Configure Basic AAA on an Access Server

Contents

Introduction

Prerequisites

- Requirements
- Conventions
- Components Used

Background Information

- Network Diagram

General AAA Configuration

- Enable AAA
- Specify the External AAA Server
- AAA Server Configuration

Authentication Configuration

- Login Authentication
  - Example 1: Exec Access with Radius then Local
  - Example 2: Console Access used with Line Password
  - Example 3: Enable Mode Access used with External AAA Server
- PPP Authentication
  - Example 1: Single PPP Authentication Method for All Users
  - Example 2: PPP Authentication used with a Specific List
  - Example 3: PPP Launched from within Character Mode Session

Configure Authorization

- Exec Authorization
  - Example 1: Same Exec Authentication Methods for All Users
  - Example 2: Assign Exec Privilege Levels from the AAA Server
  - Example 3: Assign Idle-Timeout from the AAA Server
- Network Authorization
  - Example 1: Same Network Authorization Methods for All Users
  - Example 2: Apply User-Specific Attributes
  - Example 3: PPP Authorization with a Specific List

Accounting Configuration

- Accounting Configuration Examples
  - Example 1: Generate Start and Stop Accounting Records
  - Example 2: Generate Only Stop Accounting Records
  - Example 3:GenerateResource Records for Authentication and Negotiation Failures
  - Example 4: Enable Full Resource Accounting

Related Information

Introduction

This document describes how to configure Authentication, Authorization, and Accounting (AAA) on a Cisco router with Radius or TACACS+ protocols.

Prerequisites

Requirements

There are no specific requirements for this document.

Conventions

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

Components Used

The information in this document is based on Cisco IOS® software release 12 main line.

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

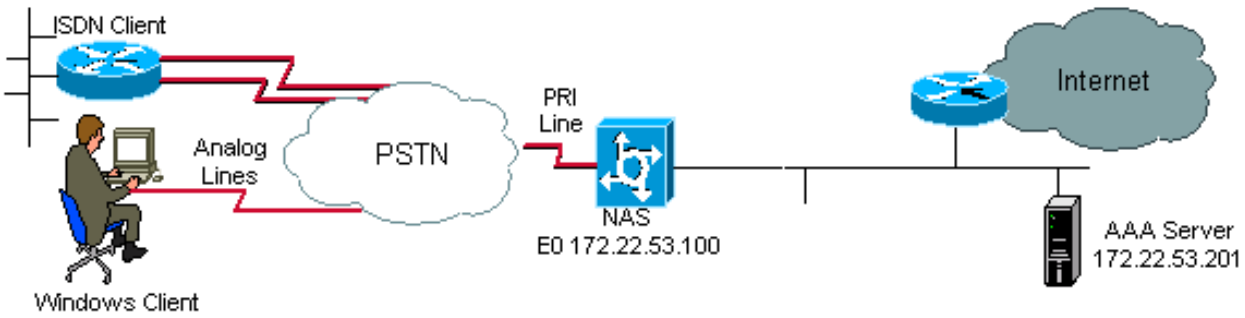
Background Information

This document explains how to configure Authentication, Authorization, and Accounting (AAA) on a Cisco router with 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: Read the section on General AAA Configuration before you proceed with the Cisco IOS configuration. Failure to do so can result in misconfiguration and subsequent lockout.

For more information, see Authentication, Authorization and Accounting Configuration Guide.

Network Diagram



Network Diagram

General AAA Configuration

Enable 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 this command is enabled (or if a connection times out and has to reconnect), then the user has to be authenticated with the local database of the router. It is recommended to define a username and password on the access server before you start the AAA configuration, so you are not locked out of the router. See the next code example.

```
<#root>

Router(config)#

username xxx password yyy
```

Tip: Before you configure your AAA commands, save your configuration. You can save the configuration again only after you have completed your AAA configuration (and are satisfied that it works correctly). This allows you to recover from unexpected lockouts as you can roll back any change with a reload of the router.

Specify 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 use TACACS+, use the **tacacs-server host <IP address of the AAA server> <key>** command.

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

AAA Server Configuration

On the AAA server, configure the next 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 it sends 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 previous parameters. If the AAA server is not correctly configured, then AAA requests from the NAS can be ignored by the AAA server and the connection can fail.

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

Authentication Configuration

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.

These authentication examples use Radius, login and Point-to-Point Protocol (PPP) authentication 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, that is, if the AAA server or local username database responses are to deny 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 with Radius then Local

<#root>

```
Router(config)#
```

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

In the previous command:

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

All users are authenticated with the Radius server (the first method). If the Radius server does not respond, then the router local database is used (the second method). For local authentication, define the username name and password:

```
<#root>

Router(config)#

username xxx password yyy
```

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

Note: The server (Radius or TACACS+) cannot 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: If you use the previous example, without **local** keyword, the result is:

```
<#root>

Router(config)#

aaa authentication login default group radius
```

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

Note: The **group** keyword provides a way to group current server hosts. The feature allows the user to select a subset of the configured server hosts and use them for a particular service.

Example 2: Console Access used with Line Password

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.

Configuration:

```
<#root>
```

```
Router(config)#
aaa authentication login CONSOLE line
```

In the previous command:

- The named list is CONSOLE.
- There is only one authentication method (line).

When a named list (in this example, CONSOLE) is created, it must be applied to a line or interface before it executes. This is done with the login authentication <list_name> command:

```
<#root>
Router(config)#
line con 0

Router(config-line)#
exec-timeout 0 0

Router(config-line)#
password cisco

Router(config-line)#
login authentication CONSOLE
```

The CONSOLE list overrides the default method list **default** on line con 0. After this configuration on line con 0, you need to enter the password **cisco** 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 the next code example:

```
<#root>
Router(config)#
aaa authentication login CONSOLE local
```

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 the next code example:

```
<#root>

Router(config)#

aaa authentication login CONSOLE none
```

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 used with External AAA Server

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

Configuration:

```
<#root>

Router(config)#

aaa authentication enable default group radius enable
```

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

If the Radius server does not reply, the enable password configured locally on the router can have to be entered.

PPP Authentication

The **aaa authentication ppp** command is used to authenticate a PPP connection. It is 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 dial-in clients. We use a **dialer rotary-group 0**, but the configuration can be done on the main interface or dialer profile interface.

Configuration:

```
<#root>

Router(config)#

aaa authentication ppp default group radius local
```

This command authenticates all PPP users with Radius. If the Radius server does not reply, the local database is used.

Example 2: PPP Authentication used with a Specific List

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

```
<#root>

Router(config)#

aaa authentication ppp ISDN_USER group radius


Router(config)#

interface dialer 0


Router(config-if)#

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). Assume that both **aaa authentication login** and **aaa authentication ppp** commands are configured.

If a modem user first accesses the router with a character mode exec session (for example, with 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, use the **if-needed** keyword:

```
<#root>

Router(config)#

aaa authentication login default group radius local

Router(config)#

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 log in access to the access server.

Configure Authorization

Authorization is the process by which you can control what a user can 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 focuses 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 .

Exec Authorization

The **aaa authorization exec** command determines if the user is allowed to run an EXEC shell. This facility can return user profile information such as auto command 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 next example uses Radius.

Example 1: Same Exec Authentication Methods for All Users

When it is authenticated with:

```
<#root>

Router(config)#

aaa authentication login default group radius local
```

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

Configuration:

```
<#root>

Router(config)#

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, therefore, the authorization is not possible, and the connection can fail.

Note: In next Examples 2 and 3, you do not have to add any command on the router. You only need to configure the profile on the access server.

Example 2: Assign Exec Privilege Levels from the AAA Server

Based on Example 1, configure the next Cisco AV-pair on the AAA server so that a user can log into the access server and enter the enable mode directly:

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

The user can now go directly to the enable mode.

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

Example 3: Assign 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 IETF Radius attribute 28: Idle-Timeout under the user profile.

Network Authorization

The aaa authorization network command runs authorization for all network-related service requests such as PPP, SLIP and ARAP. This section focuses 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 can be downloaded by the Cisco IOS software and applied for this client.

The next examples show authorization with Radius.

Example 1: Same Network Authorization Methods for All Users

The access server is used to accept PPP dial-in connections.

Users are authenticated (as was previously configured) with:

```
<#root>

Router(config)#

aaa authentication ppp default group radius local
```

Use the next command to authorize the users:

```
<#root>
Router(config)#
aaa authorization network default group radius local
```

Note: On the AAA server, configure: **Service-Type=7** (framed) and **Framed-Protocol=PPP**.

Example 2: Apply User-Specific Attributes

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

Example 3: PPP Authorization with a Specific List

Similar to authentication, configure a list name rather than a the default one :

```
<#root>
Router(config)#
aaa authorization network ISDN_USER group radius local
```

Then, apply this list to the interface:

```
<#root>
  Router(config)#
interface dialer 0

  Router(config-if)#
ppp authorization ISDN_USER
```

Accounting Configuration

The AAA accounting feature enables you to track the services that users access and the amount of network resources that they consume.

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 default method list).

3. 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, octects 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.

The next examples focuses on how information can be sent to the AAA server.

Accounting Configuration Examples

Example 1: Generate Start and Stop Accounting Records

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

```
<#root>

Router(config)#

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

Example 2: Generate Only Stop Accounting Records

If accounting information has to be sent only after a client has disconnected, use the keyword **stop** and configure the next line:

```
<#root>

Router(config)#

aaa accounting network default stop group radius local
```

Example 3: Generate 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:

```
<#root>

Router(config)#

aaa accounting send stop-record authentication failure
```

A stop record is sent to the AAA server.

Example 4: Enable 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:

```
<#root>

Router(config)#

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 with a unique session ID for the call.

Related Information

- **Cisco Technical Support & Downloads**