Monitoring AAA Configurations

AAA refers to Authentication, Authorization, and Accounting, which is a security architecture for distributed systems that determines the access given to users for specific services and the amount of resources they have used.

- Authentication—This method identifies users, including their login and password, challenge and response, messaging support, and encryption. Authentication is the way to identify a subscriber before providing access to the network and network services.

- Authorization—This method provides 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—This method collects and sends subscriber usage and access information used for billing, auditing, and reporting. For example, user identities, start and stop times, performed actions, number of packets, and number of bytes. Accounting enables an operator to analyze the services that the users access as well as the amount of network resources they consume. Accounting records comprise accounting Attribute Value Pairs (AVPs) and are stored on the accounting server. This accounting information can then be analyzed for network management, client billing, and/or auditing.

This chapter contains the following topics:

Supported Network Protocols

AAA supports the following protocols:

- Diameter—This is a networking protocol that provides centralized AAA management for devices to connect and use a network service, and an alternative to RADIUS. Diameter Applications can extend the base protocol, by adding new commands and/or attributes.

- Remote Authentication Dial In User Service (RADIUS)—This is a networking protocol that provides centralized AAA management for devices to connect and use a network service. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote Access Server (RAS), the Virtual Private Network (VPN) server, the network switch with port-based authentication, and the Network Access Server (NAS), are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server.

Viewing AAA Configurations in Prime Network Vision

Prime Network allows you to view the AAA configurations for Cisco ASR9000 and Cisco ASR5000 series network elements.

This topic contains the following sections:

Viewing AAA Group Profile

To view the AAA group profile:

Step 1   Right-click on the required device and choose the **Inventory** option.

Step 2   In the Inventory window, choose **Logical Inventory > AAA**. The AAA attribute details are displayed in the content pane.

> **Note**   These attributes are available only for Cisco ASR 9000 series network elements.

Table 23-1 describes the fields that are displayed in the content pane.

Table 23-1   AAA Attributes

Field Name	Description
Type	Customization applied to the attribute.
Key	Unique format name applied to the attribute.
Value	Formatting applied to the attribute.

Step 3   In the Inventory window, choose **AAA group** node under the AAA node.

Step 4   Under the **AAA group** node, select and expand the required group and choose the **Radius Configuration** option. The group details are displayed in the content pane.

Table 23-2 describes the fields that are displayed in the Radius Configuration dialog box.

Table 23-2   Radius Configuration Details

Field Name	Description
Load Balancing Method	The load balancing method.
Ignore Preferred Server	Indicates if a transaction associated with a single AAA session should attempt to use the same server or not.
VRF	Virtual routing and forwarding (VRF) associated with the AAA group. Click the hyperlink to view the relevant node under the VRF node in the logical inventory.
Dead Time	The deadtime for the profile.

Viewing Dynamic Authorization Profile

To view the dynamic authorization profile:

Step 1   Right-click on the required device and choose the **Inventory** option.

Step 2   In the Inventory window, choose **Logical Inventory** > **AAA** > **Dynamic Authorization**. The authorization details are displayed in the content pane. You can click on the tabs to view more details.

> **Note**   These attributes are available only for Cisco ASR 9000 series network elements.

Table 23-3 describes the fields that are displayed in the Dynamic authorization content pane.

Table 23-3   Dynamic Authorization Details

Field Name	Description
Protocol	The name of the protocol.
Server Listen Port	The port number that receives service requests.
Ignore Server Key	Indicates whether the server key must be ignored. Values are: • true • false
CoA Clients Tab	
IP Address	The IP address of the Change of Authorization (CoA) client.
VRF	The associated VRF to which the CoA client belongs. Click the hyperlink to view the relevant node under the VRF node.

Viewing Radius Global Configuration Details

To view the radius global configuration details:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory** > **AAA** > **Radius Global Configuration**. The authorization details are displayed in the content pane.

> **Note** These attributes are available only for Cisco ASR 9000 series network elements.

Table 23-4 describes the fields that are displayed in the Radius global configuration content pane.

Table 23-4   Radius Global Configuration Details

| Field Name	Description
Load Balancing Method	The load balancing method using which the next host is selected. The server with the least transactions outstanding is generally picked as the next host.
Ignored Preferred Server	Indicates if a transaction associated with a single AAA session should attempt to use the same server or not.
Request Timeout	The request timeout value for the device.
Dead Time	The amount of time (in minutes) after which the dead RADIUS server will be treated as active.
Retransmit	Indicates whether retransmission of data is allowed.
Retransmit Count	The retransmission count.
Dead Criteria Time	The time interval after which the device is considered unavailable.
Dead Criteria Retransmit Count	The retransmission count after the dead criteria time.
Accounting Servers/ Authentication Servers	
Server IP	The IP address of the server.
Server Port	The server port.
Preference	The preferred server.
Operational State	The current operational state of the interface.
Administrative Status	The administrative status of the interface.
Retain Administrative Status After Reboot	Indicates whether the administrative status must be retained after the system reboots.
Keepalive Representative Group	The keepalive representative group.
Request Timeout	The request timeout value for the device.
Retransmit Count	The retransmission count.

Viewing AAA Configuration Details for an AAA group

For a Cisco ASR5000 device, Prime Network Vision allows you to view the following configurations for an AAA group:

- Diameter Configuration
  - Accounting Configuration
  - Authentication Configuration

- Radius Configuration
  - Accounting Configuration
  - Accounting Keepalive and Detect Dead Server Configuration
  - Authentication Configuration
  - Authentication Keepalive and Detect Dead Server Configuration
  - Charging Configuration
  - Charging Triggers

Prime Network Vision displays the AAA configuration details under the AAA container as shown in Figure 23-1. You can view the individual AAA group details by choosing **Logical Inventory** > *Context* > **AAA** > **AAA Groups**.

Figure 23-1   AAA Groups in Logical Inventory
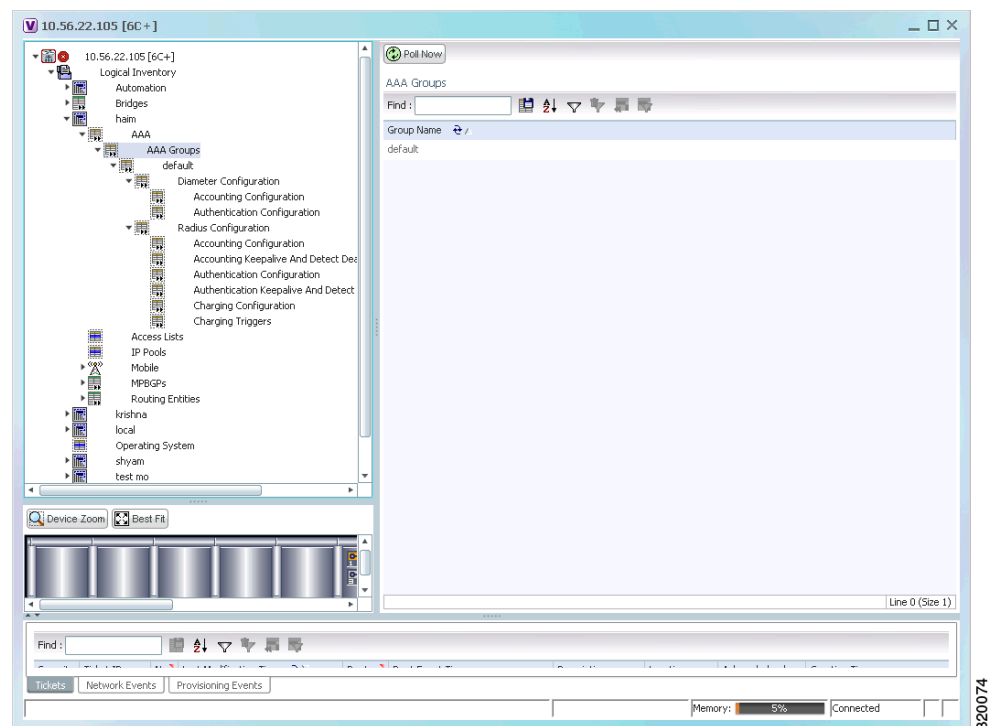
Viewing Diameter Configuration Details for an AAA group

To view the diameter configuration details for a AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Groups**.

You can view the AAA groups on the content pane.

Step 3 Choose **Diameter Configuration** under a specific AAA group node. The diameter configurations made for accounting servers and authentication servers are displayed in the respective tabs on the content pane. Click on the tabs to view more details.

Table 23-5 describes the diameter configuration details for accounting and authentication servers.

Table 23-5   Diameter Configuration

Field Name	Description
Accounting Servers/Authentication Servers	
Server Host	Host name of the diameter authentication/accounting server.
Priority	Relative priority of the diameter authentication/accounting server.
Number of Instances in Up State	Number of instances between the diameter authentication/accounting server and the AAA manager that are in UP status.
Number of Instances in Down State	Number of instances between the diameter authentication/accounting server and the AAA manager that are in DOWN status.

Step 4 In the Inventory window, choose **Accounting Configuration** or **Authentication Configuration** under the **Diameter Configuration** node. The configuration details are displayed on the content pane.

Table 23-6 describes the accounting/authentication diameter configuration details.

Table 23-6   Accounting/Authentication Diameter Configuration

Field Name	Description
Dictionary	Diameter dictionary used for accounting/authentication.
Endpoint Name	Diameter endpoint used for accounting/authentication.
Maximum Transmissions	Maximum number of transmission attempts for diameter accounting/authentication.
Maximum Retries	Number of retry attempts for diameter accounting/authentication requests.
Request Timeout	Diameter accounting/authentication request timeout period.
Redirect Host AVP	Indicates whether to use: • one returned AVP • the first returned AVP as the primary host and the second returned AVP as the secondary host. This field is applicable only for Authentication configuration.

Viewing Radius Configuration Details for an AAA Group

To view the radius configuration details for an AAA group:

Step 1   Right-click on the required device and choose the **Inventory** option.

Step 2   In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration**. The configurations made for accounting, authentication, charging, and charging accounting servers are displayed in the respective tabs on the content pane. Click on the tabs to view more details.

Table 23-7 describes the radius configuration details for accounting, authentication, charging, and charging accounting servers.

Table 23-7   Radius Configuration

Field Name	Description
Dictionary	The radius dictionary.
Strip Domain	Indicates whether the domain must be stripped from the user name prior to authentication or accounting.
Authenticator Validation	Indicates whether the MD5 authentication of the user is enabled or disabled.
Allow Server Down Authentication	Indicates whether subscriber sessions are allowed when RADIUS authentication is unavailable.
Allow Server Down Accounting	Indicates whether subscriber sessions are allowed when RADIUS accounting is unavailable.
Accounting Servers/Authentication Servers/Charging Servers/Charging Accounting Servers	
Server Name	IP address of the RADIUS server.
Server Port	Port used to communicate with the RADIUS server.
Preference	Preference of the RADIUS server.
Operational State	Status of the RADIUS server.
Administrative Status	Administrative status of the RADIUS server.
Retain Administrative Status after Reboot	Indicates whether the administrative status must be retained when the system reboots.
Keepalive Representative Group	Name of the Keepalive representative group.

Viewing Radius Accounting Configuration Details for an AAA group

To view the radius accounting configuration details for an AAA group:

Step 1   Right-click on the required device and choose the **Inventory** option.

Step 2   In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Accounting Configuration**. The accounting configuration details are displayed in the content pane.

Table 23-8 describes the radius accounting configuration details.

Table 23-8   Radius Accounting Configuration

Field Name	Description
Server Selection Algorithm	The algorithm to select the RADIUS accounting server(s) to which accounting data must be sent. Values are: • first-n n Default • first-server • round-robin
Billing Version	The billing system version of RADIUS accounting servers.
Server Deadtime	The number of minutes after which communication must be attempted with a server that is not reachable.
Maximum Outstanding Messages	The maximum number of outstanding messages that can be queued with the AAA manager.
Fire and Forget	Indicates whether RADIUS Fire-and-Forget accounting is enabled for the AAA group.
Maximum Transmissions	The maximum number of transmissions attempted for a RADIUS accounting message, before it is declared FAILED.
Maximum Retries	The maximum number of attempts with the AAA server, before it is declared Not Responding and the detect dead server's consecutive failures count is incremented.
Maximum PDU Size (Bytes)	The maximum packed data unit size, in bytes, that can be accepted or generated.
Response Timeout	The time period, in seconds, to wait for a response from the RADIUS server, before resending the message.
Remote Address	Indicates whether the remote IP address lists are configured and the collection of accounting data for the addresses in these lists are enabled.
Archive Messages	Indicates whether archiving of the RADIUS accounting messages in the system (after retries to all available RADIUS accounting servers) is enabled.
APN To Be Included	The Access Point Name (APN) associated with the RADIUS accounting.
Interim Interval	The time interval (in seconds) between sending interim accounting records.
GTP Trigger Policy	The downlink volume that triggers interim RADIUS accounting.

Viewing the Radius Keepalive and Detect Dead Server Configuration Details for an AAA group

To view the radius accounting/authentication Keepalive and Detect Dead Server Configuration details:

Step 1   Right-click on the required device and choose the **Inventory** option.

Step 2   In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Accounting Keepalive and Detect Dead Server Configuration** or **Authentication Keepalive and Detect Dead Server Configuration**. The configuration details are displayed in the content pane.

Table 23-9 describes the radius accounting keepalive and detect dead server configuration details.

Table 23-9   Radius Accounting Keepalive and Detect Dead Server Configuration details

Field Name	Description
Keepalive Interval	The time interval (in seconds) between two keepalive access requests.
Keepalive Timeout	The time period to wait for a response from the RADIUS server, before resending the message. This value is displayed in seconds.
KeepAlive Maximum Retries	The maximum number of keepalive access requests to be sent, before the server is declared as not reachable.
Keepalive Consecutive Response	The number of consecutive accounting responses after which the server is declared as reachable.
Username	The accounting user name.
Calling Station ID	The calling station ID to be used for keepalive accounting.
Keepalive Password	The password to be used for authentication. This field is available only for authentication configuration.
Keepalive Allow Access Reject	Indicates the valid response for authentication request. This field is available only for authentication configuration.
Detect Dead Server Consecutive Failures	The number of consecutive failures for an AAA manager, before the status of an accounting server is changed from Active to Down.
Detect Dead Server KeepAlive	The number of seconds to wait for a response to any message, before the status of an accounting server is changed from Active to Down.

Viewing the Radius Authentication Configuration Details for an AAA group

To view the radius authentication configuration details for an AAA group:

Step 1   Right-click on the required device and choose the **Inventory** option.

Step 2   In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Authentication Configuration**. The authentication configuration details are displayed in the content pane.

Table 23-10 describes the radius authentication configuration details.

Table 23-10   Radius Authentication Configuration

Field Name	Description
Server Selection Algorithm	The algorithm to select the RADIUS accounting server(s) to which accounting data must be sent. Values are: • first-server • round-robin
Server Deadtime	The time period after which the status of the authentication server must be changed from Down to Active.
Maximum Outstanding Messages	The maximum number of outstanding messages that can be queued with the AAA manager.
Authentication Maximum Retries	The maximum number of attempts with the AAA server, before it is declared Not Responding and the detect dead server's consecutive failures count is incremented.
Authentication Maximum Transmissions	The maximum number of transmissions attempted for a RADIUS authentication message, before it is declared FAILED.
Authentication Response Timeout	The time period to wait for a response from the RADIUS server, before resending the message. This value is displayed in seconds.
APN To Be Included	The APN associated with the RADIUS authentication.
Authenticate Null User Name	Indicates whether the authentication of user names that are blank or empty is enabled.
Modify NAS IP	Indicates whether the RADIUS authentication is attempted after NAS IP is modified.
Probe Interval	The time interval (in seconds) before sending another probe authentication request to a RADIUS server.
Probe Timeout	The time period (in seconds) to wait for a response from a RADIUS server before resending the authentication probe.
Probe Maximum Retries	The number of retries for RADIUS authentication probe response before the authentication is declared as failed.

Viewing the Charging Configuration Details for an AAA group

To view the radius charging configuration details for an AAA group:

Step 1 Right-click on the required device and choose the **Inventory** option.

Step 2 In the Inventory window, choose **Logical Inventory** > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Charging Configuration**. The charging configuration details are displayed in the content pane.

Table 23-11 describes the charging configuration details.

Table 23-11   Radius Charging Configuration

Field Name	Description
Authentication Server Selection Algorithm	The algorithm to select the RADIUS server(s) for active charging service to ensure proper load distribution amongst the available servers used for authentication requests. Value could be one of the following: • first-server • round-robin
Accounting Server Selection Algorithm	The algorithm to select the RADIUS server(s) for active charging service to ensure proper load distribution amongst the available servers for accounting requests. Value could be one of the following: • first-n n Default • first-server • round-robin
Server Deadtime	The time period after which the status of the RADIUS server must be changed from Down to Active.
Maximum Outstanding Messages	The maximum number of outstanding messages that can be queued with the AAA manager.
Maximum Retries	The maximum number of attempts with the AAA server, before it is declared Not Responding and the detect dead server's consecutive failures count is incremented.
Response Timeout	The maximum number of retransmissions for RADIUS authentication requests.
Detect Dead Server Consecutive Retries	The number of consecutive failures for an AAA manager, before the status of an charging server is changed from Active to Down.

Viewing the Charging Trigger Configuration Details for an AAA group

To view the radius charging trigger configuration details for an AAA group:

Step 1   Right-click on the required device and choose the **Inventory** option.

Step 2   In the Inventory window, choose **Logical Inventory** > *Context* > **AAA** > **AAA Group**s > *AAA Group* > **Radius Configuration** > **Charging Trigger**. The charging configuration details are displayed in the content pane.

Table 23-12 describes the charging trigger configuration details.

Table 23-12   Radius Charging Triggers Configuration

Field Name	Description
Serving Node Change	Indicates whether RADIUS trigger for serving node is enabled.
Radio Access Technology Change	Indicates whether RADIUS trigger for radio access technology change is enabled.
User Location Information Change	Indicates whether RADIUS trigger for user location information change is enabled.
Routing Area Information Change	Indicates whether RADIUS trigger for routing area information change is enabled.
Quality of Service Change	Indicates whether RADIUS trigger for quality of service change is enabled.
Mobile Station Timezone Change	Indicates whether RADIUS trigger for mobile station time zone change is enabled.

Working with AAA Commands

The following commands can be launched from the inventory by choosing *AAA Group* **> Commands > Configuration**. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 23-13   AAA Commands

Command	Inputs Required and Notes
Create Diameter Accounting Server	Server Host Name, Priority
Create Diameter Authentication Server	Server Host Name, Priority
Delete AAA Group	Click **Execute Now** to delete the AAA group.
Modify AAA Group	Diameter Authentication tab: Dictionary, Delete End Point, End Point, Delete Max Retries, Max Retries, Request Timeout Diameter Accounting tab: Dictionary, Delete End Point, End Point, Delete Max Retries, Max Retries, Request Timeout