Configuring TACACS+ on the Catalyst 1900 and 2820

Document ID: 9906

Contents

Introduction

The Catalyst 1900/2820 8.x Enterprise Edition release of software supports TACACS+ (not XTACACS). TACACS+ or CiscoSecure server user setup for authentication is the same as for router users. This technical tip describes setup on the Catalyst 1900 and 2820.

Note: Failover on the 1900 and 2820 is implemented differently than on other Cisco equipment. If the TACACS+ server is unreachable, the local passwords can be used or no authentication required (depending on how the switch is configured). Although, if the TACACS+ server is reachable but the TACACS+ daemon is down, local passwords and failover to no authentication will not be used (in other words, you will be locked out of the switch).

Note: HTTP web connections are always authenticated using the local password (not tacacs+). Use of menu options is not valid when TACACS+ is enabled. TACACS+ is used for command−line interface authentication.

Before You Begin

Conventions

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

Prerequisites

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Configuration Steps

1. From the command line interface (CLI), enable TACACS+ authentication for login using the command below.

```
login tacacs
```

2. Use the command below to tell the switch where the server is.

   ```
   tacacs−server host 1.1.1.1
   ```
3. Use the command below to tell the switch what the shared key is.

   ```
   tacacs−server key cisco
   ```
4. Choose one of the two options below.

   a. Use the command below to tell the switch the password to use if the TACACS+ server becomes unreachable.

      ```
      enable password level 1 cisco
      ```

      Use the command below to tell the switch to use the local password if the TACACS+ server becomes unreachable.

      ```
      tacacs−server last−resort password
      ```
   b. Use the command below to tell the switch to let users in without a password if the TACACS+ server becomes unreachable.

      ```
      tacacs−server last−resort succeed
      ```

   Before exiting the switch, Telnet to the switch from another session to be sure you can get in using TACACS+. Before exiting the switch, make the server unreachable to be sure you can get in without using TACACS+. The remaining steps are optional.
5. Use the command below to enable TACACS+ authentication for enable mode.

   ```
   enable use−tacacs
   ```

   Note: This step is necessary only if enable users are to be authenticated through the TACACS+ server; there also needs to be an enable entry in the server for this to work.
6. Use the command below to enable local authentication for enable mode if the TACACS+ server becomes unreachable.

   ```
   enable password level 15 cisco
   ```

   This password is valid only if tacacs−server last−resort password is also configured.
7. Use the command below to configure the number of login attempts allowed on the TACACS+ server.

   ```
   tacacs−server attempts number
   ```
8. Use the command below to set the timeout interval in which the server daemon must respond (this is optional, but could be necessary on a slow network.

   ```
   tacacs−server timeout N
   ```

Related Information

- **Technical Support − Cisco Systems**