AAA Interface Configuration

This chapter describes how to configure access control to network services, and the type of services available to subscribers once they have access. The authentication, authorization, and accounting (AAA) configuration described in this chapter provides the primary framework through which you can set up AAA functionality in your network for a service subscriber.

Procedures to configure and administer core network services are described in detail in the administration guide for the product that you are deploying. System-related configuration procedures are described in detail in the *System Administration Guide*. Before using the procedures in this chapter, it is recommended to refer the respective product administration guide and the *System Administration Guide*.

This chapter includes the following information:

Configuring RADIUS AAA Functionality

RADIUS-based AAA functionality must be configured at the context and system levels. This section describes how to configure the RADIUS-based AAA parameters at the context and system levels.

To configure RADIUS AAA functionality:

Step 1 Configure RADIUS AAA functionality at context level as described in the Configuring RADIUS AAA Functionality, on page 1 section.

Step 2 Configure system-level AAA parameters as described in the Configuring System-Level AAA Functionality, on page 11 section.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Note Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring RADIUS AAA Functionality at Context Level

This section describes how to configure context-level RADIUS parameters for subscriber authentication and accounting (optional). As noted in this reference, RADIUS-based AAA functionality can be configured within any context, even its own.

Note This section provides minimum instructions to configure context-level AAA functionality that allows the system to process data sessions. Commands that configure additional context-level AAA properties are described in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.

Note Commands except **change-authorize-nas-ip**, **accounting prepaid**, **accounting prepaid custom**, and **accounting unestablished-sessions** used in this section, or in the *Understanding the System Operation and Configuration* chapter, are also applicable to support AAA server group for AAA functionality. For details on AAA server group functionality, see the Configuring AAA Server Group for AAA Functionality, on page 12 section.

To configure RADIUS AAA functionality at the context level use the following configuration:

```
configure
     context <context_name>
          radius server <ipv4/ipv6_address> key <shared_secret> [ max <value> ]
[ oldports | port <tcp_port> ] [ priority <priority> ]
          radius [ mediation-device ] accounting server <ipv4/ipv6_address>
key <shared_secret> [ acct-on { enable | disable } ] [ acct-off { enable |
disable } ] [ max <msgs> ] [ oldports ] [ port <port_number> ] [ priority
<priority> ] [ type standard ]
          radius attribute nas-identifier <identifier>
          radius attribute nas-ip-address address <primary_ipv4/ipv6_address>
 [ backup <secondary_ipv4/ipv6_address> ]
          radius strip-domain [ authentication-only | accounting-only ]
          end
```

Notes:

- *Optional.* If you want to support more than 320 server configurations system-wide, in the Global Configuration Mode, use the following command:

  aaa large-configuration

Important After you configure this 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.

- <*context_name*> must be the system context designated for AAA configuration.
- For information on GGSN-specific additional configurations using RADIUS accounting see the *Creating and Configuring APNs* section of the *GGSN Administration Guide*.
- In this release, the configuration of NAS IP address with IPv6 prefix is currently not supported.
- <*identifier*> must be the name designated to identify the system in the Access Request message(s) it sends to the RADIUS server.
- *Optional.* Multiple RADIUS attribute dictionaries have been created for the system. Each dictionary consists of a set of attributes that can be used in conjunction with the system. As a result, users could take advantage of all of the supported attributes or only a subset. To specify the RADIUS attribute dictionary that you want to implement, in the Context Configuration Mode, use the following command:

  radius dictionary { 3gpp | 3gpp2 | 3gpp2-835 | custom*XX* **| standard | starent | starent-835 | starent-vsa1 | starent-vsa1-835 }**
- *Optional.* Configure the system to support NAI-based authentication in the event that the system cannot authenticate the subscriber using a supported authentication protocol. To enable NAI-construction, in the Context Configuration Mode, use the following command:

  aaa constructed-nai authentication [encrypted] password <*password*>
- *Optional.* If RADIUS is configured for GGSN service, the system can be configured to support NAI-based authentication to use RADIUS shared secret as password. To enable, in the Context Configuration Mode, use the following command:

  aaa constructed-nai authentication use-shared-secret-password

  If authentication type is set to allow-noauth or msid-auth and aaa constructed-nai authentication use-shared-secret-password is issued then the system will use RADIUS shared secret as password. In case the authentication type is msid-auth it will always send RADIUS shared secret as password by default in ACCESS-REQUEST.
- *Optional.* To configure the system to allow a user session even when all authentication servers are unreachable, in the Context Configuration Mode, use the following command. When enabled, the session is allowed without authentication. However, the accounting information is still sent to the RADIUS accounting server, if it is reachable.

  radius allow authentication-down
- *Optional.* To configure the maximum number of times RADIUS authentication requests must be re-transmitted, in the Context Configuration Mode, use the following command:

  radius max-transmissions <*transmissions*>
- *Optional.* If RADIUS is configured for PDSN service, to configure the accounting trigger options for R-P originated calls to generate STOP immediately or to wait for active-stop from old PCF on handoff, in the Context Configuration Mode, use the following command:

radius accounting rp handoff-stop { immediate | wait-active-stop }

For more information on configuring additional accounting trigger options for R-P generated calls for a PDSN service, refer to the **radius accounting rp** command in the *Command Line Interface Reference*.

- *Optional.* To configure the system to check for failed RADIUS AAA servers, in the Context Configuration Mode, use the following command:

  radius detect-dead-server { consecutive-failures <*count*> **| keepalive | response-timeout** <*seconds*> **}**

  After a server's state is changed to "Down", the deadtime timer is started. When the timer expires, the server's state is returned to "Active". If both **consecutive-failures** and **response-timeout** are configured, then both parameters have to be met before a server's state is changed to "Down". For a complete explanation of RADIUS server states, refer to *RADIUS Server State Behavior* appendix.

- *Optional.* To configure the system to check for failed RADIUS accounting servers, in the Context Configuration Mode, use the following command:

  radius accounting detect-dead-server { consecutive-failures <*count*> **| response-timeout** <*seconds*> **}**

  After a server's state is changed to "Down", the deadtime timer is started. When the timer expires, the server's state is returned to "Active". If both **consecutive-failures** and **response-timeout** are configured, then both parameters have to be met before a server's state is changed to "Down". For a complete explanation of RADIUS server states, refer to *RADIUS Server State Behavior*.

- *Optional.* If required, users can configure the dynamic redundancy for HA as described in the *HA Redundancy for Dynamic Home Agent Assignment* chapter of the *Home Agent Administration Guide*.

Verifying your configuration

To verify your configuration:

In the Exec mode, enter the following command:

show configuration context <*context_name*>

In the output, verify the AAA settings that you have configured in this user session.

Configuring Diameter AAA Functionality

This section describes how to configure the Diameter endpoints and system to use the Diameter servers for subscriber authentication and accounting (optional).

To configure Diameter AAA functionality:

Step 1 Configure Diameter endpoint as described in the Configuring Diameter Endpoint, on page 5 section.

Step 2 Configure Diameter context-level AAA parameters as described in the Configuring Diameter AAA Functionality at Context Level, on page 7 section.

Step 3 Configure system-level AAA parameters as described in the Configuring System-Level AAA Functionality, on page 11 section.

Step 4 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Note Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Note In releases prior to 12.0, the configuration of Diameter nodes and host strings like endpoint name, peer name, host name, realm name, and fqdn were case-sensitive. In 12.0 and later releases, all the Diameter related node IDs are considered case insensitive. This change applies to both the local configuration and communication with external nodes.

Configuring Diameter Endpoint

Before configuring the Diameter AAA functionality you must configure the Diameter endpoint.

Use the following configuration example to configure Diameter endpoint:

```
configure
     context <context_name>
          diameter endpoint <endpoint_name>
               origin host <host_name> address <ipv4/ipv6_address> [ port
<port_number> ] [ accept-incoming-connections ] [ address
<ipv4/ipv6_address_secondary> ]
              peer <peer_name> [ realm <realm_name> ] address <ipv4/ipv6_address>
 [ [ port <port_number> ] [ connect-on-application-access ] [
send-dpr-before-disconnect [ disconnect-cause <disconnect_cause> ] ] [ sctp
] ]+
               end
```

Notes:

- *Optional.* To support Diameter proxy server on per-PAC/PSC or per-system basis, in the Global Configuration Mode, use the following command:

  require diameter-proxy { master-slave | multiple | single }

  Important After you configure this 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.

- <*context_name*> must be the name of the system context designated for AAA configuration.
- *Optional.* To enable Diameter proxy for the endpoint, in the Diameter Endpoint Configuration Mode, use the following command:

  use-proxy

- *Optional.* To set the realm for the Diameter endpoint, in the Diameter Endpoint Configuration Mode, use the following command:

  origin realm <*realm_name*>

- <*realm_name*> is typically a company or service name. The realm is the Diameter identity and will be present in all Diameter messages.

- *Optional.* To create an entry in the route table for the Diameter peer, in the Diameter Endpoint Configuration Mode, use the following command:

  route-entry { [host <*host_name*> **] [peer** <*peer_id*> **] [realm** <*realm_name*> **] } [application credit-control] [weight** <*value*> **]**

- *Optional.* To specify the port for the Diameter endpoint, in the Diameter Endpoint Configuration Mode, use the following command:

  origin host *host_name* **address** *ipv4/ipv6_address* **[port** *port_number* **] [accept-incoming-connections] [address** *ipv4/ipv6_address_secondary* **]**

  Port number in the origin host should be configured only when the chassis is running in server mode, i.e. when **accept-incoming-connections** is configured.

  In this case it will open a listening socket on the specified port. For configurations where chassis is operating as a client, port number should not be included. In this case, a random source port will be chosen for outgoing connections. This is applicable for both with or without multi-homing.

  Note Currently if multi-homing is configured, then the specified port is used instead of randomly chosen port. This is done so that application knows which port is used by the kernel as it will have to use the same port while adding/removing IP address from the association. Nevertheless, configuring port number in origin host for client mode is not supported.

- *Optional.* To set how the action after failure, or recovery after failure is performed for the route table, in the Diameter Endpoint Configuration Mode, use the following command:

  route-failure { deadtime <*seconds*> **| recovery-threshold percent** <*percent*> **| result-code** <*result_code*> **| threshold** <*counter*> **}**

- *Optional.* To enable/disable the Transport Layer Security (TLS) support between Diameter client and Diameter server node, in the Diameter Endpoint Configuration Mode, use the following command:

  tls { certificate <*cert_string*> **| password** <*password*> **| privatekey** <*private_key*> **}**

- *Optional.* To set the connection timeout, in seconds, in the Diameter Endpoint Configuration Mode, use the following command:

  connection timeout <*timeout*>

- *Optional.* To set the connection retry timeout, in seconds, in the Diameter Endpoint Configuration Mode, use the following command:

  connection retry-timeout <*retry_timeout*>

- *Optional.* To set the number of Device Watchdog Requests (DWRs) to be sent before the connection with a Diameter endpoint is closed, in the Diameter Endpoint Configuration Mode, use the following command:

  device-watchdog-request max-retries <*retry_count*>

- *Optional.* To set the maximum number of Diameter messages that any ACS Manager (ACSMgr)/Session Manager (SessMgr) may send to any one peer awaiting responses, in the Context Configuration Mode, use the following command:

  max-outstanding <*msgs*>

- *Optional.* To set the response timeout for the Diameter endpoint, in seconds, in the Diameter Endpoint Configuration Mode, use the following command:

  response-timeout <*duration*>

- *Optional.* To set the watchdog timeout for the Diameter endpoint, in seconds, in the Diameter Endpoint Configuration Mode, use the following command:

  watchdog-timeout <*duration*>

Configuring Diameter AAA Functionality at Context Level

There are context-level Diameter parameters that must be configured to provide AAA functionality for subscriber sessions. As noted in *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*, AAA functionality can be configured within any context, even its own.

This section describes how to configure the Diameter-based AAA parameters at the context level. To configure Diameter-based AAA parameters at the system level, see the Configuring System-Level AAA Functionality, on page 11 section.

Note This section provides the minimum instruction set to configure context-level Diameter AAA functionality that allows the system to process data sessions. Commands that configure additional context-level AAA properties are provided in *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.

To configure Diameter AAA functionality at the context level use the following configuration:

```
configure
    context <context_name>
        diameter authentication endpoint <endpoint_name>
        diameter authentication server <host_name> priority <priority>
        diameter authentication dictionary <dictionary>
        diameter accounting endpoint <endpoint_name>
        diameter accounting server <host_name> priority <priority>
        diameter accounting dictionary <dictionary>
        end
```

Notes:

- <*context_name*> must be the name of the system context designated for AAA configuration.

- <*endpoint_name*> must be the same Diameter endpoint name configured in the Configuring Diameter Endpoint, on page 5 section.
- *Optional.* To configure the number of retry attempts for a Diameter authentication request with the same server, if the server fails to respond to a request, in the Context Configuration Mode, use the following command:

  diameter authentication max-retries <*tries*>
- *Optional.* To configure the maximum number of transmission attempts for a Diameter authentication request, in the Context Configuration Mode, use the following command. Use this in conjunction with the **max-retries** <*tries*> option to control how many servers will be attempted to communicate with.

  diameter authentication max-transmissions <*transmissions*>
- *Optional.* To configure how long the system must wait for a response from a Diameter server before re-transmitting the authentication request, in the Context Configuration Mode, use the following command:

  diameter authentication request-timeout <*duration*>
- *Optional.* To configure how many times a Diameter accounting request must be retried with the same server, if the server fails to respond to a request, in the Context Configuration Mode, use the following command:

  diameter accounting max-retries <*tries*>
- *Optional.* To configure the maximum number of transmission attempts for a Diameter accounting request, in the Context Configuration Mode, use the following command. You can use this in conjunction with the **max-retries tries** option to control how many servers will be attempted to communicate with.

  diameter accounting max-transmissions <*transmissions*>
- *Optional.* To configure how long the system will wait for a response from a Diameter server before re-transmitting the accounting request, in the Context Configuration Mode, use the following command:

  diameter accounting request-timeout <*duration*>

Verifying Your Configuration

To verify your configurations:

In the Exec mode, enter the following command:

show configuration context <*aaa_context_name*>

The output displays a concise list of settings that you have configured for the context.

Configuring Diameter Authentication Failure Handling

This section describes how to configure Diameter Authentication Failure Handling at the context level and the AAA group level.

Configuring at Context Level

This section describes how to configure context-level error handling for EAP requests / EAP termination 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.

To configure Diameter Authentication Failure Handling at the context level use the following configuration:

```
configure
     context <context_name>
         diameter authentication failure-handling { authorization-request
 | eap-request | eap-termination-request } { request-timeout action {
continue | retry-and-terminate | terminate } | result-code <result_code> {
[ to <result_code> ] action { continue | retry-and-terminate | terminate }
} }
           end
```

Notes:

- <*context_name*> must be the name of the system source context designated for subscriber configuration.

Configuring at AAA Group Level

This section describes how to configure error handling for EAP requests / EAP termination requests at the AAA group level. 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.

To configure Diameter Authentication Failure Handling at the AAA group level use the following configuration example:

```
configure
     context <context_name>
          aaa group <group_name>
               diameter authentication failure-handling {
authorization-request | eap-request | eap-termination-request } {
request-timeout action { continue | retry-and-terminate | terminate } |
result-code <result_code> { [ to <result_code> ] action { continue |
retry-and-terminate | terminate } } }
               end
```

Notes:

- <*context_name*> must be the name of the system source context designated for subscriber configuration.
- <*group_name*> must be the name of the AAA group designated for AAA functionality within the specific context.

Configuring Diameter Failure Handling Template

This section describes how to configure Diameter Failure Handling Template at the global 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 template can be used by any Diameter application that needs failure handling behavior.

To configure Diameter Failure Handling at the global level use the following configuration:

```
configure
     failure-handling <template_name>
          msg-type { any | authentication info request |
authorization-request | check-identity-request | credit-control-initial
| credit-control-terminate | credit-control-update | eap-request |
eap-termination-request | notify-request | profile-update-request |
purge-ue-request | update-location-request | user-data-request }
failure-type { any | diabase-error | diameter result-code { any-error |
result-code [ to end-result-code ] } | diameter exp-result-code { any-error |
result-code [ to end-result-code ] } | resp-timeout | tx-expiry } action {
continue [ local-fallback | send-ccrt-on-call-termination | without-retry
 ] | retry-and-terminate | terminate }
          end
```

Notes:

- A maximum of 64 templates can be configured on the system.
- Diameter applications (Gx, Gy) 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.
- For information on the commands, refer to the *Diameter Failure Handling Template Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Configuring Dynamic Diameter Dictionary

This section describes how to configure Dynamic Diameter dictionary at the global level.

The Diameter dictionaries can be configured dynamically at run time.

To configure Dynamic Diameter dictionary at the global level use the following configuration:

```
configure
     diameter dynamic-dictionary <dict_name> <url>
     end
```

Notes:

- A maximum of 10 dynamic dictionaries can be configured and loaded in to the system.
- The dynamically loaded dictionaries can be configured under application group or AAA group using the option **dynamic-load** in the **diameter accounting dictionary** or **diameter authentication dictionary** command.
- For more information on the command, refer to the *Global Configuration Mode (A-K) Commands* chapter of the *Command Line Interface Reference*.

Verifying Your Configuration

To verify your configurations:

In the Exec mode, enter the following command:

show diameter dynamic-dictionary all [contents]

The output displays a concise list of settings that you have configured.

Configuring Rate Limiting Function Template

This section describes how to configure Rate LimitingFunction (RLF) Template at the global level.

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.

The RLF template defines the rate limiting configurations for example, a threshold for rate-limiting the outgoing messages. The template can be used by any product/interface that needs to throttle and rate control the messages sent to the external network interfaces.

To configure RLF template at the global level use the following configuration:

```
configure
      rlf-template <template_name>
            delay-tolerance tolerance_value [ -noconfirm ]
            msg-rate tps_value burst-size size [ -noconfirm ]
            threshold { lower lowerThreshold_value | upper
upperThreshold_value } [ -noconfirm ]
            end
```

For information on the commands, refer to the *Rate Limiting Function Template Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Verifying Your Configuration

To verify your configurations:

In the Exec mode, enter the following command:

show rlf-template all

The output displays a concise list of settings that you have configured.

Configuring System-Level AAA Functionality

There are system-level AAA parameters that must be configured in order to provide AAA functionality for subscriber and context-level administrative user sessions. As noted in *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*, AAA functionality can be configured within any context, even its own.

Note Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

This procedure applies to both RADIUS and Diameter.

To configure system-level AAA functionality use the following configuration:

```
configure
     aaa default-domain subscriber <domain_name>
     aaa default-domain administrator <domain_name>
     aaa last-resort context subscriber <context_name>
     aaa last-resort context administrator <context_name>
     aaa username-format { domain | username } { @ | % | - | \ | # | / }
     end
```

Notes:

- <*domain_name*> is the name of the domain, or context, to use for performing AAA functions in the subscriber session. For information on the role of the default domain in the context selection process can be found in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
- <*context_name*> must be the name of the context to use for performing AAA functions in the subscriber session. Additional information on the role of the last-resort context in the context selection process can be found in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
- Up to six user name formats can be configured. The default format is username@domain.

Verifying your configuration

To verify your configuration:

In the Exec mode, enter the following command:

show configuration context <*context_name*>

In the output, verify the AAA settings that you have configured in this user session.

Configuring AAA Server Group for AAA Functionality

In addition to the AAA configurations, a AAA server group feature can be configured at the context-level to manage subscriber authentication and accounting through configuring AAA servers into groups.

In general, 128 AAA Server IP address/port per context can be configured on the system and the system selects servers from this list depending on the server selection algorithm (round robin, first server). Instead of having a single list of servers per context, this feature provides the ability to configure multiple server groups. Each server group, in turn, consists of a list of servers.

This feature works in the following way:

- All authentication/accounting servers configured at the context-level are treated as part of a server group named "default". This default server group is available to all subscribers in that context through the realm (domain)/APN without any additional configuration.
- It provides a facility to create "user defined" AAA server groups, as many as 799 (excluding "default" server group), within a context. Any of the user-defined AAA server groups are available for assignment to a subscriber through the realm (domain)/APN configuration within that context.

- Subscribers/services/APNs/etc. are bound to a AAA group, which serves to define what Diameter/RADIUS server will be used for each AAA function (authentication, accounting, charging, and so on). Based on the request type the RADIUS or Diameter protocol type is selected to handle the AAA requests to be sent to the respective server.

AAA server group configuration is performed at the context-level. Different subscribers may use the same AAA context, but different AAA server groups only. Server configuration defined in the subscriber profile/APN template supersedes the servers or server groups configuration defined in context mode.

AAA server groups are assigned to the subscriber through realm (domain) configuration for all services. For GGSN service AAA server groups can be assigned to the subscriber through APN configuration also.

To configure AAA Server Group for AAA functionality:

Step 1 Configure the AAA Server Group as described in the AAA Server Group Configuration, on page 13 section.

- Apply the AAA Server Group to subscriber as described in the Applying a AAA Server Group to a Subscriber, on page 15 section.

  –or–

- Apply the AAA server-group to an APN as described in the Applying a AAA Server Group to an APN, on page 16 section.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Note Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

AAA Server Group Configuration

This section describes how to configure the context to use a group of AAA servers for subscriber authentication and accounting through subscriber/realm (domain)/APN configuration.

There are context-level AAA parameters that must be configured in order to provide AAA server group functionality for subscriber sessions.

Note This section provides the minimum instruction set for configuring a AAA server group for AAA functionality. Commands that configure other properties of this functionality are provided in the *Command Line Interface Reference*.

To configure a AAA server group use the following configuration:

```
configure
     context <context_name>
```

```
aaa group <group_name>
end
```

Notes:

- Up to 128 authentication and/or accounting servers can be configured per AAA server group. A maximum of 1600 servers can be configured system-wide regardless of the number of groups unless **aaa large-configuration** is enabled.

Important After you configure the **aaa large-configuration** 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.

- *Optional.* If you want to support more than 64 server groups system-wide, in the Global Configuration Mode, use the following command:

  aaa large-configuration

Important After you configure the **aaa large-configuration** 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.

- <*context_name*> must be the name of the system context designated for AAA functionality configuration.
- <*group_name*> must be the name of the AAA group designated for AAA functionality within the specific context. A total of 800 server groups can be configured system-wide including default server-group unless **aaa large-configuration** is enabled.

Important After you configure the **aaa large-configuration** 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.

- The same AAA server with IP address and port number can be configured with multiple AAA server groups within a context.
- To configure and verify RADIUS authentication and accounting servers and parameters within the AAA server group, refer to the Configuring RADIUS AAA Functionality, on page 1 section.
- To configure and verify Diameter authentication and accounting servers and parameters within the AAA server group, refer to the Configuring Diameter AAA Functionality, on page 4 section.

Verifying Your Configuration

To verify your configuration:

Step 1 Change to the context in which the AAA server group was configured by entering the following command:
context <*context_name*>

Step 2 Display the context's configuration by entering the following command:
show configuration context <*context_name*>

Step 3 In the output verify the server group's configuration.

Note The "default" server group in a context is applicable to all subscribers/APNs within that context by default.

Applying a AAA Server Group to a Subscriber

The following procedure assumes that a domain alias was previously configured as described in *Creating Contexts* section of the *System Administration Guide*.

To apply AAA server group to a subscriber use the following configuration example:

```
configure
     context <context_name>
          subscriber name <subscriber_name>
               aaa group <group_name>
               end
```

Notes:

- <*context_name*> must be the name of the system source context designated for subscriber configuration.
- <*sub_name*> must be the name of the subscriber template configured as the default template for the domain. For more information on creating contexts, refer to the *Creating Contexts* section of the *System Element Configuration Procedures* chapter in the *System Administration Guide*.
- <*group_name*> must be the name of the AAA server group designated for AAA functionality within the context as described in the AAA Server Group Configuration, on page 13 section.

Verifying Subscriber Configuration

Step 1 Change to the context in which the AAA server group was configured by entering the following command:
context <*context_name*>

Step 2 Display the subscriber's configuration by entering the following command:
show subscribers configuration username <*subscriber_name*>

Step 3 In the output verify the subscriber's configuration.

Applying a AAA Server Group to an APN

After configuring a AAA server group at context-level, an APN within the same context can be configured to use the user-defined server group.

Use the following configuration example to apply a user-defined AAA server group functionality to a previously configured APN within the same context.

```
configure
    context <context_name>
          apn <apn_name>
               aaa group <group_name>
               end
```

Notes:

- <*group_name*> must be the name of the AAA server group previously configured for AAA functionality in a specific context as described in the AAA Server Group Configuration, on page 13 section.

Verifying APN Configuration

Step 1 Change to the context in which the AAA server group was configured by entering the following command:
context <*context_name*>

Step 2 Display the APN's configuration by entering the following command:
show apn name <*apn_name*>

Step 3 In the output verify the APN's configuration.

Configuring the Destination Context Attribute

Once a user has been authenticated, a AAA attribute is returned in the access-accept message that contains the name of the destination context where the subscriber will egress from. For RADIUS-based subscribers, this is the SN-VPN-NAME attribute, or SN1-VPN-NAME attribute in some RADIUS dictionaries.

Note that when performing RADIUS authentication and authorization, RADIUS attributes returned by the RADIUS server always take precedence over the default subscriber configuration.

Note Note that when RADIUS servers are not configured in the selected AAA group, the servers in the default group will be considered for destination context selection. If there are no servers in the default group, then the call will be dropped.

The system supports configuring subscriber profiles locally within a context though subscriber templates or on a RADIUS server. Subscribers configured on the system are configured within the contexts they were created. In the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*, the role of subscriber default, which is automatically configured for each context, and realm-based subscriber templates, which serves as a default subscriber template for users whose domain portion of their

user name matches a domain alias within a context, was discussed. The role of these special subscriber templates is to provide a set of default attributes that may be used to populate any missing values for an authenticated RADIUS-based subscriber. The parameter that would contain this attribute value is called the IP context-name.

Further, it was explained that these attributes must be configured manually for both the subscriber default and any realm-based subscriber template created.

One of the rules that must be configured is a parameter that allows subscriber data traffic to be routed between source and destination contexts. Use the following example configuration to configure that rule.

Note Commands used in the configuration example in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

```
configure
     context <context_name>
          subscriber name default
               ip context-name <destination_context_name>
               end
```

Notes:

- <*context_name*> must be the name of the system source context designated for Default subscriber configuration.
- <*destination_context_name*> must be the name of the destination context configured on the system containing the interfaces through which session traffic is routed.
- The "ip context-name" parameter in the subscriber profiles configured on the system corresponds to the SN-VPN-NAME and SN1-VPN-NAME RADIUS attributes.
- Configure the default subscriber in any other configured source contexts.

Verifying Your Configuration

To verify your global AAA configurations:

In the Exec mode, use the following command:

show configuration

The output displays all the settings that you have configured in this user session. Verify the default-domain, last-resort, and username-format settings.