



Troubleshooting TACACS+ and Recovering Passwords

This chapter describes troubleshooting information relating to security implementations and contains the following sections:

- Troubleshooting TACACS+ Problems, page B-1
- Recovering a Lost Password, page B-5

If you want detailed information about configuring and using TACACS+, refer to the *ATM Switch Router Software Configuration Guide* and *ATM Switch Router Command Reference* publications. For additional information about TACACS+, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference*.

Troubleshooting TACACS+ Problems

The following sections describe problems with TACACS+ operation and possible solutions.

Errors Unarchiving Source File

Symptom: Errors are generated when unarchiving the TACACS+ archive file (tac_plus.2.1.tar).

Table B-1 outlines possible problems and describes solutions.

Table B-1 TACACS+: Errors Unarchiving Source File

Possible Problem	Solution
Archive file was not transferred by using FTP ¹ binary (image) mode	The TACACS+ archive file must be transferred by using FTP binary (image) mode. FTP the tac_plus.2.1.tar file again, using FTP binary transfer mode. From the FTP command line, enter the image command to set the image mode. For other FTP software, refer to your documentation for instructions on setting the image mode.
Insufficient disk space	Make sure there is sufficient disk space for the expanded tac_plus.2.1.tar file. If there is not enough space on your UNIX system, create enough free disk space to accommodate decompression of the file. TACACS+ requires about 900 KB.

1. FTP = File Transfer Protocol

Cannot Compile Daemon

Symptom: Attempts to compile the TACACS+ daemon result in errors.

Table B-2 outlines possible problems and describes solutions.

Table B-2 TACACS+: Cannot Compile Daemon

Possible Problem	Solution
make is not in \$PATH or is not installed on the UNIX machine	<ol style="list-style-type: none"> 1. Enter the which make command at the UNIX prompt. If the output says “No make in \$PATH...,” make is not in the specified path or is not installed. 2. If make is already installed, modify the \$PATH variable to include the directory in which make is located. <p>If make is not installed, see your system administrator for help installing it.</p> <ol style="list-style-type: none"> 3. Compile the TACACS+ daemon again.
gcc is not in \$PATH or is not installed correctly	<ol style="list-style-type: none"> 1. Enter the which gcc command at the UNIX prompt. If the output says “No gcc in \$PATH...,” gcc is not in the specified path or is not installed. 2. If gcc is already installed, modify the \$PATH variable to include the directory in which gcc is located. <p>If gcc is not installed, ask your system administrator to install it.</p> <ol style="list-style-type: none"> 3. Compile the TACACS+ daemon again.
UNIX platform is commented out or is not in the Makefile	<p>Your UNIX platform must be listed and uncommented in the Makefile for make to compile the TACACS+ source code properly. The Makefile is located in the <code>tac_plus.2.1</code> directory.</p> <ol style="list-style-type: none"> 1. Make sure that your UNIX platform is not commented out in the Makefile. 2. If your platform is not listed at all, see your system administrator for help with compiling the source code. The only supported platforms are those listed in the Makefile. 3. Compile the TACACS+ daemon again.

Daemon Is Not Up and Running

Symptom: The TACACS+ daemon is not running.

Table B-3 outlines possible problems and describes solutions.

Table B-3 TACACS+: Daemon Is Not Up and Running

Possible Problem	Solution
TACACS+ has not been launched	Launch TACACS+ with the tac_plus -C configuration filename command.
TACACS+ is not specified in the /etc/services file	<ol style="list-style-type: none"> 1. Check the /etc/services file for the following line: <code>tacacs 49/tcp</code> 2. This line must be included in the file. If the line is not present, add the line to the file.
The tac_plus executable does not exist	<p>The TACACS+ daemon cannot run if the tac_plus executable does not exist.</p> <ol style="list-style-type: none"> 1. Check the directory where you installed tac_plus.2.1 to see if the tac_plus file exists. 2. If the file does not exist, use the make tac_plus command to compile tac_plus.

Daemon Does Not Run

Symptom: The TACACS+ daemon does not run when invoked.

Table B-4 outlines possible problems and describes solutions.

Table B-4 TACACS+: Daemon Does Not Run

Possible Problem	Solution
TACACS+ configuration file is not present	<ol style="list-style-type: none"> 1. Check the directory in which you installed TACACS+ for a configuration file in the TACACS+ format. 2. If there is no TACACS+ configuration file present and you are upgrading from XTACACS, convert your password file into a configuration file by issuing the following command: <code>unix_host% convert.pl /etc/passwd > configuration-file</code> <p>The configuration file can have any name you want.</p> <ol style="list-style-type: none"> 3. If there is no TACACS+ configuration file present, create one by using a text editor. At a minimum, the configuration file must contain the following text: <pre>user = userid { login = cleartext "passwd" }</pre> <p>The configuration file can be given any name.</p> <p>For more information, refer to the user guide located in the tac_plus.2.1 directory.</p>

Users Cannot Connect Using TACACS+

Symptom: Users cannot log in using TACACS+. Either users cannot get the Username prompt or they get the prompt but authentication or authorization fails.

Table B-5 outlines possible problems and describes solutions.

Table B-5 TACACS+: Users Cannot Log in Using TACACS+

Possible Problem	Solution
Switch router missing minimum configuration	<ol style="list-style-type: none"> Use the show running-config privileged EXEC command to view the local switch router configuration. Look for the following commands: <pre> aaa new-model aaa authentication login default tacacs+ enable [...] tacacs-server host name tacacs-server key key </pre> <p>where <i>name</i> is the IP address or DNS¹ host name of the TACACS+ server and <i>key</i> is the authentication and encryption key.</p> If all of these commands are not present, add the missing commands to the configuration. If there is no key configured on the TACACS+ daemon, the tacacs-server key command is not necessary.
aaa authorization command is present	<ol style="list-style-type: none"> Use the show running-config privileged EXEC command to view the local switch router configuration. Look for an aaa authorization exec tacacs+ global configuration command entry. If the command is present, remove it from the configuration by using the no version of the command.
PPP ² not functioning correctly	<p>If PPP is not functioning properly, problems will occur when using TACACS+. Use the debug ppp negotiation privileged EXEC command to see if both sides are communicating.</p> <p>For information on configuring PPP, refer to the <i>Cisco IOS Dial Solutions Configuration Guide: Terminal Services</i> and <i>Cisco IOS Dial Solutions Command Reference</i> publications.</p>
PAP ³ is misconfigured	<ol style="list-style-type: none"> Use the show running-config privileged EXEC command to make sure your configuration includes the following global configuration command: <pre> aaa authentication ppp default if-needed tacacs+ </pre> If the command is not present, add it to the configuration. In addition, check the configuration of the async interface being used. The interface must have the following commands configured: <pre> encapsulation ppp ppp authentication pap </pre> If these commands are not present, add them to the interface configuration.

Table B-5 TACACS+: Users Cannot Log in Using TACACS+ (continued)

Possible Problem	Solution
CHAP ⁴ is misconfigured	<ol style="list-style-type: none"> 1. Use the show running-config privileged EXEC command to make sure your configuration includes the following global configuration command: <pre>aaa authentication ppp default if-needed tacacs+</pre> 2. If the command is not present, add it to the configuration. 3. In addition, check the configuration of the async interface being used. The interface must have the following commands configured: <pre>encapsulation ppp ppp authentication chap</pre> 4. If these commands are not present, add them to the interface configuration. 5. Make sure your daemon configuration file, located in the <code>tac_plus.2.1</code> directory, includes one of the following lines, as appropriate: <pre>chap = cleartext password</pre> <p>or</p> <pre>global = cleartext password</pre>
Username and password are not in the <code>/etc/passwd</code> file	<ol style="list-style-type: none"> 1. Check to make sure that the appropriate username and password pairs are contained in the <code>/etc/passwd</code> file. 2. If the appropriate users are not specified, generate a new user with the correct username and password, using the add user command.
There is no TCP connection to the TACACS+ daemon	<ol style="list-style-type: none"> 1. From the switch router, try to connect to port 49 by using Telnet on the TACACS+ daemon. 2. If the attempt to connect via Telnet is unsuccessful, make sure the daemon is running. For more information, see the “Daemon Is Not Up and Running” section on page B-3. 3. If the daemon is running but the Telnet connection times out, check the IP connectivity.

1. DNS = Domain Naming System
2. PPP = Point-to-Point Protocol
3. PAP = Password Authentication Protocol
4. CHAP = Challenge Handshake Authentication Protocol

Recovering a Lost Password

This section describes the procedure to recover a lost login or to enable a password. The procedure differs depending on the platform and the software used, but in all cases, password recovery requires that the switch router be taken out of operation and powered down.

If you need to perform the following procedure, make certain that there are secondary systems that can temporarily serve the functions of the switch router undergoing the procedure. If this is not possible, advise all potential users and, if possible, perform the procedure during low-use hours.



Note

Make a note of your password, and store it in a secure place.

All of the procedures for recovering lost passwords depend on changing the configuration register of the switch router. This is done by reconfiguring the switch router software.

More recent Cisco platforms run from Flash memory or are netbooted from a network server and can ignore the contents of nonvolatile random-access memory (NVRAM) when booting. By ignoring the contents of NVRAM, you can bypass the configuration file (which contains the passwords) and gain complete access to the switch router. You can then recover the lost password or configure a new one.



Note If your password is encrypted, you cannot recover it. You must configure a new password.

Follow these steps to recover a password:

-
- Step 1** Beginning in the privileged executive mode, enter the **show version** command and the configuration register value. The default value is 0x2102.
 - Step 2** Power cycle the switch router.
 - Step 3** Within 60 seconds of turning the switch router On, press the **Break** key sequence or send a break signal, which is usually `^]`. If you do not see the `>` prompt with no switch router name, the terminal is not sending the correct **Break** signal. In that case, check the terminal or terminal emulation setup.
 - Step 4** Enter the **confreg** command at the `>` prompt.
 - Step 5** Answer **yes** to the `Do you wish to change configuration [y/n]?` prompt.
 - Step 6** Answer **no** to all the questions that appear until you reach the `Ignore system config info [y/n]` prompt. Answer **yes**.
 - Step 7** Answer **no** to the remaining questions until you reach the `Change boot characteristics [y/n]?` prompt. Answer **yes**.
 - Step 8** At the `enter to boot:` prompt, enter **2**.
 - Step 9** Answer **no** to the `Do you wish to change configuration [y/n]?` prompt.
 - Step 10** Enter the **reset** command at the `rommon>` prompt.
 - Step 11** Enter the **enable** command at the `Switch>` prompt. You'll be in enable mode and see the `Switch#` prompt.
 - Step 12** Enter the **show startup-config** command to view your password.
 - Step 13** If your password is clear text, proceed to Step 16.
or
If your password is encrypted, continue with Step 14.
 - Step 14** If your password is encrypted, enter the **configure memory** command to copy the NVRAM into memory.
 - Step 15** Enter the **copy running-config startup-config** command.
 - Step 16** Enter the **configure terminal** command.
 - Step 17** Enter the **enable secret password** command.
 - Step 18** Enter the **config-register value** command, where *value* is whatever value you entered in Step 1.
 - Step 19** Enter the **exit** command to exit configuration mode.
 - Step 20** Enter the **copy running-config startup-config** command.
 - Step 21** Enter the **reload** command at the prompt.
-