

Common Problems in Debugging TACACS+, PAP and CHAP

Document ID: 13864

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Common PC Settings

- Windows 95

- Windows NT

- Windows 98

- Windows 2000

Configurations and Debug Examples

- Commands for Other Cisco IOS Releases

- Sample Debugs – TACACS+ and PAP

- Commands for Other Cisco IOS Releases

- Sample Debugs – TACACS+ and CHAP

debug Commands

Related Information

Introduction

Note: The information in this document is based on Cisco IOS® Software Releases 11.2 and later.

This document examines common debugging problems for TACACS+ when Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) are used. Common PC settings for Microsoft Windows 95, Windows NT, Windows 98, and Windows 2000 are provided, as well as examples of configurations and examples of good and bad debugs.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Common PC Settings

Windows 95

Complete these steps:

1. In the Dialup Networking window, choose the connection name, then **File > Properties**.
2. On the Server Type tab, see if the **Require Encrypted Password** box beneath Type of Dial-up Server is checked.

- ◆ If this box is checked, the PC accepts only CHAP authentication.
- ◆ If this box is not checked, the PC accepts PAP or CHAP authentication.

Windows NT

Complete these steps:

1. In the Dial-Up Networking window, choose the connection name, and then choose **File > Properties**.
2. Check the settings on the Security tab:

- ◆ If the **Accept any authentication including clear text** box is checked, the PC accepts PAP or CHAP.
- ◆ If the **Accept only encrypted authentication** box is checked, the PC accepts only CHAP authentication.

Windows 98

Complete these steps:

1. In the Dial-Up Networking window, choose the connection name, and then choose **Properties**.
2. On the Server Types tab, check the settings in the Advanced Options area:

- ◆ If the **Require encrypted password** box is not checked, the PC accepts PAP or CHAP authentication.
- ◆ If the **Require encrypted password** box is checked, the PC accepts only CHAP authentication.

Windows 2000

Complete these steps:

1. In Network and Dial-Up Connections, choose the connection name, and then choose **Properties**.
2. On the Security tab, in the **Advanced > Settings > Allow these protocols** area:

- ◆ If the **Unencrypted password (PAP)** box is checked, the PC accepts PAP.
- ◆ If the **Challenge Handshake Authentication Protocol (CHAP)** box is checked, the PC accepts CHAP per RFC 1994 .
- ◆ If the **Microsoft CHAP (MS-CHAP)** box is checked, the PC accepts MS-CHAP version 1 and does not accept CHAP per RFC 1994.

Configurations and Debug Examples

Configuration – TACACS+ and PAP

Current configuration:

```
!  
version 11.2  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
service udp-small-servers  
service tcp-small-servers  
!  
hostname rtpkrb  
!  
aaa new-model  
!  
  
!--- The following four lines of the  
!--- configuration are specific to  
!--- Cisco IOS 11.2 and later, until 11.3.3.T.  
!--- See below this configuration  
!--- for commands for other Cisco IOS releases.  
  
!  
aaa authentication login default tacacs+ local  
aaa authentication ppp default if-needed tacacs+ local  
aaa authorization exec tacacs+ if-authenticated  
aaa authorization network tacacs+ if-authenticated  
enable secret 5 $1$pkX.$JdAysRE1SbdbDe7bj0wyt0  
enable password ww  
!  
username john password 0 doe  
username cse password 0 csecse  
ip host rtpkrb 10.31.1.5  
ip domain-name RTP.CISCO.COM  
ip name-server 171.68.118.103  
!  
interface Loopback0  
ip address 1.1.1.1 255.255.255.0  
!  
interface Ethernet0  
ip address 10.31.1.5 255.255.0.0  
no mop enabled  
!  
interface Serial0  
no ip address  
no ip mroute-cache  
shutdown  
!  
interface Serial1  
no ip address  
shutdown  
!  
interface Async1  
ip unnumbered Ethernet0  
encapsulation ppp  
async mode dedicated  
peer default ip address pool async  
no cdp enable  
ppp authentication pap  
!  
ip local pool async 15.15.15.15  
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 10.31.1.1
!
tacacs-server host 171.68.118.101
tacacs-server key cisco
snmp-server community public RW
snmp-server host 171.68.118.100 traps public
!
line con 0
line 1
session-timeout 20
exec-timeout 20 0
password ww
autoselect during-login
autoselect ppp
modem InOut
transport input all
stopbits 1
speed 38400
flowcontrol hardware
line 2
modem InOut
speed 38400
flowcontrol hardware
line 3 16
line aux 0
line vty 0 4
password ww
!
end
```

Commands for Other Cisco IOS Releases

Note: In order to use these commands, remove the commands in bold from the configuration and paste in these commands in, as dictated by your Cisco IOS release.

Cisco IOS 11.3.3.T until 12.0.5.T

```
aaa authen login default tacacs+ local
aaa authen ppp default if-needed tacacs+ local
aaa authorization exec default tacacs+ if-authenticated
aaa authorization network default tacacs+ if-authenticated
```

Cisco IOS 12.0.5.T and Later

```
aaa authen login default group tacacs+ local
aaa authen ppp default if-needed group tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization network default group tacacs+ if-authenticated
```

Sample Debugs – TACACS+ and PAP

Note: In the debug output, the bold text highlights problems in the debug. Plain text indicates a good debug.

```
rtpkrb#show debug
General OS:
TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on
PPP:
PPP authentication debugging is on
PPP protocol negotiation debugging is on
rtpkrb#
```

```
3d22h: %LINK-3-UPDOWN: Interface Async1, changed state to up
3d22h: As1 PPP: Treating connection as a dedicated line
3d22h: As1 PPP: Phase is ESTABLISHING, Active Open
3d22h: As1 LCP: O CONFREQ [Closed] id 14 len 24
3d22h: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
3d22h: As1 LCP: AuthProto PAP (0x0304C023)
3d22h: As1 LCP: MagicNumber 0xF45FB7A7 (0x0506F45FB7A7)
3d22h: As1 LCP: PFC (0x0702)
3d22h: As1 LCP: ACFC (0x0802)
```

```
!--- PC insists on doing CHAP
!--- ("accept encrypted authentication only"),
!--- but router is set up for PAP.
```

```
As1 LCP: I CONFNAK [REQsent] id 27 len 12
As1 LCP: AuthProto 0xC123 (0x0308C12301000001)
As1 PPP: Closing connection because remote won't authenticate
```

```
3d22h: As1 LCP: Interface transitioned, discarding packet
3d22h: As1 LCP: I CONFACK [REQsent] id 14 len 24
3d22h: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
3d22h: As1 LCP: AuthProto PAP (0x0304C023)
3d22h: As1 LCP: MagicNumber 0xF45FB7A7 (0x0506F45FB7A7)
3d22h: As1 LCP: PFC (0x0702)
3d22h: As1 LCP: ACFC (0x0802)
3d22h: As1 LCP: TIMEOUT: Time 0x14417CC4 State ACKrcvd
3d22h: As1 LCP: O CONFREQ [ACKrcvd] id 15 len 24
3d22h: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
3d22h: As1 LCP: AuthProto PAP (0x0304C023)
3d22h: As1 LCP: MagicNumber 0xF45FB7A7 (0x0506F45FB7A7)
3d22h: As1 LCP: PFC (0x0702)
3d22h: As1 LCP: ACFC (0x0802)
3d22h: As1 LCP: I CONFACK [REQsent] id 15 len 24
3d22h: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
3d22h: As1 LCP: AuthProto PAP (0x0304C023)
3d22h: As1 LCP: MagicNumber 0xF45FB7A7 (0x0506F45FB7A7)
3d22h: As1 LCP: PFC (0x0702)
3d22h: As1 LCP: ACFC (0x0802)
3d22h: As1 LCP: I CONFREQ [ACKrcvd] id 0 len 20
3d22h: As1 LCP: ACCM 0x00000000 (0x020600000000)
3d22h: As1 LCP: MagicNumber 0x000030A3 (0x0506000030A3)
3d22h: As1 LCP: PFC (0x0702)
3d22h: As1 LCP: ACFC (0x0802)
3d22h: As1 LCP: O CONFACK [ACKrcvd] id 0 len 20
3d22h: As1 LCP: ACCM 0x00000000 (0x020600000000)
3d22h: As1 LCP: MagicNumber 0x000030A3 (0x0506000030A3)
3d22h: As1 LCP: PFC (0x0702)
3d22h: As1 LCP: ACFC (0x0802)
3d22h: As1 LCP: State is Open
3d22h: As1 PPP: Phase is AUTHENTICATING, by this end
3d22h: As1 PAP: I AUTH-REQ id 4 len 20 from "papuser"
3d22h: As1 PAP: Authenticating peer papuser
3d22h: AAA/AUTHEN: create_user (0x16DAC0) user='papuser'
ruser='' port='Async1' rem_addr='async' authen_type=PAP
service=PPP priv=1
3d22h: AAA/AUTHEN/START (1190231344): port='Async1' list=''
action=LOGIN service=PPP
3d22h: AAA/AUTHEN/START (1190231344): using "default" list
3d22h: AAA/AUTHEN (1190231344): status = UNKNOWN
3d22h: AAA/AUTHEN/START (1190231344): Method=TACACS+
3d22h: TAC+: send AUTHEN/START packet ver=193 id=1190231344
3d22h: TAC+: Using default tacacs server list.
3d22h: TAC+: Opening TCP/IP to 171.68.118.101/49 timeout=5
```

*!--- The TAC+ server is down, producing an error.
!--- Since the user is not in the local database,
!--- the failover to local fails.*

**TAC+: TCP/IP open to 171.68.118.101/49 failed --
Connection refused by remote host
AAA/AUTHEN (866823886): status = ERROR
AAA/AUTHEN/START (866823886): Method=LOCAL
AAA/AUTHEN (866823886): status = FAIL**

3d22h: TAC+: Opened TCP/IP handle 0x16C1F8 to 171.68.118.101/49
3d22h: TAC+: 171.68.118.101 (1190231344) AUTHEN/START/LOGIN/PAP queued
3d22h: TAC+: (1190231344) AUTHEN/START/LOGIN/PAP processed

!--- The key in the router does not match that of the server.

**TAC+: received bad AUTHEN packet: length = 68, expected 67857
TAC+: Invalid AUTHEN/START packet (check keys)
AAA/AUTHEN (1771887965): status = ERROR**

3d22h: TAC+: ver=192 id=1190231344 received AUTHEN status = GETPASS
3d22h: TAC+: Closing TCP/IP 0x16C1F8 connection to 171.68.118.101/49
3d22h: TAC+: Opening TCP/IP to 171.68.118.101/49 timeout=5
3d22h: TAC+: Opened TCP/IP handle 0x16EF4C to 171.68.118.101/49
3d22h: TAC+: Opened 171.68.118.101 index=1
3d22h: AAA/AUTHEN: create_user (0x16C5EC) user='papuser' ruser=''
port='Async1' rem_addr='async' authen_type=PAP service=PPP priv=1
3d22h: TAC+: rev0 inbound pap login for id=1190231344 using id=3112896669
3d22h: TAC+: 171.68.118.101 (3112896669) AUTHEN/START/LOGIN/PAP queued
3d22h: TAC+: (3112896669) AUTHEN/START/LOGIN/PAP processed
3d22h: TAC+: ver=192 id=3112896669 received AUTHEN status = GETPASS
3d22h: TAC+: send AUTHEN/CONT packet
3d22h: TAC+: 171.68.118.101 (3112896669) AUTHEN/CONT queued
3d22h: TAC+: (3112896669) AUTHEN/CONT processed

*!--- The NT client sends the "DOMAIN\user"
!--- and the TAC+ server expects "user".*

**TAC+: ver=192 id=260507389 received AUTHEN status = FAIL
TAC+: rev0 inbound pap completed for 1139034411 status=FAIL
AAA/AUTHEN: free_user (0x16CDD4) user='CISCO\papuser' ruser=''
port='Async1' rem_addr='async' authen_type=PAP service=PPP priv=1**

*!--- The TAC+ server refuses the user
!--- because the user is set up for PAP.
!--- The user enters a bad password,
!--- or both the username and password are bad.*

**TAC+: ver=192 id=691012958 received AUTHEN status = FAIL
TAC+: rev0 inbound pap completed for 3917384959 status=FAIL
AAA/AUTHEN: free_user (0x15AD58) user='idochap' ruser=''
port='Async1' rem_addr='async' authen_type=PAP service=PPP priv=1**

3d22h: TAC+: ver=192 id=3112896669 received AUTHEN status = PASS
3d22h: TAC+: rev0 inbound pap completed for 1190231344 status=PASS
3d22h: AAA/AUTHEN: free_user (0x16C5EC) user='papuser' ruser=''
port='Async1' rem_addr='async' authen_type=PAP service=PPP priv=1
3d22h: TAC+: Closing TCP/IP 0x16EF4C connection to 171.68.118.101/49
3d22h: AAA/AUTHEN (1190231344): status = PASS
3d22h: AAA/AUTHOR/LCP As1: Authorize LCP
3d22h: AAA/AUTHOR/LCP: Async1: (1061976769): user='papuser'
3d22h: AAA/AUTHOR/LCP: Async1: (1061976769): send AV service=ppp
3d22h: AAA/AUTHOR/LCP: Async1: (1061976769): send AV protocol=lcp

```
3d22h: AAA/AUTHOR/LCP: Async1: (1061976769): Method=TACACS+
3d22h: AAA/AUTHOR/TAC+: (1061976769): user=papuser
3d22h: AAA/AUTHOR/TAC+: (1061976769): send AV service=ppp
3d22h: AAA/AUTHOR/TAC+: (1061976769): send AV protocol=lcp
3d22h: TAC+: Opening TCP/IP to 171.68.118.101/49 timeout=5
3d22h: TAC+: Opened TCP/IP handle 0x16C9E0 to 171.68.118.101/49
3d22h: TAC+: Opened 171.68.118.101 index=1
3d22h: TAC+: 171.68.118.101 (1061976769) AUTHOR/START queued
3d22h: TAC+: (1061976769) AUTHOR/START processed
```

```
!--- The user passes authentication
!--- (the username/password is good)
!--- but fails authorization
!--- (the profile is not set up to authorize PPP).
```

```
TAC+: (1793875816): received author response status = FAIL
TAC+: Closing TCP/IP 0x17054C connection to 171.68.118.101/49
AAA/AUTHOR (1793875816): Post authorization status = FAIL
AAA/AUTHOR/LCP As1: Denied
```

```
3d22h: TAC+: (1061976769): received author response status = PASS_ADD
3d22h: TAC+: Closing TCP/IP 0x16C9E0 connection to 171.68.118.101/49
3d22h: AAA/AUTHOR (1061976769): Post authorization status = PASS_ADD
3d22h: As1 PAP: O AUTH-ACK id 4 len 5
3d22h: As1 PPP: Phase is UP
3d22h: AAA/AUTHOR/FSM As1: (0): Can we start IPCP?
3d22h: AAA/AUTHOR/FSM: Async1: (3602788894): user='papuser'
3d22h: AAA/AUTHOR/FSM: Async1: (3602788894): send AV service=ppp
3d22h: AAA/AUTHOR/FSM: Async1: (3602788894): send AV protocol=ip
3d22h: AAA/AUTHOR/FSM: Async1: (3602788894): Method=TACACS+
3d22h: AAA/AUTHOR/TAC+: (3602788894): user=papuser
3d22h: AAA/AUTHOR/TAC+: (3602788894): send AV service=ppp
3d22h: AAA/AUTHOR/TAC+: (3602788894): send AV protocol=ip
3d22h: TAC+: Opening TCP/IP to 171.68.118.101/49 timeout=5
3d22h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
changed state to up
3d22h: TAC+: Opened TCP/IP handle 0x17054C to 171.68.118.101/49
3d22h: TAC+: Opened 171.68.118.101 index=1
3d22h: TAC+: 171.68.118.101 (3602788894) AUTHOR/START queued
3d22h: As1 IPCP: I CONFREQ [Closed] id 1 len 34
3d22h: As1 IPCP: Address 0.0.0.0 (0x030600000000)
3d22h: As1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
3d22h: As1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
3d22h: As1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
3d22h: As1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
3d22h: TAC+: (3602788894) AUTHOR/START processed
3d22h: TAC+: (3602788894): received author response status = PASS_ADD
3d22h: TAC+: Closing TCP/IP 0x17054C connection to 171.68.118.101/49
3d22h: AAA/AUTHOR (3602788894): Post authorization status = PASS_ADD
3d22h: AAA/AUTHOR/FSM As1: We can start IPCP
3d22h: As1 IPCP: O CONFREQ [Closed] id 10 len 10
3d22h: As1 IPCP: Address 10.31.1.5 (0x03060A1F0105)
3d22h: As1 IPCP: I CONFACK [REQsent] id 10 len 10
3d22h: As1 IPCP: Address 10.31.1.5 (0x03060A1F0105)
3d22h: As1 IPCP: I CONFREQ [ACKrcvd] id 1 len 34
3d22h: As1 IPCP: Address 0.0.0.0 (0x030600000000)
3d22h: As1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
3d22h: As1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
3d22h: As1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
3d22h: As1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
3d22h: AAA/AUTHOR/IPCP As1: Start. Her address 0.0.0.0,
we want 0.0.0.0
3d22h: AAA/AUTHOR/IPCP As1: Processing AV service=ppp
3d22h: AAA/AUTHOR/IPCP As1: Processing AV protocol=ip
3d22h: AAA/AUTHOR/IPCP As1: Authorization succeeded
```

```

3d22h: AAA/AUTHOR/IPCP As1: Done. Her address 0.0.0.0,
we want 0.0.0.0
3d22h: As1 IPCP: Using pool 'async'
3d22h: As1 IPCP: Pool returned 15.15.15.15
3d22h: As1 IPCP: O CONFREQ [ACKrcvd] id 1 len 22
3d22h: As1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
3d22h: As1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
3d22h: As1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
3d22h: As1 IPCP: I CONFREQ [ACKrcvd] id 2 len 16
3d22h: As1 IPCP: Address 0.0.0.0 (0x030600000000)
3d22h: As1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
3d22h: AAA/AUTHOR/IPCP As1: Start. Her address 0.0.0.0,
we want 15.15.15.15
3d22h: AAA/AUTHOR/IPCP As1: Processing AV service=ppp
3d22h: AAA/AUTHOR/IPCP As1: Processing AV protocol=ip
3d22h: AAA/AUTHOR/IPCP As1: Authorization succeeded
3d22h: AAA/AUTHOR/IPCP As1: Done. Her address 0.0.0.0,
we want 15.15.15.15
3d22h: As1 IPCP: O CONFNAK [ACKrcvd] id 2 len 16
3d22h: As1 IPCP: Address 15.15.15.15 (0x03060F0F0F0F)
3d22h: As1 IPCP: PrimaryDNS 171.68.118.103 (0x8106AB447667)
3d22h: As1 IPCP: I CONFREQ [ACKrcvd] id 3 len 16
3d22h: As1 IPCP: Address 15.15.15.15 (0x03060F0F0F0F)
3d22h: As1 IPCP: PrimaryDNS 171.68.118.103 (0x8106AB447667)
3d22h: AAA/AUTHOR/IPCP As1: Start. Her address 15.15.15.15,
we want 15.15.15.15
3d22h: AAA/AUTHOR/IPCP: Async1: (3654974050): user='papuser'
3d22h: AAA/AUTHOR/IPCP: Async1: (3654974050): send AV service=ppp
3d22h: AAA/AUTHOR/IPCP: Async1: (3654974050): send AV protocol=ip
3d22h: AAA/AUTHOR/IPCP: Async1: (3654974050): send AV addr*15.15.15.15
3d22h: AAA/AUTHOR/IPCP: Async1: (3654974050): Method=TACACS+
3d22h: AAA/AUTHOR/TAC+: (3654974050): user=papuser
3d22h: AAA/AUTHOR/TAC+: (3654974050): send AV service=ppp
3d22h: AAA/AUTHOR/TAC+: (3654974050): send AV protocol=ip
3d22h: AAA/AUTHOR/TAC+: (3654974050): send AV addr*15.15.15.15
3d22h: TAC+: Opening TCP/IP to 171.68.118.101/49 timeout=5
3d22h: TAC+: Opened TCP/IP handle 0x16EF4C to 171.68.118.101/49
3d22h: TAC+: Opened 171.68.118.101 index=1
3d22h: TAC+: 171.68.118.101 (3654974050) AUTHOR/START queued
3d22h: TAC+: (3654974050) AUTHOR/START processed
3d22h: TAC+: (3654974050): received author response status = PASS_ADD
3d22h: TAC+: Closing TCP/IP 0x16EF4C connection to 171.68.118.101/49
3d22h: AAA/AUTHOR (3654974050): Post authorization status = PASS_ADD
3d22h: AAA/AUTHOR/IPCP As1: Processing AV service=ppp
3d22h: AAA/AUTHOR/IPCP As1: Processing AV protocol=ip
3d22h: AAA/AUTHOR/IPCP As1: Processing AV addr*15.15.15.15
3d22h: AAA/AUTHOR/IPCP As1: Authorization succeeded
3d22h: AAA/AUTHOR/IPCP As1: Done. Her address 15.15.15.15,
we want 15.15.15.15
3d22h: As1 IPCP: O CONFACK [ACKrcvd] id 3 len 16
3d22h: As1 IPCP: Address 15.15.15.15 (0x03060F0F0F0F)
3d22h: As1 IPCP: PrimaryDNS 171.68.118.103 (0x8106AB447667)
3d22h: As1 IPCP: State is Open
3d22h: As1 IPCP: Install route to 15.15.15.15
rtpkrb#

```

Configuration – TACACS+ and CHAP

```

Current configuration:
!
version 11.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers

```

```
!  
hostname rtpkrb  
!  
aaa new-model  
!  
  
!--- The following four lines of the configuration  
!--- are specific to Cisco IOS 11.2 and later, until 11.3.3.T.  
!--- See below this configuration  
!--- for commands for other Cisco IOS releases.  
  
!  
aaa authentication login default tacacs+ local  
aaa authentication ppp default if-needed tacacs+ local  
aaa authorization exec tacacs+ if-authenticated  
aaa authorization network tacacs+ if-authenticated  
enable secret 5 $1$pkX.$JdAySRE1SbdbDe7bj0wyt0  
enable password ww  
!  
username john password 0 doe  
username cse password 0 csecse  
ip host rtpkrb 10.31.1.5  
ip name-server 171.68.118.103  
!  
interface Loopback0  
ip address 1.1.1.1 255.255.255.0  
!  
interface Ethernet0  
ip address 10.31.1.5 255.255.0.0  
no mop enabled  
!  
interface Serial0  
no ip address  
no ip mroute-cache  
shutdown  
!  
interface Serial1  
no ip address  
shutdown  
!  
interface Async1  
ip unnumbered Ethernet0  
encapsulation ppp  
async mode dedicated  
peer default ip address pool async  
no cdp enable  
ppp authentication chap  
!  
ip local pool async 15.15.15.15  
ip classless  
ip route 0.0.0.0 0.0.0.0 10.31.1.1  
!  
tacacs-server host 171.68.118.101  
tacacs-server key cisco  
snmp-server community public RW  
snmp-server host 171.68.118.100 traps public  
!  
line con 0  
line 1  
session-timeout 20  
exec-timeout 20 0  
password ww  
autoselect during-login  
autoselect ppp  
modem InOut  
transport input all
```

```
stopbits 1
speed 38400
flowcontrol hardware
line 2
modem InOut
speed 38400
flowcontrol hardware
line 3 16
line aux 0
line vty 0 4
password ww
!
end
```

Commands for Other Cisco IOS Releases

Note: Note: To use these commands, remove the commands in bold from the configuration and paste these commands in, as dictated by your Cisco IOS release.

Cisco IOS 11.3.3.T until 12.0.5.T

```
aaa authen login default tacacs+ local
aaa authen ppp default if-needed tacacs+ local
aaa authorization exec default tacacs+ if-authenticated
aaa authorization network default tacacs+ if-authenticated
```

Cisco IOS 12.0.5.T and Later

```
aaa authen login default group tacacs+ local
aaa authen ppp default if-needed group tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization network default group tacacs+ if-authenticated
```

Sample Debugs – TACACS+ and CHAP

Note: In the debug output, the bold text highlights problems in the debug. Plain text indicates a good debug.

```
General OS:
TACACS access control debugging is on
AAA Authentication debugging is on
AAA Authorization debugging is on
PPP:
PPP authentication debugging is on
PPP protocol negotiation debugging is on
rtpkrb#
3d22h: As1 LCP: I CONFREQ [Closed] id 0 len 20
3d22h: As1 LCP: ACCM 0x00000000 (0x020600000000)
3d22h: As1 LCP: MagicNumber 0x000042C5 (0x0506000042C5)
3d22h: As1 LCP: PFC (0x0702)
3d22h: As1 LCP: ACFC (0x0802)
3d22h: As1 LCP: Lower layer not up, discarding packet
3d22h: %LINK-3-UPDOWN: Interface Async1, changed state to up
3d22h: As1 PPP: Treating connection as a dedicated line
3d22h: As1 PPP: Phase is ESTABLISHING, Active Open
3d22h: As1 LCP: O CONFREQ [Closed] id 12 len 25
3d22h: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
3d22h: As1 LCP: AuthProto CHAP (0x0305C22305)
3d22h: As1 LCP: MagicNumber 0xF45D776F (0x0506F45D776F)
3d22h: As1 LCP: PFC (0x0702)
3d22h: As1 LCP: ACFC (0x0802)
3d22h: As1 LCP: I CONFACK [REQsent] id 12 len 25
3d22h: As1 LCP: ACCM 0x000A0000 (0x0206000A0000)
```

```
3d22h: As1 LCP: AuthProto CHAP (0x0305C22305)
3d22h: As1 LCP: MagicNumber 0xF45D776F (0x0506F45D776F)
3d22h: As1 LCP: PFC (0x0702)
3d22h: As1 LCP: ACFC (0x0802)
3d22h: As1 LCP: I CONFREQ [ACKRcvd] id 0 len 20
3d22h: As1 LCP: ACCM 0x00000000 (0x020600000000)
3d22h: As1 LCP: MagicNumber 0x000042C5 (0x0506000042C5)
3d22h: As1 LCP: PFC (0x0702)
3d22h: As1 LCP: ACFC (0x0802)
3d22h: As1 LCP: O CONFACK [ACKRcvd] id 0 len 20
3d22h: As1 LCP: ACCM 0x00000000 (0x020600000000)
3d22h: As1 LCP: MagicNumber 0x000042C5 (0x0506000042C5)
3d22h: As1 LCP: PFC (0x0702)
3d22h: As1 LCP: ACFC (0x0802)
3d22h: As1 LCP: State is Open
3d22h: As1 PPP: Phase is AUTHENTICATING, by this end
3d22h: As1 CHAP: O CHALLENGE id 3 len 27 from "rtppkrb"
3d22h: As1 CHAP: I RESPONSE id 3 len 29 from "chapuser"
3d22h: AAA/AUTHEN: create_user (0x15B394) user='chapuser'
ruser='' port='Async1' rem_addr='async' authen_type=CHAP
service=PPP priv=1
3d22h: AAA/AUTHEN/START (2183639772): port='Async1' list=''
action=LOGIN service=PPP
3d22h: AAA/AUTHEN/START (2183639772): using "default" list
3d22h: AAA/AUTHEN (2183639772): status = UNKNOWN
3d22h: AAA/AUTHEN/START (2183639772): Method=TACACS+
3d22h: TAC+: send AUTHEN/START packet ver=193 id=2183639772
3d22h: TAC+: Using default tacacs server list.
3d22h: TAC+: Opening TCP/IP to 171.68.118.101/49 timeout=5
```

```
!--- The TAC+ server is down, producing an error.
!--- Since the user is not in the local database,
!--- the failover to local fails.
```

```
TAC+: TCP/IP open to 171.68.118.101/49 failed --
Connection refused by remote host
AAA/AUTHEN (2546660185): status = ERROR
AAA/AUTHEN/START (2546660185): Method=LOCAL
AAA/AUTHEN (2546660185): status = FAIL
As1 CHAP: Unable to validate Response. Username chapuser: Authentication failure
```

```
3d22h: TAC+: Opened TCP/IP handle 0x17054C to 171.68.118.101/49
3d22h: TAC+: 171.68.118.101 (2183639772) AUTHEN/START/LOGIN/CHAP queued
3d22h: TAC+: (2183639772) AUTHEN/START/LOGIN/CHAP processed
```

```
!--- The key in the router does not match that of the server.
```

```
TAC+: received bad AUTHEN packet: length = 68, expected 67857
TAC+: Invalid AUTHEN/START packet (check keys)
AAA/AUTHEN (1771887965): status = ERROR
```

```
3d22h: TAC+: ver=192 id=2183639772 received AUTHEN status = GETPASS
3d22h: TAC+: Closing TCP/IP 0x17054C connection to 171.68.118.101/49
3d22h: TAC+: Opening TCP/IP to 171.68.118.101/49 timeout=5
3d22h: TAC+: Opened TCP/IP handle 0x16EF4C to 171.68.118.101/49
3d22h: TAC+: Opened 171.68.118.101 index=1
3d22h: AAA/AUTHEN: create_user (0x170940) user='chapuser' ruser=''
port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1
3d22h: TAC+: rev0 inbound chap for id=2183639772 using id=166703029
3d22h: TAC+: 171.68.118.101 (166703029) AUTHEN/START/SENDPASS/CHAP queued
3d22h: TAC+: (166703029) AUTHEN/START/SENDPASS/CHAP processed
```

```
!--- The NT client sends the "DOMAIN\user"
```

!--- and the TAC+ server expects "user".

TAC+: ver=192 id=3373385106 received AUTHEN status = FAIL
TAC+: rev0 inbound chap FAIL for id=2082151566
AAA/AUTHEN: free_user (0x170940) user='CISCO\chapuser' ruser=''
port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1

*!--- The TAC+ server refuses the user
!--- because the user is set up for PAP.
!--- The user enters a bad password,
!--- or both the username and password are bad.*

TAC+: ver=192 id=1989464562 received AUTHEN status = PASS
TAC+: rev0 inbound chap SENDPASS status=PASS for id=3657266965
TAC+: rev0 inbound chap MD5 compare FAILED
AAA/AUTHEN: free_user (0x170940) user='chapuser' ruser=''
port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1
TAC+: Closing TCP/IP 0x16EF4C connection to 171.68.118.101/49
AAA/AUTHEN (2082151566): status = FAIL
As1 CHAP: Unable to validate Response. Username papuser: Authentication failure

3d22h: TAC+: ver=192 id=166703029 received AUTHEN status = PASS
3d22h: TAC+: rev0 inbound chap SENDPASS status=PASS for id=2183639772
3d22h: TAC+: rev0 inbound chap MD5 compare OK
3d22h: AAA/AUTHEN: free_user (0x170940) user='chapuser' ruser=''
port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1
3d22h: TAC+: Closing TCP/IP 0x16EF4C connection to 171.68.118.101/49
3d22h: AAA/AUTHEN (2183639772): status = PASS
3d22h: AAA/AUTHOR/LCP As1: Authorize LCP
3d22h: AAA/AUTHOR/LCP: Async1: (683360936): user='chapuser'
3d22h: AAA/AUTHOR/LCP: Async1: (683360936): send AV service=ppp
3d22h: AAA/AUTHOR/LCP: Async1: (683360936): send AV protocol=lcp
3d22h: AAA/AUTHOR/LCP: Async1: (683360936): Method=TACACS+
3d22h: AAA/AUTHOR/TAC+: (683360936): user=chapuser
3d22h: AAA/AUTHOR/TAC+: (683360936): send AV service=ppp
3d22h: AAA/AUTHOR/TAC+: (683360936): send AV protocol=lcp
3d22h: TAC+: Opening TCP/IP to 171.68.118.101/49 timeout=5
3d22h: TAC+: Opened TCP/IP handle 0x16C1F8 to 171.68.118.101/49
3d22h: TAC+: Opened 171.68.118.101 index=1
3d22h: TAC+: 171.68.118.101 (683360936) AUTHOR/START queued
3d22h: TAC+: (683360936) AUTHOR/START processed

*!--- The user passes authentication
!--- (the username/password is good)
!--- but fails authorization
!--- (the profile is not set up to authorize PPP).*

TAC+: (3803447096): received author response status = FAIL
TAC+: Closing TCP/IP 0x16C2A4 connection to 171.68.118.101/49
AAA/AUTHOR (3803447096): Post authorization status = FAIL
AAA/AUTHOR/LCP As1: Denied
AAA/AUTHEN: free_user (0x15B2E8) user='noauth' ruser='' port='Async1'
rem_addr='async' authen_type=CHAP service=PPP priv=1
As1 CHAP: 0 FAILURE id 9 len 24 msg is "Authorization failed"

3d22h: TAC+: (683360936): received author response status = PASS_ADD
3d22h: TAC+: Closing TCP/IP 0x16C1F8 connection to 171.68.118.101/49
3d22h: AAA/AUTHOR (683360936): Post authorization status = PASS_ADD
3d22h: As1 CHAP: 0 SUCCESS id 3 len 4
3d22h: As1 PPP: Phase is UP
3d22h: AAA/AUTHOR/FSM As1: (0): Can we start IPCP?
3d22h: AAA/AUTHOR/FSM: Async1: (977509495): user='chapuser'
3d22h: AAA/AUTHOR/FSM: Async1: (977509495): send AV service=ppp
3d22h: AAA/AUTHOR/FSM: Async1: (977509495): send AV protocol=ip

3d22h: AAA/AUTHOR/FSM: Async1: (977509495): Method=TACACS+
3d22h: AAA/AUTHOR/TAC+: (977509495): user=chapuser
3d22h: AAA/AUTHOR/TAC+: (977509495): send AV service=ppp
3d22h: AAA/AUTHOR/TAC+: (977509495): send AV protocol=ip
3d22h: TAC+: Opening TCP/IP to 171.68.118.101/49 timeout=5
3d22h: TAC+: Opened TCP/IP handle 0x16EF4C to 171.68.118.101/49
3d22h: TAC+: Opened 171.68.118.101 index=1
3d22h: TAC+: 171.68.118.101 (977509495) AUTHOR/START queued
3d22h: As1 IPCP: I CONFREQ [Closed] id 1 len 34
3d22h: As1 IPCP: Address 0.0.0.0 (0x030600000000)
3d22h: As1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
3d22h: As1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
3d22h: As1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
3d22h: As1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
3d22h: TAC+: (977509495) AUTHOR/START processed
3d22h: TAC+: (977509495): received author response status = PASS_ADD
3d22h: TAC+: Closing TCP/IP 0x16EF4C connection to 171.68.118.101/49
3d22h: AAA/AUTHOR (977509495): Post authorization status = PASS_ADD
3d22h: AAA/AUTHOR/FSM As1: We can start IPCP
3d22h: As1 IPCP: O CONFREQ [Closed] id 8 len 10
3d22h: As1 IPCP: Address 10.31.1.5 (0x03060A1F0105)
3d22h: As1 IPCP: I CONFACK [REQsent] id 8 len 10
3d22h: As1 IPCP: Address 10.31.1.5 (0x03060A1F0105)
3d22h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
changed state to up
3d22h: As1 IPCP: I CONFREQ [ACKrcvd] id 1 len 34
3d22h: As1 IPCP: Address 0.0.0.0 (0x030600000000)
3d22h: As1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
3d22h: As1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
3d22h: As1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
3d22h: As1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
3d22h: AAA/AUTHOR/IPCP As1: Start. Her address 0.0.0.0,
we want 0.0.0.0
3d22h: AAA/AUTHOR/IPCP As1: Processing AV service=ppp
3d22h: AAA/AUTHOR/IPCP As1: Processing AV protocol=ip
3d22h: AAA/AUTHOR/IPCP As1: Authorization succeeded
3d22h: AAA/AUTHOR/IPCP As1: Done. Her address 0.0.0.0,
we want 0.0.0.0
3d22h: As1 IPCP: Using pool 'async'
3d22h: As1 IPCP: Pool returned 15.15.15.15
3d22h: As1 IPCP: O CONFREQ [ACKrcvd] id 1 len 22
3d22h: As1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
3d22h: As1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
3d22h: As1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
3d22h: As1 IPCP: I CONFREQ [ACKrcvd] id 2 len 16
3d22h: As1 IPCP: Address 0.0.0.0 (0x030600000000)
3d22h: As1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
3d22h: AAA/AUTHOR/IPCP As1: Start. Her address 0.0.0.0,
we want 15.15.15.15
3d22h: AAA/AUTHOR/IPCP As1: Processing AV service=ppp
3d22h: AAA/AUTHOR/IPCP As1: Processing AV protocol=ip
3d22h: AAA/AUTHOR/IPCP As1: Authorization succeeded
3d22h: AAA/AUTHOR/IPCP As1: Done. Her address 0.0.0.0,
we want 15.15.15.15
3d22h: As1 IPCP: O CONFNAK [ACKrcvd] id 2 len 16
3d22h: As1 IPCP: Address 15.15.15.15 (0x03060F0F0F0F)
3d22h: As1 IPCP: PrimaryDNS 171.68.118.103 (0x8106AB447667)
3d22h: As1 IPCP: I CONFREQ [ACKrcvd] id 3 len 16
3d22h: As1 IPCP: Address 15.15.15.15 (0x03060F0F0F0F)
3d22h: As1 IPCP: PrimaryDNS 171.68.118.103 (0x8106AB447667)
3d22h: AAA/AUTHOR/IPCP As1: Start. Her address 15.15.15.15,
we want 15.15.15.15
3d22h: AAA/AUTHOR/IPCP: Async1: (3918374858): user='chapuser'
3d22h: AAA/AUTHOR/IPCP: Async1: (3918374858): send AV service=ppp
3d22h: AAA/AUTHOR/IPCP: Async1: (3918374858): send AV protocol=ip
3d22h: AAA/AUTHOR/IPCP: Async1: (3918374858): send AV addr*15.15.15.15

```
3d22h: AAA/AUTHOR/IPCP: Async1: (3918374858): Method=TACACS+
3d22h: AAA/AUTHOR/TAC+: (3918374858): user=chapuser
3d22h: AAA/AUTHOR/TAC+: (3918374858): send AV service=ppp
3d22h: AAA/AUTHOR/TAC+: (3918374858): send AV protocol=ip
3d22h: AAA/AUTHOR/TAC+: (3918374858): send AV addr*15.15.15.15
3d22h: TAC+: Opening TCP/IP to 171.68.118.101/49 timeout=5
3d22h: TAC+: Opened TCP/IP handle 0x16C9E0 to 171.68.118.101/49
3d22h: TAC+: Opened 171.68.118.101 index=1
3d22h: TAC+: 171.68.118.101 (3918374858) AUTHOR/START queued
3d22h: TAC+: (3918374858) AUTHOR/START processed
3d22h: TAC+: (3918374858): received author response status = PASS_ADD
3d22h: TAC+: Closing TCP/IP 0x16C9E0 connection to 171.68.118.101/49
3d22h: AAA/AUTHOR (3918374858): Post authorization status = PASS_ADD
3d22h: AAA/AUTHOR/IPCP As1: Processing AV service=ppp
3d22h: AAA/AUTHOR/IPCP As1: Processing AV protocol=ip
3d22h: AAA/AUTHOR/IPCP As1: Processing AV addr*15.15.15.15
3d22h: AAA/AUTHOR/IPCP As1: Authorization succeeded
3d22h: AAA/AUTHOR/IPCP As1: Done. Her address 15.15.15.15,
we want 15.15.15.15
3d22h: As1 IPCP: O CONFACK [ACKrcvd] id 3 len 16
3d22h: As1 IPCP: Address 15.15.15.15 (0x03060F0F0F0F)
3d22h: As1 IPCP: PrimaryDNS 171.68.118.103 (0x8106AB447667)
3d22h: As1 IPCP: State is Open
3d22h: As1 IPCP: Install route to 15.15.15.15
rtpkrb#
```

debug Commands

These debug commands were used to produce the sample debug output in this document.

Note: Before you issue debug commands, refer to [Important Information on Debug Commands](#).

- **debug aaa authentication** Displays information on AAA authentication.
- **debug aaa authorization** Displays information on AAA authorization.
- **debug tacacs+** Displays detailed debugging information associated with TACACS+.
- **debug ppp negotiation** Displays PPP packets transmitted during PPP startup, where PPP options are negotiated.

Related Information

- [TACACS+ in IOS Documentation](#)
- [TACACS+ Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 19, 2006

Document ID: 13864
