

AAA Overview

Access control is the way you control who is allowed access to the network server and what services they are allowed to use once they have access. Authentication, Authorization, and Accounting (AAA) network security services provide the primary framework through which you set up access control on your router or access server.

AAA Security Services

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

- **Authentication**—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption.

Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which, by coincidence, is named “default”). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list.

All authentication methods, except for local, line password, and enable authentication, must be defined through AAA. For information about configuring all authentication methods, including those implemented outside of the AAA security services, refer to the “Configuring Authentication” chapter in this manual.

- **Authorization**—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user’s actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. All authorization methods must be defined through AAA. When AAA authorization is activated, it is applied equally to all interfaces on the access server or router. For information about configuring authorization using AAA, refer to the “Configuring Authorization” chapter in this manual.

- Accounting—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. When AAA accounting is activated, it is applied equally to all interfaces on the access server or router. For information about configuring accounting using AAA, refer to the “Configuring Accounting” chapter in this manual.

In many circumstances, AAA uses protocols such as RADIUS, TACACS+, and Kerberos to administer its security functions. If your router or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS, TACACS+, or Kerberos security server.

Although AAA is the primary (and recommended) method for access control, Cisco IOS software provides additional features for simple access control that are outside the scope of AAA, such as local username authentication, line password authentication, and enable password authentication. However, these features do not provide the same degree of access control that is possible by using AAA.

Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control
- Scalability
- Standardized authentication methods, such as RADIUS, TACACS+, and Kerberos
- Multiple backup systems

Note The deprecated protocols, TACACS and Extended TACACS, are not compatible with AAA; if you select these security protocols, you will not be able to take advantage of the AAA security services.

AAA Philosophy

AAA is designed to enable you to dynamically configure the type of authentication and authorization you want on a per-line (per-user) or per-service (for example, IP, IPX, or VPDN) basis. You define the type of authentication and authorization you want by creating method lists, then applying those method lists to specific services or interfaces.

For information about applications that use AAA, such as per-user configuration and virtual profiles, refer to the “Per-User Configuration” and “Configuring Virtual Profiles” chapters in the *Dial Solutions Configuration Guide*.

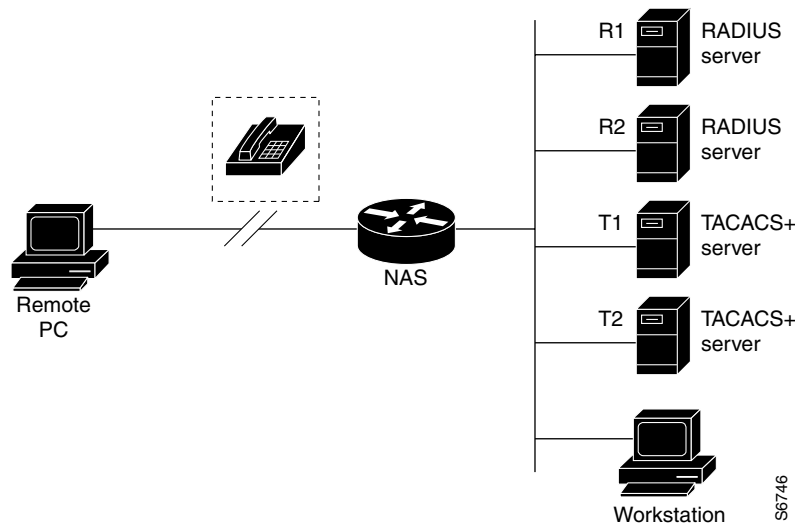
Method Lists

A method list is simply a list defining the authentication methods to be used, in sequence, to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. Cisco IOS software uses the first method listed to authenticate users; if that method fails to respond, the Cisco IOS software selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method or the authentication method list is exhausted, in which case authentication fails.

Note The Cisco IOS software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops and no other authentication methods are attempted.

Figure 2 shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers and T1 and T2 are TACACS+ servers.

Figure 2 Typical AAA Network Configuration



Suppose the system administrator has defined a method list where R1 will be contacted first for authentication information, then R2, T1, T2, and then finally the local username database on the access server itself. When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 fails to respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern would continue through the remaining designated methods until the user is either authenticated, rejected, or the session terminated. If all of the authentication methods fail, which the network access server would process as a failure, the session would be terminated.

Note A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has failed to respond to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

Where to Begin

You must first decide what kind of security solution you want to implement. You need to assess the security risks in your particular network and decide on the appropriate means to prevent unauthorized entry and attack. For more information about assessing your security risks and possible security solutions, refer to the “Security Overview” chapter in this manual. We recommend that you use AAA, no matter how minor your security needs might be.

Overview of the AAA Configuration Process

Configuring AAA is relatively simple after you understand the basic process involved. To configure security on a Cisco router or access server using AAA, follow this process:

- 1 Enable AAA by using the **aaa new-model** global configuration command.
- 2 If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
- 3 Define the method lists for authentication by using the **aaa authentication** command.
- 4 Apply the method lists to a particular interface or line, if required.
- 5 (Optional) Configure authorization using the **aaa authorization** command.
- 6 (Optional) Configure accounting using the **aaa accounting** command.

For a complete description of the commands used in this chapter, refer to the “Authentication Commands” chapter of the Security Command Reference. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Enable AAA

Before you can use any of the services AAA network security services provide, you need to enable AAA.

To enable AAA, perform the following task in global configuration mode:

Task	Command
Enable AAA.	aaa new-model

Note When you enable AAA, you can no longer access the commands to configure the older deprecated protocols, TACACS or Extended TACACS. If you decided to use TACACS or Extended TACACS in your security solution, do not enable AAA.

Disable AAA

You can disable AAA functionality with a single command if, for some reason, you decide that your security needs cannot be met by AAA but can be met by using TACACS, Extended TACACS, or a line security method that can be implemented without AAA.

To disable AAA, perform the following task in global configuration mode:

Task	Command
Disable AAA.	<code>no aaa new-model</code>

What To Do Next

Once you have enabled AAA, you are ready to configure the other elements relating to your selected security solution. Table 2 describes the configuration tasks you might want to complete and where to find that information.

Table 2 AAA Access Control Security Solutions Methods

Task	Location in Security Configuration Guide	Process Step
Configure local login authentication.	Configuring Authentication	3
Control login using security server authentication.	Configuring Authentication	3
Define method lists for authentication.	Configuring Authentication	3
Apply method lists to a particular interface or line.	Configuring Authentication	3
Configure RADIUS security protocol parameters.	Configuring RADIUS	2
Configure TACACS+ security protocol parameters.	Configuring TACACS+	2
Configure Kerberos security protocol parameters.	Configuring Kerberos	2
Enable TACACS+ authorization.	Configuring Authorization	5
Enable RADIUS authorization.	Configuring Authorization	5
View supported IETF RADIUS attributes.	RADIUS Attributes	2
View supported vendor-specific RADIUS attributes.	RADIUS Attributes	2
View supported TACACS+ AV pairs.	TACACS+ AV Pairs	2
Enable accounting.	Configuring Accounting	6

If you have elected not to use the AAA security services, Table 3 describes the configuration tasks you might want to complete and where to find that information.

Table 3 Non-AAA Access Control Security Solutions Methods

Tasks	Chapter Location
Configure login authentication.	Configuring Authentication
Configure TACACS.	Configuring TACACS and Extended TACACS
Configure Extended TACACS.	Configuring TACACS and Extended TACACS

