

Configuring TACACS+

3

This chapter explains how to enable and configure TACACS+ in your ERX system.

Topic	Page
Overview	3-1
References	3-4
Before You Configure TACACS+	3-4
Configuring TACACS+	3-4
Monitoring TACACS+	3-8

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.

Table 3-1 provides descriptions of some terms that are frequently used in this chapter.

Table 3-1 TACACS-related terms

Term	Definition
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 ERX system.
TACACS+ daemon	A program or software running on a server that accepts or denies an authentication request. The server sends a response to a TACACS+ authentication server based on the username and password. The TACACS+ daemon normally runs on a host.
TACACS+ host	The place where the TACACS+ daemon is running.

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



Note: Currently, the ERX implementation of TACACS+ does not support the Authorization or Accounting functions.

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

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 a 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.
- 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.

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.



Note: For information about RADIUS, see Chapter 1, *Configuring Remote Access to the ERX System* and Chapter 2, *Configuring RADIUS Attributes*.

Administrative Login Authentication

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

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+ daemon.

When logging in to the ERX system, a user is first prompted for a username. Once the username is available, the TACACS+ subsystem sets up a TCP connection to the TACACS+ host. The TACACS+ subsystem then sends a Start packet containing the username. The TACACS+ host responds with a Reply packet, which either grants or denies access, reports an error, or challenges the user to provide a password.

If the password challenge is made, the user is prompted to enter a password. Once the password is entered, the TACACS+ subsystem sends a Continue packet over the existing connection. The TACACS+ host again replies with a Reply packet. When the user authentication is complete, the connection is closed. Only three login retries are allowed.

The **aaa new-model** command is used to enable login authentication through both TACACS+ and RADIUS servers. The command specifies AAA authentication for Telnet sessions.

Privilege Authentication

The privilege authentication process determines the level of commands that a user is allowed. This authentication process is handled similarly to login authentication, except that the user is challenged only once. 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.

References

See these references for additional information:

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

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+

You must enable AAA to use TACACS+. To configure your ERX system to support TACACS+, perform the following tasks. Some of the tasks are optional.

- 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 163.10.1.27 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 191.6.134.63
```

- 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
```

- 5 Specify AAA new model as the authentication method for the vty lines on your system.

```
host1(config)#aaa new-model
```
- 6 Specify AAA authentication by defining an authorization methods list.

```
host1(config)#aaa authentication login tac tacacs+ radius enable
```
- 7 Specify privilege level by defining a methods list that uses TACACS+ for authentication.

```
host1(config)#aaa authentication enable default tacacs+ radius enable
```
- 8 Configure vty lines.

```
host1(config)#line vty 0 4
```
- 9 Apply an authentication list to the vty lines you specified on your system.

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

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.
- PPP authentication is applied by default to all interfaces.
- Authentication method list options include: **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.
- You can enter up to three authentication methods in an authentication list. Options include: **radius**, **line**, **tacacs+**, **none**, and **enable**.
- The system 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 system does not continue to traverse the list and denies the user a session.
- If a specific method is unavailable, the system 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 system attempts to authenticate with the next authentication type on the list, such as **radius**.
- The system 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 system.
- If you specify AAA new model and you do not create an authentication list, users will not be able to access the system through a vty line.
- Example


```
host1(config)#aaa new-model
```
- Use the **no** version to restore simple authentication (login and password).

line vty

- Use to open or configure vty lines.
- You can specify a single line or a range of lines. The range is 0–19.
- Example


```
host1(config)#line vty 6 10
host1(config-line)#
```
- Use the **no** version to remove a vty 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 system removes all lines above that line. For example, **no line vty 6** causes the system 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 system.
- Example

```
host1(config-line)#login authentication my_auth_list
```
- Use the **no** version to specify that the system 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 using this command. The hosts will be searched for in the order they are specified.
- Example

```
host1(config)#tacacs-server host 163.10.1.27 port 10 timeout 3 key your_secret primary
```
- Example

```
host1(config)#no tacacs-server host 163.10.1.27
```
- 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+ daemon.
- 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 this command 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 191.6.134.63
```
- 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.

Monitoring TACACS+

You can use commands in this section to monitor the current TACACS+ configurations.

baseline tacacs

- Use to set the baseline for TACACS+ statistics.
- Example

```
host1#baseline tacacs
```

show statistics tacacs

- Use to display TACACS+ statistics.
- Field descriptions
 - › Statistic – IP address of the host
 - › TCP Port – TCP port of the host
 - › Auth Requests – number of authentication requests sent to the host
 - › Auth Replies – number of authentication replies received from the host
 - › Auth Pending – number of expected but not received authentication replies from the host
 - › Auth Timeouts – number of authentication timeouts for the host
 - › Author Requests – number of authorization requests sent to the host
 - › Author Replies – number of authorization replies received from the host
 - › Author Pending – number of expected but not received authorization replies from the host
 - › Author Timeouts – number of authorization timeouts for the host
 - › Acct Requests – number of accounting requests sent to the host
 - › Acct Replies – number of accounting replies received from the host
 - › Acct Pending – number of expected but not received accounting replies from the host
 - › Acct Timeouts – number of accounting timeouts for the host

- Example

```

host1#show statistics tacacs
          TACACSPLUS Statistics
          -----
          Statistic          10.5.0.174    10.5.1.199
          -----
TCP Port          3049          4049
Auth Requests    128          0
Auth Replies     85          0
Auth Pending     43          0
Auth Timeouts   12          0
Author Requests  0           0
Author Replies   0           0
Author Pending   0           0
Author Timeouts  0           0
Acct Requests   0           0
Acct Replies    0           0
Acct Pending    0           0
Acct Timeouts   0           0

```

show tacacs

- Use to display TACACS+ information.
- Use the **statistics** keyword to display overall statistics.
- Field descriptions
 - › Key – authentication and encryption key
 - › Timeout – TACACS+ host response timeout in seconds
 - › Source-address – alternative source IP address configured
 - › TACACSPLUS Configuration – table contains statistics for each host
 - › IP Address – IP address of the host
 - › TCP Port – TCP port of the host for each IP address
 - › Timeout – timeout interval in seconds for each IP address
 - › Primary – this IP address's primary host; options: y = yes, n = no
 - › Key – authentication and encryption key for this IP address
- Example

```

host1#show tacacs
Key = hippo
Timeout = <NOTSET>, built-in timeout of 5 will be used
Source-address = <NOTSET>

```

```

          TACACS+ Configuration, (*) denotes inherited
          -----
          Tcp
IP Address  Port  Timeout  Primary  Key
-----
10.5.0.174  3049  5 (*)   y        hippo (*)
10.5.1.199  1049  5 (*)   n        hippo (*)

```

