AAA Server Group Configuration Mode Commands

The AAA Server Group Configuration Mode is used to create and manage the Diameter/RADIUS server groups within the context or system. AAA server group facilitates management of group (list) of servers at per subscriber/APN/realm level for AAA functionality.

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-aaa-group)#`

Important As AAA applications do not support the indirectly connected hosts, configure only the directly connected host.

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

description

Allows you to enter descriptive text for this configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

`description` *`text`*
`no description`

`no`

Clears the description for this configuration.

text

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

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

Usage Guidelines The description should provide useful information about this configuration.

diameter accounting

This command configures Diameter accounting parameters.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-aaa-group)#`

Syntax Description

diameter accounting { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus } | endpoint *endpoint_name* **| hd-mode fall-back-to-local | hd-storage-policy** *hd_policy* **| max-retries** *max_retries* **| max-transmissions** *max_transmissions* **| request-timeout** *request_timeout_duration* **| sdc-integrity | server** *host_name* **priority** *priority* **| upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel9 } }**
default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions | request-timeout | upgrade-dict-avps }
no diameter accounting { endpoint | hd-mode | hd-storage-policy | max-retries | max-transmissions | sdc-integrity | server *host_name* **| upgrade-dict-avps }**

no diameter accounting { endpoint | hd-mode | hd-storage-policy | max-retries | max-transmissions | sdc-integrity | server *host_name* | upgrade-dict-avps }

endpoint: Removes the configured accounting endpoint, and the default accounting server configured in the default AAA group will be used.

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

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

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

max-transmissions: Disables the configured maximum transmission attempts for Diameter accounting in the current AAA group.

sdc-integrity: Excludes the "SDC-Integrity-Grouping" Diameter AVP in the ACR message even if present in the "aaa-custom4" dictionary.

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

upgrade-dict-avps: Sets the release version to 3GPP Rel. 8 for upgrading Diameter accounting dictionary in the current AAA group.

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

dictionary: Sets the context's dictionary as the system default.

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

max-retries: Sets the retry attempts for Diameter accounting in the current AAA group to default 0 (disable).

max-transmissions: Sets the configured maximum transmission attempts for Diameter accounting in the current AAA group to default 0 (disable).

request-timeout: Sets the timeout duration, in seconds, for Diameter accounting requests in the current AAA group to default 20.

upgrade-dict-avps: Sets the release version to 3GPP Rel. 8 for upgrading Diameter accounting dictionary in the current AAA group.

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

Specifies the Diameter accounting dictionary.

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

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

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

rf-plus: RF Plus dictionary.

endpoint *endpoint_name*

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

endpoint_name must be a string of 1 through 63 characters.

hd-mode fall-back-to-local

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

hd-storage-policy *hd_policy*

Associates the specified HD Storage policy with the AAA group.

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

HD Storage policies are configured through the Global Configuration Mode.

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

max-retries *max_retries*

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

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

Default: 0

max-transmissions *max_transmissions*

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

max_transmissions must be an integer from 1 through 1000.

Default: 0

request-timeout *request_timeout_duration*

Specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request.

request_timeout_duration specifies the number of seconds, and must be an integer from 1 through 3600.

Default: 20

sdc-integrity

This keyword enables the SDC Integrity feature. When enabled, SDC-Integrity-Grouping AVP is included in the ACR message. This AVP contains the number of Service Data Containers (SDCs) included by P-GW and the checksum as calculated by the previously defined algorithm. The checksum calculation is done only if the AVP is included. By default, this feature is disabled i.e. the grouped AVP is not included in the ACR message even if present in the "aaa-custom4" dictionary. The CLI command will have no effect if the dictionary does not contain the SDC-Integrity-Grouping AVP.

Important This feature is customer-specific. For more information, contact your Cisco Account representative.

P-GW generates the charging data and creates a new ACR with individual SDCs based on Rating Groups, and then sends the ACR message directly to Charging Collection Function (CCF). When an intermediate node is inserted between P-GW and CCF, the node appends more SDCs in the charging record sent by P-GW through the Rf interface.

To protect the integrity of SDCs, P-GW counts the number of SDCs, runs a checksum algorithm against the bytes within the SDCs, and then adds the "SDC-Integrity-Grouping" AVP with these two values in the ACR message. This grouped AVP is optional and defined in "aaa-custom4" dictionary only. This vendor-specific AVP can be enabled only when the peer supports the vendor ID. This feature helps CCF to distinguish the SDCs included by the intermediate node.

For this feature to work, the CLI control must be enabled and "aaa-custom4" dictionary containing the grouped AVP should be used and associated with the appropriate AAA group. When this feature is enabled, there might be minimal performance impact on P-GW specifically on AAA Manager tasks due to checksum calculation.

server *host_name* priority *priority*

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

host_name specifies the Diameter host name, and must be an alphanumeric string of 1 through 63 characters.

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

upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel9 }

Specifies to upgrade Diameter accounting dictionary to 3GPP Rel. 9 version or 3GPP Rel. 10 version.

3gpp-rel10: Upgrades the dictionary to 3GPP Rel. 10 version.

3gpp-rel9: Upgrades the dictionary to 3GPP Rel. 9 version.

Default: Sets the release version to 3GPP Rel. 8

Usage Guidelines

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

Example

The following command configures the Diameter accounting dictionary, *aaa-custom10*:

```
diameter accounting dictionary aaa-custom10
```

The following command configures the Diameter endpoint, *EAP1*:

```
diameter accounting endpoint EAP1
```

The following commands configure Diameter accounting options:

```
diameter accounting max-retries 4
diameter accounting max-transmissions 2
diameter accounting request-timeout 10
diameter accounting server svc priority 1
```

diameter accounting interim

This command configures Diameter accounting interim interval to be sent to the server independently from RADIUS accounting interim interval.

Product

GGSN

P-GW

HSGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

diameter accounting interim interval *interim_interval*
no diameter accounting interim interval

no

Disables Diameter interim accounting.

interim

Specifies when system should send an interim accounting record to the server.

interval *interim_interval*

Specifies the time interval, in seconds, between sending interim accounting records. *interim_interval* must be an integer from 50 through 40000000.

Usage Guidelines

Use this command to separately configure Diameter accounting interim interval for Rf interface.

In case Diameter interim interval CLI is not configured, the P-GW retains the older behavior where Diameter accounting uses the same interim interval value configured for RADIUS accounting.

Once Diameter configuration takes effect, any change to RADIUS configuration will not affect Diameter configuration and vice versa.

Example

The following command sets the interval between sending interim accounting records to 15 minutes (900 seconds):

diameter accounting interim interval 900

diameter accounting duplicate-record

This command enables the system to create a secondary feed of Rf records and send them to the secondary AAA group.

Product

GGSN

HSGW

P-GW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

[no] diameter accounting duplicate-record

duplicate-record

This keyword creates an additional copy of Rf records and sends the duplicate Rf records to the configured secondary AAA group.

no

This keyword disables the Duplicate Rf Record Generation feature. This is the default configuration.

Usage Guidelines

Use this command to create duplicate Rf records and send them to the configured secondary AAA group.

The secondary aaa group must be configured under APN configuration mode before enabling the **diameter accounting duplicate-record** CLI command.

In releases prior to 21, gateway allows only one AAA group configuration per APN for Rf accounting. The AAA group is configured to load balance across multiple servers to pass the Rf traffic and also expect an accounting answer. Note that the secondary AAA group configuration is allowed currently but is restricted to only RADIUS accounting.

In release 21 and beyond, the gateway is provided with the ability to configure a secondary AAA group per APN for the Rf interface, and send the duplicate Diameter Rf accounting records to the secondary AAA group servers. The secondary AAA group is used for non-billing purposes only.

Important The failed duplicate records will neither be written to HDD nor added to the archival list.

For more information on this feature, see the *Rf Interface Support* chapter of the administration guide for the product you are deploying.

Example

The following command enables the system to send duplicate Rf records to secondary AAA group:

diameter accounting duplicate-record

diameter authentication

This command configures Diameter authentication parameters.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-aaa-group)#`

Syntax Description

diameter authentication { **allow any-host | dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq } | encode-supported-features pcscf-restoration-indication | endpoint** *endpoint_name* **| max-retries** *max_retries* **| max-transmissions** *max_transmissions* **| redirect-host-avp { just-primary | primary-then-secondary } | request-timeout** *request_timeout_duration* **| server** *host_name* **priority** *priority* **| upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel9 } }**
default diameter authentication { dictionary | encode-supported-features | max-retries | max-transmissions | redirect-host-avp | request-timeout | upgrade-dict-avps }
no diameter authentication {**allow any-host encode-supported-features | endpoint | max-retries | max-transmissions | server** *host_name* **| upgrade-dict-avps }**

no diameter authentication { allow any-host| encode-supported-features | endpoint | max-retries | max-transmissions | server*host_name* | upgrade-dict-avps }

allow any-host: Disables the assigned values which are applicable in diameter authentication procedures.

encode-supported-features: Disables the CLI command to not send the Supported-Features AVP.

endpoint: Removes the configured authentication endpoint, and the default server configured in default AAA group will be used.

max-retries: Disables the configured retry attempts for Diameter authentication in the current AAA group.

max-transmissions: Disables the configured maximum transmission attempts for Diameter authentication in the current AAA group.

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

upgrade-dict-avps: Sets the release version to 3GPP Rel. 8 for upgrading Diameter authentication dictionary in the current AAA group.

default diameter authentication { dictionary | encode-supported-features | max-retries | max-transmissions | redirect-host-avp | request-timeout | upgrade-dict-avps }

dictionary: Sets the context's dictionary as the system default.

encode-supported-features: Configures the default setting, that is not to send the Supported-Features AVP in AAR message.

max-retries: Sets the retry attempts for Diameter authentication requests in the current AAA group to default 0 (disable).

max-transmissions: Sets the configured maximum transmission attempts for Diameter authentication in the current AAA group to default 0 (disable).

redirect-host-avp: Sets the redirect choice to default (just-primary).

request-timeout: Sets the timeout duration, in seconds, for Diameter authentication requests in the current AAA group to default 20.

upgrade-dict-avps: Sets the release version to 3GPP Rel. 8 for upgrading Diameter authentication dictionary in the current AAA group.

allow any-host

Accepts the response from any-host.

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

Specifies the Diameter authentication dictionary.

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

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

aaa-custom9: Configures the STa standard dictionary.

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

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

encode-supported-features

Encodes Supported-Features AVP.

pcscf-restoration-indication

Enables the P-CSCF Restoration Indication feature. By default, this feature is disabled.

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

For more information on this feature, see the *Gx Interface Support* chapter in the administration guide of the product you are deploying.

endpoint *endpoint_name*

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

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

max-retries *max_retries*

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

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

Default: 0

max-transmissions *max_transmissions*

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

max_transmissions specifies the maximum number of transmission attempts, and must be an integer from 1 through 1000.

Default: 0

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

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

just-primary: Redirect only to primary host.

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

Default: just-primary

request-timeout *request_timeout_duration*

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

request_timeout_duration specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request, and must be an integer from 1 through 3600.

Default: 20 seconds

server *host_name* priority *priority*

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

host_name specifies the Diameter authentication server's host name, and must be an alphanumeric string of 1 through 63 characters.

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

upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel9 }

Specifies to upgrade Diameter authentication dictionary to 3GPP Rel. 9 version or 3GPP Rel. 10 version.

3gpp-rel10: Upgrades the dictionary to 3GPP Rel. 10 version.

3gpp-rel9: Upgrades the dictionary to 3GPP Rel. 9 version.

Default: Sets the release version to 3GPP Rel. 8

Usage Guidelines

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

Example

The following command configures the Diameter authentication dictionary, *aaa-custom1*:

```
diameter authentication dictionary aaa-custom1
```

The following command configures the Diameter endpoint, *EAP1*:

```
diameter authentication endpoint EAP1
```

The following commands configure Diameter authentication options:

```
diameter authentication max-retries 4
diameter authentication max-transmissions 2
diameter authentication redirect-host-avp primary-then-secondary
diameter authentication server svc priority 1
diameter authentication request-timeout 10
```

diameter authentication drmp

This command enables or disables the inclusion of DRMP AVP in S6b communication, and to configure DRMP value based on AAR-Initial, AAR-Interim and STR message types.

Product

All products using Diameter S6b interface.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

diameter authentication drmp [aar-initial *drmp_value* **[aar-interim** *drmp_value* **[str** *drmp_value* **]] | aar-initial** *drmp_value* **[str** *drmp_value* **[aar-interim** *drmp_value* **]] | aar-interim** *drmp_value* **[aar-initial** *drmp_value* **[str** *drmp_value* **]] | aar-interim** *drmp_value* **[str** *drmp_value* **[aar-initial** *drmp_value* **]] | str** *drmp_value* **[aar-interim** *drmp_value* **[aar-initial** *drmp_value* **]] | str** *drmp_value* **[aar-initial** *drmp_value* **[aar-interim** *drmp_value* **]]]**
no diameter authentication drmp

no

Disables encoding of DRMP AVP in S6b messages. The **no diameter authentication drmp** is the default configuration.

drmp

Specifies the settings of Diameter Routing Message Priority.

aar-initial

Includes the DRMP value in AAR-initial message. The default value is 10.

aar-interim

Includes the DRMP value in AAR-interim message. The default value is 10.

str

Includes the DRMP value in STR message. The default value is 10.

drmp_value

Specifies the DRMP value and must be an integer from 0 through 15. Zero (0) has the highest priority and 15 has the lowest. That is, lower the value, higher the priority.

Usage Guidelines

This CLI command will individually configure DRMP values for the AAR-initial, AAR-interim and STR messages. If message type priority is not specified in the CLI, default value (10) will be used. The last configured CLI line will override all values previously configured, irrespective of how many priorities are explicitly configured.

In case of configuring specific values for message types, each time the CLI is invoked, all the 3 values will be modified with the new values. If a value is not specified in CLI, it will be overwritten by default value, which is 10.

Example

The following command will include DRMP value *12* to AAR-initial, *8* to AAR-interim, and *6* to STR message:

```
diameter authentication drmp aar-initial 12 aar-interim 8 str 6
```

diameter authentication failure-handling

This command configures the failure handling for Diameter authentication requests and Diameter Extensible Authentication Protocol (EAP) requests.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

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

no

Disables Diameter authentication failure handling.

default

Configures the default Diameter authentication failure handling setting.

authorization-request

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

eap-request

Specifies configuring failure handling for EAP requests.

eap-termination-request

Specifies configuring failure handling for EAP termination requests.

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

Specifies the action to be taken for failures:

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

- **terminate**: Terminates the session

Important For any failure encountered, the "continue" option terminates the call as with the "terminate" option for all Diameter dictionaries except aaa-custom15 dictionary.

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

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

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

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

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

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

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

Example

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

```
diameter authentication failure-handling eap-request result-code 5001 to
 5005 action continue
diameter authentication failure-handling eap-request result-code 5003
action terminate
```

diameter authentication failure-handling-template

This command associates the failure-handling template with AAA group authentication for Diameter authentication requests and Diameter Extensible Authentication Protocol (EAP) requests.

Product

ePDG

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-aaa-group)#`

Syntax Description

diameter authentication failure-handling-template *template_name* **emps**
no diameter authentication failure-handling-template
no diameter authentication failure-handling-template emps

no

Disassociates a failure handling template with the AAA group authentication.

failure-handling-template *template_name*

Associates a previously created failure handling template with the authentication application in the AAA group. *template_name* specifies the name for a pre-configured failure handling template. *template_name* must be an alphanumeric string of 1 through 63 characters. By default, the template is not associated in the AAA group.

For more information on failure handling template, refer to the **failure-handling-template** command in the *Global Configuration Mode Commands* chapter.

emps

Specifies the failure-handling behavior for eMPS Sessions applicable during S6B authorization and re-authorization.

Usage Guidelines

Use this command to associate a configured failure handling template with the AAA group authentication application. The failure handling template defines the action to be taken when the Diameter application encounters a failure supposing a result-code failure, Tx-expiry or response-timeout. The application will take the action given by the template. For more information on failure handling template configurations, refer to the *Diameter Failure Handling Template Configuration Mode Commands* chapter in this guide.

This CLI command is introduced to support Overload Control on Diameter interfaces such as Gx, S6b and SWm and also to prevent network overload and outages. Whenever there is an overload condition at the Diameter Servers or DRA and request times out, the clients (ePDG/P-GW) are typically unaware of the overload condition and attempt to send the message on an alternate connection with the Diameter server causing some more traffic in the network. In order to handle this overload condition effectively, a new vendor-specific Diameter Experimental Result-Code 5198 (DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY) is defined.

When the overloaded PCRF/DRA receives a message, it includes the result-code 5198 in the response message. On receiving the experimental result-code, call is terminated based on the failure-handling configuration. If failure-handling is configured as local-policy, then the call is continued with local-policy without retrying the secondary server. For more information on the Diameter Overload Control feature, refer to the *AAA Interface Administration and Reference* document.

When the **failure-handling-template** is configured and the **failure-handling** CLI is also enabled in the AAA Group configuration, the template is given the higher preference. When the Result-Code (5198) is received

in DEA/AAA request, the call is terminated without the Session Terminate Request (STR) for S6b and SWm interfaces.

If the association is not made to the template then failure handling behavior configured in the application with the **failure-handling** command will take its effect.

Example

The following command associates the failure handling template FH_1 with the Diameter authentication interface.

```
diameter authentication failure-handling-template FH_1
```

The following command configures the failure-handling template *TEST* for eMPS subscribers during S6B authorization/re-authorization failures:

```
diameter authentication failure-handling-template TEST emps
```

diameter authentication server-selection sent-by-epdg

Use this command to disable the feature of encoding the AAA-Server-Identifier information, provided by ePDG node, into the Destination-Host/Destination-Realm in the AAR request.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

```
[ no ] diameter authentication server-selection sent-by-epdg
```

no

Causes the P-GW to ignore the AAA-Server-Identifier information received from the ePDG node.

Usage Guidelines

This CLI command is applicable to Release 21.3.5 and higher.

Use this command to disable the encoding of ePDG provided AAA-Server-Identifier information in the AAR request.

This CLI command is applicable only to servers connected through a Diameter Routing Agent (DRA).

With the default configuration (or no explicit use of the this CLI command), there is no change in behavior. That is to say, the feature of encoding an ePDG provided AAA-Server-Identifier information into the Destination-Host/Destination-Realm in the AAR request cannot be disabled.

diameter authentication strip-leading-digit

This command enables or disables stripping of leading digit from User-Name AVP of non-authentication procedures like AAR and STR.

Product

ePDG

HSGW

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

```
[ no ] diameter authentication strip-leading-digit { user-name }
```

no

Disables the stripping of leading digit from User-Name AVP of non-authentication procedures

user-name

This keyword specifies to strip off the leading digit from User-Name AVP of non-authentication procedures. By default, this feature is disabled.

Usage Guidelines

As part of 2015 4G network upgrade release, no leading digit is included in the User-Name AVP of non-authentication procedures like AAR and STR. For backward compatibility, the 3GPP AAA server accepts User-Name with and without the leading digit.

This CLI command is used to control the stripping of leading digit in the User-Name AVP. This feature is applicable to all authentication and authorization interfaces like S6b, STa and SWm and not for accounting interfaces. This CLI command is applicable only for AAR and STR messages.

If the User-Name AVP is received in RAR (for SWm and STa), the same User-Name is included in the RAA message irrespective of the CLI option. For example, if the User-Name AVP is prefixed with 0 in RAR and the CLI option for stripping is enabled, then the User-Name AVP is sent in RAA with the leading "0".

Important This CLI command will not take effect for aaa-custom17 and aaa-custom19 dictionaries. This CLI is not applicable for response messages (RAA/ASA) sent by chassis.

Example

The following command strips off the leading digit in the User-Name AVP of non-authentication procedures.

```
diameter authentication strip-leading-digit user-name
```

diameter dictionary

This command is deprecated and is replaced by the **diameter accounting dictionary** and **diameter authentication dictionary** commands. See the diameter accounting, on page 3 and diameter authentication, on page 9 commands respectively.

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **end**

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **exit**

Usage Guidelines Use this command to return to the parent configuration mode.

radius

This command configures basic RADIUS options.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-aaa-group)#`

Syntax Description

```
radius { deadtime minutes | detect-dead-server { consecutive-failures
consecutive_failures_count | response-timeout response_timeout_duration } | dictionary
 dictionary | max-outstanding max_messages | max-retries max_retries |
max-transmissions max_transmissions | probe-message local-service-address
ipv4/ipv6_address | strip-domain { authentication-only | accounting-only } |
 timeout idle_seconds }
default radius { deadtime | detect-dead-server | dictionary |
max-outstanding | max-retries | max-transmissions | timeout }
no radius { detect-dead-server | max-transmissions | radius probe-message
 local-service-address | strip-domain }
```

no

Removes the specified configuration.

default

Configures default setting for the specified keyword.

dictionary *dictionary*

Specifies which dictionary to use. The following table describes the possible values for *dictionary*:

Dictionary	Description
custom*XX*	These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative. *XX* is the integer value of the custom dictionary.
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.
3gpp	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.
starent-vsa1	This dictionary consists not only of the 3GPP2 dictionary, but also includes Starent Networks 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.

Dictionary	Description
starent-vsa1-835	This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent Networks 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.
starent	This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks 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 Starent Networks 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.

deadtime *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.

Default: 10

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 deadtime 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 StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

detect-dead-server { consecutive-failures *consecutive_failures_count* | keepalive | response-timeout *response_timeout_duration* }

consecutive-failures *consecutive_failures_count*: Specifies the number of consecutive failures, for any AAA Manager, before a server's state is changed from "Active" to "Down". *consecutive_failures_count* must be an integer from 1 through 1000. Default: 4.

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

response-timeout *response_timeout_duration*: Specifies the number of seconds, for any AAA Manager, to wait for a response to any message before a server's state is changed from "Active" to "Down". *response_timeout_duration* must be an integer from 1 through 65535.

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.

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 "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

max-transmissions *max_transmissions*

Sets the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with **max-retries** parameter for each server.

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.

max_transmissions must be an integer from 1 through 65535.

Default: Disabled

probe-message local-service-address *ipv4/ipv6_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 IP address of the 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.

strip-domain { authentication-only | accounting-only }

Specifies that the domain must be stripped 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.

timeout *idle_seconds*

Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the messages.

idle_seconds must be an integer from 1 through 65535.

Default: 3

Usage Guidelines

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

Example

The following command configures the RADIUS timeout parameter to *300* seconds.

```
radius timeout 300
```

radius accounting

This command configures the current context's RADIUS accounting parameters.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

```
radius accounting { archive [ stop-only ] | deadtime minutes |
detect-dead-server { consecutive-failures consecutive_failures_count | keepalive
 | response-timeout response_timeout_duration } | fire-and-forget | interim
```

interval *interim_interval* **| max-outstanding** *max_messages* **| max-pdu-size** *octets* **| max-retries** *max_retries* **| max-transmissions** *max_transmissions* **| timeout** *idle_seconds* **}**
default radius accounting { deadtime | detect-dead-server | fire-and-forget | max-outstanding | max-pdu-size | max-retries | max-transmissions | timeout }
no radius accounting { archive | detect-dead-server | fire-and-forget | interim interval | max-transmissions }

no

Removes the specified configuration.

default

Configures the default setting 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 serially delivered to the RADIUS accounting server. 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 only STOP accounting messages.

Default: enabled

deadtime *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.

Default: 10 minutes

Important This parameter is not applicable when **radius accounting detect-dead-server keepalive** is configured. For keepalive approach **radius accounting keepalive consecutive-response** is used instead of **radius accounting deadtime** to determine when the server is marked as reachable. For further explanation refer to **radius accounting 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 deadtime 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 StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

detect-dead-server { consecutive-failures *consecutive_failures_count* | keepalive | response-timeout *response_timeout_duration* }

consecutive-failures *consecutive_failures_count*: Specifies the number of consecutive failures, for any AAA Manager, before a server's state is changed from "Active" to "Down". *consecutive_failures_count* must be an integer from 1 through 1000. Default: 4

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

response-timeout *response_timeout_duration*: Specifies the number of seconds, for any AAA Manager, to wait for a response to any message before a server's state is changed from "Active" to "Down". *response_timeout_duration* must be an integer from 1 through 65535.

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.

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 StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

fire-and-forget

Enables RADIUS Fire-and-Forget accounting for the AAA group.

Default: Disabled

The request sent to the RADIUS accounting server configured under the AAA group with this keyword configured will not expect a response from the server. If the request must be sent to more than one such type of server, the acct-algorithm first-n configuration in the AAA group can be used.

Important The Fire-and-Forget feature is supported on GGSN, HA, PDSN and P-GW.

Keepalive feature for server state detection is supported in conjunction since there is no waiting for responses. Archiving in such a AAA group is not supported. If the server is down, the request is sent to the next server in the group. If all the servers in the group are down, the request is deleted.

This CLI is independent of the APN or subscriber profile configuration **aaa secondary-group** *aaa_group_name*.

interim interval *interim_interval*

Specifies the time interval, in seconds, for sending accounting INTERIM-UPDATE records.

interim_interval must be an integer from 50 through 40000000.

Default: Disabled

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.

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 2048.

Default: 2048

max-retries *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 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 *timeout_duration*

Specifies the duration to wait for a response from a RADIUS server before retransmitting a request.

timeout_duration must be an integer from 1 through 65535.

Default: 3

Usage Guidelines

Use this command to configure RADIUS accounting options according to the RADIUS server used for the context.

Example

The following command configures the accounting timeout parameter to *16* seconds.

```
radius accounting timeout 16
```

radius accounting apn-to-be-included

This command specifies the APN name inclusion for RADIUS accounting.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

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 use of Gi APN name in RADIUS accounting request. Gi APN represents the APN that is finally selected as part of Virtual APN selection by GGSN/P-GW.

gn

Specifies the use of Gn APN name in RADIUS accounting request. Gn APN represents the APN that is sent during "Create Session Request" from MME/S-GW to P-GW.

Usage Guidelines

Use this command to specify the APN name to be included for RADIUS accounting.

Example

The following command configures the gn APN name to be included for RADIUS accounting:

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

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 > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

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*

Default: 1 (Disabled)

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 servers, all retries are stopped.

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

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 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.

In releases to prior to 17, for subscribers with IMSI containing hexadecimal characters the round robin algorithm fails causing the messages to be forwarded to a single RADIUS server all the time. This algorithm works only for decimal based IMSI addresses. In 17 and later releases, support is extended to hexadecimal based IMSI addresses. That is, IMSI based round robin would be done for subscribers with hexadecimal based IMSI addresses.

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 configures to use the round-robin algorithm for RADIUS accounting server selection:

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

radius accounting billing-version

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

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, and must be an integer from 0 through 4294967295.

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 > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

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

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

ggsn-preservation-mode

This keyword 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 the *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 Home Agent (HA) sessions.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

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

default

Configures the default setting.

session-start-stop

Specifies sending Accounting Start when the Session is connected, and sending 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 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.
- Accounting Start is generated when a new call overwrites an existing session.

Usage Guidelines

Use this command to configure the AAA accounting behavior for an HA session.

Example

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

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

radius accounting interim

This command configures the volume of uplink and downlink volume octet counts that trigger RADIUS interim accounting, and configures the time period between the sending of interim accounting records.

Product

GGSN

PDSN

HA

HSGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

radius accounting interim { interval *interim_interval* **| volume { downlink** *bytes* **uplink** *bytes* **| total** *bytes* **| uplink** *bytes* **downlink** *bytes* **} }**
no radius accounting interim volume

no

Disables RADIUS interim accounting.

interval *interim_interval*

Specifies the time interval, in seconds, between sending interim accounting records. *interim_interval* must be an integer from 50 through 40000000.

volume { downlink *bytes* uplink *bytes* | total *bytes* | uplink *bytes* downlink *bytes* }

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

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

uplink *bytes* **downlink** *bytes*: Specifies the uplink to downlink volume limit, in bytes, for RADIUS interim accounting. *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 and/or to configure the time interval between the sending of interim accounting records.

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
```

The following command sets the interval between sending interim accounting records to 3 minutes (180 seconds):

```
radius accounting interim interval 180
```

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 > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

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

no

Removes the specified configuration.

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 > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

radius accounting keepalive { calling-station-id *id* **| consecutive-response** *consecutive_responses* **| framed-ip-address** *ipv4/ipv6_address***| interval** *seconds* **| retries** *number* **| timeout** *seconds* **| username** *user_name* **}**

```
default radius accounting keepalive { calling-station-id |
consecutive-response | interval | retries | timeout | username }
no radius accounting keepalive framed-ip-address
```

no

Removes the specified configuration.

default

Configures the default setting for the specified keyword.

calling-station-id *id*

Configures the Calling-Station-Id to be used for the keepalive authentication.

id must be an alphanumeric string of size 1 to 15 characters.

Default: 000000000000000

consecutive-response *consecutive_responses*

Configures the number of consecutive authentication response after which the server is marked as reachable.

consecutive_responses 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 accounting deadtime" parameter is not applicable.

framed-ip-address *ipv4/ipv6_address*

Configures the framed-ip-address to be used for the keepalive accounting.

ipv4/ipv6_address must be specified using IPv4 dotted-decimal notation or IPv6 colon-separated hexadecimal notation.

Notes:

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.
- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.

interval *seconds*

Configures the time interval between the two keepalive access requests.

Default: 30 seconds

retries *number*

Configures the number of times the keepalive access request to be sent before marking the server as unreachable.

number 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 seconds

username *user_name*

Configures the user name to be used for authentication.

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

Default: Test-Username

Usage Guidelines Use this command to configure the keepalive authentication parameters for the RADIUS accounting server.

Example

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

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

The following command sets the number of RADIUS accounting keepalive retries to *4*.

```
radius accounting keepalive retries 4
```

radius accounting pdif trigger-policy

This command configures the policy for generating START/STOP pairs in overflow condition.

Product PDIF

Privilege Administrator, Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

```
radius accounting pdif trigger-policy { standard | counter-rollover }
default radius accounting pdif trigger-policy
```

default

The default option configures the "standard" policy.

standard

Applies a policy as defined by the standards.

counter-rollover

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, at its discretion, send the STOP/START pair at any time, so long as it does so before the 32-bit counter has wrapped.

Usage Guidelines

Used to define the policy for dealing with overflow packet counts.

Example

Use the following example to set the default policy to *standard*.

```
default radius accounting pdif trigger-policy
```

radius accounting rp

This command configures the RADIUS accounting R-P originated call options.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

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 the specified configuration.

default

Sets the default configuration for the specified keyword.

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 individual 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 }

active-start-param-change: Enabled

active-stop: Disabled

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

Default: **active-handoff**: 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]**: Specifies 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, at its discretion, 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 when 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

For accounting, this command configures the RADIUS accounting server(s) in the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

radius [mediation-device] accounting server *ipv4/ipv6_address* **[encrypted] key** *value* **[acct-on { disable | enable }] [acct-off { disable | enable }] [admin-status { disable | enable }] [max** *max_messages* **] [max-rate** *max_value* **] [oldports] [port** *port_number* **] [priority** *priority* **] [type { mediation-device | standard }] [-noconfirm]**
no radius [mediation-device] accounting server *ipv4/ipv6_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 use to communicate with this RADIUS server.

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

ipv4/ipv6_address

Specifies the IP address of the accounting server. *ip_address* must be specified using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. A maximum of 1600 RADIUS servers per context/system and 128 servers per server group can be configured. This limit includes accounting and authentication servers.

Notes:

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.
- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.

Important The same RADIUS server IP address and port can be configured in multiple RADIUS server groups within a context.

port *port_number*

Specifies the port number to use for communications. *port_number* must be an integer from 0 through 65535. Default is 1813.

Important The same RADIUS server IP address and port can be configured in multiple RADIUS server groups within a context.

[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 StarOS 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 chassis 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 { disable | enable }

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 { disable | 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.

Default: enable

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

max-rate *max_value*

Specifies the rate at which the accounting messages should be sent to the RADIUS server by a single AAA manager task.

max_value 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.

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 }

mediation-device: Obsolete keyword.

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

standard: Use standard AAA transactions.

Default: **standard**

admin-status { disable | enable }

Configures the admin-status for the RADIUS accounting server.

enable: Enables the RADIUS accounting server.

disable: Disables the RADIUS accounting server.

-noconfirm

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

Usage Guidelines

Use this command to configure the RADIUS accounting servers with which the system must communicate for accounting.

You can configure up to 1600 RADIUS servers per context/system and 128 servers per server group. The servers can be configured as Accounting, Authentication, Charging servers, or any combination thereof.

Example

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 > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-aaa-group)#`

Syntax Description

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

default

Configures the default setting.

Default: **first-server**

first-server

Authentication data is sent to the first available authentication server based upon the relative priority of each configured server.

round-robin

Authentication data is sent in a circular queue fashion on a per Session Manager task basis where data is sent to the next available 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 authentication server selection algorithm to ensure proper load distribution amongst the available 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 for allowing subscriber sessions when RADIUS accounting and/or authentication is unavailable.

Product

All products used in CDMA deployments

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-aaa-group)#`

Syntax Description

`[ no ] radius allow { authentication-down | accounting-down }`

no

Specifies that the specified option is to be disabled.

authentication-down

Allows sessions while authentication is not available (down).

Default: Disabled

accounting-down

Allows sessions while accounting is unavailable (down).

Default: Enabled

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 > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

radius attribute { accounting *accounting_attribute* **| authentication** *authentication_attribute* **| nas-identifier** *nas_id* **| nas-ip-address address** *primary_ipv4/ipv6_address* **[backup** *secondary_ipv4/ipv6_address* **] [nexthop-forwarding-address** *nexthop_ipv4/ipv6_address* **] [mpls-label input** *in_label_value* **| output** *out_label_value1* **[** *out_label_value2* **] [vlan** *vlan_id* **]] }**
no radius attribute { accounting *accounting_attribute* **| authentication** *authentication_attribute* **| nas-identifier | nas-ip-address }**
default radius attribute { accounting | authentication | nas-identifier }

no

Removes or disables the specified configuration.

default

Configures the default setting(s).

accounting *accounting_attribute*

Enables RADIUS accounting attributes for the following options, provided they are supported in the configured RADIUS dictionary:

- **3gpp-cg-address**
- **3gpp-charging-characteristics**
- **3gpp-charging-id**
- **3gpp-ggsn-address**
- **3gpp-ggsn-mcc-mnc**
- **3gpp-gprs-qos-negotiated-profile**
- **3gpp-imeisv**
- **3gpp-imsi-mcc-mnc**
- **3gpp-ms-timezone**

- **3gpp-nsapi**
- **3gpp-pdp-type**
- **3gpp-rat-type**
- **3gpp-select-mode**
- **3gpp-session-stopindicator**
- **3gpp-sgsn-address**
- **3gpp-sgsn-mcc-mnc**
- **3gpp-user-location-info**
- **acct-authentic**
- **acct-delay-time**
- **acct-input-octets**
- **acct-input-packets**
- **acct-output-octets**
- **acct-output-packets**
- **acct-session-id**
- **acct-session-time**
- **acct-statustype**
- **called-station-id**
- **calling-station-id**
- **class**
- **event-timestamp**
- **framed-ip-address**
- **framed-ipv6-prefix**

  In Releases 19.4 and beyond, this attribute option will also include delegated-ipv6-prefix to support DHCPv6 Prefix Delegation via RADIUS server.
- **imsi**
- **nas-identifier**
- **nas-ip-address**
- **nas-port-id**
- **nas-port-type**
- **service-type**
- **username**

By default, all of the attributes are enabled except for nas-port-id attribute.

authentication *authentication_attribute*

Enables RADIUS authentication attributes for the following options, provided they are supported in the configured RADIUS dictionary:

- **3gpp-cg-address**
- **3gpp-charging-characteristics**
- **3gpp-ggsn-address**
- **3gpp-ggsn-mcc-mnc**
- **3gpp-gprs-qos-negotiated-profile**
- **3gpp-imeisv**
- **3gpp-imsi-mcc-mnc**
- **3gpp-ms-timezone**
- **3gpp-nsapi**
- **3gpp-pdp-type**
- **3gpp-rat-type**
- **3gpp-select-mode**
- **3gpp-sgsn-address**
- **3gpp-sgsn-mcc-mnc**
- **3gpp-user-location-info**
- **called-station-id**
- **calling-station-id**
- **chap-challenge**
- **framed-ipaddress**
- **framed-ipv6-prefix**
- **imsi**
- **nas-identifier**
- **nas-ip-address**
- **nas-port-id**
- **nas-port-type**
- **service-type**
- **username**

By default, all of the attributes are enabled except for nas-port-id attribute.

nas-identifier *nas_id*

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

nas-ip-address address *primary_ipv4/ipv6_address*

Specifies the AAA interface IP address(es) used to identify the system. Up to two addresses can be configured.

primary_ipv4/ipv6_address: The IP address of the primary interface to use in the current context. This must be specified using the IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Notes:

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In this release, a combination of IPv4 and IPv6 addresses is not supported.
- When a RADIUS server is configured in non-default AAA group without nas-ip, the NAS IP is taken from the default group. In this scenario, the IP address should be of the same transport type.
- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.
- It is recommended that the primary and secondary server IP addresses should be of the same transport type.

backup *secondary_ipv4/ipv6_address*

backup: The IP address of the secondary interface to use in the current context. This must be specified using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Notes:

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In this release, a combination of IPv4 and IPv6 addresses is not supported.
- When a RADIUS server is configured in non-default AAA group without nas-ip, the NAS IP is taken from the default group. In this scenario, the IP address should be of the same transport type.
- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.
- It is recommended that the primary and secondary server IP addresses should be of the same transport type.

nexthop-forwarding-address *nexthop_ipv4/ipv6_address*

Configures next hop IP address for this NAS IP address. It optionally sets the RADIUS client to provide VLAN ID and nexthop forwarding address to system when running in single nexthop gateway mode.

nexthop_ipv4/ipv6_address must be specified using IPv4 dotted-decimal notation.

Notes:

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.

- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.

Important To define more than one NAS IP address per context, in Global Configuration Mode use the **aaa large-configuration** command. If enabled, for a PDSN a maximum of 400 and for a GGSN a maximum of 800 NAS IP addresses/NAS identifiers (1 primary and 1 secondary per server group) can be configured per context.

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

Configures the traffic from the specified RADIUS client NAS IP address to use the specified MPLS labels.

- *in_label_value* is the MPLS label that will identify inbound traffic destined for the configured NAS IP address.
- *out_label_value1* and *out_label_value2* identify the MPLS labels to be added to 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 to 1048575.

vlan *vlan_id*

This optional keyword sets the RADIUS client to provide VLAN ID with nexthop forwarding address to system when running in single nexthop gateway mode.

vlan_id must be a pre-configured VLAN ID, and must be an integer from 1 through 4096. It is the VLAN ID to be provided to the system in RADIUS attributes.

This option is available only when nexthop-forwarding gateway is also configured with nexthop-forwarding-address *nexthop_address* keyword and **aaa-large configuration** is enabled at Global Configuration level.

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 identification parameter, NAS IP address to *10.2.3.4*.

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

radius authenticate

This command configures RADIUS authentication related parameters.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

```
radius authenticate { apn-to-be-included { gi | gn } | null-username }
default radius authenticate { apn-to-be-included | null-username }
no radius authenticate null-username
```

default

Configures the default setting.

no radius authenticate null-username

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

apn-to-be-included

Specifies the APN name to be included for RADIUS authentication.

gi: Specifies the usage of Gi APN name in RADIUS authentication request. Gi APN represents the APN received in the Create PDP Context request message from SGSN.

gn: Specifies the usage of Gn APN name in RADIUS authentication request. Gn APN represents the APN selected by the GGSN.

null-username

Specifies attempting RADIUS authentication even if the provided user name is NULL (empty).

Default: Enables authenticating, sending Access-Request messages to the AAA server, all user names, including NULL user names.

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 authenticator-validation

This command enables/disables the MD5 authentication of RADIUS user. MD5 authentication is enabled by default.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

```
[ default | no ] radius authenticator-validation
```

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 authenticator-validation
```

radius charging

This command configures basic RADIUS options for Active Charging Service (ACS).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

```
radius charging { deadtime dead_time | detect-dead-server {
consecutive-failures consecutive_failures_count | response-timeout
response_timeout_duration } | max-outstanding max_messages | max-retries max_retries
 | max-transmissions max_transmissions | timeout idle_seconds }
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 the specified configuration.

default

Configures the default setting for the specified keyword.

deadtime *dead_time*

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

dead_time must be an integer from 0 through 65535.

Default: 10

detect-dead-server { consecutive-failures *consecutive_failures_count* | response-timeout *response_timeout_duration* }

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

consecutive_failures_count must be an integer from 1 through 1000.

Default: 4

response-timeout *response_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.

response_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 *max_transmissions*

Sets the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with the **max-retries** parameter for each server.

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.

max_transmissions must be an integer from 1 through 65535.

Default: Disabled

timeout *idle_seconds*

Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the messages.

idle_seconds must be an integer from 1 through 65535.

Default: 3

Usage Guidelines

Use this command to 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 > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

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

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

radius charging accounting server

This command configures RADIUS charging accounting servers in the current context for ACS Prepaid Accounting.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

radius charging accounting server *ipv4/ipv6_address* **[encrypted] key** *value* **[max** *max_messages* **] [oldports] [port** *port_number* **] [priority** *priority* **] [admin-status { enable | disable }] [-noconfirm]**
no radius charging accounting server *ipv4/ipv6_address* **[oldports | port** *port_number* **]**

no

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

ipv4/ipv6_address

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

Notes:

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.
- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.

[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 StarOS 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 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 communication.

port_number must be an integer from 0 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.

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

Specifies that the command must execute without any prompts 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 ACS 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 10.1.2.3, port to 1024, priority to 10:

```
radius charging accounting server 10.1.2.3 key sharedKey212 port 1024 max
 127
radius charging accounting server 10.1.2.3 encrypted key scrambledKey234
 oldports priority 10
```

radius charging algorithm

This command specifies the RADIUS authentication server selection algorithm for ACS for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

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

default

Configures the default setting.

Default: **first-server**

first-server

Accounting data is sent to the first available server based upon the relative priority of each configured server.

round-robin

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 configure the context's RADIUS server selection algorithm for ACS to ensure proper load distribution amongst the available servers.

Example

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

```
radius algorithm round-robin
```

radius charging server

This command configures the RADIUS charging server(s) in the current context for ACS Prepaid Authentication.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

radius charging server *ipv4/ipv6_address* **[encrypted] key** *value* **[max** *max_messages* **] [oldports] [port** *port_number* **] [priority** *priority* **] [admin-status { enable | disable }] [-noconfirm]**
no radius charging server *ipv4/ipv6_address* **[oldports | port** *port_number* **]**

no

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

ipv4/ipv6_address

Specifies the IP address of the server. *ipv4/ipv6_address* must be specified using IPv4 dotted-decimal notation or IPv6 colon-separated hexadecimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

Notes:

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.

- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.

[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 StarOS 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

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.

port_number must be 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 which server to send accounting data to.

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, or charging server functionality and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm

Specifies that the command must execute without any prompts 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 ACS 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, priority to 10:

```
radius charging server 10.2.3.4 key sharedKey212 port 1024 max 127
radius charging server 10.2.3.4 encrypted key scrambledKey234 oldports
priority 10
```

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 > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

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 name of a pre-configured virtual routing and forwarding (VRF) context configured in Context configuration mode through **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 the "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 RADIUS keepalive authentication parameters.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

```
radius keepalive { calling-station-id id | consecutive-response number |
encrypted | interval seconds | password | retries number | timeout seconds |
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 keyword.

calling-station-id *id*

Specifies the Calling-Station-Id to be used for the keepalive authentication.

id must be an alphanumeric string of size 1 to 15 characters.

Default: 000000000000000

consecutive-response *number*

Specifies the number of consecutive authentication responses after which the server is marked as reachable.

number 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

Specifies encrypting the password.

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

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

Default password: Test-Password

interval *seconds*

Specifies the time interval, in seconds, between two keepalive access requests.

Default: 30 seconds

password

Specifies the password to be used for authentication.

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

Default password: Test-Password

retries *number*

Specifies the number of times the keepalive access request to be sent before marking the server as unreachable.

number must be an integer from 3 through 10.

Default: 3

timeout *timeout_duration*

Specifies the time interval between keepalive access request retries.

timeout_duration must be an integer from 1 through 30.

Default: 3 seconds

username *user_name*

Specifies the user name to be used for authentication.

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

Default: Test-Username

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

Specifies 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 configures the user name for RADIUS keepalive access requests to *Test-Username2*:

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

The following command configures the number of RADIUS keepalive retries to *4*:

```
radius keepalive retries 4
```

radius mediation-device

See the radius accounting server, on page 40 command.

radius probe-interval

This command configures the time interval between two RADIUS authentication probes.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

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

default

Configures the default setting.

seconds

Specifies the number of seconds to wait before sending another probe authentication request to a RADIUS server.

seconds must be an integer from 1 through 65535.

Default: 60

Usage Guidelines

Use this command for Interchassis Session Recovery (ICSR) support to set the duration between two authentication probes to the RADIUS server.

Example

The following command sets the RADIUS 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

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

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

default

Configures the default setting.

retries

Specifies the number of retries for RADIUS authentication probe response before the authentication is declared as failed.

retries must be an integer from 0 through 65535.

Default: 5

Usage Guidelines Use this command with Interchassis Session Recovery (ICSR) 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 configures the maximum number of retries to *6* seconds.

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

radius probe-timeout

This command configures the timeout duration for Interchassis Session Recovery (ICSR) to wait for a response for RADIUS authentication probes.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

```
radius probe-timeout idle_seconds
default radius probe-timeout
```

default

Configures the default setting.

idle_seconds

Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the authentication probe.

idle_seconds must be an integer from 0 through 65535.

Default: 3

Usage Guidelines Use this command to set the time duration for ICSR, 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 for authentication.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > **context** *context_name* > **aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

radius server *ipv4/ipv6_address* **[encrypted] key** *value* **[admin-status { disable | enable }] [max** *max_messages* **] [max-rate** *max_value* **] [oldports] [port** *port_number* **] [priority** *priority* **] [probe | no-probe] [probe-username** *user_name* **] [probe-password [encrypted] password** *password* **] [type { mediation-device | standard }] [-noconfirm]**
no radius server *ipv4/ipv6_address* **[oldports | port** *port_number* **]**

no

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

ipv4/ipv6_address

Specifies the IP address of the server.

ipv4/ipv6_address: Must be specified using IPv4 dotted-decimal notation or IPv6 colon-separated hexadecimal notation. A maximum of 1600 RADIUS servers per context/system and 128 servers per Server group can be configured. This limit includes accounting and authentication servers.

Notes:

- The gateway supports only one type of transport within one AAA group. The AAA group should have the NAS IP and RADIUS servers of same transport type (IPv4 or IPv6). In Release 19, a combination of IPv4 and IPv6 addresses is not supported.
- The IPv6 Address Configuration support is available for GGSN, HA, PDSN and P-GW products only. If other products are used in conjunction with these supported products and shared the same AAA group, then the IPv6 address should not be configured.

Important The same RADIUS server IP address and port can be configured in multiple RADIUS server groups within a context.

port *port_number*

Specifies the port number of the server.

port_number: Specifies the port number to use for communications. *port_number* must be an integer from 1 through 65535.

Default: 1812.

Important The same RADIUS server IP address and port can be configured in multiple RADIUS server groups within a context.

[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 StarOS 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 chassis 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.

admin-status { disable | enable }

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

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_value*

Specifies the rate at which the authentication messages should be sent to the RADIUS server by a single AAA manager task.

max_value 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.

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

probe

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

no-probe

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

probe-username *user_name*

The user name sent to the RADIUS server to authenticate probe messages. *user_name* 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 chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

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 Cisco representative for licensing information.

standard: Specifies standard AAA transactions. (Default)

-noconfirm

Specifies that the command must execute without any prompts 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.

You can configure up to 1600 RADIUS servers per context/system and 128 servers per Server group. 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, priority to 10:

```
radius server 10.2.3.4 key sharedKey212 port 1024 max 127
radius server 10.2.3.4 encrypted key scrambledKey234 oldports priority
10
```

radius trigger

This command enables specific RADIUS triggers.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context *context_name* **> aaa group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

Syntax Description

```
[ no ] radius trigger { ms-timezone-change | qos-change | rai-change |
rat-change | serving-node-change | uli-change }
default radius trigger
```

no

Disables 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
```