Chapter 9

Configuring TACACS+

This chapter explains how to enable and configure TACACS+ in your E-series router. It has the following sections:

Overview

With the increased use of remote access, the need for managing more network access servers (NAS) has increased. Additionally, the need for control access on a per-user basis has escalated, as has the need for central administration of users and passwords.

Terminal Access Controller Access Control System (TACACS) is a security protocol that provides centralized validation of users who are attempting to gain access to a router or NAS. TACACS+, a more recent version of the original TACACS protocol, provides separate authentication, authorization, and accounting (AAA) services.

NOTE: TACACS+ is a completely new protocol and is not compatible with TACACS or XTACACS.

The TACACS+ protocol provides detailed accounting information and flexible administrative control over the authentication, authorization, and accounting process. The protocol allows a TACACS+ client to request detailed access control and allows the TACACS + process to respond to each component of that request. TACACS+ uses Transmission Control Protocol (TCP) for its transport.

TACACS+ provides security by encrypting all traffic between the NAS and the process. Encryption relies on a secret key that is known to both the client and the TACACS+ process.

Table 38 describes terms that are frequently used in this chapter.

Table 38: TACACS-Related Terms

Term	Description
NAS	Network access server. A device that provides connections to a single user, to a network or subnetwork, and to interconnected networks. In reference to TACACS+, the NAS is the E-series router.
TACACS+ process	A program or software running on a security server that provides AAA services using the TACACS+ protocol. The program processes authentication, authorization, and accounting requests from an NAS. When processing authentication requests, the process might respond to the NAS with a request for additional information, such as a password.
TACACS+ host	The security server on which the TACACS+ process is running. Also referred to as a TACACS+ server.

AAA Overview

TACACS+ allows effective communication of AAA information between NASs and a central server. The separation of the AAA functions is a fundamental feature of the TACACS+ design:

- Authentication—Determines who a user is, then determines whether that user should be granted access to the network. The primary purpose is to prevent intruders from entering your networks. Authentication uses a database of users and passwords.

- Authorization—Determines what an authenticated user is allowed to do. Authorization gives the network manager the ability to limit network services to different users. Also, the network manager can limit the use of certain commands to various users. Authorization cannot occur without authentication.

- Accounting—Tracks what a user did and when it was done. Accounting can be used for an audit trail or for billing for connection time or resources used. Accounting can occur independent of authentication and authorization.

Central management of AAA means that the information is in a single, centralized, secure database, which is much easier to administer than information distributed across numerous devices. Both RADIUS and TACACS+ protocols are client-server systems that allow effective communication of AAA information.

For information about RADIUS, see *Chapter 1, Configuring Remote Access* and *Chapter 3, Configuring RADIUS Attributes*.

Administrative Login Authentication

Fundamentally, TACACS+ provides the same services as RADIUS. Every authentication login attempt on an NAS is verified by a remote TACACS+ process.

TACACS+ authentication uses three packet types. Start packets and Continue packets are always sent by the user. Reply packets are always sent by the TACACS+ process.

TACACS+ sets up a TCP connection to the TACACS+ host and sends a Start packet. The TACACS+ host responds with a Reply packet, which either grants or denies access, reports an error, or challenges the user.

TACACS+ might challenge the user to provide username, password, passcode, or other information. Once the requested information is entered, TACACS+ sends a Continue packet over the existing connection. The TACACS+ host sends a Reply packet. Once the authentication is complete, the connection is closed. Only three login retries are allowed.

To enable login authentication through both TACACS+ and RADIUS servers, use the **aaa new-model** command to specify AAA authentication for Telnet sessions.

Privilege Authentication

The privilege authentication process determines whether a user is allowed to use commands at a particular privilege level. This authentication process is handled similarly to login authentication, except that the user is limited to one authentication attempt. An empty reply to the challenge forces an immediate access denial. The **aaa authentication enable default** command allows you to set privilege authentication for users.

Login Authorization

To allow login authorization through the TACACS+ server, you can use the following commands: **aaa authorization**, **aaa authorization config-commands**, and **authorization**. For information about using these commands, see *JUNOSe System Basics Configuration Guide, Chapter 9, Passwords and Security*.

Accounting

The TACACS+ accounting service enables you to create an audit trail of User Exec sessions and command-line interface (CLI) commands that have been executed within these sessions. For example, you can track user CLI connects and disconnects, when configuration modes have been entered and exited, and which configuration and operational commands have been executed.

You configure TACACS+ accounting in the JUNOSe software by defining accounting method lists and then associating consoles and lines with the method lists. You define an accounting method list with a service type, name, accounting mode, and method:

- service type—Specifies the type of information being recorded
- name—Uniquely identifies an accounting method list within a service type
- accounting mode—Specifies what type of accounting records will be generated
- method—Specifies the protocol for sending the accounting records to a security server

You can then configure consoles and lines with an accounting method list name for each service type:

- Method list—A specified configuration that defines how the NAS performs the AAA accounting service. A service type can be configured with multiple method lists with different names, and a method list name can be used for different service types. Initially, no accounting method list is defined; therefore TACACS+ accounting is disabled.
  - Default method list—Configuration used by consoles and lines when no named method list is assigned. You enable TACACS+ accounting by defining default accounting method lists for each service type.
  - Named method list—Assigned to a console, specific line, or group of lines; overrides the default method list.
- Service type—Specifies the type of information provided by the TACACS+ accounting service:
  - Exec—Provides information about User Exec terminal sessions, such as telnet, Local Area Transport (LAT), and rlogin, on the NAS.
  - Commands <0-15>—Provides information about User Exec mode CLI commands for a specified privilege level that are being executed on the NAS. Each of the sixteen command privilege levels is a separate service type. Accounting records are generated for commands executed by users, CLI scripts, and macros.
- Accounting mode—Specifies the type of accounting records that are recorded on the TACACS+ server. Accounting records track user actions and resource usage. You can analyze and use the records for network management, billing, and auditing purposes.
  - start-stop—A start accounting record is generated just before a process begins, and a stop accounting record is generated after a process successfully completes. This mode is supported only for the Exec service type.
  - stop-only—A stop accounting record is generated after a process successfully completes. This mode is supported only for the Commands service types.

The NAS sends TACACS+ accounting packets to the TACACS+ host. The accounting packets contain data in the packet header, packet body, and attribute-value pairs (AVPs). Table 39 provides descriptions of the TACACS+ accounting data.

Table 39: TACACS+ Accounting Information

Field/Attribute	Location	Description
major_version	Packet header	Major TACACS+ version number
minor_version	Packet header	Minor TACACS+ version number
type	Packet header	Type of the AAA service: Accounting
flags	Packet body	Bitmapped flags representing the record type: start accounting record or stop accounting record
priv-level	Packet body	Privilege level of the user executing the Exec session or CLI command: 0 - 15
user	Packet body	Name of user running the Exec session or CLI command
port	Packet body	NAS port used by the Exec session or CLI command
rem-addr	Packet body	User's remote location; either an IP address or the caller ID
service	AVP	User's primary service: Shell
cmd	AVP	CLI command that is to be executed: specified for Command-level accounting only
task_id	AVP	Unique sequential identifier used to match start and stop records for a task
elapsed_time	AVP	Elapsed time in seconds for the task execution: specified for Exec-level accounting stop records only
timezone	AVP	Time zone abbreviation used for all timestamps

Platform Considerations

TACACS+ is supported on all E-series routers. For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

References

For additional information about the TACACS+ protocol, see the following resources:

- The TACACS+ Protocol, Version 1.78—draft-grant-tacacs-02.txt (January 1997 expiration)
- RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)

NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at http://www.ietf.org for the latest drafts.

Before You Configure TACACS+

Before you begin to configure TACACS+, you must determine the following for the TACACS+ authentication and accounting servers:

- IP addresses
- TCP port numbers
- Secret keys

Configuring TACACS+ Support

To use TACACS+, you must enable AAA. To configure your router to support TACACS+, perform the following tasks. Some of the tasks are optional. Once you configure TACACS+ support on the router, you can configure TACACS+ authentication, authorization, and accounting independent of each other.

1. Specify the names of the IP host or hosts maintaining a TACACS+ server. Optionally, you can specify other parameters, such as port number, timeout interval, and key.

   host1(config)#**tacacs-server host 192.168.1.27 port 10 timeout 3 key your_secret primary**

2. (Optional) Set the authentication and encryption key value shared by all TACACS+ servers that do not have a server-specific key set up by the **tacacs-server host** command.

   host1(config)#**tacacs-server key “&#889P^”**

3. (Optional) Set alternative source address(es) to be used for TACACS+ server communications.

   host1(config)#**tacacs-server source-address 192.168.134.63**

4. (Optional) Set the timeout value for all TACACS+ servers that do not have a server-specific timeout set up by the **tacacs-server host** command.

   host1(config)#**tacacs-server timeout 15**

Configuring Authentication

Once TACACS+ support is enabled on the router, you can configure TACACS+ authentication. Perform the following steps:

1. Specify AAA new model as the authentication method for the vty lines on your router.

   host1(config)#**aaa new-model**

2. Specify AAA authentication by defining an authorization methods list.

   host1(config)#**aaa authentication login tac tacacs+ radius enable**

3. Specify the privilege level by defining a methods list that uses TACACS+ for authentication.

   host1(config)#**aaa authentication enable default tacacs+ radius enable**

4. Configure vty lines.

   host1(config)#**line vty 0 4**

5. Apply an authentication list to the vty lines you specified on your router.

   host1(config-line)#**login authentication tac**

Configuring Accounting

Once TACACS+ support is enabled on the router, you can configure TACACS+ accounting. Perform the following steps:

1. Specify AAA new model as the accounting method for your router.

   host1(config)#**aaa new-model**

2. Enable TACACS+ accounting on the router, and configure accounting method lists. For example:

   host1(config)#**aaa accounting exec default start-stop tacacs+**
   host1(config)#**aaa accounting commands 0 listX stop-only tacacs+**
   host1(config)#**aaa accounting commands 1 listX stop-only tacacs+**
   host1(config)#**aaa accounting commands 13 listY stop-only tacacs+**
   host1(config)#**aaa accounting commands 14 default stop-only tacacs+**
   host1(config)#**aaa accounting commands 15 default stop-only tacacs+**

3. (Optional) Specify that accounting records are not generated for users without explicit user names.

   host1(config)#**aaa accounting suppress null-username**

4. Apply accounting method lists to a console or lines. For example:

   host1(config)#**line console 0**
   host1(config-line)#**accounting commands 0 listX**
   host1(config-line)#**accounting commands 1 listX**
   host1(config-line)#**accounting commands 13 listY**
   host1(config-line)#**exit**
   host1(config)#**line vty 0 4**
   host1(config-line)#**accounting commands 13 listY**

Note that Exec accounting and User Exec mode commands accounting for privilege levels 14 and 15 are now enabled for all lines and consoles with the creation of their default method list, as shown in Step 2.

aaa accounting commands

- Use to enable TACACS+ accounting and capture accounting information for a specific JUNOSe privilege level on the router and to create accounting method lists.
- Specify the JUNOSe privilege level (0 through 15) for which to capture accounting information.
- Specify **default** to configure the default method list, or configure a named method list. The default method list is used by lines and consoles unless a named method list is configured for them.
- Specify **stop-only** to send a stop accounting notice at the end of a process and **tacacs+** as the accounting protocol.
- Example

  host1(config)#**aaa accounting commands 12 listX stop-only tacacs+**

- Use the **no** version to delete the accounting method list.

aaa accounting exec

- Use to enable TACACS+ accounting and capture accounting information for User Exec terminal session on the router and to create accounting method lists.
- Specify **default** to configure the default method list, or configure a named method list. The default method list is used by lines and consoles unless a named method list is configured for them.
- Specify **start-stop** to send a start accounting notice at the beginning of a process and a stop accounting notice at the end of a successful process. Specify **tacacs+** as the accounting protocol.
- Example

  host1(config)#**aaa accounting exec default start-stop tacacs+**

- Use the **no** version to delete the accounting method list.

aaa accounting suppress null-username

- Use to prevent JUNOSe software from generating accounting records for users who do not have explicit usernames.
- Example

  host1(config)#**aaa accounting suppress null-username**

- Use the **no** version to generate accounting records for users with null usernames.

aaa authentication enable default

- Use to allow privilege determination to be authenticated through the TACACS+ server. This command specifies a list of authentication methods that are used to determine whether a user is granted access to the privilege command level.
- The authentication methods that you can use in a list include these options: **radius**, **line**, **tacacs+**, **none**, and **enable**.
- To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.
- Requests sent to a TACACS+ server include the username that is entered for login authentication.
- If a default authentication routine is not set for a function, the default is **none**, and no authentication is performed.
- If the authentication method list is empty, the local **enable** password is used.
- Example

  host1(config)#**aaa authentication enable default tacacs+ radius**

- Use the **no** version to empty the list.

aaa authentication login

- Use to set AAA authentication at login. This command creates a list that specifies the methods of authentication.
- Once you specify **aaa new-model** as the authentication method for vty lines, an authentication list called "default" is automatically assigned to the vty lines. To allow users to access the vty lines, you must create an authentication list and either:
  - Name the list "default."
  - Assign a different name to the authentication list, and assign the new list to the vty line using the **login authentication** command.
- The authentication methods that you can use in a list include these options: **radius**, **line**, **tacacs+**, **none**, and **enable**.
- The router traverses the list of authentication methods to determine whether a user is allowed to start a Telnet session. If a specific method is available but the user information is not valid (such as an incorrect password), the router does not continue to traverse the list and denies the user a session.

- If a specific method is unavailable, the router continues to traverse the list. For example, if **tactacs +** is the first authentication type element on the list and the TACACS + server is unreachable, the router attempts to authenticate with the next authentication type on the list, such as **radius**.
- The router assumes an implicit denial of service if it reaches the end of the authentication list without finding an available method.
- Example

  host1(config)#**aaa authentication login my_auth_list tacacs+ radius line none**

- Use the **no** version to remove the authentication list from your configuration.

aaa new-model

- Use to specify AAA new model as the authentication method for the vty lines on your router.
- If you specify AAA new model and you do not create an authentication list, users will not be able to access the router through a vty line.
- Example

  host1(config)#**aaa new-model**

- Use the **no** version to restore simple authentication (login and password).

accounting

- Use to specify accounting method lists used on a console or vty line. Consoles and lines are initially configured with the default method list for all accounting service types (for example, Exec, Commands).
- Specify **exec** to capture accounting information for User Exec terminal sessions or **commands** to capture accounting information for User Exec mode commands at the indicated JUNOSe privilege level (0 through 15).
- Specify the name of the method list to be applied to the line or console.
- To disable accounting for a line or console, specify a nonexisting accounting method list name (for example, noAccounting).
- Example

  host1(config)#**accounting commands 12 listY**

- Use the **no** version to restore the default method list.

line

- Use to open or configure console or vty lines.
- You can specify a single line or a range of lines. The range is 0 though 29 for vty lines, 0 for the console line.
- Example

  host1(config)#**line vty 6 10**
  host1(config-line)#

- Use the **no** version to remove a line or a range of lines from the configuration. Lines that you remove will no longer be available for use by telnet, FTP, or SSH. When you remove a vty line, the router removes all lines above that line. For example, **no line vty 6** causes the router to remove lines 6 through 19. You cannot remove lines 0 through 4.

login authentication

- Use to apply an authentication list to the vty lines you specified on your router.
- Example

  host1(config-line)#**login authentication my_auth_list**

- Use the **no** version to specify that the router should use the default authentication list.

tacacs-server host

- Use to add or delete a host to or from the list of TACACS+ servers.
- You can optionally specify a nondefault port number, a host-specific key, a single connection and a timeout interval.
- Use the **primary** keyword to assign the host as the primary host.
- If a timeout value is specified, it overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
- You can configure additional hosts by using this command. The designated primary host is always the first in the search order; the remaining hosts are contacted in the order in which they were created. If the primary host is deleted, or if you modify the primary host without specifying the **primary** keyword, the next host in the search order becomes the primary host. The search order is maintained when the NAS is reloaded.
- Example

  host1(config)#**tacacs-server host 192.168.1.27 port 10 timeout 3 key your_secret primary**
  host1(config)#**no tacacs-server host 192.168.1.27**

- Use the **no** version to delete the host from the list of TACACS+ servers.

tacacs-server key

- Use to set or reset the authentication encryption key value shared by all TACACS+ servers that do not have a server-specific key set up by the **tacacs-server host** command.
- This key must match the key configured on the TACACS+ process.
- Leading spaces are ignored; however, spaces at the end of the key are recognized. If you use spaces in the key, do not enclose the key in quotation marks.
- Example

  host1(config)#**tacacs-server key &# 889khj**

- Use the **no** version to reset a key value shared by all TACACS+ servers.

tacacs-server source-address

- Use to set or reset an alternative source address to be used for TACACS+ server communications.
- Existing connections are not affected by this command.
- Example

  host1(config)#**tacacs-server source-address 192.168.134.63**

- Use the **no** version to remove the address.

tacacs-server timeout

- Use to set the interval in seconds that the server waits for the server host to reply. The specified interval is shared by all TACACS+ servers that do not have a server-specific timeout set up by **tacacs-server host** command.
- The timeout interval is between 1 and 300. The default is 5 seconds.
- Example

  host1(config)#**tacacs-server timeout 15**

- Use the **no** version to reset the timeout to the default.