified keyword.

default

Configures this command with the default settings.

handoff-stop { immediate | wait-active-stop }

Specifies the behavior of generating accounting STOP when handoff occurs.

- **immediate**: Indicates that accounting STOP should be generated immediately on handoff, i.e. not to wait active-stop from the old PCF.
- **wait-active-stop**:Indicates that accounting STOP is generated only when active-stop received from the old PCF when handoff occurs.

Default: **wait-active-stop**

tod *minute hour*

Specifies the time of day a RADIUS event is to be generated for accounting. Up to four different times of the day may be specified through separate commands.

minute must be an integer from 0 through 59.

hour must be an integer from 0 through 23.

trigger-event { active-handoff | active-start-param-change | active-stop }

Configures the events for which a RADIUS event is generated for accounting as one of the following:

- **active-handoff**: Disables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Instead, two R-P events occur (one for the Connection Setup, and the second for the Active-Start). Default: Disabled

- **active-start-param-change**: Disables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change. Default: Enabled
- **active-stop**: Disables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF. Default: Disabled

Important This keyword has been obsoleted by the **trigger-policy** keyword. Note that if this command is used, if the context configuration is displayed, RADIUS accounting RP configuration is represented in terms of the trigger-policy.

trigger-policy { airlink-usage [counter-rollover] | custom [active-handoff | active-start-param-change | active-stop] | standard }

Default:**airlink-usage**: Disabled

custom:

- **active-handoff**: Disabled
- **active-start-param-change**: Disabled
- **active-stop**: Disabled
- **standard**:Enabled

Configures the overall accounting policy for R-P sessions as one of the following:

- **airlink-usage [counter-rollover]**:Designates the use of Airlink-Usage RADIUS accounting policy for R-P, which generates a start on Active-Starts, and a stop on Active-Stops.

If the **counter-rollover** option is enabled, the system generates a STOP/START pair before input/output data octet counts (or input/output data packet counts) become larger than (2^32 - 1) in value. This setting is used to guarantee that a 32-bit octet count in any STOP message has not wrapped to larger than 2^32 thus ensuring the accuracy of the count. The system, may send the STOP/START pair at any time, so long as it does so before the 32-bit counter has wrapped. Note that a STOP/START pair is never generated unless the subscriber RP session is in the Active state, since octet/packet counts are not accumulated in the Dormant state.

- **custom**: specifies the use of custom RADIUS accounting policy for R-P. The custom policy can consist of the following:
- **active-handoff**: Enables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Normally two R-P events will occur (one for the Connection Setup, and the second for the Active-Start).
- **active-start-param-change**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change.

Important Note that a custom trigger policy with only **active-start-param-change** enabled is identical to the **standard** trigger-policy.

- **active-stop**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF.

Important If the **radius accounting rp trigger-policy custom** command is executed without any of the optional keywords, all custom options are disabled.

- **standard**: Specifies the use of Standard RADIUS accounting policy for R-P in accordance with IS-835B.

trigger-stop-start

Specifies that a stop/start RADIUS accounting pair should be sent to the RADIUS server when an applicable R-P event occurs.

Usage Guidelines Use this command to configure the events for which a RADIUS event is sent to the server when the accounting procedures vary between servers.

Example

The following command enables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF:

```
radius accounting rp trigger-event active-stop
```

The following command generates the STOP only when active-stop received from the old PCF when handoff occurs:

```
default radius accounting rp handoff-stop
```

radius accounting server

This command configures RADIUS accounting server(s) in the current context.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius [ mediation-device ] accounting server ip_address [ encrypted ] key
 value [ acct-on { enable | disable } ] [ acct-off { enable | disable } ]
 [ max max_messages ] [ oldports ] [ port port_number ] [ priority priority ] [
 type { mediation-device | standard } ] [ admin-status { enable | disable
 } ] [ -noconfirm ]
```

no radius [mediation-device] accounting server *ip_address* **[oldports | port** *port_number* **]**

no

Removes the server or server port(s) specified from the list of configured servers.

mediation-device

Enables mediation-device specific AAA transactions used to communicate with this RADIUS server.

Important If this option is not used, the system by default enables standard AAA transactions.

ip_address

Specifies the IP address of the accounting server.

ip_address must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[encrypted] key *value*

Specifies the shared secret key used to authenticate the client to the servers. The **encrypted** keyword indicates the key specified is encrypted.

In 12.1 and earlier releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.

In 12.2 and later releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.

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 **key** keyword is the encrypted version of the plaint text key. Only the encrypted key is saved as part of the configuration file.

acct-on { enable | disable }

This keyword enables/disables sending of the Accounting-On message when a new RADIUS server is added to the configuration. By default, this keyword will be disabled.

When enabled, the Accounting-On message is sent when a new RADIUS server is added in the configuration. However, if for some reason the Accounting-On message cannot be sent at the time of server configuration (for example, if the interface is down), then the message is sent as soon as possible. Once the Accounting-On message is sent, if it is not responded to after the configured RADIUS accounting timeout, the message is retried the configured number of RADIUS accounting retries. Once all retries have been exhausted, the system no longer attempts to send the Accounting-On message for this server.

In releases prior to 18.0, whenever a chassis boots up or when a new RADIUS accounting server or RADIUS mediation-device accounting server is configured with Acct-On configuration enabled, the state of the RADIUS server in all the AAA manager instances was initialized to "Waiting-for-response-to-Accounting-On". The Acct-On transmission and retries are processed by the Admin-AAAmgr.

When the Acct-On transaction is complete (i.e., when a response for Accounting-On message is received or when Accounting-On message is retried and timed-out), Admin-AAAmgr changes the state of the RADIUS accounting server to Active in all the AAA manager instances. During the period when the state of the server is in "Waiting-for-response-to-Accounting-On", any new RADIUS accounting messages which are generated as part of a new call will not be transmitted towards the RADIUS accounting server but it will be queued. Only when the state changes to Active, these queued up messages will be transmitted to the server.

During ICSR, if the interface of the radius nas-ip address is srp-activated, then in the standby chassis, the sockets for the nas-ip will not be created. The current behavior is that if the interface is srp-activated Accounting-On transaction will not happen at ICSR standby node and the state of the RADIUS server in all the AAAmgr instances will be shown as "Waiting-for-response-to-Accounting-On" till the standby node becomes Active.

In 18.0 and later releases, whenever the chassis boots up or when a new RADIUS accounting server or RADIUS mediation-device accounting server is configured with Acct-On configuration enabled, the state of the RADIUS server will be set to Active for all the non-Admin-AAAmgr instances and will be set to "Waiting-for-response-to-Accounting-On" for only Admin-AAAmgr instance. The Accounting-On transaction logic still holds good from Admin-AAAmgr perspective. However, when any new RADIUS accounting messages are generated even before the state changes to Active in Admin-AAAmgr, these newly generated RADIUS accounting messages will not be queued at the server level and will be transmitted to the RADIUS server immediately.

During ICSR, even if the interface of radius nas-ip address is srp-activated, the state of the RADIUS accounting server will be set to Active in all non-Admin-AAAmgr instances and will be set to "Waiting-for-response-to-Accounting-On" in Admin-AAAmgr instance.

acct-off { enable | disable }

Default: **enable**

Disables and enables the sending of the Accounting-Off message when a RADIUS server is removed from the configuration.

The Accounting-Off message is sent when a RADIUS server is removed from the configuration, or when there is an orderly shutdown. However, if for some reason the Accounting-On message cannot be sent at this time, it is never sent. The Accounting-Off message is sent only once, regardless of how many accounting retries are enabled.

max *max_messages*

Specifies the maximum number of outstanding messages that may be allowed to the server. *max_messages* must be an integer from 0 through 4000. Default: 0

oldports

Sets the UDP communication port to the out of date standardized default for RADIUS communications to 1646.

port *port_number*

Specifies the port number to use for communications as an integer from 1 through 65535. Default:1813

priority *priority*

Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to.

priority must be an integer from 1 through 1000, where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the **-noconfirm** option, you are not asked for confirmation and multiple servers could be assigned the same priority.

Default: 1000

type { mediation-device | standard }

Specifies the type of AAA transactions to use to communicate with this RADIUS server.

- **standard**:Use standard AAA transactions.
- **mediation-device**: This keyword is obsolete.

Default: **standard**

type standard

Specifies the use of standard AAA transactions to use to communicate with this RADIUS server. Default: **standard**

admin-status { enable | disable }

Enables or disables the RADIUS authentication/accounting/ charging server functionality, and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm

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

Usage Guidelines

This command is used to configure the RADIUS accounting servers with which the system is to communicate for accounting.

Up to 128 RADIUS servers can be configured per context. The servers can be configured as Accounting, Authentication, charging servers, or any combination thereof.

Example

The following commands configure the RADIUS accounting server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

```
radius accounting server 10.2.3.4 key sharedKey port 1024 max 127
radius accounting server 10.2.3.4 encrypted key scrambledKey oldports
priority 10
no radius accounting server 10.2.5.6
```

The following command sets the accounting server with mediation device transaction for AAA server *10.2.3.4*:

```
radius mediation-device accounting server 10.2.3.4 key sharedKey port
1024 max 127
```

radius algorithm

This command configures the RADIUS authentication server selection algorithm 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

```
radius algorithm { first-server | round-robin }
default radius algorithm
```

default

Configures this command with the default setting. Default: **first-server**

first-server

Sends authentication data to the first available RADIUS authentication server based upon the relative priority of each configured server.

round-robin

Sends authentication data in a circular queue fashion on a per Session Manager task basis where data is sent to the next available RADIUS authentication server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.

Usage Guidelines

Use this command to configure the context's RADIUS server selection algorithm to ensure proper load distribution through the available RADIUS authentication servers.

Example

The following command configures to use the round-robin algorithm for RADIUS authentication server selection:

```
radius algorithm round-robin
```

radius allow

This command configures the system behavior to allow subscriber sessions when RADIUS accounting and/or authentication is unavailable.

Product

PDSN

HA

FA

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 ] radius allow { accounting-down | authentication-down }`

no

Removes earlier configuration for the specified keyword.

accounting-down

Allows sessions while accounting is unavailable (down). Default: Enabled

authentication-down

Allows sessions while authentication is not available (down). Default: Disabled

Usage Guidelines

Allow sessions during system troubles when the risk of IP address and/or subscriber spoofing is minimal. The denial of sessions may cause dissatisfaction with subscribers at the cost/expense of verification and/or accounting data.

Important

Please note that this command is applicable ONLY to CDMA products. To configure this functionality in UMTS/LTE products (GGSN/P-GW/ SAEGW), use the command **mediation-device delay-GTP-response** in APN Configuration mode.

Example

The following command configures the RADIUS server to allow the sessions while accounting is unavailable:

`radius allow accounting-down`

radius attribute

This command configures the system's RADIUS identification parameters.

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

```
radius attribute { nas-identifier id | nas-ip-address address primary_address
 [ backup secondary_address ] [ nexthop-forwarding-address nexthop_ip_address ]
[ vlan vlan_id ] [ mpls-label input in_label_value output out_label_value1
out_label_value1 ] }
no radius attribute { nas-identifier | nas-ip-address }
default radius attribute nas-identifier
```

no

Removes earlier configuration for the specified keyword.

default

Configures the default setting.

nas-identifier *id*

Specifies the attribute name by which the system will be identified in Access-Request messages. *id* must be a alphanumeric string of 1 through 32 characters that is case sensitive.

nas-ip-address address *primary_address*

Specifies the AAA interface IP address(es) used to identify the system. Up to two addresses can be configured. *primary_address* is the IP address of the primary interface to use in the current context in IPV4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

backup *secondary_address*

Specifies the IP address of the secondary interface to use in the current context in IPV4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

mpls-label input *in_label_value* | output *out_label_value1* [*out_label_value2*]

This command configures the traffic from the specified AAA client NAS IP address to use the specified MPLS labels.

- *in_label_value* is the MPLS label that identifies inbound traffic destined for the configured NAS IP address.
- *out_label_value1* and *out_label_value2* identify the MPLS labels to be added to the packets sent from the specified NAS IP address.
  - *out_label_value1* is the inner output label.
  - *out_label_value2* is the outer output label.

MPLS label values must be an integer from 16 through 1048575.

Important This option is available only when nexthop-forwarding gateway is also configured with the **nexthop-forwarding-address** keyword.

nexthop-forwarding-address *nexthop_ip_address*

Configures the next hop IP address for this NAS IP address in IPV4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

vlan *vlan_id*

Specifies the VLANID to be associated with the next-hop IP address as an integer from 1 through 4094.

Usage Guidelines

This is necessary for NetWare Access Server usage such as the system must be identified to the NAS.

The system supports the concept of the active nas-ip-address. The active nas-ip-address is defined as the current source ip address for RADIUS messages being used by the system. This is the content of the nas-ip-address attribute in each RADIUS message.

The system will always have exactly one active nas-ip-address. The active nas-ip-address will start as the primary nas-ip-address. However, the active nas-ip-address may switch from the primary to the backup, or the backup to the primary. The following events will occur when the active nas-ip-address is switched:

- All current in-process RADIUS accounting messages from the entire system are cancelled. The accounting message is re-sent, with retries preserved, using the new active nas-ip-address. Acct-Delay-Time, however, is updated to reflect the time that has occurred since the accounting event. The value of Event-Timestamp is preserved.
- All current in-process RADIUS authentication messages from the entire system are cancelled. The authentication message is re-sent, with retries preserved, using the new active nas-ip-address. The value of Event-Timestamp is preserved.
- All subsequent in-process RADIUS requests uses the new active nas-ip-address.

The system uses a revertive algorithm when transitioning active NAS IP addresses as described below:

- If the configured primary nas-ip-address transitions from UP to DOWN, and the backup nas-ip-address is UP, then the active nas-ip-address switches from the primary to the backup nas-ip-address
- If the backup nas-ip-address is active, and the primary nas-ip-address transitions from DOWN to UP, then the active nas-ip-address switches from the backup to the primary nas-ip-address

Example

The following command configures the RADIUS attribute nas-ip-address as *10.2.3.4*:

```
radius attribute nas-ip-address 10.2.3.4
```

radius authenticate null-username

This command enables (allows) or disables (prevents) the authentication of user names that are blank or empty. This is enabled by default.

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

```
[ no | default ] radius authenticate null-username
```

default

Configures the default setting.

Default: Authenticate, send Access-Request messages to the AAA server, all user names, including NULL user names.

no

Disables sending an Access-Request message to the AAA server for user names (NAI) that are blank.

null-username

Enables sending an Access-Request message to the AAA server for user names (NAI) that are blank.

Usage Guidelines

Use this command to disable, or re-enable, sending Access-Request messages to the AAA server for user names (NAI) that are blank (NULL).

Example

The following command disables sending of Access-Request messages for user names (NAI) that are blank:

```
no radius authenticate null-username
```

The following command re-enables sending of Access-Request messages for user names (NAI) that are blank:

```
radius authenticate null-username
```

radius authenticate apn-to-be-included

This command configures the Access Point Name (APN) to be included for RADIUS authentication.

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

```
[ default ] radius authenticate apn-to-be-included { gi | gn }
```

default

Configures the default setting.

gi

Specifies the use of the Gi APN name in the RADIUS authentication request. The Gi APN represents the APN received in the Create PDP Context Request message from the SGSN.

gn

Specifies the use of the Gn APN name in the RADIUS authentication request. The Gn APN represents the APN selected by the GGSN.

Usage Guidelines

Use this command to configure the APN name for RADIUS authentication. This can be set to either gi or gn.

Example

The following command specifies the usage of Gn APN name in the RADIUS authentication request.

```
radius authenticate apn-to-be-included gn
```

radius authenticator-validation

This command enables (allows) or disables (prevents) the MD5 authentication of RADIUS users. By default this feature is enabled.

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

`[ default | no ] radius authenticator-validation`

default

Enables MD5 authentication validation for an Access-Request message to the AAA server.

no

Disables MD5 authentication validation for an Access-Request message to the AAA server.

Usage Guidelines

Use this command to disable, or re-enable, sending Access-Request messages to the AAA server for MD5 validation.

Example

The following command disables MD5 authentication validation for Access-Request messages for user names (NAI):

`no radius authenticator-validation`

The following command enables MD5 authentication validation for Access-Request messages for user names (NAI):

`radius radius authenticator-validation`

radius change-authorize-nas-ip

This command configures the NAS IP address and UDP port on which the current context will listen for Change of Authorization (COA) messages and Disconnect Messages (DM). If the NAS IP address is not defined with this command, any COA or DM messages from the RADIUS server are returned with a Destination Unreachable error.

Product

FA

GGSN

HA

LNS

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

radius change-authorize-nas-ip *ip_address* **[encrypted] key** *value* **[port** *port* **] [event-timestamp-window** *window* **] [no-nas-identification-check] [no-reverse-path-forward-check] [mpls-label input** *in_label_value* **| output** *out_label_value1* **[** *out_label_value2* **]**
no radius change-authorize-nas-ip

no

Deletes the NAS IP address information which disables the system from receiving and responding to COA and DM messages from the RADIUS server.

ip_address

Specifies the NAS IP address of the current context's AAA interface that was defined with the **radius attribute** command.

ip_address can be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

[encrypted] key *value*

Specifies the shared secret key used to authenticate the client to the servers. The **encrypted** keyword indicates the key specified is encrypted.

In 12.1 and earlier releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.

In 12.2 and later releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.

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 **key** keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

port *port*

The UDP port on which to listen for CoA and DM messages. Default: 3799

event-timestamp-window *window*

When a COA or DM request is received with an event-time-stamp, if the current-time is greater than the received-pkt-event-time-stamp plus the event-time-stamp-window, the packet is silently discarded

When a COA or DM request is received without the event-time stamp attribute, the packet is silently discarded.

window must be an integer from 0 through 4294967295. If *window* is specified as 0 (zero), this feature is disabled; the event-time-stamp attribute in COA or DM messages is ignored and the event-time-stamp attribute is not included in NAK or ACK messages. Default: 300

no-nas-identification-check

Disables the context from checking the NAS Identifier/NAS IP Address while receiving the CoA/DM requests. By default this check is enabled.

no-reverse-path-forward-check

Disables the context from checking whether received CoA or DM packets are from one of the AAA servers configured under the default AAA group in the current context. Only the src-ip address in the received CoA or DM request is validated and the port and key are ignored. The reverse-path-forward-check is enabled by default.

If **reverse-path-forward-check** is disabled, the CoA and DM messages will be accepted from AAA servers from any groups. If the check is enabled, then the CoA and DM messages will be accepted only from servers under default AAA group.

mpls-label input *in_label_value* | output *out_label_value1* [*out_label_value2*]

This command configures COA traffic to use the specified MPLS labels.

- *in_label_value* is the MPLS label that identifies inbound COA traffic.
- *out_label_value1* and *out_label_value2* identify the MPLS labels to be added to COA response.
  - *out_label_value1* is the inner output label.
  - *out_label_value2* is the outer output label.

MPLS label values must be an integer from 16 through 1048575.

Usage Guidelines

Use this command to enable the current context to listen for COA and DM messages.

Any one of the following RADIUS attributes may be used to identify the subscriber:

- **3GPP-IMSI**: The subscriber's IMSI. It may include the 3GPP-NSAPI attribute to delete a single PDP context rather than all of the PDP contexts of the subscriber when used with the GGSN product.
- **Framed-IP-address**: The subscriber's IP address.
- **Acct-Session-Id**:Identifies a subscriber session or PDP context.

Important For the GGSN product, the value for Acct-Session-Id that is mandated by 3GPP is used instead of the special value for Acct-Session-Id that we use in the RADIUS messages we exchange with a RADIUS accounting server.

Important When this command is used in conjunction with the GGSN, CoA functionality is not supported.

Example

The following command specifies the IP address *192.168.100.10* as the NAS IP address, a key value of *123456* and uses the default port of *3799*:

```
radius change-authorize-nas-ip 192.168.100.10 key 123456
```

The following command disables the nas-identification-check for the above parameters:

```
radius change-authorize-nas-ip 192.168.100.10 key 123456
no-nas-identification-check
```

radius charging

This command configures basic RADIUS options for Active Charging 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

```
radius charging { deadtime dead_minutes | detect-dead-server {
consecutive-failures consecutive_failures | response-timeout timeout_duration }
| max-outstanding max_messages | max-retries max_retries | max-transmissions
transmissions | timeout timeout_duration }
default radius charging { deadtime | detect-dead-server | max-outstanding
 | max-retries | max-transmissions | timeout }
no radius charging { detect-dead-server | max-transmissions | timeout }
```

no

Removes configuration for the specified keyword.

default

Configures the default settings.

deadtime *dead_minutes*

Specifies the number of minutes to wait before attempting to communicate with a server which has been marked as unreachable.

dead_minutes must be an integer from 0 through 65535.

Default: 10

detect-dead-server { consecutive-failures *consecutive_failures* | response-timeout *timeout_duration* }

consecutive-failures *consecutive_failures*: Default: 4. Specifies the number of consecutive failures, for each AAA manager, before a server is marked as unreachable. *consecutive_failures* must be an integer from 0 through 1000.

response-timeout *timeout_duration*: Specifies the number of seconds for each AAA manager to wait for a response to any message before a server is detected as failed, or in a down state. *timeout_duration* must be an integer from 1 through 65535.

max-outstanding *max_messages*

Specifies the maximum number of outstanding messages a single AAA manager instance will queue. *max_messages* must be an integer from 1 through 4000. Default: 256

max-retries *max_retries*

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as unreachable and the detect dead servers consecutive failures count is incremented. *max_retries* must be an integer from 0 through 65535. Default: 5

max-transmissions *transmissions*

Sets the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with the **max-retries** for each server. *transmissions* must be an integer from 1 through 65535. Default: Disabled

When failing to communicate with a RADIUS sever, the subscriber is failed once all of the configured RADIUS servers have been exhausted or once the configured number of maximum transmissions is reached.

For example, if 3 servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried 4 times (once plus 3 retries), the secondary server is tried 4 times, and then a third server is tried 4 times. If there is a fourth server, it is not tried because the maximum number of transmissions (12) has been reached.

timeout *timeout_duration*

Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the messages. *timeout_duration* must be an integer from 1 through 65535. Default: 3

Usage Guidelines

Manage the basic Charging Service RADIUS options according to the RADIUS server used for the context.

Example

The following command configures the AAA server to be marked as unreachable when the consecutive failure count exceeds 6:

```
radius charging detect-dead-server consecutive-failures 6
```

The following command sets the timeout value to 300 seconds to wait for a response from RADIUS server before resending the messages:

```
radius charging timeout 300
```

radius charging accounting algorithm

This command specifies the fail-over/load-balancing algorithm to be used for selecting RADIUS servers for charging services.

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

radius charging accounting algorithm { first-n *n* **| first-server | round-robin }**

first-n *n*

Specifies that the AGW must send accounting data to *n* (more than one) AAA servers based on their priority. Response from any one of the *n* AAA servers would suffice to proceed with the call. The full set of accounting data is sent to each of the *n* AAA servers.

n is the number of AAA servers to which accounting data will be sent, and must be an integer from 2 through 128. Default: 1 (Disabled)

first-server

Specifies that the context must send accounting data to the RADIUS server with the highest configured priority. In the event that this server becomes unreachable, accounting data is sent to the server with the next-highest configured priority. This is the default algorithm.

round-robin

Specifies that the context must load balance sending accounting data among all of the defined RADIUS servers. Accounting data is sent in a circular queue fashion on a per Session Manager task basis, where data is sent to the next available server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.

Usage Guidelines

Use this command to specify the accounting algorithm to use to select RADIUS servers for charging services configured in the current context.

Example

The following command specifies to use the round-robin algorithm to select the RADIUS server:

```
radius charging accounting algorithm round-robin
```

radius charging accounting server

This command configures RADIUS charging accounting servers in the current context for Active Charging Services prepaid accounting.

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

radius charging accounting server *ip_address* **[encrypted] key** *key* **[max** *max_messages* **] [max-rate** *max_rate* **] [oldports] [port** *port_number* **] [priority** *priority* **] [admin-status { enable | disable }] [-noconfirm]**
no radius charging accounting server *ip_address* **[oldports | port** *port_number* **]**

no

Removes the server or server port(s) specified from the list of configured servers.

ip_address

Specifies IP address of the accounting server in IPv4 dotted-decimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[encrypted] key *key*

Specifies the shared secret key used to authenticate the client to the servers. The **encrypted** keyword indicates the key specified is encrypted.

In 12.1 and earlier releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.

In 12.2 and later releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.

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 **key** keyword is the encrypted version of the plaint text key. Only the encrypted key is saved as part of the configuration file.

max *max_messages*

Specifies the maximum number of outstanding messages that may be allowed to the server. *max_messages* must be integer from 0 through 4000. Default: 0

max-rate *max_rate*

Specifies the rate (number of messages per second) at which the authentication messages should be sent to the RADIUS server. *max_rate* must be an integer from 0 through 1000. Default: 0 (Disabled)

oldports

Sets the UDP communication port to the out of date standardized default for RADIUS communications to 1646.

port *port_number*

Specifies the port number to use for communications as an integer from 1 through 65535. Default: 1813

priority *priority*

Specifies the relative priority of this accounting server. The priority is used in server selection for determining to which server to send accounting data. *priority* must be an integer 1 through 1000 where 1 is the highest priority. Default:1000

admin-status { enable | disable }

Enables or disables the RADIUS authentication/ accounting/charging server functionality, and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm

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

Usage Guidelines

This command is used to configure the RADIUS charging accounting server(s) with which the system is to communicate for Active Charging Services prepaid accounting requests.

Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA. Up to 16 servers are supported per context when the system is functioning as a GGSN.

Example

The following commands configure RADIUS charging accounting server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

```
radius charging accounting server 10.2.3.4 key sharedKey port 1024 max
127
radius charging accounting server 10.2.3.4 encrypted key scrambledKey
oldports priority 10
```

radius charging algorithm

This command configures the RADIUS authentication server selection algorithm for Active Charging Services 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

```
radius charging algorithm { first-server | round-robin }
default radius charging algorithm
```

default

Configures the default setting. Default: **first-server**

first-server

Sends accounting data to the first available server based upon the relative priority of each configured server.

round-robin

Sends accounting data in a circular queue fashion on a per Session Manager task basis where data is sent to the next available server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.

Usage Guidelines

Set the context's RADIUS server selection algorithm for Active Charging Services to ensure proper load distribution through the servers available.

Example

The following command configures to use the round-robin algorithm for RADIUS server selection:

```
radius charging algorithm round-robin
```

radius charging server

This command configures the RADIUS charging server(s) in the current context for Active Charging Services prepaid authentication.

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

```
radius charging server ip_address [ encrypted ] key key [ max max_messages ] [
 max-rate max_rate ] [ oldports ] [ port port_number ] [ priority priority ] [
 admin-status { enable | disable } ] [ -noconfirm ]
no radius charging server ip_address [ oldports | port port_number ]
```

no

Removes the server or server port(s) specified from the list of configured servers.

ip_address

Specifies the IP address of the server in IPv4 dotted-decimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[encrypted] key *key*

Specifies the shared secret key used to authenticate the client to the servers. The **encrypted** keyword indicates the key specified is encrypted.

In 12.1 and earlier releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.

In 12.2 and later releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.

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 **key** keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

max *max_messages*

Specifies the maximum number of outstanding messages that may be allowed to the server. *max_messages* must be an integer from 0 through 4000. Default: 256

max-rate *max_rate*

Specifies the rate (number of messages per second), at which the authentication messages should be sent to the RADIUS server. *max_rate* must be an integer from 0 through 1000. Default: 0 (Disabled)

oldports

Sets the UDP communication port to the old default for RADIUS communications to 1645.

port *port_number*

Specifies the port number to use for communications as an integer from 1 through 65535. Default:1812

priority *priority*

Specifies the relative priority of this accounting server. The priority is used in server selection for determining to which server to send accounting data. *priority* must be an integer from 1 through 1000 where 1 is the highest priority. Default: 1000

admin-status { enable | disable }

Enables or disables the RADIUS authentication/accounting/charging server functionality and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm

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

Usage Guidelines

This command is used to configure the RADIUS charging server(s) with which the system is to communicate for Active Charging Services prepaid authentication requests.

Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA. Up to 16 servers are supported per context when the system is functioning as a GGSN.

Example

The following commands configure RADIUS charging server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

```
radius charging server 10.2.3.4 key sharedKey port 1024 max 127
radius charging server 10.2.3.4 encrypted key scrambledKey oldports
priority 10
```

radius deadtime

This command configures the maximum period of time (in minutes) that must elapse between when a context marks a RADIUS server as unreachable and when it can re-attempt to communicate with the server.

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

radius deadtime *minutes*
default radius deadtime

default

Configures the default setting.

Default: 10 minutes

minutes

Specifies the number of minutes to wait before changing the state of a RADIUS server from "Down" to "Active". *minutes* must be an integer from 0 through 65535.

Important

Configuring deadtime as 0 disables the feature and the server is never marked as DOWN.

Usage Guidelines

Use this command to configure the basic RADIUS parameters according to the RADIUS server used for the context.

Important This parameter is not applicable when **radius detect-dead-server keepalive** is configured. For keepalive approach **radius keepalive consecutive-response** is used instead of **radius deadtime** to determine when the server is marked as reachable. For further explanation refer to **radius keepalive consecutive-response** command's description.

Important This parameter should be set to allow enough time to remedy the issue that originally caused the server's state to be changed to "Down". After the dead time timer expires, the system returns the server's state to "Active" regardless of whether or not the issue has been fixed.

Important For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the *RADIUS Server State Behavior* appendix in the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

Example

The following command configures the RADIUS deadtime to 100 minutes:

```
radius deadtime 100
```

radius detect-dead-server

This command configures how the system detects a dead RADIUS server.

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

```
radius detect-dead-server { consecutive-failures consecutive_failures_count |
 keepalive | response-timeout timeout_duration }
{ default | no } radius detect-dead-server
```

no

Removes the configuration.

default

Configures the default setting.

- **consecutive-failures**:Enabled; 4 consecutive failures
- **keepalive**: Disabled
- **response-timeout**: Disabled

consecutive-failures *consecutive_failures_count*

Specifies the consecutive number of times that the system must find the AAA server unreachable for the server to be marked unreachable, that is the server's state is changed from "Active" to "Down".

consecutive_failures_count must be an integer from 1 through 1000. Default: Enabled; 4 consecutive failures

keepalive

Enables the AAA server alive-dead detect mechanism based on sending keepalive authentication messages to all authentication servers. Default: Disabled

response-timeout *timeout_duration*

Specifies the time duration, in seconds, that the system must wait for a response from the AAA server to any message before the server is marked unreachable, that is the server's state is changed from "Active" to "Down".

timeout_duration must be an integer from 1 through 65535. Default: Disabled

Usage Guidelines

Use this command to configure how the system detects a dead RADIUS server.

Important If both **consecutive-failures** and **response-timeout** are configured, then both parameters must be met before a server's state is changed to "Down".

Important The "Active" or "Down" state of a RADIUS server as defined by the system, is based on accessibility and connectivity. For example, if the server is functional but the system has placed it into a "Down" state, it could be the result of a connectivity problem. When a RADIUS server's state is changed to "Down", a trap is sent to the management station and the **deadtime** timer is started.

Example

The following command enables the detect-dead-server consecutive-failures mechanism and configures the consecutive number of failures to *10*:

```
radius detect-dead-server consecutive-failures 10
```

radius dictionary

Configures the RADIUS dictionary.

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

radius dictionary *dictionary*
default radius dictionary

default

Configures the default setting.

dictionary

Specifies which dictionary to use.

dictionary must be one of the following values:

Table 1: RADIUS Dictionary Types

Dictionary	Description
3gpp	This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835.
custom*XX*	These are customized dictionaries. For information on custom dictionaries, contact your local service representative. *XX* is the integer of the custom dictionary. NOTE: RADIUS dictionary *custom23* should be used in conjunction with Active Charging Service (ACS).

Dictionary	Description
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC2869.
starent	This dictionary consists of all the attributes in the starent-vsa1 dictionary and incorporates additional VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.
starent-835	This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.
starent-vsa1	This dictionary consists not only of the 3gpp2 dictionary, but also includes vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs(0–255). This is the default dictionary. **Important** In 12.0 and later releases, no new attributes can be added to the **starent-vsa1** dictionary. If there are any new attributes to be added, these can only be added to the **starent** dictionary. For more information, please contact your Cisco account representative.
starent-vsa1-835	This dictionary consists not only of the 3gpp2-835 dictionary, but also includes vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0–255). This is the default dictionary.

Usage Guidelines

Use this command to configure the RADIUS dictionary.

Example

The following command configures the RADIUS dictionary standard.

```
radius dictionary standard
```

radius group

This command has been deprecated and is replaced by AAA Server Group configurations. Seethe *AAA Server Group Configuration Mode Commands* chapter.

radius ip vrf

This command associates the specific AAA group (NAS-IP) with a Virtual Routing and Forwarding (VRF) Context instance for BGP/MPLS, GRE, and IPSec tunnel functionality which needs VRF support for RADIUS communication. By default the VRF is NULL, which means that AAA group is associated with global routing table.

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

radius ip vrf *vrf_name*
no radius ip vrf

no

Disables the configured IP Virtual Routing and Forwarding (VRF) context instance and removes the association between the VRF context instance and the AAA group instance (NAS-IP).

By default this command is disabled, which means the NAS-IP being used is assumed a non-VRF IP and specific AAA group does not have any VRF association.

vrf_name

Specifies the name of a pre-configured VRF context instance. *vrf_name* is the alphanumeric string of a pre-configured VRF context configured in Context Configuration Mode via the **ip vrf** command.

Caution

Any incorrect configuration, such as associating AAA group with wrong VRF instance or removing a VRF instance, will fail the RADIUS communication.

Usage Guidelines

Use this command to associate/disassociate a pre-configured VRF context for a feature such as BGP/MPLS VPN or GRE, and IPSec tunneling which needs VRF support for RADIUS communication.

By default the VRF is NULL, which means that AAA group (NAS-IP) is associated with global routing table and NAS-IP being used is assumed a non-VRF IP.

This IP VRF feature can be applied to RADIUS communication, which associates the VRF with the AAA group. This command must be configured whenever a VRF IP is used as a NAS-IP in the AAA group or at the Context level for 'default' AAA group.

This is a required configuration as VRF IPs may be overlapping hence AAA needs to know which VRF the configured NAS-IP belongs to. By this support different VRF-based subscribers can communicate with different RADIUS servers using the same, overlapping NAS-IP address, if required across different AAA groups.

Example

The following command associates VRF context instance *ip_vrf1* with specific AAA group (NAS-IP):

```
radius ip vrf ip_vrf1
```

radius keepalive

This command configures the keepalive authentication parameters for the RADIUS server.

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

```
radius keepalive [ calling-station-id id | consecutive-response responses_no_of
 | encrypted | interval interval_duration | password | retries retries_no_of |
timeout timeout_duration | username user_name | valid-response access-accept
[ access-reject ] ]
default radius keepalive { calling-station-id | consecutive-response |
interval | password | retries | timeout | username | valid-response }
```

default

Configures the default setting for the specified parameter.

calling-station-id *id*

Configures the Calling-Station ID to be used for the keepalive authentication. *id* must bean alphanumeric string of size 1 to 15 characters. Default: 000000000000000

consecutive-response *responses_no_of*

Configures the number of consecutive authentication responses after which the server is marked as reachable. *responses_no_of* must be an integer from 1 through 10. Default: 1

Important The keepalive request is tried every 0.5 seconds (non-configurable) to mark the server as up.

Important In this case (for keepalive approach) "radius deadtime"' parameter is not applicable.

encrypted password

Designates use of encryption for the password.

In 12.1 and earlier releases, *password* must be an alphanumeric string of 1 through 63 characters.

In 12.2 and later releases, *password* must be an alphanumeric string of 1 through 132 characters.

Default: Test-Password

interval *interval_duration*

Configures the time interval (in seconds) between two keepalive access requests. *interval_duration* must be an integer from 30 through 65535. Default: 30

password

Configures the password to be used for the authentication as an alphanumeric string of 1 through 63 characters. Default: Test-Password

retries *retries_no_of*

Configures the number of times the keepalive access request are sent before marking the server as unreachable. *retries_no_of* must be an integer from 3 through 10. Default: 3

timeout *timeout_duration*

Configures the time interval (in seconds) between keepalive access request retries. *timeout_duration* must be an integer from 1 through 30. Default: 3

username *user_name*

Configures the username to be used for authentication as an alphanumeric string of 1 through 127 characters. Default: Test-Username

valid-response access-accept [*access-reject*]

Configures the valid response for the authentication request.

If *access-reject* is configured, then both access-accept and access-reject are considered as success for the keepalive authentication request.

If *access-reject* is not configured, then only access-accept is considered as success for the keepalive access request.

Default: **keepalive valid-response access-accept**

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

Example

The following command sets the user name for the RADIUS keepalive access requests to *Test-Username2*:

```
radius keepalive username Test-Username2
```

The following command sets the number of retries to *4*:

```
radius keepalive retries 4
```

radius max-outstanding

This command configures the maximum number of outstanding messages a single AAA Manager instance will queue.

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

```
radius max-outstanding max_messages
default radius max-outstanding
```

default

Configures the default setting.

Default: 256

max_messages

Specifies the maximum number of outstanding messages a single AAA Manager instance will queue. *max_messages* must be an integer from 1 through 4000. Default: 256

Usage Guidelines Use this command to configure the maximum number of outstanding messages a single AAA Manager instance will queue.

Example

The following command configures the maximum number of outstanding messages a single AAA Manager instance will queue to *100*:

```
radius max-outstanding 100
```

radius max-retries

This command configures the maximum number of times communication with a AAA server will be attempted before it is marked as "Not Responding".

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

`radius max-retries` *`max_retries`*
`default radius max-retries`

default

Configures the default setting.

max_retries

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as "Not Responding", and the detect dead server's consecutive failures count is incremented. *max_retries* must be an integer from 0 through 65535. Default: 5

Usage Guidelines

Use this command to configure the maximum number of times communication with a AAA server will be attempted before it is marked as "Not Responding".

Example

The following command configures the maximum number of times communication with a AAA server will be attempted before it is marked as "Not Responding" to *10*:

```
radius max-retries 10
```

radius max-transmissions

This command configures the maximum number of re-transmissions for RADIUS authentication 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

radius max-transmissions *max_transmissions*
{ default | no } radius max-transmissions

no

Deletes the RADIUS max-transmissions configuration.

default

Configures the default setting.

Default: Disabled

max_transmissions

Specifies the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with **radius max-retries** configuration for each server. *max_transmissions* must be an integer from 1 through 65535. Default: Disabled

When failing to communicate with a RADIUS sever, the subscriber is failed once all of the configured RADIUS servers have been exhausted, or once the configured number of maximum transmissions is reached.

For example, if three servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried four times (once plus three retries), the secondary server is tried four times, and then a third server is tried four times. If there is a fourth server, it is not tried because the maximum number of transmissions (12)has been reached.

Usage Guidelines

Use this command to configure the maximum number of re-transmissions for RADIUS authentication requests.

Example

The following command configures the maximum number of re-transmissions for RADIUS authentication requests to *10*:

```
radius max-transmissions 10
```

radius mediation-device

See the **radius accounting server** command.

radius probe-interval

This command configures the interval between two RADIUS authentication probes.

Product

All products supporting Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius probe-interval *seconds*
default radius probe-interval

default

Configures the default setting of 3.

seconds

Specifies the time duration (in seconds) to wait before sending another probe authentication request to a RADIUS server. The value must be an integer from 1 through 65535. Default: 3

Usage Guidelines

Use this command for ICSR support to set the duration between two authentication probes to the RADIUS server.

Example

The following command sets the authentication probe interval to 30 seconds.

```
radius probe-interval 30
```

radius probe-max-retries

This command configures the number of retries for RADIUS authentication probe response.

Product

All products supporting Inter chassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius probe-max-retries *retries*
default radius probe-max-retries

default

Configures the default setting.

Default: 5

retries

Specifies the number of retries for RADIUS authentication probe response before the authentication is declared as failed. *retries* must be an integer from 1 through 65535. Default: 5

Usage Guidelines

Use this command for ICSR support to set the number of attempts to send RADIUS authentication probe without a response before the authentication is declared as failed.

Example

The following command sets the maximum number of retries to *6*:

```
radius probe-max-retries 6
```

radius probe-message

This command configures the service ip-address to be sent as an AVP in RADIUS authentication probe messages.

Product

All products supporting Inter chassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius probe-message local-service-address ipv4/ipv6_address
no radius probe-message local-service-address
```

no

Disables sending of AVPs configured under probe-message cli in RADIUS authentication probe messages.

radius probe-message local-service-address

radius probe-message

Configures AVPs to be sent in RADIUS authentication probe messages.

local-service-address

Configures the service ip-address to be sent as an AVP in RADIUS authentication probe messages.

ipv4/ipv6_address

Specifies the IPv4/IPv6 address of the server in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

Example

The following command configures the service ip-address *21.32.36.25* to be sent as an AVP in RADIUS authentication probe messages:

```
radius probe-message local-service-address 21.32.36.25
```

radius probe-timeout

This command configures the timeout duration to wait for a response for RADIUS authentication probes.

Product

All products supporting Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius probe-timeout *timeout_duration*
default radius probe-timeout

default

Configures the default setting.

Default: 3

timeout_duration

Specifies the time duration (in seconds) to wait for a response from the RADIUS server before resending the authentication probe. *timeout_duration* must bean integer from 1 through 65535. Default: 3

Usage Guidelines

Use this command for ICSR support to set the duration to wait for a response before re-sending the RADIUS authentication probe to the RADIUS server.

Example

The following command sets the authentication probe timeout to *120* seconds:

```
radius probe-timeout 120
```

radius server

This command configures RADIUS authentication server(s) in the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius server *ip_address* **[encrypted] key** *value* **[max** *max_messages* **] [max-rate** *max_rate* **] [oldports] [port** *port_number* **] [priority** *priority* **] [probe | no-probe] [probe-username** *user_name* **] [probe-password [encrypted] password** *password* **] [type { mediation-device | standard }] [admin-status { enable | disable }] [-noconfirm]**
no radius server *ip_address* **[oldports | port** *port_number* **]**

no

Removes the server or server port(s) specified from the list of configured servers.

ip_address

Specifies the IP address of the server in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[encrypted] key *value*

Specifies the shared secret key used to authenticate the client to the servers. The **encrypted** keyword indicates the key specified is encrypted.

In 12.1 and earlier releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.

In 12.2 and later releases, the key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.

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 **key** keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

max *max_messages*

Specifies the maximum number of outstanding messages that may be allowed to the server. *max_messages* must be an integer from 0 through 4000. Default: 256

max-rate *max_rate*

Specifies the rate (number of messages per second), at which the authentication messages should be sent to the RADIUS server. *max_rate* must be an integer from 0 through 1000. Default: 0 (Disabled)

oldports

Sets the UDP communication port to the old default for RADIUS communications to 1645.

port *port_number*

Specifies the port number to use for communications as an integer from 1 through 65535. Default: 1812

priority *priority*

Specifies the relative priority of this accounting server. The priority is used in server selection for determining to which server is to send accounting data.

priority must be an integer from 1 through 1000 where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the **-noconfirm** option, you are not asked for confirmation and multiple servers could be assigned the same priority.

Default: 1000

probe

Enables probe messages to be sent to the specified RADIUS server.

no-probe

Disables probe messages from being sent to the specified RADIUS server. This is the default behavior.

probe-username *username*

Specifies the username sent to the RADIUS server to authenticate probe messages. *username* must be an alphanumeric string of 1 through 127 characters.

probe-password [encrypted] password *password*

The password sent to the RADIUS server to authenticate probe messages.

encrypted: This 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.

password *password*: Specifies the probe-user password for authentication. *password* must be an alphanumeric string of 1 through 63 characters.

type { mediation-device | standard }

Specifies the type of transactions the RADIUS server accepts.

mediation-device: Specifies mediation-device specific AAA transactions. This device is available if you purchased a transaction control services license. Contact your local sales representative for licensing information.

standard: Specifies standard AAA transactions. (Default)

admin-status { enable | disable }

Enables or disables the RADIUS authentication/accounting/charging server functionality, and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm

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

Usage Guidelines

This command is used to configure the RADIUS authentication server(s) with which the system is to communicate for authentication.

Up to 128 RADIUS servers can be configured per context. The servers can be configured as Accounting, Authentication, charging servers, or any combination thereof.

Example

The following commands configure RADIUS server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

```
radius server 10.2.3.4 key sharedKey port 1024 max 127
radius server 10.2.3.4 encrypted key scrambledKey oldports priority 10
```

radius strip-domain

This command configures the stripping of the domain from the user name prior to authentication or accounting.

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

```
radius strip-domain { authentication-only | accounting-only }
no radius strip-domain
```

no

Removes the RADIUS strip-domain configuration.

authentication-only

Specifies that the domain must be stripped from the user name prior to authentication.

accounting-only

Specifies that the domain must be stripped from the user name prior to accounting.

Usage Guidelines Use this command to configure the stripping of domain from the user name prior to authentication or accounting.

By default, strip-domain configuration will be applied to both authentication and accounting messages, if configured. When the argument **authentication-only** or **accounting-only** is present, **strip-domain** is applied only to the specified RADIUS message types.

Example

The following command configures the stripping of domain from the user name prior to authentication:

```
radius strip-domain authentication-only
```

radius timeout

This command configures the time duration to wait for a response from the RADIUS server before resending the messages.

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

```
radius timeout timeout_duration
default radius timeout
```

default

Configures the default setting.

timeout_duration

Specifies the time duration (in seconds) to wait for a response from the RADIUS server before resending the messages. *timeout_duration* must be an integer from 1 through 65535. Default: 3

Usage Guidelines Use this command to configure the time duration to wait for a response from the RADIUS server before resending the messages.

Example

The following command configures the RADIUS timeout parameter to 300 seconds:

```
radius timeout 300
```

radius trigger

This command enables specific RADIUS triggers. The RADIUS Trigger configuration in the Context Configuration Mode is to enable backward compatibility. To configure RADIUS triggers for the default AAA group, you must configure them in the Context Configuration Mode.

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 ] radius trigger { ms-timezone-change | qos-change | rai-change |
rat-change | serving-node-change | uli-change }
default radius trigger
```

no

Disables the specified RADIUS trigger.

default

Configures the default setting.

Default: All RADIUS triggers are enabled.

ms-timezone-change

Specifies to enable RADIUS trigger for MS time zone change.

qos-change

Specifies to enable RADIUS trigger for Quality of Service change.

rai-change

Specifies to enable RADIUS trigger for Routing Area Information change.

rat-change

Specifies to enable RADIUS trigger for Radio Access Technology change.

serving-node-change

Specifies to enable RADIUS trigger for Serving Node change.

uli-change

Specifies to enable RADIUS trigger for User Location Information change.

Usage Guidelines

Use this command to enable RADIUS triggers.

Example

The following command enables RADIUS trigger for RAT change:

```
radius trigger rat-change
```

realtime-trace-module

This command is used to create, configure, or delete the module for Real Time Cell Traffic Tracing in a context.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] realtime-trace-module
```

no

Removes the real time trace module configuration for the current context.

realtime-trace-module

Creates the module for real time cell traffic tracing.

Once the realtime trace module is configured, the real time trace file transfer parameters can be configured.

Usage Guidelines

Use this command to configure the module for Real Time Cell Traffic Tracing in a context. The user must be in a non-local context when specifying the **realtime-trace-module** command.

On entering this command, the CLI prompt changes to:

[*context_name*]*host_name*(config-realtime-trace)#

remote-server-list

Creates or specifies the name of an existing remote server list for this context and enters the Remote Access List Configuration Mode.

Product All

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

```
remote-server-list name list_name
no remote-server-list name list_name
```

no

Removes the specified remote server list from the context.

list_name

Specifies the name of the remote server list. If *list_name* does not refer to an existing list, the new list is created if resources allow. *list_name* is an alphanumeric string of 1 through 31 characters.

Usage Guidelines Enter the Remote Server List Configuration Mode for an existing list or for a newly defined list. This command is also used to remove an existing remote access list.

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

Entering this command results in the following prompt:

```
[context_name]hostname(config-remote-server-list)#
```

Remote Server List Configuration Mode commands are defined in the *remote Server List Configuration Mode Commands* chapter.

Example

The following command enters the Remote Server List Configuration Mode for the list named *remote_list_1*:

```
remote-server-list remote_list_1
```

The following command will remove *remote_list_1* from the system:

```
no remote-server-list remote_list_1
```

route-access-list extended

Configures an access list for filtering routes based on a specified range of IP addresses.

Product PDSN

HA

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] route-access-list extended *identifier* **{ deny | permit } ip {** *network_parameter* **} {** *mask_parameter*

no

Deletes the specified route access list.

identifier

Specifies a value to identify the route access list as an integer from 100 through 999.

deny

Deny routes that match the specified criteria.

permit

Permit routes that match the specified criteria.

ip *network_parameter ip_address wildcard_mask*

Specifies the network portion of the route to match. The network portion of the route is mandatory and must be expressed in one of the following ways:

- *ip_address wildcard_mask*: Matches a network address and wildcard mask expressed in IPv4 dotted-decimal notation.
- **any**: Matches any network address.
- **host** *network_address*: Match the specified network address exactly. *network_address* must be an IPv4 address specified in dotted-decimal notation.

mask_parameter

This specifies the mask portion of the route to match. The mask portion of the route is mandatory and must be expressed in one of the following ways:

- *mask_address wildcard_mask*: A mask address and wildcard mask expressed in IPv4 dotted-decimal notation.
- **any**: Match any network mask.
- **host** *mask_address*: Match the specified mask address exactly. *mask_address* must be an IPv4 address specified in dotted-decimal notation.

Usage Guidelines Use this command to create an extended route-access-list that matches routes based on network addresses and masks.

Example

Use the following command to create an extended route-access-list:

```
route-access-list extended 100 permit ip 192.168.100.0 0.0.0.255
```

route-access-list named

Configures an access list for filtering routes based on a network address and net mask.

Product PDSN

HA

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 ] route-access-list named`** *`list_name`* **`{ deny | permit } {`** *`ip_address/mask`* **`| any } [ exact-match ]`**

no

Deletes the specified route access list.

list_name

Specifies name that identifies the route access list as an alphanumeric string of 1 through 79 characters.

deny

Denies routes that match the specified criteria.

permit

Permits routes that match the specified criteria.

ip_address/mask

Specifies the IP address (in IPv4 dotted-decimal notation) and the number of subnet bits, representing the subnet mask in CIDR notation (for example 10.1.1.1/24).

any

Matches any route.

exact-match

Matches the IP address prefix exactly.

Usage Guidelines

Use this command to create route-access lists that specify routes that are accepted.

Up to 16 routes can be added to each route-access-list.

Example

Use the following command to create a route access list named *list27* that permits routes that match *192.168.1.0/24* exactly:

```
route-access-list named list 27 permit 192.168.1.0/24 exact-match
```

To delete the list, use the following command:

```
no route-access-list named list 27 permit 192.168.1.0/24 exact-match
```

route-access-list standard

Configures an access-list for filtering routes based on network addresses.

Product

PDSN

HA

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] route-access-list standard *identifier* **{ permit | deny } {** *ip_address wildcard_mask* **| any | host** *network_address* **}**

no

Deletes the specified route access list.

identifier

Specifies a value that identifies the route-access-list as an integer from 1 through 99.

deny

Denies routes that match the specified criteria.

permit

Permits routes that match the specified criteria.

ip_address wildcard_mask

Specifies the IP address and subnet mask to match for routes. Both *ip_address* and *wildcard_mask* must be entered in IPv4 dotted-decimal notation. (For example, 192.168.100.0 255.255.255.0)

any

Matches any route.

host *network_address*

Matches only route shaving the specified network address as if it had a 32-bit network mask. *network_address* must be an IPv4 address specified in dotted-decimal notation.

Usage Guidelines

Use this command to create route-access-lists that specify routes that are accepted.

Example

Use the following command to create a route access list with an identifier of *10* that permits routes:

```
route-access-list standard 10 permit 192.168.1.0 255.255.255.0
```

To delete the list, use the following command:

```
no route-access-list standard 10 permit 192.168.1.0 255.255.255.0
```

route-map

Creates a route-map that is used by the routing features and enters Route-map Configuration mode. A route-map allows redistribution of routes and includes a list of match and set commands associated with it. The match commands specify the conditions under which redistribution is allowed; the set commands specify the particular redistribution actions to be performed if the criteria specified by match commands are met. Route-maps are used for detailed control over route distribution between routing processes. Up to eight route-maps can be created in each context. Refer to the *Route-map Configuration Mode Commands* chapter for more information.

Product

PDSN

HA

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

```
route-map map_name { deny | permit } seq_number
no route-map map_name
```

no

Deletes the specified route map.

map_name

Specifies the name of the route map to create or edit as an alphanumeric string of 1 through 69 characters.

deny

If the deny parameter is specified and the match command criteria are met, the route is not redistributed and any other route maps with the same map name are not examined. Set commands have no affect on deny route-maps.

permit

If the permit parameter is specified, and the match criteria are met, the route is redistributed as specified by set actions. If the match criteria are not met, the next route map with the same name is tested.

seq_number

Specifies the sequence number that indicates the position a new route map is to have in the list of route maps already configured with the same name. Route maps with the same name are tested in ascending order of their sequence numbers. This must be an integer from 1 through 65535.

Usage Guidelines

Use this command to create route maps that allow redistribution of routes based on specified criteria and set parameters for the routes that get redistributed. The chassis supports a maximum of 64 route maps per context.

Example

To create a route map named map1 that permits routes that match the specified criteria, use the following command:

```
route-map map1 permit 10
```

To delete the route-map, enter the following command:

```
no route-map map1 permit 10
```

router

Enables BGP, Open Shortest Path First (OSPF) or OSPF version 3 (OSPFv3) routing functionality and enters the corresponding Configuration Mode. Refer to the *BGP Configuration Mode Commands*, *OSPF Configuration*

Mode Commands or *OSPFv3 Configuration Mode Commands* chapter for details on associated Configuration mode commands.

Product

PDSN

HA

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] router { bgp *as_number* **| ospf | ospfv3 | rip }**

no

Disables the specified routing support in the current context.

bgp *as_number*

Enables a BGP routing service for this context and assigns it the specified Autonomous System (AS) number before entering the BGP Configuration mode. *as_number* must be an integer from 1 through 4294967295.

Important BGP routing is supported only for use with the HA.

ospf

Enables OSPF routing in this context and enters OSPF Configuration mode.

ospfv3

Enables OSPFv3 routing in this context and enter OSPFv3 Configuration mode.

Usage Guidelines

Use this command to enable and configure OSPF and BGP routing in the current context.

Important You must obtain and install a valid license key to use these features. Refer to the *System Administration Guide* for details on obtaining and installing feature use license keys.

Example

The following command enables the OSPF routing functionality and enters the OSPF Configuration Mode:

```
router ospf
```

The following command enables the OSPFv3 routing functionality and enters the OSPFv3 Configuration Mode:

```
router ospfv3
```

The following command enables a BGP routing service with an AS number of *100*, and enters the BGP Configuration Mode:

```
router bgp 100
```