

AAA Introduction and Overview

This chapter provides the information on how to configure the AAA interface to enable authentication, authorization, and accounting (AAA) functionality for your core network service subscribers in a wireless carrier network.

This chapter provides information on basic AAA features. For information on product-specific AAA features and product-specific AAA interface configurations, refer to the administration guide for the product that you are deploying.

- Overview, on page 1
- Diameter Proxy, on page 4
- Supported Features, on page 4

Overview

The Authentication, authorization, and accounting (AAA) subsystem on the chassis provides the basic framework to configure access control on your network. The AAA subsystem in core network supports Remote Authentication Dial-In User Service (RADIUS) and Diameter protocol based AAA interface support. The AAA subsystem also provides a wide range of configurations for AAA servers in groups, which in effect contain a series of RADIUS/Diameter parameters for each application. This allows a single group to define a mix of Diameter and RADIUS servers for the various application functions.

Although AAA functionality is available through AAA subsystem, the chassis provides onboard access control functionality for simple access control through subscriber/APN authentication methods.

AAA functionality provides capabilities to operator to enable authentication and authorization for a subscriber or a group of subscriber through domain or APN configuration. The AAA interface provides the following AAA support to a network service:

- **Authentication**: It is the method of identifying users, including login and password, challenge and response, messaging support, and encryption. Authentication is the way to identify a subscriber prior to being allowed access to the network and network services. An operator can configure AAA authentication by defining a list of authentication methods, and then applying that list to various interfaces.

  All authentication methods, except for chassis-level authentication, must be defined through AAA configuration.

- **Authorization**: It is the method to provide access control, including authorization for a subscriber or domain profile. AAA authorization sends a set of attributes to the service describing the services that the user can access. These attributes determine the user's actual capabilities and restrictions.

- **Accounting**: Collects and sends subscriber usage and access information used for billing, auditing, and reporting, such as user identities, start and stop times, performed actions, number of packets, and number of bytes.

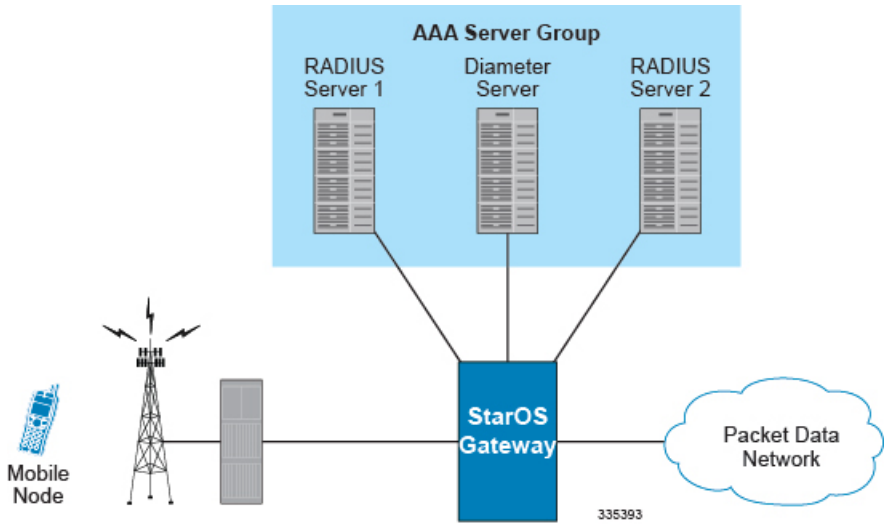
  Accounting enables operator to analyze the services users are accessing as well as the amount of network resources they are consuming. Accounting records are comprised of accounting AVPs and are stored on the accounting server. This accounting information can then be analyzed for network management, client billing, and/or auditing.

Advantages of using AAA are:

- Higher flexibility for subscriber access control configuration
- Better accounting, charging, and reporting options
- Industry standard RADIUS and Diameter authentication

The following figure shows a typical AAA server group configuration that includes three AAA servers (RADIUS and Diameter).

Figure 1: AAA Server Group Configuration in Core Network



Product Support Matrix for AAA

The following table provides the information on AAA (RADIUS and Diameter) support with our series of core multimedia gateway products. The symbol (X) indicates that the support for the identified AAA function exists for that particular product.

Note In Release 20.0 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

Product Name	Diameter Accounting	Diameter Authentication	RADIUS
Access Service Network Gateway (ASN-GW)	X	X (EAP)	X

Product Name	Diameter Accounting	Diameter Authentication	RADIUS
Femto Network Gateway (FN-GW)	N/A	N/A	X
Gateway GPRS Support Node (GGSN)	X	X (S6b)	X
Home Agent (HA)	N/A	N/A	X
Home NodeB Gateway (HNB-GW)	N/A	N/A	X
HRPD Serving Gateway (HS-GW)	X	X (STa)	N/A
IP Services Gateway (IPSG)	N/A	N/A	X
Mobility Management Entity (MME)	N/A	X (S6a/S13)	N/A
Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG)	N/A	X (SWm)	X
Packet Data Interworking Function (PDIF)	N/A	X (EAP)	X
Packet Data Support Node (PDSN)	N/A	N/A	X
Packet Data Network (PDN) Gateway (P-GW)	X	X (S6b)	X
Session Control Manager (SCM)	X	X (Cx)	X
Serving GPRS Support Node (SGSN)	N/A	X (S6d)	N/A
Serving Gateway (S-GW)	X	N/A	X

Qualified Platforms

AAA is a StarOS service that runs on Cisco ASR 5500 and virtualized platforms. For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

License Requirements

AAA is a licensed Cisco feature. Separate feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Diameter Proxy

The proxy acts as an application gateway for Diameter. It gets the configuration information at process startup and decides which Diameter peer has to be contacted for each application. It establishes the peer connection if no peer connection already exists. Upon receiving the answer, it uses the Diameter session ID to identify to which application the message is intended.

Each PSC has a Diameter proxy identified by the IPv6 origin host address. If the number of configured origin hosts is lesser than the number of active PSCs, some (i.e. those number where no origin hosts associated with) PSCs will not activate Diameter processing at all, and instead notify administrators of the erroneous configuration with syslog/traps.

If the number of configured origin hosts is greater than the number of active PSCs, the application will automatically select which configured host is to be used per PSC.

In 18.0 and later releases, Diameter Proxy has been scaled to handle more number of transactions per proxy, and support the requirement for the DPC2 card in ASR 5500. To support this scaling architecture, a new framework "proclet-map-frwk" has been developed. This framework works in Client-Server model. For diamproxy enhancement, diactrl will act as the server and the proclets (sessmgr and aaamgr) act as client. The framework will maintain a set of tables in both Client and Server which contains details about the endpoint to diamproxy association.

In support of this feature, the existing CLI command **require diameter-proxy** has been enhanced to allow multiple Diameter proxies per card and specify the proxy selection algorithm type in ASR 5500. For more information on this command, refer to the *Command Line Interface Reference*.



Important After you configure the **require diameter-proxy** CLI command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Supported Features

This section provides the list of features that are supported by RADIUS and Diameter.

Diameter Host Select Template Configuration

This feature allows the user to configure Diameter host template at Global Configuration level. Diameter host template is a table of peer servers that can be shared by different Diameter services. This template can be configured using **diameter-host-template** command in the Global Configuration Mode.



Note Currently, only Gx service can be associated with the template.

When this command is configured, it allows the user to specify the name of a new or existing Diameter host template and then enters the Diameter Host Select mode. You can configure up to 256 templates on the system.

To use the template, Diameter applications must be associated with the template. For example, using **diameter host-select-template** command in Policy Control Configuration Mode will bind the IMS authorization service to the configured Diameter host select template. When an association is made to the template, the system selects the Diameter peer to be contacted based on rows configured in the table and the algorithm configured for selecting rows in the table. The system uses the returned host name(s) to contact the primary PCRF (and secondary if configured) and establish the call.

If no association is made to the template then the **diameter peer-select** command configured at the application level will be used for peer selection.

If more than one service is using the same set of **peer-select** commands, then it is better to define all the peer selection CLI commands in the template and associate the services to the template.

For information on the command used for configuring this feature, refer to the *Command Line Interface Reference*.

Diameter Server Selection for Load-balancing

Diameter load balancing implementation maintains a fixed number of servers active at all times for load balancing in case of failures. This can be done by selecting a server with lower weight and adding it to the set of active servers.

Consider the following requirements in the Diameter Endpoint configuration for load balancing:

- Endpoint configuration is needed to specify the minimum number of servers that needs to be active for the service.
- If any one of the servers in the current active group fails, one of the idle servers needs to be selected for servicing the new requests.
- New sessions should be assigned to idle servers with higher weight.
- New session should be assigned to idle servers with lower weight only if
  - The number of active servers are less than the minimum number of servers required for the service
  - Idle servers with higher priority are not available

For information on the commands used for configuring the load-balancing feature, refer to the *Command Line Interface Reference*.

DSCP Marking for Signaling Traffic

This feature is introduced to prioritize the signaling traffic based on DSCP marking on the IP packets of the signaling messages. Diameter signaling messages also need to be marked with DS code points to classify/manage network traffic and provide Quality of Service (QoS).

Command **dscp** in the Diameter endpoint configuration mode is used to set the Differential Services Code Point (DSCP) in the IP header of the Diameter messages sent from the Diameter endpoint.

The following recommended Per-Hop-Behaviours are predefined:

PHB	Description	DSCP value	TOS value
BE	Best effort PHB (Default)	000 000 (0)	0

PHB	Description	DSCP value	TOS value
EF	Expedited Forwarding PHB	101 110 (46)	184
AF11	Assured Forwarding Class 1 low drop PHB	001 010 (10)	40
AF12	Assured Forwarding Class 1 medium drop PHB	001 100 (12)	48
AF13	Assured Forwarding Class 1 high drop PHB	001 110 (14)	56
AF21	Assured Forwarding Class 2 low drop PHB	001 010 (18)	72
AF22	Assured Forwarding Class 2 medium drop PHB	001 100 (20)	80
AF23	Assured Forwarding Class 2 high drop PHB	001 110 (22)	88
AF31	Assured Forwarding Class 3 low drop PHB	001 010 (26)	104
AF32	Assured Forwarding Class 3 medium drop PHB	001 100 (28)	112
AF33	Assured Forwarding Class 3 high drop PHB	001 110 (30)	120
AF41	Assured Forwarding Class 4 low drop PHB	001 010 (34)	136
AF42	Assured Forwarding Class 4 medium drop PHB	001 100 (36)	144
AF43	Assured Forwarding Class 4 high drop PHB	001 110 (38)	152
CS1	Class Selector 1 PHB	001 000 (8)	32
CS2	Class Selector 2 PHB	010 000 (16)	64
CS3	Class Selector 3 PHB	011 000 (24)	96
CS4	Class Selector 4 PHB	100 000 (32)	128
CS5	Class Selector 5 PHB	101 000 (40)	160
CS6	Class Selector 6 PHB	110 000 (48)	192
CS7	Class Selector 7 PHB	111 000 (56)	224

Note the difference between DSCP and the TOS values. TOS is an 8 bit field, but DSCP uses only the leading 6 bits of the TOS field.

For more information on the command used for configuring this feature, refer to the *Command Line Interface Reference*.

Dynamic Diameter Dictionary Configuration

Apart from the standard and customer-specific dictionaries supported currently in the Diameter application, this feature allows the dynamic configuration of any new Diameter dictionaries at run time. This feature can be configured using **diameter dynamic-dictionary** command in the Global Configuration Mode. For more information on this command, refer to the *Command Line Interface Reference*.



Note Up to a maximum of 10 dynamic dictionaries can be configured and loaded in to the system.

To perform this configuration, a text file should be created in ABNF format and all the required Diameter AVPs and command codes should be configured in the file. Then, the file should be saved in flash or some URL that will be accessible by the system. Now, run the **dict_validate.exe** authentication tool on the created dynamic dictionary text file. This authentication tool does basic syntax checks on the file and prepends the file contents with an MD5 checksum. This checksum ensures that the dictionary cannot be modified once created. Currently, only Cisco personnel can access the authentication tool **dict_validate.exe**.



Note It is highly necessary that you must not create dynamic dictionary for your customization needs. Contact your Cisco account representative for any new dynamic dictionary creation request.

Now, configure a dynamic dictionary with an unique name and map it to the URL of the file to be loaded dynamically in to the system at the global configuration level.

When the names of the dynamic dictionaries and their URLs are configured, the corresponding files at the respective URLs are parsed and populated in all SessMgr and AAAmgr facilities as new dictionaries and kept available to be used when these dictionary names are configured under any Diameter application level or AAA group.

When a dynamic dictionary name is configured under an application such as IMS authorization service or in a AAA group, the corresponding dictionary (which is already loaded in SessMgrs and AAAMgrs) entry will be used.

There will be only one instance of a dynamic dictionary loaded in to a task for one dynamic dictionary name even if the same dictionary name is configured in multiple AAA groups or multiple application configurations. That is, even if the same dictionary name is configured in several applications or several AAA groups, all these applications and AAA groups will refer to the same dynamic dictionary instance.

Failure Handling Template Configuration

This feature allows the user to configure Failure Handling template at Global Configuration level. The failure handling template defines the action to be taken when the Diameter application encounters a failure for example, a result-code failure, tx-expiry or response-timeout. The application will take the action given by the template. This template can be configured using **failure-handling-template** command in the Global Configuration Mode.



Note A maximum of 64 templates can be configured on the system.

This command specifies the name of a new or existing failure handling template and enters the Failure Handling Template mode. Lookup is done first to identify if there is an exact match for message-type and failure-type. If not present, lookup is done for 'any' match for message and failure type.

If there are different failure handling configurations present within the template for the same message type, the action is applied as per the latest error encountered.

To use the template, Diameter applications must be associated with the template. For example, using **associate failure-handling-template** command in Credit Control Configuration Mode will bind the Diameter Credit Control Application (DCCA) service to the configured failure handling template. When an association is made to the template, in the event of a failure, the system takes the action as defined in the failure handling template. Both IMS Authorization (Gx) and DCCA (Gy) services can be currently associated with the template.

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

For information on the command used for configuring this feature, refer to the *Command Line Interface Reference*.

Fire-and-Forget Feature

The current release supports configuring secondary AAA accounting group for the APN. This supports the RADIUS Fire-and-Forget feature in conjunction with GGSN and P-GW for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server.

This feature also supports configuring secondary AAA accounting group for the subscriber template. This supports the No-ACK RADIUS Targets feature in conjunction with PDSN and HA for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting the acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server.

Typically, the request sent to the Radius Accounting Server configured under the AAA group with the CLI **radius accounting fire-and-forget** configured will not expect a response from the server. If there is a need to send the request to multiple servers, the accounting algorithm first-n will be used in the AAA group.

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, then the request is deleted.



Note Please note that on-the-fly change in the configuration is not permitted. Any change in the configuration will have effect only for the new calls.

For information on the commands used for configuring this feature, refer to the *Command Line Interface Reference*.

Realm-based Routing

In StarOS 12.0 and later releases, the Diameter routing logic has been modified to enable routing to destination hosts that are not directly connected to the Diameter clients like GGSN, MME, PGW, and that does not have a route entry configured. Message routing to the host is based on the realm of the host.

For a given session towards a Destination Host, all the messages belonging to the session will be routed through the same peer until the peer is down. If the peer goes down, for the subsequent messages failure handling mechanism will be triggered and the message will be sent using other available peers connected to the destination host.

Dynamic Route Addition

Dynamic routes are added when a response to a Diameter request message arrives with Origin-Host AVP. If there is no route entry corresponding to the Origin-Host, realm and peer, a new dynamic route entry is created and added to the table. This route entry will be flagged as Dynamic and a Path Cache entry. The following entries will be added to the dynamic route entry.

- Flag (Dynamic and Path-Cache)
- Host name (Corresponding to the Origin-Host from the response)
- Realm (Obtained from the session)
- Application id (Obtained from the session)
- Peer (From which the response was received)
- Weight (Inherit the weight of the realm-based route entry based on which the request was routed)

Dynamic Route Deletion

The dynamic route will be deleted from the routing table in the following conditions:

- The peer associated with the route-entry is deleted.
- When the route is not used by any of the sessions for a given period of time.
- When the realm based route from which the dynamic route is derived, is deleted.

The route deletion can be accomplished by introducing a new CLI in the Diameter Endpoint configuration mode. This CLI allows configuring an expiry timeout based on which the route entry will be deleted.

For information on the commands used for configuring the realm-based routing feature, refer to the *Command Line Interface Reference*.

Wildcard based Diameter Routing

This feature provides customers the ability to configure wildcard based Diameter realm routing to avoid configuring individual Diameter peers and/or realms for all possible Diameter servers in their network.

The wildcard Diameter routes can be statically configured under a Diameter endpoint configuration using the CLI "**route-entry realm * peer** *peer_name*".

These route entries are treated as default route entries and they will be selected when there is no matching host@realm based or no realm based route entry available.

The wildcard route entry can be configured in the following ways:

route-entry realm * peer *peer_name*

- or -

route-entry host * realm * peer *peer_name*

Both these configurations have the same effect; matches to any host and any realm.

The wildcard Diameter route is added along with other realm based route entries in diabase. The wildcard route entry will be selected to route a message only if the message's destination realm does not match with any of the other static realm based routes.

For example,

route-entry realm abc.com peer *peer1*

route-entry realm def.com peer *peer2*

route-entry realm * peer peer-default

If the message's destination realm is *abc.com* then the message will be routed to *peer1*. If the message's destination realm is *def.com* then the message will be routed to *peer2*. If the destination realm is *xyz.com* then the message will be routed to "*peer-default*".

When multiple wildcard route entries are configured with same weights, then the routes are selected in a round robin fashion. When multiple wildcard route entries are configured with different weights, then the route with the highest weight will be selected.

In case when there are multiple wildcard routes with higher and equal weights and some routes with lower weights, then only the higher weight routes will be selected in round robin-fashion. The lower weight route can be selected only when the higher weight routes are not valid because of the peers being not in good state.

Rate Limiting Function (RLF)

Note Rate Limiting Function (RLF) is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Th RLF feature implements a generic framework that can be used by multiple interfaces and products for rate-limiting/throttling outgoing messages like Diameter messages on Gx, Gy interface towards PCRF.

When applications send messages to peers at a high rate, (e.g. when a large number of sessions goes down at the same time, accounting stop messages for all the sessions are generated at the same time) the peer may not be able to handle the messages at such high rates. To overcome this situation, the Rate Limiting Function (RLF) framework is developed so that the application sends messages at an optimal rate such that peer is capable of receiving all the messages and does not enter an overload condition.

This feature can be enabled using the CLI command **rlf-template**in the Global Configuration mode. The users can define the rate limiting configurations within this template. For more information on the command, see the *Command Line Interface Reference*.

Note RLF template cannot be deleted if it is bound to any application (peers/endpoints).

When RLF feature is enabled, all the messages from the application are pushed to the RLF module for throttling and rate control, and depending on the message-rate configured the RLF module sends the messages to the peer. Once the rate or a threshold value is reached, the RLF module notifies the application to slow down or stop sending messages. RLF module also notifies the application when it is capable of accepting more messages to be sent to the peer. RLF module typically uses a Token Bucket Algorithm to achieve rate limiting.

Currently in the deployment of the Diameter applications (Gx, Gy, etc.), many operators make use of "**max-outstanding** <*number*>" as a means of achieving some rate-limiting on the outgoing control traffic. With RLF in place, this is no longer required since RLF takes care of rate-limiting in all cases. If RLF is used and **max-outstanding** is also used, there might be undesirable results.



Note If RLF is being used with an "**diameter endpoint**", then set the **max-outstanding** value of the peer to be 255.

To use the template, Diameter or any other applications must be associated with the template. The RLF provides only the framework to perform the rate limiting at the configured Transactions Per Second (TPS). The applications (like Diameter) should perform the configuration specific to each application.

Truncation of Diameter Origin Host Name

Diameter host name is too long for the customer network to handle and process. The host name cannot be changed as it remains constant throughout the lifecycle of client application. So, a new CLI configuration **require diameter origin-host-abbreviation** is introduced in the Global Configuration mode to control the truncation of Diameter origin-host name.

The Diameter origin-host-name is represented as <*instance-number*>-<*procletname*>.<*name*>, where the proclet name can be sessmgr, diamproxy or aaamgr.

The **require diameter origin-host-abbreviation** CLI command aids in reducing the length of Diameter origin-host names by using "d" instead of "diamproxy", "s" instead of "sessmgr", and "a" instead of "aaamgr". If this CLI command is configured then the Diameter origin-host-name value is constructed with the corresponding proclet name abbreviations.

For example, if a Diameter proxy is used to connect to a peer then the origin host will be *0001-diamproxy.endpoint* without the CLI configuration. When the **require diameter origin-host-abbreviation** CLI command is enabled, the origin host will be *0001-d.endpoint*.



Note This CLI configuration is applicable only at the time of system boot. If the CLI command is configured during run time, the following warning message is displayed "Warning: System already has running services, save config and reboot to take effect".

For more information on CLI configuration, see the *Command Line Interface Reference* guide.