Configure Cisco Router for Dial Authentication using TACACS+

Document ID: 13866

Contents

Introduction

This document describes how to configure a Cisco router for dial authentication with the TACACS+ that runs on UNIX. TACACS+ does not offer as many features as the commercially available Cisco Secure ACS for Windows or Cisco Secure ACS for UNIX.

TACACS+ Software previously provided by Cisco Systems has been discontinued and is no longer supported by Cisco Systems.

Today, you can find many available TACACS+ freeware versions when you search for "TACACS+ freeware" on your favorite Internet search engine. Cisco does not specifically recommend any particular TACACS+ freeware implementation.

Cisco Secure Access Control Server (ACS) is available for purchase through regular Cisco sales and distribution channels worldwide. Cisco Secure ACS for Windows includes all the necessary components needed for an independent installation on a Microsoft Windows workstation. The Cisco Secure ACS Solution Engine is shipped with a pre−installed Cisco Secure ACS software license. Refer to the Cisco Secure ACS 4.0 Product Bulletin for product numbers. Visit the Cisco Ordering Home Page (registered customers only) to place an order.

Note: You need a CCO account with an associated Service Contract to get the 90−day trial version for Cisco Secure ACS for Windows (registered customers only) .

The router configuration in this document was developed on a router that runs Cisco IOS® Software Release 11.3.3. Cisco IOS Software Releases 12.0.5.T and later use **group tacacs**+ instead of **tacacs**+. Statements such as **aaa authentication login default tacacs+ enable** appear as **aaa authentication login default group tacacs+ enable**.

You can download the TACACS+ freeware and User's Guide by anonymous ftp to ftp−eng.cisco.com in the /pub/tacacs directory.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configurations

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find additional information on the commands used in this document.

This document uses these configurations:

- Router Configuration
- TACACS+ Configuration File on Freeware Server

Router Configuration

```
!
aaa new−model
aaa authentication login default tacacs+ enable
aaa authentication ppp default if-needed tacacs+
aaa authorization exec default tacacs+ if-authenticated
aaa authorization commands 1 default tacacs+ if-authenticated
aaa authorization commands 15 default tacacs+ if-authenticated
aaa authorization network default tacacs+
enable password ww
!
chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
!
interface Ethernet0
 ip address 10.6.1.200 255.255.255.0
!

!--- Challenge Handshake Authentication Protocol
!--- (CHAP/PPP) authentication user.

  interface Async1
  ip unnumbered Ethernet0
  encapsulation ppp
  async mode dedicated
  peer default ip address pool async
  no cdp enable
  ppp authentication chap
```

```
 !

!--- Password Authentication Protocol (PAP/PPP) authentication user.

  interface Async2
  ip unnumbered Ethernet0
  encapsulation ppp
  async mode dedicated
  peer default ip address pool async
  no cdp enable
  ppp authentication pap
 !

!--- Authentication user with autocommand PPP.

  interface Async3
  ip unnumbered Ethernet0
  encapsulation ppp
  async mode interactive
  peer default ip address pool async
  no cdp enable
 !
 ip local pool async 10.6.100.101 10.6.100.103
 tacacs-server host 171.68.118.101
 tacacs-server timeout 10
 tacacs-server key cisco
 !
 line 1
  session-timeout 20
  exec-timeout 120 0
  autoselect during-login
  script startup default
  script reset default
  modem Dialin
  transport input all
  stopbits 1
  rxspeed 115200
  txspeed 115200
  flowcontrol hardware
 !
 line 2
  session-timeout 20
  exec-timeout 120 0
  autoselect during-login
  script startup default
  script reset default
  modem Dialin
  transport input all
  stopbits 1
  rxspeed 115200
  txspeed 115200
  flowcontrol hardware
 !
 line 3
  session-timeout 20
  exec-timeout 120 0
  autoselect during-login
  autoselect ppp
  script startup default
  script reset default
  modem Dialin
  autocommand ppp
  transport input all
  stopbits 1
  rxspeed 115200
  txspeed 115200
```

```
   flowcontrol hardware
 !
 end
```

Microsoft Windows Setup

Microsoft Windows Setup for Users 1 and 2

In this section, you are presented with the information to configure the features described in this document.

Step−by−Step Instructions

Complete these steps.

Note: The PC configuration can vary slightly based on the operating system version you use.

1. Select **Start** > **Programs** > **Accessories** > **Dial−Up Networking** to open the Dial−Up Networking window.
2. Choose **Make New Connection** from the Connections menu, and enter a name for your connection.
3. Enter your modem−specific information and click **Configure**.
4. On the General Properties page select the highest speed of your modem, but do not check the **Only connect at this speed**... box.
5. On the Configure/Connection Properties page, use 8 data bits, no parity, and 1 stop bit. Call preferences to use are **Wait for dial tone before dialing** and **Cancel the call if not connected after 200 seconds**.
6. On the Connection page, click **Advanced**. In the Advanced Connection Settings, select only **Hardware Flow Control** and **Modulation Type Standard**.

   On the Configure/Options properties page, nothing should be checked except the box under Status Control.
7. Click **OK** and then click **Next**.
8. Enter the telephone number of the destination, click **Next** again, and then click **Finish**.
9. Once the new connection icon appears, right−click it and choose **Properties > Server Type**.
10. Choose **PPP:WINDOWS 95, WINDOWS NT 3.5, Internet** and do not check any Advanced options.
11. Check **TCP/IP** under Allowed Network Protocols.
12. Under TCP/IP Settings..., choose **Server assigned IP address**, **Server assigned name server addresses**, and **Use default gateway on remote network** and then click **OK**.
13. When the user double−clicks the icon to make the Connect To window display in order to dial, the user must fill in the User Name and Password fields, and then click **Connect**.

Microsoft Windows Setup for User 3

Configuration for User 3 (authentication user with autocommand PPP) is the same as for Users 1 and 2 with these exceptions:

- On the Configure/Options properties page (step 6), check **Bring up terminal window after dialing**.
- When the user double−clicks the icon to open the Connect To window to dial (Step 13), the user does not fill in the User name and Password fields. The user clicks **Connect**. After the connection to the router is made, the user types in the username and password in the black window that appears. After authentication, the user presses **Continue (F7)**.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Router

Refer to Important Information on Debug Commands before you issue **debug** commands.

- **terminal monitor** Displays **debug** command output and system error messages for the current terminal and session.
- **debug ppp negotiation** Displays PPP packets sent during PPP startup, where PPP options are negotiated.

- **debug ppp packet** Displays PPP packets that are sent and received. (This command displays low–level packet dumps.)
- **debug ppp chap** Displays information about whether a client passes authentication (for Cisco IOS Software Releases earlier than 11.2) .
- **debug aaa authentication** Displays information on authentication, authorization, and accounting (AAA)/TACACS+ authentication.
- **debug aaa authorization** Displays information on AAA/TACACS+ authorization.

Server

Note: This assumes Cisco's TACACS+ Freeware server code.

```
tac_plus_executable −C config.file −d 16
  tail −f /var/tmp/tac_plus.log
```

Related Information

- **TACACS+ Support Page**
- **TACACS+ in IOS Documentation**
- **Cisco Secure Access Control Server**
- **Setting Up and Debugging CiscoSecure 2.x TACACS+**
- **Technical Support & Documentation – Cisco Systems**

Updated: May 14, 2009   Document ID: 13866