Managing and Monitoring the AAA Servers

This chapter provides information for managing and monitoring the AAA server status and performance using the commands found in the Command Line Interface (CLI). These command have many related keywords that allow them to provide useful information on all aspects of the AAA interface activity and status.

The selection of keywords described in this chapter is intended to provided the most useful and in-depth information for monitoring AAA managers, interface, and servers on the system. For additional information on these command keywords, refer to the *Command Line Interface Reference*.

In addition to the CLI, the system supports the sending of Simple Network Management Protocol (SNMP) traps that indicate status and alarm conditions. Refer to the *SNMP MIB Reference* for a detailed listing of these traps.

This chapter includes the following sections:

Managing the AAA Servers

This section provides information and instructions for using the system Command Line Interface (CLI) for troubleshooting the network reachability issues for AAA servers that may arise during system operation.

The following topics are discussed in this section:

Using the RADIUS Testing Tools

The CLI provides a mechanism for testing network connectivity with and configuration of RADIUS authentication and accounting servers. This functionality can be extremely useful in determining the accuracy of the system's RADIUS configuration, the configuration of the subscriber profile on the RADIUS server, and troubleshooting the server's response time.

Testing a RADIUS Authentication Server

When used to test a RADIUS authentication server, the tool generates an authentication request message for a specific user name.

Note The user name must already be configured on the RADIUS authentication server prior to executing the test.

To execute the RADIUS authentication test tool, in the Exec mode, use the following command:

radius test authentication { all | radius group *<group_name>* **| server** *<server_name>* **port** *<server_port>* **}** *<user_name> <password>*

Notes:

- **all** specifies that all configured RADIUS authentication servers be tested.
- **radius group** *<group_name>* specifies the configured RADIUS authentication servers in a RADIUS server group named *<group_name>* for server group functionality.
- *<server_name>* specifies the IP address of a specific RADIUS authentication server to test.
- *<server_port>* specifies the TCP port over that the system should use when communicating with the RADIUS authentication server to test.
- *<user_name>* specifies a username that is supplied to the RADIUS server for authentication.
- *<password>* specifies the password associated with the username that is supplied to the RADIUS server for authentication.

The following is a sample of this command's output for a successful response when testing a RADIUS authentication server with an IP address of 192.168.250.150 on port 1812.

```
Authentication from authentication server 192.168.250.150, port 1812
Authentication Success: Access-Accept received
Round-trip time for response was 8.8 ms
```

Testing a RADIUS Accounting Server

When used to test a RADIUS accounting server, the tool generates an accounting start/stop pair for a specific username.

Note The user name must already be configured on the RADIUS authentication server prior to executing the test.

To execute the RADIUS authentication test tool, enter the following command:

radius test accounting { all | radius group *<group_name>* **| server** *<server_name>* **port** *<server_port>* **}** *<user_name>*

Notes:

- **all** specifies that all configured RADIUS accounting servers be tested.
- **radius group** *<group_name>* specifies the configured RADIUS authentication servers in a RADIUS server group named *<group_name>* for server group functionality.
- *<server_name>* specifies the IP address of a specific RADIUS accounting server to test.
- *<server_port>* specifies the TCP port over that the system should use when communicating with the RADIUS accounting server to test.

- *<user_name>* specifies a username that is supplied to the RADIUS server for accounting.

The following is a sample of this command's output for a successful response when testing a RADIUS accounting server with an IP address of 192.168.1.102 on port 1813.

```
RADIUS Start to accounting server 192.168.1.102, port 1813
Accounting Success: response received
Round-trip time for response was 554.6 ms

RADIUS Stop to accounting server 192.168.1.102, port 1813
Accounting Success: response received
Round-trip time for response was 85.5 ms
```

Monitoring AAA Status and Performance

This section describes the commands used to monitor the status of AAA servers in the service. Output descriptions for most of the commands are available in the *Statistics and Counters Reference*.

To do this:	Enter this command:
View AAA Manager statistics	**show session subsystem facility aaamgr all**
View AAA and RADIUS Counters	
Display Local AAA Counters	
View Local AAA counters for the current context	**show aaa local counters**
Display RADIUS Server States **Note** These commands can display 10 state transition histories of RADIUS accounting and authentication servers (Active/Not responding/Down States). For explanation of RADIUS server states, refer to the *RADIUS Server State Behavior* Appendix.	
View RADIUS accounting server states	**show radius accounting servers detail**
View RADIUS authentication server states	**show radius authentication servers detail**
Display RADIUS Server Group Server States **Note** RADIUS Server Group functionality is a license controlled feature. A valid feature license must be installed prior to configuring RADIUS group for AAA functionality. If you have not previously purchased this enhanced feature, contact your sales representative for more information. For explanation of RADIUS server states, refer to the *RADIUS Server State Behavior* Appendix.	
View RADIUS authentication server group server states for a specific group	**show radius authentication servers radius group** *<group_name>* **detail**
View RADIUS accounting server group server states for a specific group	**show radius accounting servers radius group** *<group_name>* **detail**
Display RADIUS Protocol Counters	
View cumulative RADIUS protocol counters	**show radius counters all**

To do this:	Enter this command:
View RADIUS protocol counter summary of RADIUS authentication and accounting	**show radius counters summary**

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping (PPP, MIPHA, MIPFA, etc.).

Statistics and counters can be cleared using the CLI **clear** commands. For detailed information on using this command, refer to the *Command Line Interface Reference*.

Session Recovery and AAA Statistics Behavior

After a Session Recovery operation, some statistics/counters, such as those collected and maintained on a per manager basis (AAA Manager, Session Manager, etc.) are in general not recovered, only accounting/billing related information is checkpointed/recovered.

For more information, refer to the *System Administration Guide*.