

Configuring Basic AAA on an Access Server

Document ID: 10384

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

Network Diagram

General AAA Configuration

Enabling AAA

Specifying the External AAA Server

AAA Server Configuration

Configuring Authentication

Login Authentication

PPP Authentication

Configuring Authorization

Exec Authorization

Network Authorization

Configuring Accounting

Configuring Accounting Examples

Related Information

Introduction

This document explains how to configure Authentication, Authorization, and Accounting (AAA) on a Cisco router using Radius or TACACS+ protocols. The goal of this document is not to cover all AAA features, but to explain the main commands and provide some examples and guidelines.

Note: Please read the section on General AAA Configuration before proceeding with the Cisco IOS® configuration. Failure to do so may result in misconfiguration and subsequent lockout.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

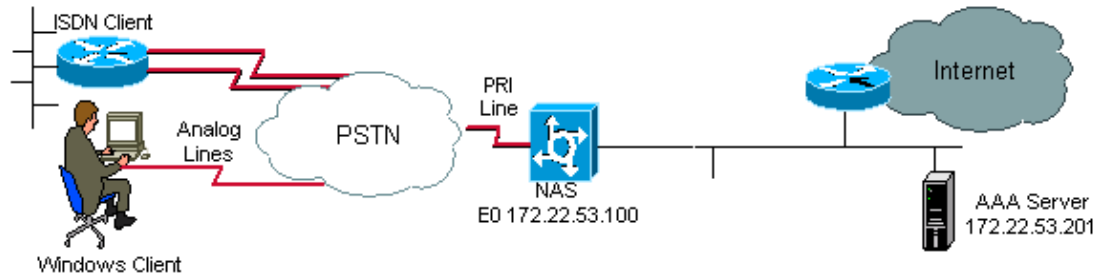
To get an overview of AAA, and for complete details about AAA commands and options, please refer to the IOS 12.2 Security Configuration Guide:Authentication, Authorization, and Accounting.

Components Used

The information in this document is based on Cisco IOS software release 12.1 main line.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Network Diagram



General AAA Configuration

Enabling AAA

To enable AAA, you need to configure the **aaa new-model** command in global configuration.

Note: Until this command is enabled, all other AAA commands are hidden.



Warning: The **aaa new-model** command immediately applies local authentication to all lines and

interfaces (except console line **line con 0**). If a telnet session is opened to the router after enabling this command (or if a connection times out and has to reconnect), then the user has to be authenticated using the local database of the router. To avoid being locked out of the router, we recommend that you define a username and password on the access server before starting the AAA configuration. Do this as follows:

```
username xxx password yyy
```

Tip: Save your configuration prior to configuring your AAA commands. Only after you have completed all your AAA configuration (and are satisfied that it works correctly) should you save the configuration again. This allows you to recover from unforeseen lockouts (prior to saving the configuration) by reloading the router.

Specifying the External AAA Server

In global configuration, define the security protocol used with AAA (Radius, TACACS+). If you do not want to use either of these two protocols, you can use the local database on the router.

If you are using TACACS+, use the **tacacs-server host** *<IP address of the AAA server>* *<key>* command.

If you are using Radius, use the **radius-server host** *<IP address of the AAA server>* *<key>* command.

AAA Server Configuration

On the AAA server, configure the following parameters:

- The name of the access server.
- The IP address the access server uses to communicate with the AAA server.

Note: If both devices are on the same Ethernet network then, by default, the access server uses the IP address defined on the Ethernet interface when sending out the AAA packet. This issue is important

when the router has multiple interfaces (and hence multiple addresses).

- The exact same key <key> configured in the access server.

Note: The key is case-sensitive.

- The protocol used by the access server (TACACS+ or Radius).

Refer to your AAA server documentation for the exact procedure used to configure the above parameters. If the AAA server is not correctly configured, then AAA requests from the NAS will be ignored by the AAA server and the connection may fail.

The AAA server has to be IP reachable from the access server (conduct a **ping** test to verify connectivity).

Configuring Authentication

Authentication verifies users before they are allowed access to the network and network services (which are verified with authorization).

To configure AAA authentication :

1. First define a named list of authentication methods (in global configuration mode).
2. Apply that list to one or more interfaces (in interface configuration mode).

The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

The authentication examples below use Radius, login and Point-to-Point Protocol (PPP) authentication (the most commonly-used) to explain concepts such as methods, and named lists. In all the examples, TACACS+ can be substituted for Radius or local authentication.

The Cisco IOS software uses the first method listed to authenticate users. If that method fails to respond (indicated by an ERROR), 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 all methods defined in the method list are exhausted.

It is important to note that 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 AAA server or local username database responds by denying the user access (indicated by a FAIL), the authentication process stops and no other authentication methods are attempted.

To allow a user authentication, you must configure the username and the password on the AAA server.

Login Authentication

You can use the **aaa authentication login** command to authenticate users who want exec access into the access server (tty, vty, console and aux).

Example 1: Exec Access using Radius then Local

```
aaa authentication login default group radius local
```

In the command above:

- the named list is the default one (default).
- there are two authentication methods (group radius and local).

All users are authenticated using the Radius server (the first method). If the Radius server doesn't respond, then the router's local database is used (the second method). For local authentication, define the username name and password:

```
username xxx password yyy
```

Because we are using the list default in the **aaa authentication login** command, login authentication is automatically applied for all login connections (such as tty, vty, console and aux).

Note: The server (Radius or TACACS+) will not reply to an **aaa authentication** request sent by the access server if there is no IP connectivity, if the access server is not correctly defined on the AAA server or the AAA server is not correctly defined on the access server.

Note: Using the example above, if we do not include the local keyword, we have:

```
aaa authentication login default group radius
```

Note: If the AAA server does not reply to the authentication request, the authentication will fail (since the router does not have an alternate method to try).

Note: The **group** keyword provides a way to group existing server hosts. The feature allows the user to select a subset of the configured server hosts and use them for a particular service. For more information on this advanced feature, refer to the document AAA Server–Group.

Example 2: Console Access Using Line Password

Let's expand the configuration from Example 1 so that console login is only authenticated by the password set on line con 0.

The list CONSOLE is defined and then applied to line con 0.

We configure:

```
aaa authentication login CONSOLE line
```

In the command above:

- the named list is CONSOLE.
- there is only one authentication method (line).

Once a named list (in this example, CONSOLE) is created, it must be applied to a line or interface for it to come into effect. This is done using the **login authentication list_name** command:

```
line con 0
  exec-timeout 0 0
  password cisco
  login authentication CONSOLE
```

The CONSOLE list overrides the default method list default on line con 0. You need to enter the password "cisco" (configured on line con 0) to get console access. The default list is still used on tty, vty and aux.

Note: To have console access authenticated by a local username and password, use:

```
aaa authentication login CONSOLE local
```

Note: In this case, a username and password have to be configured in the local database of the router. The list must also be applied to the line or interface.

Note: To have no authentication, use

```
aaa authentication login CONSOLE none
```

Note: In this case, there is no authentication to get to the console access. The list must also be applied to the line or interface.

Example 3: Enable Mode Access Using External AAA Server

You can issue authentication to get to enable mode (privilege 15).

We configure :

```
aaa authentication enable default group radius enable
```

Only the password will be requested, the username is \$enab15\$. Hence the username \$enab15\$ must be defined on the AAA server.

If the Radius server doesn't reply, the enable password configured locally on the router will have to be entered.

PPP Authentication

The **aaa authentication ppp** command is used to authenticate a PPP connection. It's typically used to authenticate ISDN or analog remote users who want to access the Internet or a central office through an access server.

Example 1: Single PPP Authentication Method for All Users

The access server has an ISDN interface which is configured to accept PPP dialin clients. We use a **dialer rotary-group 0** but the configuration can be done on the main interface or dialer profile interface.

We configure

```
aaa authentication ppp default group radius local
```

This command authenticates all PPP users using Radius. If the Radius server doesn't reply, the local database is used.

Example 2: PPP Authentication using a Specific List

To use a named list rather than the default list, configure the following commands:

```
aaa authentication ppp ISDN_USER group radius  
  
int dialer 0  
  ppp authentication chap ISDN_USER
```

In this example, the list is ISDN_USER and the method is Radius.

Example 3 : PPP Launched from within Character Mode Session

The access-server has an internal modem card (Mica, Microcom or Next Port). Let's assume that both **aaa authentication login** and **aaa authentication ppp** commands are configured.

If a modem user first accesses the router using a character mode exec session (for example, using Terminal Window after Dial), the user is authenticated on a tty line. To launch into a packet mode session, users must type **ppp default** or **ppp**. Since PPP authentication is explicitly configured (with **aaa authentication ppp**), the user is authenticated at the PPP level again.

To avoid this second authentication, we can use the **if-needed** keyword.

```
aaa authentication login default group radius local
aaa authentication ppp default group radius local if-needed
```

Note: If the client starts a PPP session directly, PPP authentication is directly performed since there is no login access to the access server.

For more information on AAA authentication, refer to the documents *IOS 12.2 Security Configuration Guide: Configuring Authentication and Cisco AAA Implementation Case Study*.

Configuring Authorization

Authorization is the process by which you can control what a user can and cannot do.

AAA authorization has the same rules as authentication:

1. First define a named list of authorization methods.
2. Then apply that list to one or more interfaces (except for the default method list).
3. The first listed method is used. If it fails to respond, the second one is used, and so on.

Method lists are specific to the authorization type requested. This document focusses on the Exec and Network authorization types.

For more information on the other types of authorization, please refer to the *Cisco IOS Security Configuration Guide, Release 12.2*.

Exec Authorization

The **aaa authorization exec** command determines if the user is allowed to run an EXEC shell. This facility might return user profile information such as autocommand information, idle timeout, session timeout, access-list and privilege and other per-user factors.

Exec authorization is only carried out over vty and tty lines.

The following example uses Radius.

Example 1: Same Exec Authentication Methods for All Users

Once authenticated with:

```
aaa authentication login default group radius local
```

All users who want to log in to the access server have to be authorized using Radius (first method) or local database (second method).

We configure:

```
aaa authorization exec default group radius local
```

Note: On the AAA server, Service-Type=1 (login) must be selected.

Note: With this example, if the **local** keyword is not included and the AAA server does not respond, then authorization will never be possible and the connection will fail.

Note: In Examples 2 and 3 below, we don't need to add any command on the router but only configure the profile on the access server.

Example 2: Assigning Exec Privilege Levels from the AAA Server

Based on Example 1, if a user who logs into the access server is to be allowed to enter enable mode directly, configure the following Cisco AV-pair on the AAA server:

```
shell:priv-lvl=15
```

This means that the user will go directly to the enable mode.

Note: If the first method fails to respond, then the local database is used. However, the user will not go directly to the enable mode, but will have to enter the enable command and supply the **enable** password.

Example 3 : Assigning Idle-Timeout from the AAA Server

To configure an idle timeout (so that the session is disconnected in case of no traffic after the idle timeout) use the the IETF Radius attribute 28: Idle-Timeout under the user's profile.

Network Authorization

The aaa authorization network command runs authorization for all network-related service requests such as PPP, SLIP and ARAP. This section focusses on PPP, which is most commonly used.

The AAA server checks if a PPP session by the client is allowed. Moreover, PPP options can be requested by the client: callback, compression, IP address, and so on. These options have to be configured on the user profile on the AAA server. Moreover, for a specific client, the AAA profile can contain idle-timeout, access-list and other per-user attributes which will be downloaded by the Cisco IOS software and applied for this client.

The following example show authorization using Radius:

Example 1: Same Network Authorization Methods for All Users

The access server is used to accept PPP dialin connections.

Firstly, users are authenticated (as was previously configured) using:

```
aaa authentication ppp default group radius local
```

then they have to be authorized using:

```
aaa authorization network default group radius local
```

Note: On the AAA server, configure:

- Service-Type=7 (framed)
- Framed-Protocol = PPP

Example 2: Applying User-Specific Attributes

You can use the AAA server to assign per-user attributes such IP address, callback number, dialer idle timeout value or access-list etc.. In such an implementation, the NAS downloads the appropriate attributes from the AAA server user profile.

Example 3: PPP Authorization with a Specific List

Like for authentication, we can configure a list name rather than using the default one :

```
aaa authorization network ISDN_USER group radius local
```

Then, this list is applied to the interface:

```
int dialer 0
  ppp authorization ISDN_USER
```

For more information on AAA authentication, refer to the documents IOS 12.2 Security Configuration Guide: Configuring Authentication and Cisco AAA Implementation Case Study.

Configuring Accounting

The AAA accounting feature enables you to track the services that users are accessing and the amount of network resources that they are consuming.

AAA accounting has the same rules as authentication and authorization:

1. You must first define a named list of accounting methods.
2. Then apply that list to one or more interfaces (except for the the default method list).
3. The first listed method is used, if it fails to respond, the second one is used and so on.

The first listed method is used, if it fails to respond, the second one is used and so on.

- Network accounting provides information for all PPP, Slip and AppleTalk Remote Access Protocol (ARAP) sessions: packet count, octets count, session time, start and stop time.
- Exec accounting provides information about user EXEC terminal sessions (a telnet session for instance) of the network access server: session time, start and stop time.

For more information on the other types of authorization, please refer to the Cisco IOS Security Configuration Guide, Release 12.2.

The examples below focus on how information can be sent to the AAA server.

Configuring Accounting Examples

Example 1: Generating Start and Stop Accounting Records

For every dialin PPP session, accounting information is sent to the AAA server once the client is authenticated and after the disconnect using the keyword **start-stop**.

```
aaa accounting network default start-stop group radius local
```

Example 2 : Generating Only Stop Accounting Records

If accounting information has to be sent only after a client's disconnection, use the keyword **stop** and configure the following line:

```
aaa accounting network default stop group radius local
```

Example 3 : Generating Resource Records for Authentication and Negotiation Failures

Until this point, AAA accounting provides start and stop record support for calls that have passed user authentication.

If authentication or PPP negotiation fails, there is no record of authentication.

The solution is to use AAA resource failure stop accounting:

```
aaa accounting send stop-record authentication failure
```

A stop record is sent to the AAA server.

Example 4 : Enabling Full Resource Accounting

To enable full resource accounting, which generates both a start record at call setup and a stop record at call termination, configure:

```
aaa accounting resource start-stop
```

This command was introduced in Cisco IOS Software Release 12.1(3)T.

With this command, a call setup and call disconnect start-stop accounting record tracks the progress of the resource connection to the device. A separate user authentication start-stop accounting record tracks the user management progress. These two sets of accounting records are interlinked using a unique session ID for the call.

For more information on AAA authentication, refer to the documents [IOS 12.2 Security Configuration Guide: Configuring Authentication](#) and [Cisco AAA Implementation Case Study](#).

Related Information

- [Technical Support – Cisco Systems](#)

