61200820E1-29.2A
November 2009

ADTRAN

Configuration Guide

Configuring AAA in AOS

This configuration guide will aid in the setup of authentication, authorization, and accounting (AAA) for ADTRAN Operating System (AOS) products. An overview of the AAA processes and functionality combined with detailed command descriptions, sample configurations, and troubleshooting tips provides step-by-step assistance for AAA configuration.

This guide consists of the following sections:

AAA Overview

Authentication, authorization, and accounting is a triple-threat security software system implemented on all AOS products. Made up of three distinct, configurable processes, AAA provides a malleable security system for all networks, in addition to the more static security implementations such as firewalls, making it an optimal security package for any network configuration. AAA is the basic framework for user-based security measures, providing the familiar network login methods through user name and password, as well as user restrictions from certain network areas and network usage monitoring. The main function of AAA is to govern which users are allowed network access, which services they are allowed to use, and to keep track of what users do while on the network. AAA is made up of three independent, configurable security measures: authentication, authorization, and accounting.

Authentication

Authentication validates the identity of the user attempting to gain access to the network, most often through a user name and password. In authentication, the most typical application is that a connecting user is prompted for information which is then checked by the server against a local user name database. There are other methods for authentication which will be discussed later in this guide, but the user name and password are the most frequently used and the most familiar.

Authorization

Authorization allows the connected user access to specified areas of the network, based on preconfigured parameters. In authorization, most often the information gained in authentication is checked against stored user parameters in a Remote Authentication Dial-In User Service (RADIUS) server or in a Terminal Access Controller Access Control System Plus (TACACS+) server. There are other methods, as well as multiple types of authorization, which will be discussed later in this guide but the basic procedure remains checking user information against stored access allowances.

Accounting

Accounting collects data about user activities while using the network and compiles it into printouts and reports that enable network administrators to see how the network is being used and by whom. Most often this data is collected from one or more of the servers employed in the network itself and compiled through AOS.

Benefits of AAA

AAA provides many security benefits for today’s networks. Not only does it operate dynamically, to address any network configuration, but it also tends to the security needs of traditional, partitioned, and wireless networks.

AAA is also concerned not only with the access and activities of incoming users to the network, but also those users already on the network, providing a whole network security package.

Another benefit to AAA is that it is software and not hardware. This has a smaller impact on network performance and budget, providing a perfect solution for all network sizes, as well as the scalability to grow as the network grows.

Lastly, the AAA architecture allows the optional configuration or implementation of any of the three AAA processes independent of the other two. This malleability provides total security for any network configuration, making it a necessity in today's security-conscious world.

The AAA Process

The following section describes the basic processes of AAA in typical network applications and includes a brief description of the two servers most frequently used in conjunction with AAA.

Figure 1 displays each AAA component in a typical network application:

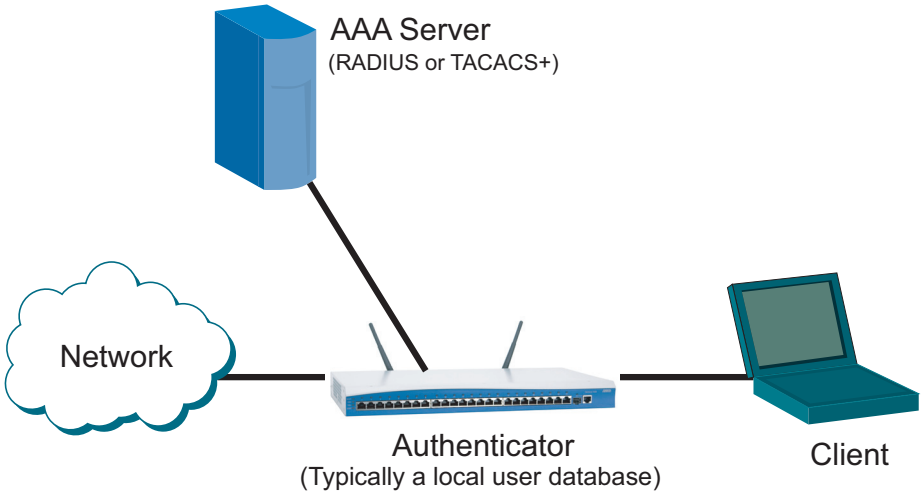

Figure 1. AAA Components

Basic AAA Process

The AAA process works through communication between the three major components: the client, the authenticator, and the AAA server. Figure 2 illustrates this basic communication:

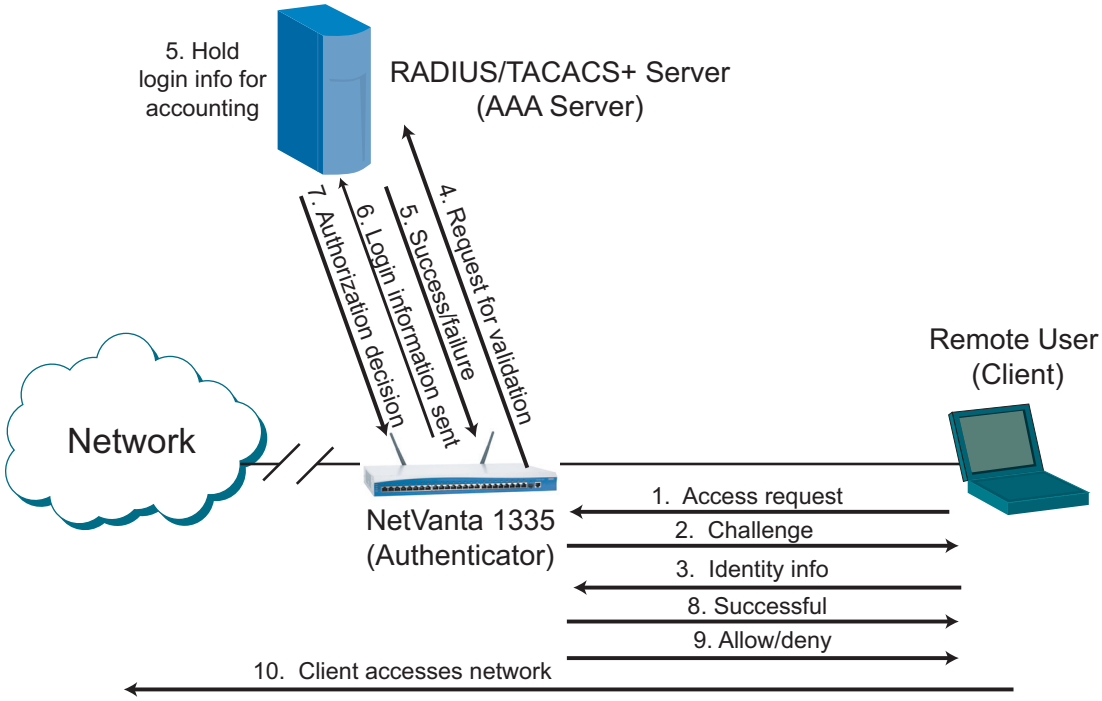

Figure 2. AAA Process

Communication Steps

1. The client attempts to connect to the network, presenting an access request to the authenticator (NetVanta 1335).
2. The authenticator responds to the client with a challenge requesting the client's identity information. This information is most often a user name and password.
3. The client responds (because of user input) to the authenticator with the requested information.
4. The authenticator forwards the client's information to the AAA server for validation from the server.
5. After searching for information regarding the client, the server sends a success or failure message to the authenticator, as well as any additional information the server has about the client. If there were a separate accounting server in this network, at this point the AAA server would send a copy of the login information to the accounting server.
6. After the authenticator receives a success message for the user login, login information is sent to the AAA server for accounting purposes if accounting is enabled for logins.
7. The AAA server makes an authorization decision based on its configured policies, and passes this decision back to the authenticator.
8. The authenticator sends a message to the client that the authentication was successful.

9. The authenticator then applies the proper authorization profile for the client as provided by the AAA server, stores the information for accounting, and then allows or denies the client based on the decision made by the AAA server.
10. The client gains access to the network after being allowed by the authenticator.

AAA Server Types

There are two main server types used in conjunction with AAA, one is the RADIUS server and the other is the TACACS+ server. AAA works with both server types, although there are certain benefits to each type depending on specific network needs and configurations. In AOS AAA, authorization and accounting only work with TACACS+ servers, and are not available on RADIUS servers. The benefits of each server, as well as the difference between the two are detailed in the following sections.

RADIUS Server

RADIUS servers are the industry standard for AAA. RADIUS servers use User Datagram Protocol (UDP) for communication between clients and authenticators. RADIUS servers are usually UNIX or Windows NT machines running a daemon process in the background. Remote access servers, virtual private network (VPN) servers, network switches with port-based authentication, and network access servers are all RADIUS enabled with RADIUS client components that communicate with the RADIUS server to control access to the network. Generally, issues related to server availability, retransmission, and timeouts are handled by the RADIUS enabled devices rather than the transmission protocol.

RADIUS servers encrypt only the password in the access-request packet from the client, which can be less secure than TACACS+ servers. RADIUS servers also combine authentication and authorization and have limited support for accounting features. RADIUS servers generally operate on either UDP port 1645 or UDP port 1812.

TACACS+ Server

TACACS+ servers are similar to the RADIUS servers in that they also use a background daemon for AAA. Other than daemon use, TACACS+ servers operate differently than RADIUS servers. TACACS+ servers use Transmission Control Protocol (TCP) rather than UDP, which provides connection oriented transport and more reliable transmission than UDP. TACACS+ servers also encrypt entire packets for more secure transmissions.

In a TACACS+ server, authentication, authorization, and accounting are all separate features. This means each service receives separate requests and acknowledgements, whereas with a RADIUS server access-accept packets also contain authorization information. This separation of features allows a TACACS+ server to control which commands can be executed on access servers, whereas RADIUS does not allow users to control which commands can be executed.

TACACS+ servers also require fewer programmable variables than do RADIUS servers. RADIUS servers require specified retransmit attempts and timeouts to support best-effort packet transport, but TACACS+ servers do not. TACACS+ servers provide more network reliability because they can immediately indicate a non-running network server by using reset (RST) packets, TCP acknowledgement, and TCP keepalives.

TACACS+ servers operate on TCP port 49.

Hardware and Software Requirements and Limitations

The AAA feature is available on AOS products as outlined in the ADTRAN knowledge base article number 2272, *Product Feature Matrix*. This matrix is available online at http://kb.adtran.com.

General Guidelines for Configuring AAA

This section describes two very important features of using and configuring AAA. Most AAA services rely on the configuration of RADIUS or TACACS+ servers for their functionality, and all AAA services rely on method lists to take the appropriate actions for managing your network at the interface level. The following sections describe these two features.

Configuring RADIUS Servers, TACACS+ Servers, and Named Server Groups

There are many AAA services that rely on the use of RADIUS or TACACS+ servers. The servers play a role in storing and maintaining user information for authentication and authorization, and each server holds accounting information about user activity. AOS supports all three AAA services on TACACS+ servers, whereas only authentication is supported on RADIUS servers.

RADIUS and TACACS+ servers can be used by AOS AAA services as a group of *all* RADIUS or *all* TACACS+ servers, or a subset of all servers can be configured by creating a named server group. These groups of servers can be used in AAA method lists as objects with which AOS products check to verify authentication and authorization or to report accounting information.

Configuring RADIUS Servers

To configure RADIUS servers for use with AAA, you must first configure the server itself. To configure a RADIUS server, follow these steps:

1. Configure the global parameters for the behavior of all RADIUS servers.

Changing global RADIUS parameters changes the parameters for all configured RADIUS servers.

You can configure RADIUS servers globally by using the following commands:

- **radius-server challenge-noecho**

The **radius-server challenge-noecho** command specifies that when users enter text in response to challenge questions the entered text does not appear on the screen. By default, no echo is enabled and users do not see what they are typing as it is entered. If the echo value has been changed, enter the command from the Global Configuration mode prompt as follows to return to hiding the text:

(config)**#radius-server challenge-noecho**

- **radius-server deadtime** <*value*>

The **radius-server deadtime** <*value*> command specifies the time to wait before attempting to reconnect to a RADIUS server that has timed out. The <*value*> parameter is the time period in minutes. By default, there is a **0** minute wait time before attempting to reconnect to a timed out server. Leaving the wait time at 0 minutes means that the server will never be declared dead. The time period value is **0** to **1440** minutes, although you should enter a value of at least **1** minute or greater. Using the **no** form of this command returns the dead time to the default value. Enter the command from the Global Configuration mode prompt as follows:

(config)**#radius-server deadtime 3**

- **radius-server enable-username** <*name*>

The **radius-server enable-username** <*name*> command specifies a user name to be used for authentication to enter the Enable mode. The <*name*> parameter is the user name sent to the server for enable AAA requests. By default, all RADIUS servers use the user name **$enab15$** for Enable mode authentication. Changing this parameter changes the user name used by all RADIUS servers to the specified entry. Using the **no** form of this command returns the Enable mode user name to the default value. Enter the command from the Global Configuration mode prompt as follows:

(config)**#radius-server enable-username fantastico**

It is recommended that you use a user name that is a unique name for your network and one that only the network administrators know. If the default user name is used, it is possible for unauthorized users to gain access to the network.

- **radius-server key** <*key*>

The **radius-server key** <*key*> command specifies the encryption key shared with the RADIUS servers. By default, no key is configured. Using this command specifies the same key is used by all RADIUS servers; however, the global encryption key can be overridden on a per-server basis. Using the **no** form of this command returns the key to the default value. Enter the command from the Global Configuration mode prompt as follows:

(config)**#radius-server key passphrase**

- **radius-server retry** <*number*>

The **radius-server retry** <*number*> command specifies the number of connection attempts to a RADIUS server. By default, **0** connection attempts are made. The valid attempt range is **0** to **10**. Using this command specifies that the number of attempts to all RADIUS servers is the same; however, the global number of connection attempts can be overridden on a per-server basis. Using the **no** form of this command returns the retry number to the default value. Enter the command from the Global Configuration mode prompt as follows:

(config)**#radius-server retry 5**

- **radius-server timeout** <*value*>

The **radius-server timeout** <*value*> command specifies the amount of time (in seconds) that RADIUS servers have to respond to a request before an error is declared. The <*value*> parameter is the time period in seconds. By default, a RADIUS server times out in **5** seconds. The valid time range is **1** to

1000 seconds. Using this command specifies that all RADIUS servers timeout in the same specified time period; however, the global timeout period can be overridden on a per-server basis. Use the **no** form of this command to return the timeout period to the default value. Enter the command from the Global Configuration mode prompt as follows:

(config)**#radius-server timeout 10**

2. Configure settings for individual RADIUS servers using the **radius-server host** <*hostname | ip address*> **[acct-port** <*port*>**] [auth-port** <*port*>**] [retransmit** <*number*>**] [timeout** <*value*>**] [key** <*key*>**]** command.

*The optional parameters can be entered in almost any order. However, the **key** parameter must be entered at the end of the command because the rest of the command is read before the **key** parameter. Each parameter can be used only once.*

Settings for individual servers will override the global settings. Any setting left unspecified will default to the global setting.

The <*hostname | ip address*> parameter specifies either the fully qualified domain name (FQDN) or IP address of the RADIUS server. IP addresses should be expressed in dotted decimal notation, for example, **10.10.10.1**. The command can be entered at this point, specifying only the host name or IP address of the server. The rest of the parameters are optional, and will override default or global settings.

*If a host name is used, a domain naming system (DNS) server should be learned by the AOS device using Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol (PPP), or specified in the Global Configuration mode with the **ip name-server** command.*

The **acct-port** <*port*> parameter optionally changes the default UDP port used by the AOS device for communication with the RADIUS accounting server. By default, the port used is **1813**. The port range is **0** to **65535**.

This parameter is reserved for future use, as accounting is not currently supported with RADIUS servers.

The **auth-port** <*port*> parameter optionally changes the default UDP port used by the AOS device for communication with the RADIUS authentication server. By default, the port used is **1812**. Port range is **0** to **65535**.

The **retransmit** <*number*> parameter optionally specifies the number of connection attempts made to the server. The range of attempts is **1** to **100**. The number of connection attempts will default to the global setting (set using the **radius-server retry** command from the Global Configuration mode). If the

number of attempts is changed on this server, it overrides the global setting.

The **timeout** <*value*> parameter optionally specifies the time to wait (in seconds) for the server to reply to requests. The time period range is **1** to **1000** seconds. By default, the timeout value is set to the global setting (set using the **radius-server timeout** command from the Global Configuration mode). If the timeout period is changed on this server, it overrides the global setting.

The **key** <*key*> parameter optionally specifies the encryption key used by this server. This key overrides the key specified at the global level (set using the **radius-server key** command from the Global Configuration mode). The <*key*> value defaults to the global key setting if no key is specified.

To specify that the RADIUS server (**10.10.10.2**) use the global key setting (left unspecified), a timeout value of **10** seconds, the default accounting and authorization ports (left unspecified), and a retransmit number of **5**, enter the command from the Global Configuration mode prompt as follows:

```
(config)#radius-server host 10.10.10.2 retransmit 5 timeout 10
(config)#
```

Configuring TACACS+ Servers

To configure TACACS+ servers for use with AAA, you must first configure the server itself. To configure the TACACS+ server, follow these steps:

1. Configure the global parameters for the behavior of all TACACS+ servers.

> NOTE *Changing global TACACS+ parameters changes the parameters for all configured TACACS+ servers.*

You can configure TACACS+ servers globally by using the following commands:

- **tacacs-server key** <*key*>

The **tacacs-server key** <*key*> command specifies the encryption key used by all TACACS+ servers. By default, there is no encryption key set. Using this command specifies that all TACACS+ servers use the same encryption key; however, the global encryption key can be overridden on a per-server basis. Using the **no** form of this command returns the key to the default value. Enter the command from the Global Configuration mode prompt as follows:

```
(config)#tacacs-server key passphrase
```

- **tacacs-server packet maxsize** <*value*>

The **tacacs-server packet maxsize** <*value*> command specifies the maximum packet size that can be sent to the TACACS+ server. The <*value*> parameter specifies the packet size in kilobytes and the valid range is **10240** to **65535**. By default, the packet size is set to **10240**. Using the **no** form of this command returns the packet size to the default value. Enter the command from the Global Configuration mode prompt as follows:

```
(config)#tacacs-server packet maxsize 15000
```


- **tacacs-server timeout** <*value*>

The **tacacs-server timeout** <*value*> command specifies the time (in seconds) that TACACS+ servers have to respond to a request before an error is declared. The <*value*> range is **1** to **1000** seconds. By default, the timeout period is set to **5** seconds. Using this command specifies that all TACACS+ servers use the same timeout period; however, the global timeout period can be overridden on a per-server basis. Using the **no** form of this command returns the timeout period to the default value. Enter the command from the Global Configuration mode prompt as follows:

(config)**#tacacs-server timeout 200**

2. Configure settings for individual TACACS+ servers using the **tacacs-server host** <*hostname | ip address*> **[port** <*port*>**] [timeout** <*value*>**] [key** <*key*>**]** command.

> NOTE *The optional parameters can be entered in almost any order. The **key** parameter must be entered at the end of the command because the rest of the command is read before the **key** parameter. Each parameter can be used only once.*

> NOTE *Settings for individual servers will override the global settings. Any setting left unspecified will default to the global setting.*

The <*hostname | ip address*> parameter specifies either the FQDN or IP address of the TACACS+ server. IP addresses should be expressed in dotted decimal notation, for example, **10.10.10.1**. The command can be entered at this point, specifying only the host name or IP address of the server. The rest of the parameters are optional, and will override default or global settings.

> NOTE *If a host name is used, a DNS server should be learned by the AOS device using DHCP, PPP, or specified in the Global Configuration mode with the **ip name-server** command.*

The **port** <*port*> parameter optionally changes the default TCP port used by the AOS device to communicate with the TACACS+ server. By default, the port used is **49**. The valid port range is **1** to **65535**.

The **timeout** <*value*> parameter optionally specifies the time to wait for the server to reply. The time period range is **1** to **1000** seconds. If left unspecified, the timeout value will default to the global setting (set using the **tacacs-server timeout** command from the Global Configuration mode). If the timeout period is changed on this server, it overrides the global setting.

The **key** <*key*> parameter optionally specifies the encryption key used by this server. This key overrides the key specified at the global level (set using the **tacacs-server key** command from the Global Configuration mode). The <*key*> value defaults to the global key setting if no key is specified.

To specify that the TACACS+ server (**10.10.10.4**) use the global key setting (left unspecified), a timeout value of **10** seconds, and the default TCP port (left unspecified), enter the command from the Global Configuration mode prompt as follows:

(config)**#tacacs-server host 10.10.10.4 timeout 10**
(config)#

Configuring Named Server Groups

You can create specific groups of servers to be used as methods for the method lists that help AAA to function. You can choose to use all RADIUS servers or all TACACS+ servers as methods in the AAA methods list, or you can create a subset of the servers to use in the method lists. It is beneficial for some network configurations to use a subset server group for particular AAA services. These subset server groups are named server groups, and use the name you configure when you group them together.

Server groups can have multiple host entries for the same server as long as each entry has a unique identifier (an IP address and a UDP port for RADIUS servers). If you configure two host entries on the same RADIUS server and are using both host entries for the same service (for example, using both entries for authentication), then the second entry functions as a failover. RADIUS host entries are tried in the order they are configured, so the failover entry is the second configured entry.

To understand how server groups function, refer to Figure 3 below, which displays a typical AAA server configuration.

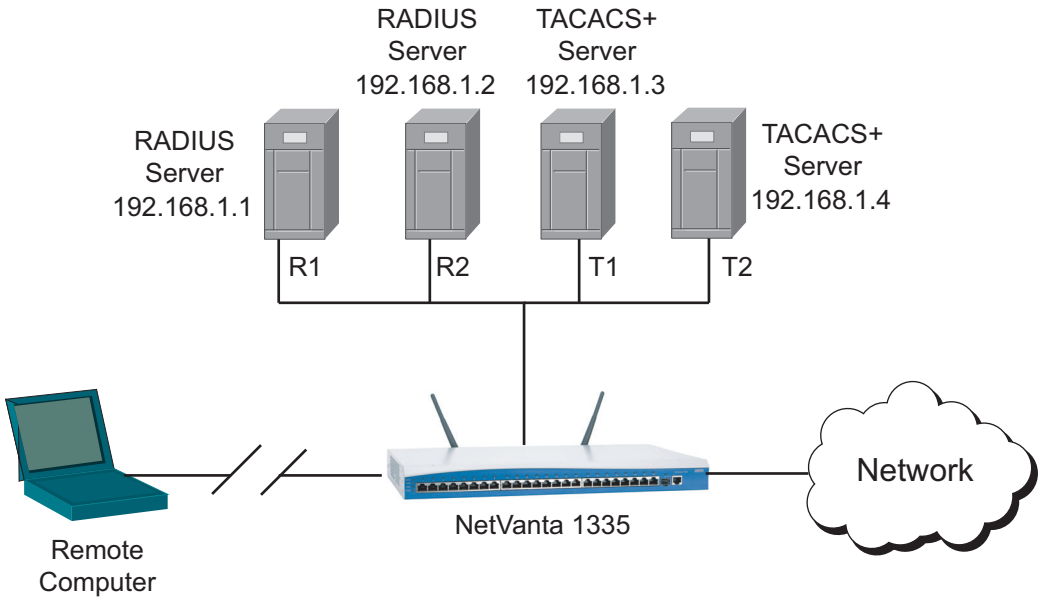

Figure 3. Typical AAA Server Configuration

In Figure 3, there are four AAA servers used in this configuration. Two of these servers are RADIUS servers (R1 and R2), and they constitute the default RADIUS server group of *all* RADIUS servers. The other two servers are TACACS+ servers (T1 and T2), and they constitute the default TACACS+ server group of *all* TACACS+ servers.

To create a subset of these servers, for example, to use R1 and R2 for authentication and T2 for accounting, you must first configure the servers and then group them accordingly. To configure each server, follow the steps outlined in *Configuring RADIUS Servers, TACACS+ Servers, and Named Server Groups on page 6*.

Once the servers are configured, you must configure a server group and add the servers to it. To create a named server group, follow these steps:

1. Create a named server group using the **aaa group server [radius | tacacs+]** <*group name*> command from the Global Configuration mode prompt. If you are adding RADIUS servers to the group, use the **radius** keyword. If you are adding TACACS+ servers to the group, use the **tacacs+** keyword. The <*group name*> parameter is the name of the group you are creating. To configure a new server group, enter the command from the Global Configuration mode prompt as follows:

   (config)**#aaa group server radius AUTHENTICATIONGROUP**
   (config-sg-radius)**#**

2. After creating the named server group, you must assign the servers to the group at the server group configuration prompt using the **server** <*hostname* | *ip address*> command. The <*hostname* | *ip address*> parameter is the FQDN or IP address of the server to add to the group. IP addresses should be expressed in dotted decimal notation, for example, **10.10.10.1**. Enter the predefined servers at the prompt as follows:

   (config-sg-radius)**#server 192.168.1.1**

   > NOTE *If a host name is used, a DNS server should be learned by the AOS device using DHCP, PPP, or specified in the Global Configuration mode with the **ip name-server** command.*

3. If you are configuring RADIUS servers, you can also specify the authentication port for the server to use by using the **auth-port** <*port*> keyword in addition to the **server** command. By defining the port yourself, you can create multiple host entries for the same server. By default, the authentication port is **1812**. To change the authentication port on a RADIUS server you are adding to the group, enter the command as follows:

   (config-sg-radius)**#server 192.168.1.2 auth-port 1851**

4. The servers are now added to the group, and the server group can be used as a method for performing AAA services.

   > NOTE *Empty RADIUS groups are not saved. When the last server is removed from a group, AOS automatically deletes the group. Conversely, empty TACACS+ groups are saved.*

AAA Method Lists

Method lists are lists of the methods used by AAA for verifying authentication, authorization, or reporting accounting. Each service type uses method lists, although the methods used by each service vary depending upon the service. Specific methods for each service are described in detail in the section pertaining to the service type.

There are two types of method lists for most AAA services. They are default method lists and named method lists. Default method lists are created and applied globally; once they are created, they are automatically applied to the line interfaces as long as AAA is enabled. Named method lists must be applied to each interface manually, and once they are applied to an interface they take precedence over the default method list. Each type of method list uses the same methods (depending on AAA service), but are configured separately.

Method lists are created for each AAA service, as named lists, and then applied to a line interface. In a manner similar to access control lists (ACLs), the methods included in the method lists are order-dependent and do not take effect until they are applied to an interface. AOS supports AAA configured on console, Telnet, and secure shell (SSH) line interfaces. AAA method lists can also be applied to multiple other features in AOS, such as File Transfer Protocol (FTP) authentication, Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) authentication, port authentication, and authentication for Internet Key Exchange (IKE) policies. For more information on method lists and their use with these features, refer to *Applying Authentication Method Lists on page 18*.

The AAA method lists work by performing the specified methods in the order in which they were entered into the list. If a method is tried and an error is produced, the AAA service moves to the next method in the list. It is important to note that an error is different from a failure. An error occurs if something is dysfunctional with the AAA method specified (for example, a server has timed out or is unavailable). A failure occurs when the AAA method specified is unverifiable (for example, an incorrect password is entered during login).

The methods must be entered into the method list in the order that they are to be used for AAA services. For example, if you wanted AAA authentication to verify a user's login authentication primarily by entering a password, you would specify that method as the first method in the authentication methods list. If that method produced an error, the second method entered would then be tried for verification. And so on.

For more details on method lists specific to authentication, authorization, or accounting, refer to the following sections:

- *Configuring Authentication Method Lists on page 15*
- *Applying Authentication Method Lists on page 18*
- *Configuring Authorization Method Lists on page 20*
- *Applying Authorization Method Lists on page 23*
- *Configuring Accounting Method Lists on page 25*
- *Applying Accounting Method Lists on page 28*

AAA Configuration Summary

In the three areas of AAA, each service is configured in roughly the same way using the command line interface (CLI). In general, the configuration of authentication, authorization, and accounting services follow this pattern:

1. Configure the necessary RADIUS servers, TACACS+ servers, or server groups.
2. Enable AAA.
3. Configure the service method lists.
4. Apply the service method lists to the appropriate line interface.
5. Configure any additional parameters on a global level.

The following sections describe in detail the configuration of authentication, authorization, and accounting.

Configuring Authentication

Authentication is the AAA service that validates the identity of the user attempting to gain access to the network. In AOS, authentication can be used to verify user login credentials, verify user access to Enable mode privileges, and verify the ports used.

To begin configuring AAA authentication, ensure that AAA is enabled on the global level. To activate AAA, enter the **aaa on** command from the Global Configuration mode prompt as follows:

```
(config)#aaa on
```

Without AAA enabled prior to service configuration, many AAA options will not be available. Once AAA is enabled, the next steps configure the authentication method lists and apply them to a line interface.

You can optionally define the number of threads available for AAA background process using the **aaa processes** <*value*> command from the Global Configuration mode prompt. The value range is **1** to **64**, with a default of **1** thread available for AAA processes. Note that increasing the number of threads can speed up simultaneous authentication processes, but it does so at the expense of other system resources (for example, memory). Enter the command as follows:

```
(config)#aaa processes 5
```


Configuring Authentication Method Lists

The three functions of AAA authentication (verifying user logins, verifying user access to the Enable mode, and verifying port usage) are completed by using either a default method list or a named method list. Login authentication supports both a default and named list, but Enable and port authentication verification support only a default list. The difference between the default and named method lists is that the default list is applied at a global level. Once the default list is created, it is automatically applied to all line interfaces. Named lists, however, are applied manually to the line interface from the interface's configuration mode.

If authentication is enabled, but no authentication method list is specified, the default list is applied to all line interfaces. If the default method list is not defined, then local authentication (authentication using the local user name database) takes place by default.

Each AAA authentication method list relies on a combination of seven authentication methods. Each method must be entered into the list in the order that they are to be performed. Although these methods can be entered in any order, each can only be used once. The exception is the named server group method, which can be entered multiple times to accommodate multiple configured groups. Not all methods are available on all AAA authentication method list configurations.

The seven main methods used for AAA authentication in AOS are:

- **Enable Authentication Method:** This authentication method specifies that the Enable mode password is used as the login authenticator. To use this method for authentication, an Enable mode password must be defined prior to configuring AAA. The Enable mode password can be up to 30 characters in length. To create an Enable mode password for a user, enter the **enable password** <*password*> command from the Global Configuration mode prompt as follows:

  (config)**#enable password Mypassword**

- **Line Authentication Method:** This authentication method specifies that the line password is used as the login authenticator. The line password is the password used to access the line interface through one of the multiple lines available. For the Telnet interface, there are four lines available, and the line password is used to access one of those four lines. For example, if Line 0 on the Telnet interface is not available upon login, the login transfers to the next available line and uses the authentication method applied to that line. The same occurs until all the lines are used. To use this method for authentication, a line password must be defined prior to configuring AAA. To create a login password, enter the **login** and **password** <*password*> commands from the line interface configuration prompt. For example:

  (config)**#line telnet 0 4**
  (config-telnet0-4)**#login**
  (config-telnet0-4)**#password Mypassword**

- **Local Authentication Method:** This authentication method specifies that the local user name database is used for verifying login authentication. To use this method for authentication, users must be configured and entered into the local user name database prior to configuring AAA. To create a user name in the local database, enter the **username** <*username*> **password** <*password*> command from the Global Configuration mode prompt. Both user names and passwords are alphanumerical strings up to 30 characters in length. For example:

  (config)**#username Admin password Password**

- **Group RADIUS Authentication Method:** This authentication method specifies that the group of all RADIUS servers is used to verify login authentication. To use this method for authentication, RADIUS servers must be configured prior to configuring AAA. For more information about configuring RADIUS servers, refer to *Configuring RADIUS Servers, TACACS+ Servers, and Named Server Groups on page 6*.

- **Group TACACS+ Authentication Method:** This authentication method specifies that the group of all TACACS+ servers is used to verify login authentication. To use this method for authentication, TACACS+ servers must be configured prior to configuring AAA. For more information about configuring TACACS+ servers, refer to *Configuring RADIUS Servers, TACACS+ Servers, and Named Server Groups on page 6*.

- **Named Server Group Authentication Method:** This authentication method specifies that the previously configured group of servers is used to verify login authentication. To use this method for authentication, a named server group must be configured prior to configuring AAA. For more information about configuring named server groups, refer to *Configuring RADIUS Servers, TACACS+ Servers, and Named Server Groups on page 6*.

- **None Authentication Method:** This authentication method specifies that no authentication is performed. This method is useful in preventing a lock-out situation if all previous authentication methods produce errors and should always be placed at the end of the methods list.

*For security reasons, ADTRAN recommends that the **local** authentication method be used instead of the **none** authentication method. Using the **local** authentication method prevents unauthorized users from gaining access to the device during a period in which the links to all authentication servers are down. The local user database contained within the AOS device will always be available and serves as the last line of defense.*

Creating Login Authentication Method Lists

To create a default login authentication method list (a method list named **default**), enter the **aaa authentication login default [enable] [group radius] [group tacacs+] [group** <*name*>**] [line] [local] [none]** command from the Global Configuration mode prompt. The **enable** parameter specifies using the Enable mode password for authentication. The **group radius** parameter specifies using all RADIUS servers for authentication. The **group tacacs+** parameter specifies using all TACACS+ servers for authentication. The **group** <*name*> parameter specifies that a named server group is used for

authentication. The **line** parameter specifies using the line password for authentication. The **local** parameter specifies using the local user name database for authentication. The **none** parameter specifies that no authentication is performed. For example, enter the command as follows (making sure the order of parameters matches the authentication needs of your network):

(config)**#aaa authentication login default enable group AUTHENTICATIONGROUP group radius local**

Remember that once the default list is configured, it is automatically applied to all line interfaces at a global level.

To create a named login authentication method list, enter the **aaa authentication login** <*listname*> **[enable] [group radius] [group tacacs+] [group** <*name*>**] [line] [local] [none]** command from the Global Configuration mode prompt. Each parameter specifies the authentication method to be attempted in the order in which they are to be tried. For example, enter the command as follows (making sure the order of the parameters matches the authentication needs of your network):

(config)**#aaa authentication login AuthList1 line enable group tacacs+ local**

Creating Enable Mode Access Authentication Method Lists

Enable mode access authentication method lists are created the same way as login authentication method lists except that only a default list is available. To configure an Enable mode access authentication list, enter the **aaa authentication enable default [enable] [group radius] [group tacacs+] [group** <*name*>**] [line] [none]** command from the Global Configuration mode prompt. Each parameter specifies the authentication method to be attempted in the order in which they are to be tried. For example, enter the command as follows (making sure the order of parameters matches the authentication needs of your network):

(config)**#aaa authentication enable default enable line group radius local**

Remember that once the default list is configured, it is automatically applied to all line interfaces at a global level.

Creating Port Authentication Method Lists

Port authentication method lists are created in the same way as login authentication method lists except that only a default list is available. To create a port authentication method list, enter the **aaa authentication port-auth default [group radius] [group** <*name*>**] [local] [none]** command from the Global Configuration mode prompt. Each parameter specifies the authentication method to be attempted in the order in which they are to be tried. For example, enter the command as follows (making sure that the order of parameters matches the authentication needs of your network):

(config)**#aaa authentication port-auth default group radius local**

*Port authentication is typically used in conjunction with the **port-auth port-control auto** command when used on switchports to enable 802.1x port authentication. For more information, refer to the **Configuring 802.1x in AOS** quick configuration guide (article number 2221) available online at* http://kb.adtran.com.

Applying Authentication Method Lists

Once the authentication method lists have been created, named method lists must be applied to a line interface (console, Telnet, or SSH) before they are active. To apply an AAA authentication method list to a line interface, enter the **login authentication** <*listname*> command from the interface's configuration mode prompt. Only the login authentication method list needs to be applied to a line interface because it is the only AAA authentication method list with the named list option. Enter the command as follows:

(config)**#line telnet 0 4**
(config-telnet0-4)**#login authentication AuthList1**

If you have previously configured a line interface to use a named authentication method list and want to return to using the default list, enter the **login authentication default** command from the line interface's configuration mode prompt as follows:

(config)**#line telnet 0 4**
(config-telnet0-4)**#login authentication default**

Additionally, named authentication method lists can be used to authenticate client, FTP, and HTTP or HTTPS authentication. To use a named authentication method list for client/server authentication in the IKE policy, enter the **client authentication server list** <*listname*> command from the Crypto IKE Policy Configuration mode prompt as follows:

(config)**#crypto ike policy 1**
(config-ike)**#client authentication server list AuthList1**

*For more information about using extended authentication with VPN, refer to the **Configuring Extended Authentication with VPN Mobile Users in AOS** quick configuration guide (article number 2226) available online at* http://kb.adtran.com.

To use a named authentication method list for FTP authentication to the AOS device's internal FTP server, use the **ftp authentication** <*listname*> command from the Global Configuration mode prompt. Note that AAA must be enabled for this list to work with FTP, and if AAA is enabled, but no list is assigned to FTP, FTP automatically uses the local user list for authentication. Enter the command as follows:

(config)**#ftp authentication AuthList1**

To use a named authentication method list for HTTP or HTTPS authentication to the AOS device's internal HTTP server, use the **ip http authentication** <*listname*> command from the Global Configuration mode prompt. Enter the command as follows:

(config)**#ip http authentication AuthList1**

Additional Authentication Configurations (Global)

There are additional configuration options for how AAA authentication functions and appears to the user. These options include specifying the number of login attempts allowed, the authentication banner seen by the user, the authentication fail message seen by the user, the authentication password prompt seen by the user, and the authentication user name prompt seen by the user. These options are all configured from the Global Configuration mode and are automatically applied to all types of AAA authentication.

To specify the maximum number of login attempts allowed before the session is closed, enter the **aaa local authentication attempts max-fail** <*number*> command. The number range is **1** to **25**. By default, this number is set to **3**. To change the default number, enter the command as follows:

(config)**#aaa local authentication attempts max-fail 5**

To specify the AAA authentication banner, enter the **aaa authentication banner** <*banner*> command. This command sets the message the user sees when starting login authentication. The <*banner*> parameter is the actual text the user will see; however, it must begin with a delimiter (for example, **:**, **“**, #, etc.) to begin recording the typed text. The banner must end with the same delimiter to indicate an end to the banner. By default, the AAA authentication banner is **User Access Verification**. To change the default banner, enter the command as follows:

(config)**#aaa authentication banner #**
Enter TEXT message. End with the character ‘**#**’.
User Login Authentication:#
(config)#

To specify the AAA authentication fail message, enter the **aaa authentication fail-message** <*message*> command. This command sets the message shown if the user authentication fails. Like the AAA authentication banner, the <*message*> parameter must begin and end with the same delimiter (for example, **:**, **“**, #, etc.) to properly record the text. By default, the fail message is **Authentication failed**. To change the default fail message, enter the command as follows:

(config)**#aaa authentication fail-message #**
Enter TEXT message. End with the character ‘**#**’.
Failed Authentication. Please try again.#
(config)#

To specify the AAA authentication password prompt, enter the **aaa authentication password-prompt** <*prompt*> command. This command sets the message seen when prompting the user for their password. The <*prompt*> parameter is a single-line text string enclosed in quotation marks. By default, the password prompt is **Password:**. To change the default prompt, enter the command as follows:

(config)**#aaa authentication password-prompt “Please Enter Your Password:”**

To specify the AAA authentication user name prompt, enter the **aaa authentication username-prompt** <*prompt*> command. This command sets the message seen when prompting the user for their user name. The <*prompt*> parameter is a single-line text string enclosed in quotation marks. By default, the user name prompt is **Username:**. To change the default prompt, enter the command as follows:

(config)**#aaa authentication username-prompt “Please Enter Your User Name:”**

Configuring Authorization

AAA authorization is an AAA service that helps to limit the network services available to users. Authorization works by retrieving information from the user's profile (stored either on the local database or security server) and uses that information to determine the areas of the network to which the user is allowed access. In AOS, AAA authorization can limit the commands available to a specific user and specify whether or not users can access privileged CLI sessions.

To begin configuring AAA authorization, ensure that AAA is enabled on the AOS unit by entering the **aaa on** command from the Global Configuration mode prompt. Enter the command as follows:

(config)**#aaa on**

Without AAA enabled prior to service configuration, many AAA options will not be available. Once AAA is enabled, the next steps configure the authorization method lists and apply them to a line interface.

Configuring Authorization Method Lists

The two functions of AAA authorization (allowing or restricting the use of certain commands or privileged modes) are completed by using either a default method list or a named method list. Command authorization and Executive authorization method lists support both default and named method lists. The difference between the default and named method lists is that the default list is applied at a global level. Once the default list is created, it is automatically applied to all line interfaces. Named lists, however, are applied manually to the line interface from the interface's configuration mode.

By default, AAA authorization is not configured, so no authorization takes place.

If authorization is enabled, but no authorization method list is specified, the default list is applied to all line interfaces.

Each AAA authorization methods list relies on a combination of four authentication methods. Each method must be entered into the list in the order that they are to be performed. Although these methods can be entered in any order, each can only be used once. The exception is the named server group method which can be entered multiple times to accommodate multiple configured groups.

RADIUS servers are not used for authorization in AOS AAA.

Authorization takes place on a per-command basis, and therefore it has no effect on Web graphical user interface (GUI) users. The GUI accesses configurations in a different way than the CLI and does not actually enter commands, therefore, GUI users are not subject to authorization. If authorization or accounting are desired, it is recommended that the GUI be disabled.

The four main methods used for AAA authorization in AOS are:

- **Group TACACS+ Authorization Method:** This authorization method specifies that the group of all TACACS+ servers is used to verify command and privilege authorization. To use this method for authorization, TACACS+ servers must be configured prior to configuring AAA. For more information about configuring TACACS+ servers, refer to *Configuring RADIUS Servers, TACACS+ Servers, and Named Server Groups on page 6*.
- **Named Server Group Authorization Method:** This authorization method specifies that the previously configured group of servers is used to verify command and privilege authorization. To use this method for authorization, a named server group must be configured prior to configuring AAA. For more information about configuring named server groups, refer to *Configuring RADIUS Servers, TACACS+ Servers, and Named Server Groups on page 6*.
- **If-Authenticated Authorization Method:** This authorization method specifies that authorization is granted to the user if the user has already been authenticated successfully.
- **None Authorization Method:** This authorization method specifies that no authorization is performed. This method is useful in preventing a lock-out situation if all previous authorization methods produce errors and should always be placed at the end of the method list.

Creating Command Authorization Method Lists

Command authorization method lists specify the methods used to determine if a user can access either Level 1 (unprivileged) or Level 15 (privileged) commands in the CLI.

If command authorization is used in conjunction with a TACACS+ server, the same user name that is used to access AOS must be configured on the server.

To create a default command authorization method list, enter the **aaa authorization commands** <*level*> **default [group tacacs+] [group** <*name*>**] [if-authenticated] [none]** command from the Global Configuration mode prompt. The <*level*> parameter specifies the command level to which this method list pertains. Choices are Level 1 (unprivileged) and Level 15 (privileged). The **group tacacs+** parameter specifies using all TACACS+ servers for authorization. The **group** <*name*> specifies using a named server group for authorization. The **if-authenticated** parameter specifies that authorization will be granted if the user has already been authenticated successfully. The **none** parameter specifies that no authorization is performed. Enter the command as follows (making sure the order of parameters matches the authorization needs of your network):

(config)**#aaa authorization commands 15 default group tacacs+ if-authenticated**

The user command privilege level (1 or 15) must be defined in addition to specifying all of the commands available on a per-user basis in the configuration of the TACACS+ server. Commands of a particular level are not checked for authorization unless explicitly defined in the configuration with a method list. For example, if a method list is defined for Level 1 commands but not Level 15, then a user is able to enter any Level 15 commands since no authorization takes place due to the lack of a Level 15 commands method list. The same user will only be allowed to enter the Level 1 commands configured for the user in the Level 1 commands method list.

Remember that once the default list is configured, it is automatically applied to all line interfaces at a global level.

To create a named command authorization method list, enter the **aaa authorization commands** <*level*> <*listname*> **[group tacacs+] [group** <*name*>**] [if-authenticated] [none]** command from the Global Configuration mode prompt. Each parameter specifies the authorization method to be attempted in the order in which they are to be tried. Enter the command as follows (making sure the order of parameters matches the authentication needs of your network):

(config)**#aaa authorization commands 15 Authorization1 group AUTHORT1 none**

The user command privilege level (1 or 15) must be defined in addition to specifying all of the commands available on a per-user basis in the configuration of the TACACS+ server. Commands of a particular level are not checked for authorization unless explicitly defined in the configuration with a method list. For example, if a method list is defined for Level 1 commands but not Level 15, then a user is able to enter any Level 15 commands since no authorization takes place due to the lack of a Level 15 commands method list. The same user will only be allowed to enter the Level 1 commands configured for the user in the Level 1 commands method list.

Creating Executive Mode Access Authorization Method Lists

Executive mode access authorization method lists are created the same way as command authorization method lists. These method lists enable users to directly access the Enable mode upon login.

If a TACACS+ server is used in conjunction with an executive mode access authorization method list, the user name used to access the AOS device must be configured as a Level 15 user on the TACACS+ server.

To configure a default executive mode access authorization method list, enter the **aaa authorization exec default [group tacacs+] [group** <*name*>**] [if-authenticated] [none]** command from the Global Configuration mode prompt. Each parameter specifies the authorization method to be attempted in the order in which they are to be tried. Enter the command as follows (making sure the order of parameters matches the authorization needs of your network):

(config)**#aaa authorization exec default group tacacs+ if-authenticated**

Remember that once the default list is configured, it is automatically applied to all line interfaces at a global level.

To configure a named executive mode access authorization list, enter the **aaa authorization exec** <*listname*> **[group tacacs+] [group** <*name*>**] [if-authenticated] [none]** command from the Global Configuration mode prompt. Each parameter specifies the authorization method to be used. Enter the command as follows (making sure the order of parameters matches the authorization needs of your network):

(config)**#aaa authorization exec ExecList1 group AUTHORT1 if-authenticated**

Applying Authorization Method Lists

Once the authorization method lists have been created, named method lists must be applied to a line interface (console, Telnet, or SSH) before they are active. Before the named method list can be applied to the line interface, the appropriate **aaa authorization** commands must be enabled at a global level and then applied to the line interface from the interface's configuration mode. By default, AAA authorization commands are enabled.

If command-level authorization was disabled in the AOS configuration, enter the **aaa authorization config-command** command from the Global Configuration mode prompt as follows to enable it and restore the default behavior:

(config)**#aaa authorization config-command**

To enable console authorization, enter the **aaa authorization console** command from the Global Configuration mode prompt. This command only controls authorization on console line interfaces. By default, authorization is not enabled on a console line interface. This measure prevents accidental lockout issues on directly-connected lines. If you want authorization to occur on the console line interface, enter the command as follows:

(config)**#aaa authorization console**

There is no one command to disable authorization on non-console line interfaces.

By default, command authorization is enabled and console authorization is disabled.

To apply an AAA authorization command method list to a line interface, enter the **authorization commands** <*level*> <*listname*> command from the line interface's configuration mode prompt. The <*level*> parameter is the command level: Level 1 (unprivileged) or Level 15 (privileged). Enter the command as follows:

(config)**#line telnet 0 4**
(config-telnet0-4)**#authorization commands 15 Authorization1**

If a default list for command authorization is not configured, and only one level of command authorization is configured, all commands are allowed for the command level not configured.

If you have previously configured a line interface to use a named command authorization method list and want to return to using the default method list, enter the **authorization commands** <*level*> **default** command from the line interface's configuration mode prompt as follows:

(config)**#line telnet 0 4**
(config-telnet0-4)**#authorization commands 15 default**

To apply an AAA authorization executive method list to a line interface, enter the **authorization exec** <*listname*> command from the line interface's configuration mode prompt as follows:

(config)**#line telnet 0 4**
(config-telnet0-4)**#authorization exec ExecList1**

If you have previously configured a line interface to use a named executive method list and want to return to using the default list, enter the **authorization exec default** command from the line interface's configuration mode prompt as follows:

(config)**#line telnet 0 4**
(config-telnet0-4)**#authorization exec default**

Configuring Accounting

AAA accounting is an AAA service that helps to track the services and resources that users are accessing and using. Accounting works by sending records of user activity to a configured server which can then be used by network administrators to monitor network management, client billing, and auditing. In AOS, AAA accounting can record the commands users are entering, the inbound connections (user executive terminal sessions), and the outbound connections users make and report them to a configured TACACS+ server.

To begin configuring AAA accounting, ensure that AAA is enabled on the AOS unit by entering the **aaa on** command from the Global Configuration mode prompt. Enter the command as follows:

(config)**#aaa on**

Without AAA enabled prior to service configuration, many AAA options will not be available. Once AAA is enabled, the next steps configure the accounting method lists and apply them to a line interface.

Configuring Accounting Method Lists

The three functions of AAA accounting (recording commands, inbound connections, and outbound connections) are completed by using either a default method list or a named method list. Command accounting, connection accounting (outbound), and executive accounting (inbound connection) method lists support both default and a named method lists. The difference between the default and named method lists is that the default list is applied at a global level. Once the default list is created, it is automatically applied to all line interfaces. Named lists, however, are applied manually to the line interface from the interface's configuration mode.

Each AAA accounting method list relies on a combination of five accounting methods. Each method must be entered into the list in the order that they are to be performed. Although these methods can be entered in any order, each can only be used once. The exception is the named server group method which can be entered multiple times to accommodate multiple configured groups. Not all methods are available on all AAA accounting method lists configurations.

RADIUS servers are not supported for accounting in AOS AAA.

The five main methods used for AAA accounting in AOS are:

- **Start-Stop Accounting Method:** This accounting method specifies that user activity is recorded from the beginning of the service use until the service is terminated. This means if a user accesses a certain command level, the moment they enter that level until they exit that level AAA accounting keeps track of their activity. In relation to connections, whether inbound or outbound, this means AAA accounting begins recording as soon as a connection is made until it is terminated.
- **Stop-Only Accounting Method:** This accounting method specifies that user activity is recorded at the point of service termination. This means that if a user accesses a certain command level, the moment they exit that level AAA accounting records a summary of their activity. In relation to connections, whether inbound or outbound, this means that AAA accounting records a summary of connection information when the connection is terminated.
- **Group TACACS+ Accounting Method:** This accounting method specifies that the group of all TACACS+ servers is used to record command entry and connection creation activity on a per-user basis. To use this method for accounting, TACACS+ servers must be configured prior to configuring AAA. For more information about configuring TACACS+ servers, refer to *Configuring RADIUS Servers, TACACS+ Servers, and Named Server Groups on page 6*.
- **Named Server Group Accounting Method:** This accounting method specifies that the previously configured group of servers is used to record command entry and connection creation activity on a per-user basis. To use this method for accounting, a named server group must be configured prior to configuring AAA. For more information about configuring named server groups, refer to *Configuring RADIUS Servers, TACACS+ Servers, and Named Server Groups on page 6*.
- **None Accounting Method:** This authorization method specifies that no accounting is performed.

Creating Command Accounting Method Lists

Command accounting method lists specify the types of information recorded when users access specified command levels. Command levels that are included in command accounting method lists are either Level 1 (unprivileged) or Level 15 (privileged) commands.

To create a default command accounting method list, enter the **aaa accounting commands** <*level*> **default [none] [stop-only] [group tacacs+] [group** <*name*>**]** command from the Global Configuration mode prompt. The <*level*> parameter specifies the command level to which this method list pertains. Choices are Level 1 (unprivileged) and Level 15 (privileged). The **none** parameter specifies that no accounting is performed. The **stop-only** parameter specifies that information is recorded only when the connection is terminated. The **group tacacs+** parameter specifies using all TACACS+ servers to store accounting information. The **group** <*name*> parameter specifies using a named server group to store accounting information. The **group** parameters can only be specified once the accounting action has been defined (**none** or **stop-only**). Enter the command as follows (making sure the specified parameters match the accounting needs of your network):

(config)**#aaa accounting commands 15 default stop-only group tacacs+**

Remember that once the default list is configured, it is automatically applied to all line interfaces at a global level.

To create a named command accounting method list, enter the **aaa accounting commands** <*level*> <*listname*> **[none] [stop-only] [group tacacs+] [group** <*name*>**]** command from the Global Configuration mode prompt. Each parameter specifies the accounting method to be attempted. Enter the command as follows (making sure the specified parameters match the accounting needs of your network):

(config)**#aaa accounting commands 15 Accounting1 stop-only group ACCTT1**

Creating Connection Accounting Method Lists

Connection accounting method lists specify the types of information recorded about outbound connections made from the network access server.

To create a default connection accounting method list, enter the **aaa accounting connection default [none] [start-stop] [stop-only] [group tacacs+] [group** <*name*>**]** command from the Global Configuration mode prompt. The **none** parameter specifies that no accounting is performed. The **start-stop** parameter specifies that information is recorded from the beginning of the connection until the connection is terminated. The **stop-only** parameter specifies that information is recorded only when the connection is terminated. The **group tacacs+** parameter specifies using all TACACS+ servers to store accounting information, and the **group** <*name*> specifies using a named server group to store accounting information. The **group** parameters can only be specified once the accounting action has been defined (**none**, **start-stop**, or **stop-only**). Enter the command as follows (making sure the specified parameters match the accounting needs of your network):

(config)**#aaa accounting connection default stop-only group tacacs+**

Remember that once the default list is configured, it is automatically applied to all line interfaces at a global level.

To create a named connection accounting method list, enter the **aaa accounting connection** <*listname*> **[none] [start-stop] [stop-only] [group tacacs+] [group** <*name*>**]** command from the Global Configuration mode prompt. Each parameter specifies the accounting method to be attempted. Enter the command as follows (making sure the order of parameters match the accounting needs of your network):

(config)**#aaa accounting connection Accounting1 start-stop group ACCTT1**

Creating Executive Accounting Method Lists

Executive accounting method lists specify the types of information recorded about inbound connections made by connecting to the line interfaces and creating a terminal session.

To create a default executive accounting method list, enter the **aaa accounting exec default [none] [start-stop] [stop-only] [group tacacs+] [group** <*name*>**]** command from the Global Configuration mode prompt. The **none** parameter specifies that no accounting is performed. The **start-stop** parameter specifies that information is recorded from the beginning of the connection until the connection is terminated. The **stop-only** parameter specifies that information is recorded only when the connection is terminated. The **group tacacs+** parameter specifies using all TACACS+ servers to store accounting information, and the **group** <*name*> specifies using a named server group to store accounting information. The **group** parameters can only be specified once the accounting action has been defined (**none**, **start-stop**, or **stop-only**). Enter the command as follows (making sure the specified parameters match the accounting needs of your network):

(config)**#aaa accounting exec default stop-only group tacacs+**

Remember that once the default list is configured, it is automatically applied to all line interfaces at a global level.

To create a named executive accounting method list, enter the **aaa accounting exec** <*listname*> **[none] [start-stop] [stop-only] [group tacacs+] [group** <*name*>**]** command from the Global Configuration mode prompt. Each parameter specifies the accounting method to be attempted. Enter the command as follows (making sure the specified parameters match the accounting needs of your network):

(config)**#aaa accounting exec Accounting1 start-stop group ACCTT1**

Applying Accounting Method Lists

To apply an AAA accounting command method list to an interface, enter the **accounting commands** <*level*> <*listname*> command from the line interface's configuration mode prompt. The <*level*> parameter is the command level: Level 1 (unprivileged) or Level 15 (privileged). Enter the command as follows:

(config)**#line telnet 0 4**
(config-telnet0-4)**#accounting commands 15 Accounting1**

If you have previously configured a line interface to use a named command accounting method list and want to return to using the default list, enter the **accounting commands** <*level*> **default** command from the interface's configuration mode prompt as follows:

(config)**#line telnet 0 4**
(config-telnet0-4)**#accounting commands 15 default**

To apply an AAA accounting connection method list to a line interface, enter the **accounting connection** <*listname*> command from the line interface's configuration mode prompt as follows:

(config)**#line telnet 0**
(config-telnet0-4)**#accounting connection AcctConn1**

If you have previously configured a line interface to use a named connection accounting method list and want to return to using the default list, enter the **accounting connection default** command from the line interface's configuration mode prompt as follows:

(config)**#line telnet 0 4**
(config-telnet0-4)**#accounting connection default**

To apply an AAA accounting executive method list to a line interface, enter the **accounting exec** <*listname*> command from the line interface's configuration mode prompt as follows:

(config)**#line telnet 0 4**
(config-telnet0-4)**#accounting exec Inboundacct1**

If you have previously configured a line interface to use a named executive method list and want to return to using the default list, enter the **accounting exec default** command from the line interface's configuration mode prompt as follows:

(config)**#line telnet 0 4**
(config-telnet0-4)**#accounting exec default**

Additional Accounting Configurations (Global)

There are additional configuration options for how AAA accounting functions. These options include specifying the handling of users with a NULL user name and specifying how often accounting updates are sent to the server(s). These options are all configured from the Global Configuration mode and are automatically applied to all types of AAA accounting.

Null users are those users whose user name string is NULL. Users might end up with this user name if they come in on a line whose record type is **none** (typically these are users that authenticated with a password-only login or no login). To specify how null user records are handled, use the **aaa accounting suppress null-username** command. By default, all user account information is sent to the accounting server. Entering this command specifies that users with the user name NULL are not sent to the server. Enter the command as follows:

(config)**#aaa accounting suppress null-username**

To specify how often AAA accounting sends recorded information to the accounting server(s), use the **aaa accounting update [newinfo | periodic** <*interval*>**]** command. The **newinfo** parameter specifies that information is sent to the server only when there is new recorded information. The **periodic** parameter specifies recorded information is periodically sent to the server. The <*interval*> parameter specifies the amount of time (in minutes) between sending records. The <*interval*> range is **1** to **2147483647** minutes. By default, accounting records are sent to the server every **5** minutes. To change how often accounting records are sent, enter the command as follows:

(config)**#aaa accounting update newinfo**

AAA Example Configuration

The following example describes some of the common real-world applications of AAA. All configurations are provided through the CLI. The configuration parameters entered in these examples are sample configurations only. You should configure these applications in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration examples to provide you with a method of copying and pasting configurations directly into the CLI. Before copying this configuration into your CLI, you should first make the necessary adjustments to ensure they will function properly in your network.

Figure 4 describes the network in which AAA is configured for this example.

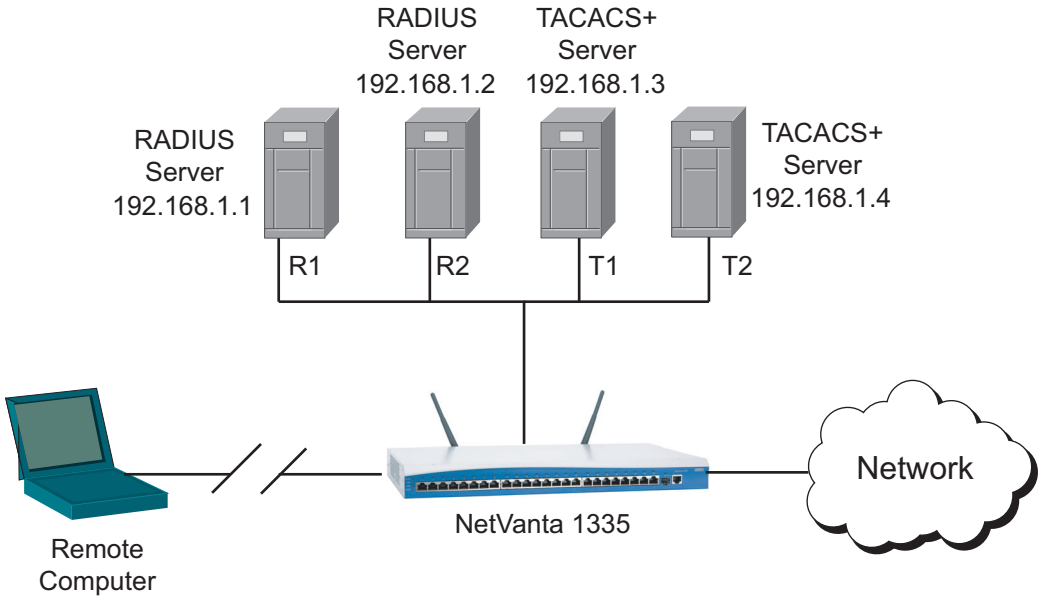

Figure 4. Network with AAA using RADIUS and TACACS+ Servers

In this example, AAA is configured to operate in a typical network situation, in which there are two RADIUS and two TACACS+ servers. The configuration provided configures all four servers, configures the necessary server groups (R1 for authentication, T1 for authorization, and T2 for accounting), and then configures the AAA method lists and applies them to the appropriate line interface.

```
!
aaa on
aaa authentication banner #
User Login Authentication:#
aaa authentication fail-message #
Failed Authentication. Please try again.#
aaa authentication username-prompt Please enter your user name:
aaa authentication password-prompt Please enter your password:
aaa local authentication attempts max-fail 3
aaa processes 2
radius-server key passphrase
!
radius-server host 192.168.1.1
```



```
radius-server host 192.168.1.2
tacacs-server key mykey
tacacs-server host 192.168.1.3
tacacs-server host 192.168.1.4
!
aaa authentication login MyAuth1 group R1Authent enable none
!
aaa authentication enable default enable group radius none
!
aaa authorization console
aaa authorization config-command
aaa authorization command 15 PrivList group T1Author if-authenticated none
aaa authorization exec default if-authenticated
aaa accounting suppress null-username
aaa accounting update periodic 10
aaa accounting commands 15 AcctList stop-only group T2Acct
aaa accounting connection AcctList2 stop-only group T2Acct
aaa accounting exec default start-stop group tacacs+
!
aaa group server radius R1Authent
    server 192.168.1.1
!
aaa group server tacacs+ T1Author
    server 192.168.1.3
aaa group server tacacs+ T2Acct
    server 192.168.1.4
!
line telnet 0 4
    accounting commands 15 AcctList
    accounting connection AcctList2
    login authentication MyAuth1
    authorization commands 15 PrivList
    password mypassword
    no shutdown
!
```

*The commands **aaa local authentication attempts max-fail 3** and **aaa authorization config-command** are enabled by default; therefore, these commands will not appear in the output when the **show running-config** command is issued.*

Command Summary

The following tables provide a summary of the commands necessary to configure AAA in AOS.

Table 1. AAA Global Configuration Commands

Command	Subcommand	Prompt	Description
aaa on		(config)#	Enables AAA. AAA must be enabled for additional AAA configuration commands to be available. If AAA is enabled, AAA methods will override other security methods specified in the line interface.
aaa processes <*value*>		(config)#	Specifies the number of threads available for AAA background processes. By default, the number of threads is set to **1**. Range is **1** to **64**. Increasing the number of threads can speed up simultaneous authentication processes, but can do so at the cost of system resources (for example, memory).
aaa local authentication attempts max-fail <*number*>		(config)#	Specifies the maximum number of login attemps allowed before closing the session during AAA authentication. Attempt range is **1** to **25**. By default, the session closes after **3** failed attempts.
aaa authentication banner <*banner*>		(config)#	Specifies the banner shown during AAA login/authentication. The <*banner*> parameter is the text message which must begin with a delimiter (for example, **:**, **'**, or **#**) and must end with the same delimiter. By default, the authentication banner is **User Access Verification**.
aaa authentication fail-message <*message*>		(config)#	Specifies the message shown if user authentication fails. The <*message*> parameter is the text message which must begin with a delimiter (for example, **:**, **'**, or **#**) and must end with the same delimiter. By default, the failed authentication message is **%Authentication failed**.

Table 1. AAA Global Configuration Commands *(Continued)*

Command	Subcommand	Prompt	Description
aaa authentication password-prompt *<prompt>*		(config)#	Specifies the message shown when prompting a user for their password. The *<prompt>* parameter is a single line of text enclosed in quotation marks. The default prompt is **Password:**.
aaa authentication username-prompt *<prompt>*		(config)#	Specifies the message shown when prompting a user for their user name. The *<prompt>* parameter is a single line of text enclosed in quotation marks. The default prompt is **Username:**.
aaa authorization config-command		(config)#	Enables AAA authorization for configuration mode commands. By default, authorization for configuration commands is enabled.
aaa authorization console		(config)#	Enables AAA authorization to be applied to the console. By default, authorization for console access is disabled.
aaa accounting suppress null-username		(config)#	Specifies that AAA accounting records for users with a NULL user name are not sent to the AAA accounting server. By default, records of all user accounts, including NULL user names, are sent to the server.
aaa accounting update [newinfo | periodic *<interval>***]**		(config)#	Specifies when AAA accounting records are sent to the AAA accounting server. The **newinfo** parameter specifies records are sent whenever there is new information. The **periodic** parameter specifies records are sent at periodic intervals. The *<interval>* parameter specifies the amount of time (in minutes) between sending records. By default, accounting records are sent to the server every **5** minutes. Interval range is **1** to **2147483647**.

Table 2. Global RADIUS and TACACS+ Server Configuration Commands

Command	Subcommand	Prompt	Description
radius-server challenge-noecho		(config)#	Specifies that when users enter text in response to challenge questions the entered text does not appear on the screen. By default, echo is disabled and users do not see on-screen what they enter.
radius-server deadtime <*value*>		(config)#	Specifies the time to wait before attempting to reconnect to a RADIUS server that has timed out. The <*value*> parameter is the time period in minutes. Range is **0** to **1440** minutes. By default, the time to wait is set to **0** minutes. Changing this parameter changes the time to wait for all configured RADIUS servers.
radius-server enable-username <*name*>		(config)#	Specifies a user name to be used for authentication to enter the Enable mode. This user name is the name sent for AAA Enable mode access requests. By default, all RADIUS servers use the user name **$enab15$**. Changing this parameter changes the user name for all configured RADIUS servers.
radius-server key <*key*>		(config)#	Specifies the encryption key shared with all RADIUS servers. By default, no key is configured. Using this command specifies the same key is used by all RADIUS servers, although the key used by a server can be changed on a per-server basis.
radius-server retry <*number*>		(config)#	Specifies the number of connection attempts to a RADIUS server. By default, **0** attempts are made. Range is **0** to **10**. This is a global setting; however, it can be overridden on a per-server basis.

Table 2. Global RADIUS and TACACS+ Server Configuration Commands *(Continued)*

Command	Subcommand	Prompt	Description
radius-server timeout *<value>*		(config)#	Specifies the amount of time (in seconds) that RADIUS servers have to respond to a request. The *<value>* range is **1** to **1000** seconds. By default, the timeout value is set to **5** seconds. This is a global setting; however, it can be overridden on a per-server basis.
tacacs-server key *<key>*		(config)#	Specifies the encryption key used by all TACACS+ servers. By default, no key is configured. This is a global setting; however, it can be overridden on a per-server basis.
tacacs-server packet maxsize *<value>*		(config)#	Specifies the maximum packet size that can be sent to any TACACS+ server. The *<value>* range is **10240** to **65535** kilobytes. By default, the packet size is set to **10240** kb.
tacacs-server timeout *<value>*		(config)#	Specifies the time (in seconds) that the AOS unit will wait for the server's reply before declaring an error. The *<value>* range is **1** to **1000** seconds. By default, the AOS unit will wait **5** seconds before declaring an error. This is a global setting; however, it can be overridden on a per-server basis.

Table 3. Individual RADIUS and TACACS+ Server Configuration Commands

Command	Subcommand	Prompt	Description
radius-server host *<hostname | ip address>*		(config)#	Specifies a RADIUS server and enters the server's configuration mode. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). This command has various subcommands that are entered in the same command line. The subcommands can be entered in any order (except the **key** subcommand which must come last). Each subcommand can only be used once.

Table 3. Individual RADIUS and TACACS+ Server Configuration Commands *(Continued)*

Command	Subcommand	Prompt	Description
	acct-port <*port*>	After previous command	Specifies the UDP port used by the AAA accounting server. The <*port*> range is **0** to **65535**. By default, servers will use port **1813** for accounting. This command is reserved for future use as currently AOS does not allow RADIUS servers for use with accounting.
	auth-port <*port*>	After previous command	Specifies the UDP port used by the AAA authentication server. The <*port*> range is **0** to **65535**. By default, servers will use port **1812** for authorization.
	key <*key*>	After previous command	Specifies the encryption key used by the RADIUS server. This subcommand overrides the global RADIUS key setting. This subcommand must be entered last in the line because everything after the **key** keyword is read as the new key.
	retransmit <*number*>	After previous command	Specifies the number of connection attempts made to the server. The <*number*> range is **1** to **100**. The default value of this subcommand is the value set by the **radius-server retry** command.
	timeout <*value*>	After previous command	Specifies the time to wait (in seconds) for this server to reply to requests. The <*value*> range is **1** to **1000** seconds. The default value of this subcommand is the value set by the **radius-server timeout** command.

Table 3. Individual RADIUS and TACACS+ Server Configuration Commands *(Continued)*

Command	Subcommand	Prompt	Description
tacacs-server host <*hostname* | *ip address*>		(config)#	Specifies a TACACS+ server and enters the server's configuration mode. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). This command has various subcommands that are entered in the same command line. The subcommands can be entered in any order (except the **key** subcommand) but can only be used once.
	key <*key*>	After previous command	Specifies the encryption key used by the TACACS+ server. This subcommand overrides the global TACACS+ key setting. This subcommand must be entered last in the line because everything after the **key** keyword is read as the new key.
	port <*port*>	After previous command	Specifies the TCP port used by the TACACS+ server. Port range is **1** to **65535**. By default, the TACACS+ server is set to use TCP port **49**.
	timeout <*value*>	After previous command	Specifies the time to wait (in seconds) for the server to reply to requests. The <*value*> range is **1** to **1000** seconds. The default value is the value set by the **tacacs-server timeout** command.

Table 4. AAA Server Groups Configuration Commands

Command	Subcommand	Prompt	Description
aaa group server [radius | tacacs+] <*group name*>		(config)#	Creates a group of RADIUS or TACACS+ servers. Servers must be configured before they can be added to the group.
	server <*hostname* | *ip address*>	(config-sg-radius)#	Specifies a RADIUS or TACACS+ server to add to the server group. Express IP addresses in decimal dotted notation (for example, **10.10.10.1**).

Table 4. AAA Server Groups Configuration Commands *(Continued)*

Command	Subcommand	Prompt	Description
	acct-port <*port*>	After previous command (only applies if the **aaa group server radius** command was entered previously)	Specifies the UDP port for accounting services with the RADIUS server being added to the RADIUS server group. Port range is **0** to **65535**. By default, the accounting port is set to **1813**. This command is reserved for future use as currently AOS does not allow RADIUS servers for use with accounting.
	auth-port <*port*>	After previous command (only applies if the **aaa group server radius** command was entered previously)	Specifies the UDP port for authentication services with the RADIUS server being added to the RADIUS server group. Port range is **0** to **65535**. By default, the authentication port is set to **1812**.

Table 5. Authentication Methods List Configuration Commands

Command	Subcommand	Prompt	Description
aaa authentication login [default | <*listname*>**]**		(config)#	Creates and defines a default or named methods list for authentication. Methods are entered using the subcommands. The order in which the methods are entered is the order in which they are used.
	enable	After previous command	Specifies using the Enable mode password as the authentication method. To use this method, the Enable mode password must be defined (using the **enable password** <*password*> command from the Global Configuration mode prompt).
	group radius	After previous command	Specifies using all RADIUS servers for authentication. RADIUS servers must be configured to use this method.
	group tacacs+	After previous command	Specifies using all TACACS+ servers for authentication. TACACS+ servers must be configured to use this method.

Table 5. Authentication Methods List Configuration Commands *(Continued)*

Command	Subcommand	Prompt	Description
	group <*name*>	After previous command	Specifies using a subset of either RADIUS or TACACS+ servers for authentication. Subsets are named server groups created using the **aaa group server** command. A server group must be configured to use this method.
	local	After previous command	Specifies using the local user name for authentication. User names must be in the local user name database to use this method. User names are set using the **username** <*user name*> **password** <*password*> command from the Global Configuration mode prompt.
	line	After previous command	Specifies using the password applied to the line the user is logged into (Telnet or console) for authentication. The line password must be configured to use this method (using the **password** <*password*> command from the line interface configuration mode).
	none	After previous command	Specifies that no authentication is used. This method should appear at the end of the methods list and is used primarily to prevent a lock-out situation.
aaa authentication enable default		(config)#	Creates and defines the default authentication methods list used for access to Enable (privileged) mode. Methods are entered using the subcommands. The order in which the methods are entered is the order in which they are used.

Table 5. Authentication Methods List Configuration Commands *(Continued)*

Command	Subcommand	Prompt	Description
	enable	After previous command	Specifies using the Enable mode password as the authentication method. The Enable mode password must be defined to use this method (using the **enable password** <*password*> command from the Global Configuration mode prompt). If the request is going to a RADIUS server, the user name **$enab15$** is sent by default. If the request is going to a TACACS+ server, the user name used for login authentication is sent by default.
	group radius	After previous command	Specifies using all RADIUS servers for authentication. RADIUS servers must be configured to use this method.
	group tacacs+	After previous command	Specifies using all TACACS+ servers for authentication. TACACS+ servers must be configured to use this method.
	group <*name*>	After previous command	Specifies using a subset of either RADIUS or TACACS+ servers for authentication. Subsets are named server groups created using the **aaa group server** command. A server group must be configured to use this method.
	line	After previous command	Specifies using the password applied to the line the user is logged into (Telnet or console) for authentication. The line password must be configured to use this method (using the **password** <*password*> command from the line interface configuration mode).
	none	After previous command	Specifies that no authentication is used. This method should appear at the end of the methods list and is used primarily to prevent a lock-out situation.

Table 5. Authentication Methods List Configuration Commands *(Continued)*

Command	Subcommand	Prompt	Description
aaa authentication port-auth default		(config)#	Creates and defines the default methods list for port authentication. Methods are entered using the subcommands. The order in which the methods are entered is the order in which they are used.
	group radius	After previous command	Specifies using all RADIUS servers for authentication. RADIUS servers must be configured to use this method.
	group <*name*>	After previous command	Specifies using a subset of RADIUS servers for authentication. Subsets are named server groups created using the **aaa group server** command. A server group must be configured to use this method.
	local	After previous command	Specifies using the local user name for authentication. User names must be in the local user name database to use this method. User names are set using the **username** <*user name*> **password** <*password*> command from the Global Configuration mode prompt.
	none	After previous command	Specifies that no authentication is used. This method should appear at the end of the methods list and is used primarily to prevent a lock-out situation.

Table 6. Authentication Methods List Application Commands

Command	Subcommand	Prompt	Description
login authentication *<listname>*		(config-line interface)#	Applies a specific AAA login method list to the line interface, and uses this list to authenticate users connecting to the interface. If AAA is enabled, but no login authentication list is specified, the default list is used. If the default list is used but the default list is not configured, the behavior for consoles is to allow all users and Telnet/SSH interfaces use the local user database. AAA must be enabled to apply a login authentication list to a line interface.
client authentication server list *<listname>*		(config-ike)#	Specifies an authentication list to use in client/server authentication in the IKE policy. AAA must be enabled to apply this list.
ftp authentication *<listname>*		(config)#	Specifies an AAA authentication list to be used by the AOS FTP server. AAA must be enabled to apply this list. If AAA is enabled but no list has been assigned to the FTP server, the FTP server automatically uses the local user list for authentication.
ip http authentication *<listname>*		(config)#	Specifies an AAA authentication list to use in authentication to the AOS device's HTTP server. AAA must be enabled to apply this list.

Table 7. Authorization Methods List Configuration Commands

Command	Subcommand	Prompt	Description
aaa authorization commands *<level>* **[default |** *<listname>***]**		(config)#	Creates and defines a default or named authorization methods list for command use authorization. Methods are entered using the subcommands. The order in which the methods are entered is the order in which they are used. The *<level>* parameter specifies the command level, choosing between Level **1** (unprivileged) or Level **15** (privileged).
	group tacacs+	After previous command	Specifies using all TACACS+ servers for authorization. TACACS+ servers must be configured to use this method.

Table 7. Authorization Methods List Configuration Commands *(Continued)*

Command	Subcommand	Prompt	Description
	group <*name*>	After previous command	Specifies using a subset of TACACS+ servers for authorization. Subsets are named server groups created using the **aaa group server** command. A server group must be configured to use this method.
	if-authenticated	After previous command	Specifies that authorization is successful if the user has already been authenticated. AAA authentication must be configured to use this method.
	none	After previous command	Specifies no authorization methods are used. This method should appear at the end of the methods list and is used primarily to prevent a lock-out situation.
aaa authorization exec [default | <*listname*>**]**		(config)#	Creates and defines a default or named authorization methods list for access to the Enable mode in the CLI. Methods are entered using the subcommands. The order in which the methods are entered is the order in which they are used.
	group tacacs+	After previous command	Specifies using all TACACS+ servers for authorization. TACACS+ servers must be configured to use this method.
	group <*name*>	After previous command	Specifies using a subset of TACACS+ servers for authorization. Subsets are named server groups created using the **aaa group server** command. A server group must be configured to use this method.
	if-authenticated	After previous command	Specifies that authorization is successful if the user has already been authenticated. AAA authentication must be configured to use this method.
	none	After previous command	Specifies no authorization methods are used. This method should appear at the end of the method list and is used primarily to prevent a lock-out situation.

Table 8. Authorization Methods List Application Commands

Command	Subcommand	Prompt	Description
authorization commands *<level>* **[default |** *<listname>***]**		(config-line interface)#	Applies the default or named command authorization method list to the line interface. The *<level>* parameter specifies whether the list applies to Level **1** (unprivileged) or Level **15** (privileged) commands. AAA must be enabled to apply an authorization list to a line interface.
authorization exec [default | *<listname>***]**		(config-line interface)#	Applies the default or named CLI Enable mode authorization method list to the line interface. AAA must be enabled to apply an authorization list to a line interface.

Table 9. Accounting Methods List Configuration Commands

Command	Subcommand	Prompt	Description
aaa accounting commands *<level>* **[default |** *<listname>***]**		(config)#	Creates and defines a default or named accounting method list that provides information about the executive commands a user enters. The *<level>* parameter specifies whether the list applies to Level **1** (unprivileged) or Level **15** (privileged) commands. Methods are entered using the subcommands. The order in which the methods are entered is the order in which they are used.
	none	After previous command	Specifies no accounting methods are used. This method should appear at the end of the method list.
	stop-only	After previous command	Specifies that information is recorded when the connection terminates.
	group tacacs+	After previous command	Specifies using all TACACS+ servers for accounting records. TACACS+ servers must be configured to use this method.
	group *<name>*	After previous command	Specifies using a subset of TACACS+ servers for accounting. Subsets are named server groups created using the **aaa group server** command. A server group must be configured to use this method.
aaa accounting connection [default | *<listname>***]**		(config)#	Creates and defines a default or named accounting method list that focuses on providing information about outbound connections made from the AOS unit. Methods are entered using the subcommands. The order in which the methods are entered is the order in which they are used.

Table 9. Accounting Methods List Configuration Commands *(Continued)*

Command	Subcommand	Prompt	Description
	none	After previous command	Specifies no accounting methods are used. This method should appear at the end of the method list.
	start-stop	After previous command	Specifies that information is recorded when the connection begins and when the connection terminates.
	stop-only	After previous command	Specifies that information is recorded when the connection terminates.
	group tacacs+	After previous command	Specifies using all TACACS+ servers for accounting records. TACACS+ servers must be configured to use this method.
	group <*name*>	After previous command	Specifies using a subset of TACACS+ servers for accounting. Subsets are named server groups created using the **aaa group server** command. A server group must be configured to use this method.
aaa accounting exec [default | <*listname*>**]**		(config)#	Creates and defines a default or named accounting method list that focuses on information about inbound connections (user terminal sessions). Methods are entered using the subcommands. The order in which the methods are entered is the order in which they are used.
	none	After previous command	Specifies no accounting methods are used. This method should appear at the end of the method list.
	start-stop	After previous command	Specifies that information is recorded when the connection begins and when the connection terminates.
	stop-only	After previous command	Specifies that information is recorded when the connection terminates.
	group tacacs+	After previous command	Specifies using all TACACS+ servers for accounting records. TACACS+ servers must be configured to use this method.
	group <*name*>	After previous command	Specifies using a subset of TACACS+ servers for accounting. Subsets are named server groups created using the **aaa group server** command. A server group must be configured to use this method.

Table 10. Accounting Methods List Application Commands

Command	Subcommand	Prompt	Description
accounting commands *<level>* **[default |** *<listname>*		(config-line interface)#	Applies the default or named command accounting list to the line interface. The *<level>* parameter specifies whether the list applies to Level **1** (unprivileged) or Level **15** (privileged) commands. AAA must be enabled to apply accounting lists to a line interface.
accounting connection [default | *<listname>***]**		(config-line interface)#	Applies the default or named connection accounting list to the line interface. Connection lists record information about outbound connections made from the AOS unit. AAA must be enabled to apply accounting lists to a line interface.
accounting exec [default | *<listname>***]**		(config-line interface)#	Applies the default or named executive accounting list to the interface. Executive lists record information about inbound connections made to the AOS unit (user terminal sessions). AAA must be enabled to apply accounting lists to a line interface.

Troubleshooting

Troubleshooting can be done from the CLI, providing AAA debug information that can help you analyze your AAA configuration.

CLI troubleshooting for AAA works by using the **debug aaa**, **debug radius**, and **debug tacacs+** commands. By enabling **debug** commands, debug messages are sent to alert you when specified events occur. These messages can be beneficial when troubleshooting your configuration.

The **debug aaa** command is issued from the Enable mode prompt and records and displays AAA events, such as connection notices, applied method lists, login attempts, and session tracking. The following is sample output from the **debug aaa** command:

```
>enable
#debug aaa
AAA: New Session on portal 'TELNET 0 (172.22.12.60:4867)'.
AAA: No list mapped to 'TELNET 0'. Using 'default'.
AAA: Attempting authentication (username/password).
AAA: RADIUS authentication failed.
AAA: Authentication failed.
AAA: Closing Session on portal 'TELNET 0 (172.22.12.60:4867)'.
```

*Using **debug** commands can be very processor intensive, and should be used with caution.*

The **debug radius** command is also issued from the Enable mode prompt and records and displays information about the RADIUS server operation. The following is sample output from the **debug radius** command:

```
>enable
#debug radius
RADIUS AUTHENTICATION: Sending packet to 172.22.48.1 (1645).
RADIUS AUTHENTICATION: Received response form 172.22.48.1.
```

The **debug tacacs+ [events] [packets]** command is also issued from the Enable mode prompt and records and displays information about the TACACS+ subsystem. The **events** parameter specifies that TACACS+ event messages are displayed, and the **packets** parameter specifies that TACACS+ packet messages are displayed. The following is sample output from the **debug tacacs+** command:

```
>enable
#debug tacacs+
TAC+ EVENT: Trying group 'tacacs+'
    TAC+ EVENT: Attempting connection to host '10.23.131.200'.
    TAC+ EVENT: Sending Authentication START pkt
    TAC+ TX: Authentication START
        TAC+ TX: version=0xc0, type=Authentication, seq_no=1, flags=00
        TAC+ TX: action=Login
        TAC+ TX: level=1
```



```
        TAC+ TX: authen type=ASCII
        TAC+ TX: requested service=Login
        TAC+ TX: username=
        TAC+ TX: port=TELNET 1 (10.23.1.189:3183)
        TAC+ TX: remote address=10.23.1.189
    TAC+ EVENT: Received Authentication REPLY pkt
    TAC+ RX: Authentication REPLY
        TAC+ RX: version=0xc0, type=Authentication, seq_no=2, flags=00
        TAC+ RX: status=GETUSER
        TAC+ RX: flags=00
        TAC+ RX: server msg=
            User Access Verification
            Username:
    TAC+ EVENT: Sending Authentication CONTINUE pkt
    TAC+ TX: Authentication CONTINUE
        TAC+ TX: version=0xc0, type=Authentication, seq_no=3, flags=00
        TAC+ TX: user message=********
        TAC+ TX: flags=0x00
    TAC+ EVENT: Received Authentication REPLY pkt
    TAC+ RX: Authentication REPLY
        TAC+ RX: version=0xc0, type=Authentication, seq_no=4, flags=00
        TAC+ RX: status=GETPASS
        TAC+ RX: flags=0x01
        TAC+ RX: server msg=Password:
    TAC+ EVENT: Sending Authentication CONTINUE pkt
    TAC+ TX: Authentication CONTINUE
        TAC+ TX: version=0xc0, type=Authentication, seq_no=5, flags=00
        TAC+ TX: user message=********
        TAC+ TX: flags=0x00
    TAC+ EVENT: Received Authentication REPLY pkt
    TAC+ RX: Authentication REPLY
        TAC+ RX: version=0xc0, type=Authentication, seq_no=6, flags=00
        TAC+ RX: status=PASS
        TAC+ RX: flags=00
        TAC+ RX: server msg=
    TAC+ EVENT: Authentication PASSED
```

