Configuring Cisco IOS Software and Windows 2000 for PPTP Using Microsoft IAS

Document ID: 3885

Contents

Introduction

Point−to−Point Tunnel Protocol (PPTP) support was added to Cisco IOS® Software Release 12.0.5.XE5 on the Cisco 7100 and 7200 router platforms. Support for more platforms was added in Cisco IOS Software Release 12.1.5.T.

Request for Comments (RFC) 2637 describes PPTP. According to this RFC, the PPTP Access Concentrator (PAC) is the client (that is, the PC or the caller) and the PPTP Network Server (PNS) is the server (that is, the router or the device being called).

Prerequisites

Requirements

This document assumes that you have set up PPTP connections to the router with local Microsoft−Challenge Handshake Authentication Protocol (MS−CHAP) V1 authentication (and optionally Microsoft Point−to−Point Encryption [MPPE] which requires MS−CHAP V1) using these documents, and that they are already working. Remote Authentication Dial−In User Service (RADIUS) is required for MPPE encryption support; TACACS+ works for authentication, but not for MPPE keying.

Components Used

The information in this document is based on the software and hardware versions below.

- Microsoft IAS optional component installed on a Microsoft 2000 advanced server with Active Directory.
- A Cisco 3600 router.
- Cisco IOS Software Release c3640−io3s56i−mz.121−5.T.

This configuration uses Microsoft IAS installed on a Windows 2000 advanced server as the RADIUS server.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Conventions

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

Background Theory

This sample configuration demonstrates how to set up a PC to connect to the router (at the address 10.200.20.2), which then authenticates the user to Microsoft's Internet Authentication Server (IAS) (at 10.200.20.245) before allowing the user into the network. PPTP support is available with Cisco Secure Access Control Server (ACS) Version 2.5 for Windows. However, it may not work with the router due to Cisco Bug ID CSCds92266. If you are using Cisco Secure, we recommend using Cisco Secure Version 2.6 or above. Cisco Secure UNIX does not support MPPE. Two other RADIUS applications with MPPE support are Microsoft RADIUS and Funk RADIUS.

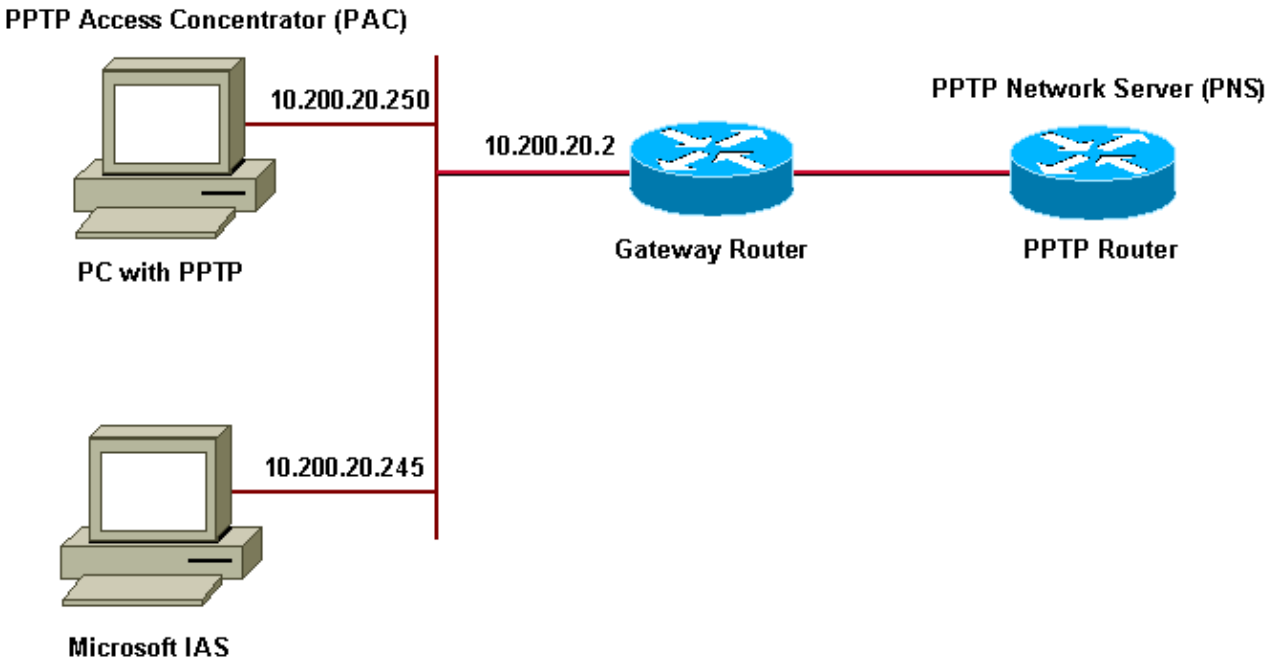
Configure

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

Note: To find additional information on the commands used in this document, use the IOS Command Lookup tool

Network Diagram

This document uses the network setup shown in the diagram below.



IP Pool for dial−up clients:

- Gateway Router: 192.168.1.2 ~ 192.168.1.254
- LNS: 172.16.10.1 ~ 172.16.10.10

Although the above setup uses a dial−up client to connect to the Internet service provider (ISP) router via dial−up, you can connect the PC and Gateway router via any media, such as a LAN.

Configuring the Windows 2000 Advanced Server for Microsoft IAS

This section shows how to configure the Windows 2000 advanced server for Microsoft IAS:

1. Ensure that Microsoft IAS is installed. To install Microsoft IAS, log in as an administrator. Under **Network Services**, verify that all check boxes are cleared. Select the Internet Authentication Server check box and then click **OK**.
2. In the **Windows Components** wizard, click **Next**. If prompted, insert the Windows 2000 CD.
3. After the required files have been copied click **Finish** and then close all windows. You do not need to reboot.

Configuring Radius Clients

This section shows the steps to configure radius clients:

1. From **Administrative Tools**, open the **Internet Authentication Server** Console and click on **Clients**.
2. In the **Friendly Name** box, type the IP address of the network access server (NAS).
3. Click on the **Use this IP** option.
4. In the **Client−Vendor** drop down list box, ensure that the **RADIUS Standard** option is selected.
5. In the **Shared Secret** and **Confirm Shared Secret** boxes, type the password and then click **Finish**.
6. In the console tree, right click on **Internet Authentication Service**, and then click **Start**.
7. Close the console.

Configuring Users on IAS

Unlike Cisco Secure, The Windows 2000 RADIUS user database is tightly bound to the Windows user database. In case an **Active Directory** is installed on your Windows 2000 server, create your new dial−up users from **Active Directory Users and Computers**. If **Active Directory** is not installed, use **Local Users and Groups** from **Administrative tools** to create new users.

Configuring Users in the Active Directory

This section shows the steps to configure users in the active directory:

1. In the **Active Directory Users and Computers** console, expand your domain. Right−click **Users**. Scroll to select **New User**. Create a new user called **tac**.
2. Type a password in the **Password** and **Confirm Password** dialog boxes.
3. Clear the **User Must Change Password at Next Logon** field and click **Next**.
4. Open the **User tac Properties** box. Switch to the **Dial−In** tab. Under **Remote Access Permission (Dial−in or VPN)**, click Allow Access, then click **OK**.

Configuring Users If No Active Directory is Installed

This section shows the steps to configure users if no active directory is installed:

1. From the **Administrative Tools** section, click on **Computer Management**. Expand the **Computer Management** console and click on **Local Users and Groups**. Right−click on the **Users** scroll bar to select **New User**. Create a new user called **tac**.
2. Type a password in the **Password** and **Confirm Password** dialog boxes.
3. Clear the **User Must Change Password at Next Logon** option and click **Next**.
4. Open the new user called **tac's Properties** box. Switch to the **Dial−in** tab. Under **Remote Access Permission (Dial−in or VPN)**, click **Allow Access**, then click **OK**.

Applying a Remote Access Policy to the Windows User

This section shows the steps to apply a remote access policy to the Windows user:

1. From **Administrative Tools**, open the **Internet Authentication Server** Console and click on **Remote Access Policies**.
2. Click the **Add** button on **Specify the Conditions to Match**, and add **Service−Type**. Choose the available type as **Framed** and add it to the **Selected Types** list. Press **OK**.
3. Click the **Add** button on **Specify the Conditions to Match** and add **Framed Protocol**. Choose the available type as **ppp** and add it to the **Selected Types** list. Press **OK**.
4. Click the **Add** button on **Specify the Conditions to Match** and add **Windows−Groups** to add the Windows group the user belongs to. Choose the group and add it to the **Selected Types** and press **OK**.
5. On the **Allow Access if Dial−in Permission is Enabled** properties, select **Grant remote Access permission**.
6. Close the console.

Configuring the Windows 2000 Client for PPTP

The section below shows the steps to configure the Windows 2000 client for PPTP:

1. From the **Start** menu, select **Settings**, then either:

- **Control Panel** and **Network and Dial−up Connections**, or
- **Network and Dial−up Connections** then **Make New Connection**.

Use the **Wizard** to create a connection called **PPTP**. This connection connects to a private network through the Internet. You also need to specify the PPTP Network Server (PNS) IP address or name.

2. The new connection appears in the **Network and Dial−up Connections** window under **Control Panel**.

   From here, click on the right hand mouse button to edit its properties. Under the **Networking Tab**, make sure that the **Type of Server I Am Calling** field is set to PPTP. If you plan to allocate a dynamic internal address to this client from the gateway, either via a local pool or Dynamic Host Configuration Protocol (DHCP), select **TCP/IP protocol**, and make sure the client is configured to obtain an IP address automatically. You may also issue DNS information automatically.

   The **Advanced** button allows you to define static Windows Internet Naming Service (WINS) and DNS information.

   The **Options** tab allows you to turn off IPSec or assign a different policy to the connection.
3. Under the **Security** tab, you can define the user authentication parameters. For example, PAP, CHAP or MS−CHAP, or Windows domain logon. Once the connection is configured, you can double click on it to display the login screen and then connect.

Configurations

Using the following router configuration, the user is able to connect with username **tac** and password **admin** even if the RADIUS server is unavailable (this is possible when the Microsoft IAS is yet to be configured). The following sample configuration outlines the commands required for L2tp without IPSec.

angela

```
angela#show running−config
Building configuration...
Current configuration : 1606 bytes
!
version 12.1
no service single−slot−reload−enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password−encryption
!
hostname angela
!
logging rate−limit console 10 except errors

!−−−Enable AAA services here

aaa new−model
aaa authentication login default group radius local
aaa authentication login console none
aaa authentication ppp default group radius local
aaa authorization network default group radius local
enable password
!
username tac password 0 admin
memory−size iomem 30
ip subnet−zero
!
!
no ip finger
no ip domain−lookup
ip host rund 172.17.247.195
```

```
!
ip audit notify log
ip audit po max-events 100
ip address-pool local

!---Enable VPN/Virtual Private Dialup Network (VPDN) services
!---and define groups and their respective parameters.

vpdn enable
no vpdn logging
!
!
vpdn-group PPTP_WIN2KClient

!---Default PPTP VPDN group
!---Allow the router to accept incoming Requests

accept-dialin
protocol pptp
virtual-template 1
!
!
!
call rsvp-sync
!
!
!
!
!
!
!
controller E1 2/0
!
!
interface Loopback0
ip address 172.16.10.100 255.255.255.0
!
interface Ethernet0/0
ip address 10.200.20.2 255.255.255.0
half-duplex
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool default

!--- The following encryption command is optional
!--- and could be added later.

ppp encrypt mppe 40
ppp authentication ms-chap
!
ip local pool default 172.16.10.1 172.16.10.10
ip classless
ip route 0.0.0.0 0.0.0.0 10.200.20.1
ip route 192.168.1.0 255.255.255.0 10.200.20.250
no ip http server
!
radius-server host 10.200.20.245 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
!
dial-peer cor custom
!
!
!
!
```

```
!
line con 0
exec−timeout 0 0
login authentication console
transport input none
line 33 50
modem InOut
line aux 0
line vty 0 4
exec−timeout 0 0
password
!
end

angela#show debug
General OS:
AAA Authentication debugging is on
AAA Authorization debugging is on
PPP:
MPPE Events debugging is on
PPP protocol negotiation debugging is on
VPN:
L2X protocol events debugging is on
L2X protocol errors debugging is on
VPDN events debugging is on
VPDN errors debugging is on
Radius protocol debugging is on

angela#
*Mar  7 04:21:07.719: L2X: TCP connect reqd from 0.0.0.0:2000
*Mar  7 04:21:07.991: Tnl 29 PPTP: Tunnel created; peer initiated
*Mar  7 04:21:08.207: Tnl 29 PPTP: SCCRQ−ok −>
state change wt−sccrq to estabd
*Mar  7 04:21:09.267: VPDN: Session vaccess task running
*Mar  7 04:21:09.267: Vi1 VPDN: Virtual interface created
*Mar  7 04:21:09.267: Vi1 VPDN: Clone from Vtemplate 1
*Mar  7 04:21:09.343: Tnl/Cl 29/29 PPTP: VAccess created
*Mar  7 04:21:09.343: Vi1 Tnl/Cl 29/29 PPTP: vacc−ok −>
#state change wt−vacc to estabd
*Mar  7 04:21:09.343: Vi1 VPDN: Bind interface direction=2
*Mar  7 04:21:09.347: %LINK−3−UPDOWN: Interface Virtual−Access1, changed
state to up
*Mar  7 04:21:09.347: Vi1 PPP: Using set call direction
*Mar  7 04:21:09.347: Vi1 PPP: Treating connection as a callin
*Mar  7 04:21:09.347: Vi1 PPP: Phase is ESTABLISHING,
Passive Open [0 sess, 0 load]
*Mar  7 04:21:09.347: Vi1 LCP: State is Listen
*Mar  7 04:21:10.347: %LINEPROTO−5−UPDOWN: Line protocol on Interface
Virtual−Access1, changed state to up
*Mar  7 04:21:11.347: Vi1 LCP: TIMEout: State Listen
*Mar  7 04:21:11.347: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Mar  7 04:21:11.347: Vi1 LCP: O CONFREQ [Listen] id 7 len 15
*Mar  7 04:21:11.347: Vi1 LCP:    AuthProto MS−CHAP (0x0305C22380)
*Mar  7 04:21:11.347: Vi1 LCP:    MagicNumber 0x3050EB1F (0x05063050EB1F)
*Mar  7 04:21:11.635: Vi1 LCP: I CONFACK [REQsent] id 7 len 15
*Mar  7 04:21:11.635: Vi1 LCP:    AuthProto MS−CHAP (0x0305C22380)
*Mar  7 04:21:11.635: Vi1 LCP:    MagicNumber 0x3050EB1F (0x05063050EB1F)
*Mar  7 04:21:13.327: Vi1 LCP: I CONFREQ [ACKrcvd] id 1 len 44
*Mar  7 04:21:13.327: Vi1 LCP:    MagicNumber 0x35BE1CB0 (0x050635BE1CB0)
*Mar  7 04:21:13.327: Vi1 LCP:    PFC (0x0702)
*Mar  7 04:21:13.327: Vi1 LCP:    ACFC (0x0802)
*Mar  7 04:21:13.327: Vi1 LCP:    Callback 6  (0x0D0306)
*Mar  7 04:21:13.327: Vi1 LCP:    MRRU 1614 (0x1104064E)
*Mar  7 04:21:13.327: Vi1 LCP:    EndpointDisc 1 Local
*Mar  7 04:21:13.327: Vi1 LCP:     (0x1317016AC616B006CC4281A1CA941E39)
*Mar  7 04:21:13.331: Vi1 LCP:     (0xB9182600000008)
```

```
*Mar  7 04:21:13.331: Vi1 LCP: O CONFREJ [ACKrcvd] id 1 len 34
*Mar  7 04:21:13.331: Vi1 LCP:    Callback 6  (0x0D0306)
*Mar  7 04:21:13.331: Vi1 LCP:    MRRU 1614 (0x1104064E)
*Mar  7 04:21:13.331: Vi1 LCP:    EndpointDisc 1 Local
*Mar  7 04:21:13.331: Vi1 LCP:     (0x1317016AC616B006CC4281A1CA941E39)
*Mar  7 04:21:13.331: Vi1 LCP:     (0xB9182600000008)
*Mar  7 04:21:13.347: Vi1 LCP: TIMEout: State ACKrcvd
*Mar  7 04:21:13.347: Vi1 LCP: O CONFREQ [ACKrcvd] id 8 len 15
*Mar  7 04:21:13.347: Vi1 LCP:    AuthProto MS-CHAP (0x0305C22380)
*Mar  7 04:21:13.347: Vi1 LCP:    MagicNumber 0x3050EB1F (0x05063050EB1F)
*Mar  7 04:21:13.647: Vi1 LCP: I CONFREQ [REQsent] id 2 len 14
*Mar  7 04:21:13.651: Vi1 LCP:    MagicNumber 0x35BE1CB0 (0x050635BE1CB0)
*Mar  7 04:21:13.651: Vi1 LCP:    PFC (0x0702)
*Mar  7 04:21:13.651: Vi1 LCP:    ACFC (0x0802)
*Mar  7 04:21:13.651: Vi1 LCP: O CONFACK [REQsent] id 2 len 14
*Mar  7 04:21:13.651: Vi1 LCP:    MagicNumber 0x35BE1CB0 (0x050635BE1CB0)
*Mar  7 04:21:13.651: Vi1 LCP:    PFC (0x0702)
*Mar  7 04:21:13.651: Vi1 LCP:    ACFC (0x0802)
*Mar  7 04:21:13.723: Vi1 LCP: I CONFACK [ACKsent] id 8 len 15
*Mar  7 04:21:13.723: Vi1 LCP:    AuthProto MS-CHAP (0x0305C22380)
*Mar  7 04:21:13.723: Vi1 LCP:    MagicNumber 0x3050EB1F (0x05063050EB1F)
*Mar  7 04:21:13.723: Vi1 LCP: State is Open
*Mar  7 04:21:13.723: Vi1 PPP: Phase is AUTHENTICATING,
by this end [0 sess, 0 load]
*Mar  7 04:21:13.723: Vi1 MS-CHAP: O CHALLENGE id 20 len 21 from "angela "
*Mar  7 04:21:14.035: Vi1 LCP: I IDENTIFY [Open] id 3 len 18 magic
0x35BE1CB0 MSRASV5.00
*Mar  7 04:21:14.099: Vi1 LCP: I IDENTIFY [Open] id 4 len 24 magic
0x35BE1CB0 MSRAS-1-RSHANMUG
*Mar  7 04:21:14.223: Vi1 MS-CHAP: I RESPONSE id 20 len 57 from "tac"
*Mar  7 04:21:14.223: AAA: parse name=Virtual-Access1 idb type=21 tty=-1
*Mar  7 04:21:14.223: AAA: name=Virtual-Access1 flags=0x11 type=5 shelf=0
slot=0 adapter=0 port=1 channel=0
*Mar  7 04:21:14.223: AAA/MEMORY: create_user (0x62740E7C) user='tac' ruser=''
port='Virtual-Access1' rem_addr='' authen_type=MSCHAP service=PPP priv=1
*Mar  7 04:21:14.223: AAA/AUTHEN/START (2474402925): port='Virtual-Access1'
list='' action=LOGIN service=PPP
*Mar  7 04:21:14.223: AAA/AUTHEN/START (2474402925): using "default" list
*Mar  7 04:21:14.223: AAA/AUTHEN/START (2474402925): Method=radius (radius)
*Mar  7 04:21:14.223: RADIUS: ustruct sharecount=0
*Mar  7 04:21:14.223: RADIUS: Initial Transmit Virtual-Access1 id 116
10.200.20.245:1645, Access-Request, len 129
*Mar  7 04:21:14.227:         Attribute 4 6 0AC81402
*Mar  7 04:21:14.227:         Attribute 5 6 00000001
*Mar  7 04:21:14.227:         Attribute 61 6 00000005
*Mar  7 04:21:14.227:         Attribute 1 5 7461631A
*Mar  7 04:21:14.227:         Attribute 26 16 000001370B0AFD11
*Mar  7 04:21:14.227:         Attribute 26 58 0000013701341401
*Mar  7 04:21:14.227:         Attribute 6 6 00000002
*Mar  7 04:21:14.227:         Attribute 7 6 00000001
*Mar  7 04:21:14.239: RADIUS: Received from id 116 10.200.20.245:1645,
Access-Accept, len 116
*Mar  7 04:21:14.239:         Attribute 7 6 00000001
*Mar  7 04:21:14.239:         Attribute 6 6 00000002
*Mar  7 04:21:14.239:         Attribute 25 32 64080750
*Mar  7 04:21:14.239:         Attribute 26 40 000001370C223440
*Mar  7 04:21:14.239:         Attribute 26 12 000001370A06144E
*Mar  7 04:21:14.239: AAA/AUTHEN (2474402925): status = PASS
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606):
Port='Virtual-Access1' list='' service=NET
*Mar  7 04:21:14.243: AAA/AUTHOR/LCP: Vi1 (2434357606) user='tac'
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606): send AV service=ppp
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606): send AV protocol=lcp
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606): found list "default"
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP (2434357606): Method=radius
```

```
(radius)
*Mar  7 04:21:14.243: RADIUS: unrecognized Microsoft VSA type 10
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR (2434357606): Post authorization
status = PASS_REPL
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP: Processing AV service=ppp
*Mar  7 04:21:14.243: Vi1 AAA/AUTHOR/LCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar  7 04:21:14.243: Vi1 MS-CHAP: O SUCCESS id 20 len 4
*Mar  7 04:21:14.243: Vi1 PPP: Phase is UP [0 sess, 0 load]
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM: (0): Can we start IPCP?
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (1553311212):
Port='Virtual-Access1' list='' service=NET
*Mar  7 04:21:14.247: AAA/AUTHOR/FSM: Vi1 (1553311212) user='tac'
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (1553311212): send AV service=ppp
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (1553311212): send AV protocol=ip
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (1553311212): found list "default"
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (1553311212): Method=radius
(radius)
*Mar  7 04:21:14.247: RADIUS: unrecognized Microsoft VSA type 10
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR (1553311212): Post authorization
status = PASS_REPL
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM: We can start IPCP
*Mar  7 04:21:14.247: Vi1 IPCP: O CONFREQ [Not negotiated] id 4 len 10
*Mar  7 04:21:14.247: Vi1 IPCP:    Address 172.16.10.100 (0x0306AC100A64)
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM: (0): Can we start CCP?
*Mar  7 04:21:14.247: Vi1 AAA/AUTHOR/FSM (3663845178):
Port='Virtual-Access1' list='' service=NET
*Mar  7 04:21:14.251: AAA/AUTHOR/FSM: Vi1 (3663845178) user='tac'
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR/FSM (3663845178): send AV service=ppp
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR/FSM (3663845178): send AV protocol=ccp
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR/FSM (3663845178): found list "default"
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR/FSM (3663845178): Method=radius
(radius)
*Mar  7 04:21:14.251: RADIUS: unrecognized Microsoft VSA type 10
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR (3663845178): Post authorization
status = PASS_REPL
*Mar  7 04:21:14.251: Vi1 AAA/AUTHOR/FSM: We can start CCP
*Mar  7 04:21:14.251: Vi1 CCP: O CONFREQ [Closed] id 3 len 10
*Mar  7 04:21:14.251: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar  7 04:21:14.523: Vi1 CCP: I CONFREQ [REQsent] id 5 len 10
*Mar  7 04:21:14.523: Vi1 CCP:    MS-PPC supported bits 0x010000F1
(0x1206010000F1)
*Mar  7 04:21:14.523: Vi1 MPPE: don't understand all options, NAK
*Mar  7 04:21:14.523: Vi1 AAA/AUTHOR/FSM:
Check for unauthorized mandatory AV's
*Mar  7 04:21:14.523: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar  7 04:21:14.523: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar  7 04:21:14.523: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar  7 04:21:14.523: Vi1 CCP: O CONFNAK [REQsent] id 5 len 10
*Mar  7 04:21:14.523: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar  7 04:21:14.607: Vi1 IPCP: I CONFREQ [REQsent] id 6 len 34
*Mar  7 04:21:14.607: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  7 04:21:14.607: Vi1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  7 04:21:14.607: Vi1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  7 04:21:14.607: Vi1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  7 04:21:14.607: Vi1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 0.0.0.0
*Mar  7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar  7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  7 04:21:14.607: Vi1 AAA/AUTHOR/IPCP: Done.
```

```
Her address 0.0.0.0, we want 0.0.0.0
*Mar  7 04:21:14.607: Vi1 IPCP: Pool returned 172.16.10.1
*Mar  7 04:21:14.607: Vi1 IPCP: O CONFREJ [REQsent] id 6 len 28
*Mar  7 04:21:14.607: Vi1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  7 04:21:14.611: Vi1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  7 04:21:14.611: Vi1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  7 04:21:14.611: Vi1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  7 04:21:14.675: Vi1 IPCP: I CONFACK [REQsent] id 4 len 10
*Mar  7 04:21:14.675: Vi1 IPCP:    Address 172.16.10.100 (0x0306AC100A64)
*Mar  7 04:21:14.731: Vi1 CCP: I CONFACK [REQsent] id 3 len 10
*Mar  7 04:21:14.731: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar  7 04:21:14.939: Vi1 CCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar  7 04:21:14.939: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar  7 04:21:14.939: Vi1 AAA/AUTHOR/FSM:
Check for unauthorized mandatory AV's
*Mar  7 04:21:14.939: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar  7 04:21:14.939: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar  7 04:21:14.939: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar  7 04:21:14.939: Vi1 CCP: O CONFACK [ACKrcvd] id 7 len 10
*Mar  7 04:21:14.939: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar  7 04:21:14.943: Vi1 CCP: State is Open
*Mar  7 04:21:14.943: Vi1 MPPE: Generate keys using RADIUS data
*Mar  7 04:21:14.943: Vi1 MPPE: Initialize keys
*Mar  7 04:21:14.943: Vi1 MPPE: [40 bit encryption]  [stateless mode]
*Mar  7 04:21:14.991: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar  7 04:21:14.991: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  7 04:21:14.991: Vi1 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 172.16.10.1
*Mar  7 04:21:14.991: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  7 04:21:14.995: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar  7 04:21:14.995: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  7 04:21:14.995: Vi1 AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 172.16.10.1
*Mar  7 04:21:14.995: Vi1 IPCP: O CONFNAK [ACKrcvd] id 8 len 10
*Mar  7 04:21:14.995: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar  7 04:21:15.263: Vi1 IPCP: I CONFREQ [ACKrcvd] id 9 len 10
*Mar  7 04:21:15.263: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar  7 04:21:15.263: Vi1 AAA/AUTHOR/IPCP: Start.
Her address 172.16.10.1, we want 172.16.10.1
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766):
Port='Virtual-Access1' list='' service=NET
*Mar  7 04:21:15.267: AAA/AUTHOR/IPCP: Vi1 (2052567766) user='tac'
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766): send AV service=ppp
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766): send AV protocol=ip
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766): send AV
addr*172.16.10.1
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766): found list
"default"
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP (2052567766): Method=radius
(radius)
*Mar  7 04:21:15.267: RADIUS: unrecognized Microsoft VSA type 10
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR (2052567766): Post authorization
status = PASS_REPL
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Reject 172.16.10.1, using
172.16.10.1
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Processing AV addr*172.16.10.1
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  7 04:21:15.267: Vi1 AAA/AUTHOR/IPCP: Done.
```

```
Her address 172.16.10.1, we want 172.16.10.1
*Mar  7 04:21:15.271: Vi1 IPCP: O CONFACK [ACKrcvd] id 9 len 10
*Mar  7 04:21:15.271: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar  7 04:21:15.271: Vi1 IPCP: State is Open
*Mar  7 04:21:15.271: Vi1 IPCP: Install route to 172.16.10.1
*Mar  7 04:21:22.571: Vi1 LCP: I ECHOREP [Open] id 1 len 12 magic
0x35BE1CB0
*Mar  7 04:21:22.571: Vi1 LCP: Received id 1, sent id 1, line up
*Mar  7 04:21:30.387: Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic
0x35BE1CB0
*Mar  7 04:21:30.387: Vi1 LCP: Received id 2, sent id 2, line up

angela#show vpdn
%No active L2TP tunnels
%No active L2F tunnels
PPTP Tunnel and Session Information Total tunnels 1 sessions 1
LocID Remote Name     State    Remote Address  Port  Sessions
29                    estabd   192.168.1.47    2000  1
LocID RemID TunID Intf    Username      State   Last Chg
29    32768 29    Vi1     tac           estabd  00:00:31
%No active PPPoE tunnels
angela#

*Mar  7 04:21:40.471: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic
0x35BE1CB0
*Mar  7 04:21:40.471: Vi1 LCP: Received id 3, sent id 3, line up
*Mar  7 04:21:49.887: Vi1 LCP: I ECHOREP [Open] id 4 len 12 magic
0x35BE1CB0
*Mar  7 04:21:49.887: Vi1 LCP: Received id 4, sent id 4, line up

angela#ping 192.168.1.47
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.47, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 484/584/732 ms

*Mar  7 04:21:59.855: Vi1 LCP: I ECHOREP [Open] id 5 len 12 magic
0x35BE1CB0
*Mar  7 04:21:59.859: Vi1 LCP: Received id 5, sent id 5, line up
*Mar  7 04:22:06.323: Tnl 29 PPTP: timeout -> state change estabd to estabd
*Mar  7 04:22:08.111: Tnl 29 PPTP: EchoRQ -> state change estabd to estabd
*Mar  7 04:22:08.111: Tnl 29 PPTP: EchoRQ -> echo state change Idle to Idle
*Mar  7 04:22:09.879: Vi1 LCP: I ECHOREP [Open] id 6 len 12 magic
0x35BE1CB0
*Mar  7 04:22:09.879: Vi1 LCP: Received id 6, sent id 6, line up

angela#ping 172.16.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 584/707/1084 ms

*Mar  7 04:22:39.863: Vi1 LCP: I ECHOREP [Open] id 7 len 12 magic
0x35BE1CB0
*Mar  7 04:22:39.863: Vi1 LCP: Received id 7, sent id 7, line up

angela#clear vpdn tunnel pptp tac
Could not find specified tunnel

angela#show vpdn tunnel
%No active L2TP tunnels
%No active L2F tunnels
PPTP Tunnel Information Total tunnels 1 sessions 1
LocID Remote Name     State    Remote Address  Port  Sessions
29                    estabd   192.168.1.47    2000  1
%No active PPPoE tunnels
```

```
angela#
*Mar  7 04:23:05.347: Tnl 29 PPTP: timeout -> state change estabd to estabd

angela#
*Mar  7 04:23:08.019: Tnl 29 PPTP: EchoRQ -> state change estabd to estabd
*Mar  7 04:23:08.019: Tnl 29 PPTP: EchoRQ -> echo state change Idle to Idle

angela#
*Mar  7 04:23:09.887: Vi1 LCP: I ECHOREP [Open] id 10 len 12 magic 0x35BE1CB0
*Mar  7 04:23:09.887: Vi1 LCP: Received id 10, sent id 10, line up
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter tool, which allows you to view an analysis of **show** command output.

- **show vpdn** − Displays information about active Level 2 Forwarding (L2F) protocol tunnel and message identifiers in a VPDN.

You can also use **show vpdn ?** to see other VPDN−specific **show** commands.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter tool, which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

- **debug aaa authentication** − Displays information about AAA/TACACS+ authentication.
- **debug aaa authorization** − Displays information on AAA/TACACS+ authorization.
- **debug ppp negotiation** − Displays PPP packets transmitted during PPP startup, where PPP options are negotiated.
- **debug ppp authentication** − Displays authentication protocol messages, including Challenge Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges.
- **debug radius** − Displays detailed debugging information associated with the RADIUS. If authentication works, but there are problems with MPPE encryption, use one of the debug commands below.
- **debug ppp mppe packet** − Displays all incoming outgoing MPPE traffic.
- **debug ppp mppe event** − Displays key MPPE occurrences.
- **debug ppp mppe detailed** − Displays verbose MPPE information.
- **debug vpdn l2x−packets** − Displays messages about L2F protocol headers and status.
- **debug vpdn events** − Displays messages about events that are part of normal tunnel establishment or shutdown.
- **debug vpdn errors** − Displays errors that prevent a tunnel from being established or errors that cause an established tunnel to be closed.
- **debug vpdn packets** − Displays each protocol packet exchanged. This option may result in a large

number of debug messages and should generally only be used on a debug chassis with a single active session.

Split Tunneling

Let us assume the gateway router is an ISP Router. When the PPTP tunnel comes up on the PC, the PPTP route is installed with a higher metric than the previous default, so we lose Internet connectivity. To remedy this, modify the Microsoft routing to delete the default and reinstall the default route (this requires knowing the IP address the PPTP client has been assigned; for the current example, this was 172.16.10.1):

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 192.168.1.47 metric 1
route add 172.16.10.1 mask 255.255.255.0 192.168.1.47 metric 1
```

If the Client Is Not Configured for Encryption

Under the **Security** tab on the dial−up connection used for the PPTP session, you can define the user authentication parameters. For example, this can be PAP, CHAP, MS−CHAP, or Windows domain logon. If you have chosen the **No Encryption Allowed** (server disconnects if it requires encryption) option in the **Properties** section of the VPN connection, you may see a PPTP Error message on the client:

```
Registering your computer on the network..
Error 734:  The PPP link control protocol was terminated.
Debugs on the  router:
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Processing AV protocol=ccp
*Mar  8 22:38:52.496: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar  8 22:38:52.500: Vi1 CCP: O CONFACK [ACKrcvd] id 7 len 10
*Mar  8 22:38:52.500: Vi1 CCP:    MS−PPC supported bits 0x01000020
(0x120601000020)
*Mar  8 22:38:52.500: Vi1 CCP: State is Open
*Mar  8 22:38:52.500: Vi1 MPPE: RADIUS keying material missing
*Mar  8 22:38:52.500: Vi1 CCP: O TERMREQ [Open] id 5 len 4
*Mar  8 22:38:52.524: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar  8 22:38:52.524: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 172.16.10.1
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Processing AV protocol=ip
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  8 22:38:52.524: Vi1 AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 172.16.10.1
*Mar  8 22:38:52.524: Vi1 IPCP: O CONFNAK [ACKrcvd] id 8 len 10
*Mar  8 22:38:52.524: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar  8 22:38:52.640: Vi1 CCP: I TERMACK [TERMsent] id 5 len 4
*Mar  8 22:38:52.640: Vi1 CCP: State is Closed
*Mar  8 22:38:52.640: Vi1 MPPE: Required encryption not negotiated
*Mar  8 22:38:52.640: Vi1 IPCP: State is Closed
*Mar  8 22:38:52.640: Vi1 PPP: Phase is TERMINATING [0 sess, 0 load]
*Mar  8 22:38:52.640: Vi1 LCP: O TERMREQ [Open] id 13 len 4
*Mar  8 22:38:52.660: Vi1 IPCP: LCP not open, discarding packet
*Mar  8 22:38:52.776: Vi1 LCP: I TERMACK [TERMsent] id 13 len 4
*Mar  8 22:38:52.776: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Mar  8 22:38:52.780: Vi1 LCP: State is Closed
*Mar  8 22:38:52.780: Vi1 PPP: Phase is DOWN [0 sess, 0 load]
*Mar  8 22:38:52.780: Vi1 VPDN: Cleanup
*Mar  8 22:38:52.780: Vi1 VPDN: Reset
*Mar  8 22:38:52.780: Vi1
Tnl/Cl 33/33 PPTP: close −> state change estabd to terminal
*Mar  8 22:38:52.780: Vi1 Tnl/Cl 33/33 PPTP:
```

```
Destroying session, trace follows:
*Mar  8 22:38:52.780: −Traceback= 60C4A150 60C4AE48 60C49F68 60C4B5AC
60C30450 60C18B10 60C19238 60602CC4 605FC380 605FB730 605FD614 605F72A8
6040DE0C 6040DDF8
*Mar  8 22:38:52.784: Vi1 Tnl/Cl 33/33 PPTP:
Releasing idb for tunnel 33 session 33
*Mar  8 22:38:52.784: Vi1 VPDN: Reset
*Mar  8 22:38:52.784: Tnl 33 PPTP:
no−sess −> state change estabd to wt−stprp
*Mar  8 22:38:52.784: Vi1 VPDN: Unbind interface
*Mar  8 22:38:52.784: Vi1 VPDN: Unbind interface
*Mar  8 22:38:52.784: Vi1 VPDN: Reset
*Mar  8 22:38:52.784: Vi1 VPDN: Unbind interface
```

If the Client Is Configured for Encryption and the Router Is Not

We can see the following message on the PC:

```
Registering your computer on the network..
Errror 742: The remote computer doesnot support the required data
encryption type.
On the Router:
*Mar  9 01:06:00.868: Vi2 CCP: I CONFREQ [Not negotiated] id 5 len 10
*Mar  9 01:06:00.868: Vi2 CCP:    MS−PPC supported bits 0x010000B1
(0x1206010000B1)
*Mar  9 01:06:00.868: Vi2 LCP: O PROTREJ [Open] id 18 len 16 protocol CCP
(0x80FD0105000A1206010000B1)
*Mar  9 01:06:00.876: Vi2 IPCP: I CONFREQ [REQsent] id 6 len 34
*Mar  9 01:06:00.876: Vi2 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  9 01:06:00.876: Vi2 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Start.
Her address 0.0.0.0, we want 0.0.0.0
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#1
1Z1`1k1}111
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar  9 01:06:00.880: Vi2 AAA/AUTHOR/IPCP: Done.
Her address 0.0.0.0, we want 0.0.0.0
*Mar  9 01:06:00.880: Vi2 IPCP: Pool returned 172.16.10.1
*Mar  9 01:06:00.880: Vi2 IPCP: O CONFREJ [REQsent] id 6 len 28
*Mar  9 01:06:00.880: Vi2 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar  9 01:06:00.880: Vi2 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar  9 01:06:00.880: Vi2 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar  9 01:06:00.880: Vi2 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar  9 01:06:00.884: Vi2 IPCP: I CONFACK [REQsent] id 8 len 10
*Mar  9 01:06:00.884: Vi2 IPCP:    Address 172.16.10.100 (0x0306AC100A64)
*Mar  9 01:06:01.024: Vi2 LCP: I TERMREQ [Open] id 7 len 16
(0x79127FBE003CCD74000002E6)
*Mar  9 01:06:01.024: Vi2 LCP: O TERMACK [Open] id 7 len 4
*Mar  9 01:06:01.152: Vi2 Tnl/Cl 38/38 PPTP: ClearReq −> state change
estabd to terminal
*Mar  9 01:06:01.152: Vi2 Tnl/Cl 38/38 PPTP: Destroying session, trace
follows:
*Mar  9 01:06:01.152: −Traceback= 60C4A150 60C4AE48 60C49F68 60C4B2CC
60C4B558 60C485E0 60C486E0 60C48AB8 6040DE0C 6040DDF8
*Mar  9 01:06:01.156: Vi2 Tnl/Cl 38/38 PPTP: Releasing idb for tunnel 38
session 38
*Mar  9 01:06:01.156: Vi2 VPDN: Reset
*Mar  9 01:06:01.156: Tnl 38 PPTP: no−sess −> state change estabd to
wt−stprp
*Mar  9 01:06:01.160: %LINK−3−UPDOWN: Interface Virtual−Access2, changed
```

```
state to down
*Mar  9 01:06:01.160: Vi2 LCP: State is Closed
*Mar  9 01:06:01.160: Vi2 IPCP: State is Closed
*Mar  9 01:06:01.160: Vi2 PPP: Phase is DOWN [0 sess, 0 load]
*Mar  9 01:06:01.160: Vi2 VPDN: Cleanup
*Mar  9 01:06:01.160: Vi2 VPDN: Reset
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
*Mar  9 01:06:01.160: Vi2 VPDN: Reset
*Mar  9 01:06:01.160: Vi2 VPDN: Unbind interface
*Mar  9 01:06:01.160: AAA/MEMORY: free_user (0x6273D528) user='tac' ruser=''
port='Virtual−Access2' rem_addr='' authen_type=MSCHAP service=PPP priv=1
*Mar  9 01:06:01.324: Tnl 38 PPTP: StopCCRQ −> state change wt−stprp to wt−stprp
*Mar  9 01:06:01.324: Tnl 38 PPTP: Destroy tunnel
*Mar  9 01:06:02.160: %LINEPROTO−5−UPDOWN: Line protocol on Interface
Virtual−Access2, changed state to down
```

Disabling MS−CHAP when the PC Is Configured for Encryption

We can see the following message on the PC:

```
The current encryption selection requires EAP or some version of
MS−CHAP logon security methods.
```

If the user specifies an incorrect username or password, we can see the following output.

On the PC:

```
Verifying Username and Password..
Error 691: Access was denied because the username and/or password
was invalid on the domain.
```

On the Router:

```
*Mar  9 01:13:43.192: RADIUS: Received from id 139 10.200.20.245:1645,
Access−Reject, len 42
*Mar  9 01:13:43.192: Attribute 26 22 0000013702101545
*Mar  9 01:13:43.192: AAA/AUTHEN (608505327): status = FAIL
*Mar  9 01:13:43.192: Vi2 CHAP: Unable to validate Response. Username tac:
Authentication failure
*Mar  9 01:13:43.192: Vi2 MS−CHAP: O FAILURE id 21 len 13 msg is "E=691 R=0"
*Mar  9 01:13:43.192: Vi2 PPP: Phase is TERMINATING [0 sess, 0 load]
*Mar  9 01:13:43.192: Vi2 LCP: O TERMREQ [Open] id 20 len 4
*Mar  9 01:13:43.196: AAA/MEMORY: free_user (0x62740E7C) user='tac'
ruser='' port='Virtual−Access2' rem_addr='' authen_type=MSCHAP service=PPP
priv=1
```

When the Radius Server Is Uncommunicative

We can see the following output on the router:

```
*Mar  9 01:18:32.944: RADIUS: Retransmit id 141
*Mar  9 01:18:42.944: RADIUS: Tried all servers.
*Mar  9 01:18:42.944: RADIUS: No valid server found. Trying any viable server
*Mar  9 01:18:42.944: RADIUS: Tried all servers.
*Mar  9 01:18:42.944: RADIUS: No response for id 141
*Mar  9 01:18:42.944: Radius: No response from server
*Mar  9 01:18:42.944: AAA/AUTHEN (374484072): status = ERROR
```

Related Information

- **PPTP with MPPE**
- **PPTP Technology Page**
- **Understanding VPDN**
- **Understanding Radius**
- **Configuring CiscoSecure ACS for Windows Router PPTP Authentication**
- **Technical Support & Documentation − Cisco Systems**

Updated: Sep 06, 2004 Document ID: 3885