Configuring Cisco IOS and Windows 2000 Clients for L2TP Using Microsoft IAS

Document ID: 3886

Contents

Introduction

This document provides instructions on how to configure Cisco IOS® software and Windows 2000 clients for Layer 2 Tunnel Protocol (L2TP) using Microsoft's Internet Authentication Server (IAS).

Refer to L2TP Over IPsec between Windows 2000/XP PC and PIX/ASA 7.2 Using Pre−shared Key Configuration Example for more information on how to configure L2TP over IP Security (IPSec) from remote Microsoft Windows 2000/2003 and XP clients to a PIX Security Appliance corporate office using pre−shared keys with Microsoft Windows 2003 IAS RADIUS Server for user authentication.

Refer to Configuring L2TP over IPSec from a Windows 2000 or XP Client to a Cisco VPN 3000 Series Concentrator Using Pre−Shared Keys for more information on how to configure L2TP over IPSec from remote Microsoft Windows 2000 and XP clients to a corporate site using an encrypted method.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on these software and hardware versions:

- 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

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.
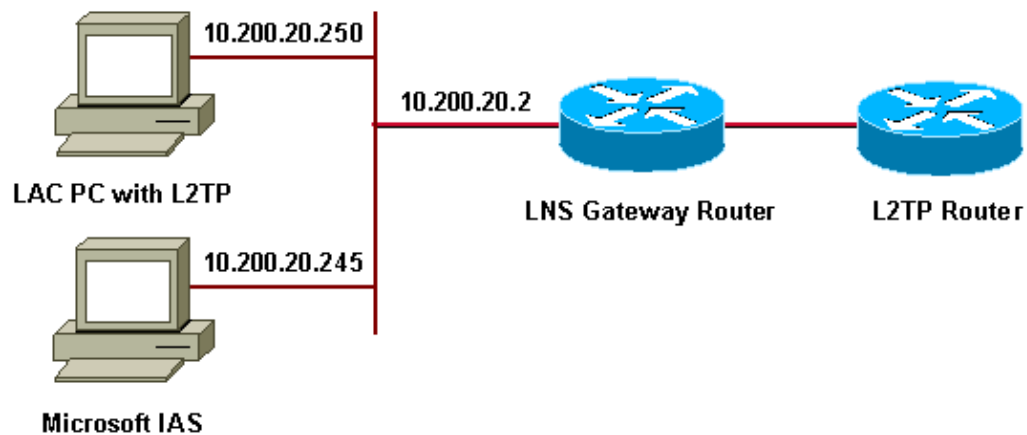
Configure

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 more information on the commands used in this document.

Network Diagram

This document uses this network setup:

This document uses these IP pools for dial–up clients:

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

Configuring the Windows 2000 Advanced Server for Microsoft IAS

Ensure that Microsoft IAS is installed. In order to install Microsoft IAS, log in as an administrator and complete these steps:

1. Under **Network Services**, verify that all check boxes are cleared.
2. Check the **Internet Authentication Server (IAS)** check box and then click **OK**.
3. In the Windows Components wizard, click **Next**. If prompted, insert the Windows 2000 CD.
4. When the required files have been copied, click **Finish** and then close all windows. You do not need to reboot.

Configuring RADIUS Clients

Complete these steps:

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

Configuring Users on IAS

Unlike CiscoSecure, the Windows 2000 Remote Authentication Dial−In User Server (RADIUS) user database is tightly bound to the Windows user database.

- If 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, you can use **Local Users and Groups** from **Administrative Tools** in order to create new users.

Configuring Users in Active Directory

Complete these steps in order to configure users with Active Directory:

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

Configuring Users if No Active Directory Is Installed

Complete these steps in order to configure users if Active Directory is not installed:

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

Applying a Remote Access Policy to the Windows User

Complete these steps in order to apply a remote access policy:

1. From **Administrative Tools**, open the **Internet Authentication Server** console and click **Remote Access Policies**.
2. Click the **Add** button on **Specify the Conditions to Match** and add **Service–type**. Choose the available type as **Framed**. Add it to the selected types and press **OK**.
3. Click the **Add** button on **Specify the Conditions to Match** and add **Framed Protocol**. Choose the available type as **PPP**. Add it to the selected types and 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. Press **OK**.
5. On **Allow Access if Dial–in Permission is Enabled Properties**, select **Grant Remote Access Permission**.
6. Close the console.

Configuring the Windows 2000 Client for L2TP

Complete these steps in order to configure the Windows 2000 client for L2TP:

1. From the **Start Menu**, choose **Settings**, and then follow one of these paths:

     ♦ **Control Panel** > **Network and Dial–up Connections**
   OR

     ♦ **Network and Dial–up Connections** > **Make New Connection**
2. Use the Wizard to create a connection called **L2TP**. This connection connects to a private network through the Internet. You also need to specify the L2TP tunnel gateway's IP address or name.
3. The new connection appears in the **Network and Dial–up Connections** window under **Control Panel**. From here, click on the right mouse button to edit the properties.
4. Under the **Networking** tab, make sure that the **Type Of Server I Am Calling** is set to L2TP.
5. If you plan to allocate a dynamic internal address to this client from the gateway, either via a local pool or DHCP, select **TCP/IP protocol**. Make sure that the client is configured to obtain an IP address automatically. You can also issue DNS information automatically.

     ♦ The **Advanced** button allows you to define static WINS and DNS information.
     ♦ The **Options** tab allows you to turn off IPSec, or assign a different policy to the connection.
     ♦ Under the **Security** tab, you can define the user authentication parameters, such as PAP, CHAP or MS–CHAP, or Windows domain logon.
6. When the connection is configured, you can double–click on it to launch the login screen, then **Connect**.

Disabling IPSec for the Windows 2000 Client

1. Edit the properties of the dial–up connection L2TP you have just created. Right–click the new connection **L2TP** to get the **L2TP Properties** window.
2. Under the **Networking** tab, click **Internet Protocol (TCP/IP) properties**. Double–click the **Advanced** tab. Go to the **Options** tab, click **IP security properties** and, if **Do not use IPSEC** is selected, double–check it.

Note: Microsoft Windows 2000 clients have a default Remote access and Policy Agent services which, by default, create a policy for L2TP traffic. This default policy does not allow L2TP traffic without IPSec and encryption. You can disable the Microsoft default behavior by editing the Microsoft client Registry Editor.

The procedure to edit Windows registry and to disable the default policy of IPSec for L2TP traffic is given in this section. Refer to the Microsoft documentation for editing Windows Registry.

Use the Registry Editor (Regedt32.exe) to add the new registry entry to disable IPSec. Refer to Microsoft's documentation or the Microsoft help topic for Regedt32.exe for more information.

You must add the ProhibitIpSec registry value to each Windows 2000−based endpoint computer of an L2TP or IPSec connection to prevent the automatic filter for L2TP and IPSec traffic from being created. When the ProhibitIpSec registry value is set to one, your Windows 2000−based computer does not create the automatic filter that uses CA authentication. Instead, it checks for a local or Active Directory IPSec policy. In order to add the ProhibitIpSec registry value to your Windows 2000−based computer, use Regedt32.exe to locate this key in the registry:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

Add this registry value to this key:

```
Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1
```

Note: You must restart your Windows 2000−based computer for the changes to take effect. Refer to these Microsoft articles for further details:

- Q258261 − Disabling IPSEC Policy Used with L2TP
- Q240262− How to Configure a L2TP/IPSec Connection Using a Pre−shared Key

Configuring Cisco IOS for L2TP

These configurations outline the commands required for L2TP without IPSec. Once this basic configuration is working, you can also configure IPSec.

angela
| ```
Building configuration...
Current configuration : 1595 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 ww
!
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/VPDN services and define groups and
!--- specific variables required for the group.

vpdn enable
no vpdn logging
!
vpdn-group L2TP_Windows 2000Client

!--- Default L2TP VPDN group.
!--- Allow the Router to accept incoming requests.

accept-dialin
protocol L2TP
virtual-template 1
no L2TP tunnel authentication

!--- Users are authenticated at the NAS or LNS
!--- before the tunnel is established. This is not
!--- required for client-initiated tunnels.

!
!
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
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 ww
!
end
angela#




*Mar 12 23:10:54.176: L2TP: I SCCRQ from  RSHANMUG-W2K1.cisco.com tnl 5
*Mar 12 23:10:54.176: Tnl 8663 L2TP: New tunnel created for remote
RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:10:54.176: Tnl 8663 L2TP: O SCCRP  to  RSHANMUG-W2K1.cisco.com
tnlid 5
*Mar 12 23:10:54.180: Tnl 8663 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Mar 12 23:10:54.352: Tnl 8663 L2TP: I SCCCN from  RSHANMUG-W2K1.cisco.com
tnl 5
*Mar 12 23:10:54.352: Tnl 8663 L2TP: Tunnel state change from
wait-ctl-reply to established
*Mar 12 23:10:54.352: Tnl 8663 L2TP: SM State established
*Mar 12 23:10:54.356: Tnl 8663 L2TP: I ICRQ from  RSHANMUG-W2K1.cisco.com
tnl 5
*Mar 12 23:10:54.356: Tnl/Cl 8663/44 L2TP: Session FS enabled
*Mar 12 23:10:54.356: Tnl/Cl 8663/44 L2TP: Session state change from idle
to wait-connect
*Mar 12 23:10:54.356: Tnl/Cl 8663/44 L2TP: New session created
*Mar 12 23:10:54.356: Tnl/Cl 8663/44 L2TP: O ICRP to
RSHANMUG-W2K1.cisco.com 5/1
*Mar 12 23:10:54.544: Tnl/Cl 8663/44 L2TP: I ICCN from
RSHANMUG-W2K1.cisco.com tnl 5, cl 1
*Mar 12 23:10:54.544: Tnl/Cl 8663/44 L2TP: Session state change from
wait-connect to established
*Mar 12 23:10:54.544: Vi1 VPDN: Virtual interface created for
*Mar 12 23:10:54.544: Vi1 PPP: Phase is DOWN, Setup [0 sess, 0 load]
*Mar 12 23:10:54.544: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
*Mar 12 23:10:54.620: Tnl/Cl 8663/44 L2TP: Session with no hwidb
*Mar 12 23:10:54.624: %LINK-3-UPDOWN: Interface Virtual-Access1, changed
state to up
*Mar 12 23:10:54.624: Vi1 PPP: Using set call direction
*Mar 12 23:10:54.624: Vi1 PPP: Treating connection as a callin
*Mar 12 23:10:54.624: Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess,
0 load]
*Mar 12 23:10:54.624: Vi1 LCP: State is Listen
*Mar 12 23:10:54.624: Vi1 VPDN: Bind interface direction=2
*Mar 12 23:10:56.556: Vi1 LCP: I CONFREQ [Listen] id 1 len 44
*Mar 12 23:10:56.556: Vi1 LCP:    MagicNumber 0x595E7636 (0x0506595E7636)
*Mar 12 23:10:56.556: Vi1 LCP:    PFC (0x0702)
*Mar 12 23:10:56.556: Vi1 LCP:    ACFC (0x0802)
```

```
*Mar 12 23:10:56.556: Vi1 LCP:    Callback 6  (0x0D0306)
*Mar 12 23:10:56.556: Vi1 LCP:    MRRU 1614 (0x1104064E)
*Mar 12 23:10:56.556: Vi1 LCP:    EndpointDisc 1 Local
*Mar 12 23:10:56.556: Vi1 LCP:     (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:10:56.556: Vi1 LCP:     (0x10D0AC00000002)
*Mar 12 23:10:56.556: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Mar 12 23:10:56.556: Vi1 LCP: O CONFREQ [Listen] id 1 len 15
*Mar 12 23:10:56.556: Vi1 LCP:    AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:10:56.556: Vi1 LCP:    MagicNumber 0x4E1B09B8 (0x05064E1B09B8)
*Mar 12 23:10:56.560: Vi1 LCP: O CONFREJ [Listen] id 1 len 34
*Mar 12 23:10:56.560: Vi1 LCP:    Callback 6  (0x0D0306)
*Mar 12 23:10:56.560: Vi1 LCP:    MRRU 1614 (0x1104064E)
*Mar 12 23:10:56.560: Vi1 LCP:    EndpointDisc 1 Local
*Mar 12 23:10:56.560: Vi1 LCP:     (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:10:56.560: Vi1 LCP:     (0x10D0AC00000002)
*Mar 12 23:10:56.700: Vi1 LCP: I CONFACK [REQsent] id 1 len 15
*Mar 12 23:10:56.700: Vi1 LCP:    AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:10:56.704: Vi1 LCP:    MagicNumber 0x4E1B09B8 (0x05064E1B09B8)
*Mar 12 23:10:56.704: Vi1 LCP: I CONFREQ [ACKrcvd] id 2 len 14
*Mar 12 23:10:56.704: Vi1 LCP:    MagicNumber 0x595E7636 (0x0506595E7636)
*Mar 12 23:10:56.704: Vi1 LCP:    PFC (0x0702)
*Mar 12 23:10:56.704: Vi1 LCP:    ACFC (0x0802)
*Mar 12 23:10:56.704: Vi1 LCP: O CONFACK [ACKrcvd] id 2 len 14
*Mar 12 23:10:56.708: Vi1 LCP:    MagicNumber 0x595E7636 (0x0506595E7636)
*Mar 12 23:10:56.708: Vi1 LCP:    PFC (0x0702)
*Mar 12 23:10:56.708: Vi1 LCP:    ACFC (0x0802)
*Mar 12 23:10:56.708: Vi1 LCP: State is Open
*Mar 12 23:10:56.708: Vi1 PPP: Phase is AUTHENTICATING, by this end [0
sess, 0 load]
*Mar 12 23:10:56.708: Vi1 MS-CHAP: O CHALLENGE id 28 len 21 from angela
*Mar 12 23:10:56.852: Vi1 LCP: I IDENTIFY [Open] id 3 len 18 magic
0x595E7636 MSRASV5.00
*Mar 12 23:10:56.872: Vi1 LCP: I IDENTIFY [Open] id 4 len 27 magic
0x595E7636 MSRAS-1- RSHANMUG-W2K1
*Mar 12 23:10:56.880: Vi1 MS-CHAP: I RESPONSE id 28 len 57 from tac
*Mar 12 23:10:56.880: AAA: parse name=Virtual-Access1 idb type=21 tty=-1
*Mar 12 23:10:56.880: AAA: name=Virtual-Access1 flags=0x11 type=5 shelf=0
slot=0 adapter=0 port=1 channel=0
*Mar 12 23:10:56.884: AAA/MEMORY: create_user (0x6273D024) user='tac'
ruser='' port='Virtual-Access1' rem_addr='' authen_type=MSCHAP service=PPP
priv=1
*Mar 12 23:10:56.884: AAA/AUTHEN/START (3634835145): port='Virtual-Access1'
list='' action=LOGIN service=PPP
*Mar 12 23:10:56.884: AAA/AUTHEN/START (3634835145): using default list
*Mar 12 23:10:56.884: AAA/AUTHEN/START (3634835145): Method=radius (radius)
*Mar 12 23:10:56.884: RADIUS: ustruct sharecount=0
*Mar 12 23:10:56.884: RADIUS: Initial Transmit Virtual-Access1 id 173
10.200.20.245:1645, Access-Request, len 129
*Mar 12 23:10:56.884:          Attribute 4 6 0AC81402
*Mar 12 23:10:56.884:          Attribute 5 6 00000001
*Mar 12 23:10:56.884:          Attribute 61 6 00000001
*Mar 12 23:10:56.884:          Attribute 1 5 7461631A
*Mar 12 23:10:56.884:          Attribute 26 16 000001370B0A0053
*Mar 12 23:10:56.884:          Attribute 26 58 0000013701341C01
*Mar 12 23:10:56.884:          Attribute 6 6 00000002
*Mar 12 23:10:56.884:          Attribute 7 6 00000001
*Mar 12 23:10:56.900: RADIUS: Received from id 173 10.200.20.245:1645,
Access-Accept, len 116
*Mar 12 23:10:56.900:          Attribute 7 6 00000001
*Mar 12 23:10:56.900:          Attribute 6 6 00000002
*Mar 12 23:10:56.900:          Attribute 25 32 502605A6
*Mar 12 23:10:56.900:          Attribute 26 40 000001370C22F6D5
*Mar 12 23:10:56.900:          Attribute 26 12 000001370A061C4E
*Mar 12 23:10:56.900: AAA/AUTHEN (3634835145): status = PASS
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469):
```

```
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:10:56.900: AAA/AUTHOR/LCP: Vi1 (1995716469) user='tac'
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469): send AV service=ppp
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469): send AV protocol=lcp
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469): found list default
*Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/LCP (1995716469): Method=radius
(radius)
*Mar 12 23:10:56.904: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:10:56.904: Vi1 AAA/AUTHOR (1995716469): Post authorization
status = PASS_REPL
*Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/LCP: Processing AV service=ppp
*Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/LCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:10:56.904: Vi1 MS-CHAP: O SUCCESS id 28 len 4
*Mar 12 23:10:56.904: Vi1 PPP: Phase is UP [0 sess, 0 load]
*Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM: (0): Can we start IPCP?
*Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:10:56.904: AAA/AUTHOR/FSM: Vi1 (2094713042) user='tac'
*Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042): send AV service=ppp
*Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042): send AV protocol=ip
*Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042): found list default
*Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042): Method=radius
(radius)
*Mar 12 23:10:56.908: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:10:56.908: Vi1 AAA/AUTHOR (2094713042): Post authorization
status = PASS_REPL
*Mar 12 23:10:56.908: Vi1 AAA/AUTHOR/FSM: We can start IPCP
*Mar 12 23:10:56.908: Vi1 IPCP: O CONFREQ [Closed] id 1 len 10
*Mar 12 23:10:56.908: Vi1 IPCP:    Address 172.16.10.100 (0x0306AC100A64)
*Mar 12 23:10:57.040: Vi1 CCP: I CONFREQ [Not negotiated] id 5 len 10
*Mar 12 23:10:57.040: Vi1 CCP:    MS-PPC supported bits 0x01000001
(0x120601000001)
*Mar 12 23:10:57.040: Vi1 LCP: O PROTREJ [Open] id 2 len 16 protocol CCP
(0x80FD0105000A120601000001)
*Mar 12 23:10:57.052: Vi1 IPCP: I CONFREQ [REQsent] id 6 len 34
*Mar 12 23:10:57.052: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar 12 23:10:57.052: Vi1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:10:57.052: Vi1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:10:57.052: Vi1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:10:57.052: Vi1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:10:57.052: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:10:57.056: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:10:57.056: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:10:57.056: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:10:57.056: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:10:57.056: Vi1 IPCP: Pool returned 172.16.10.1
*Mar 12 23:10:57.056: Vi1 IPCP: O CONFREJ [REQsent] id 6 len 28
*Mar 12 23:10:57.056: Vi1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:10:57.056: Vi1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:10:57.056: Vi1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:10:57.056: Vi1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:10:57.060: Vi1 IPCP: I CONFACK [REQsent] id 1 len 10
*Mar 12 23:10:57.060: Vi1 IPCP:    Address 172.16.10.100 (0x0306AC100A64)
*Mar 12 23:10:57.192: Vi1 IPCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar 12 23:10:57.192: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0, we
want 172.16.10.1
*Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0, we
```

```
want 172.16.10.1
*Mar 12 23:10:57.192: Vi1 IPCP: O CONFNAK [ACKrcvd] id 7 len 10
*Mar 12 23:10:57.192: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:10:57.324: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar 12 23:10:57.324: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:10:57.324: AAA/AUTHOR/IPCP: Vi1 (413757991) user='tac'
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991): send AV service=ppp
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991): send AV protocol=ip
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991): send AV
addr*172.16.10.1
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991): found list default
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991): Method=radius
(radius)
*Mar 12 23:10:57.324: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR (413757991): Post authorization status
= PASS_REPL
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP: Reject 172.16.10.1, using
172.16.10.1
*Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Processing AV addr*172.16.10.1
*Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:10:57.328: Vi1 IPCP: O CONFACK [ACKrcvd] id 8 len 10
*Mar 12 23:10:57.328: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:10:57.328: Vi1 IPCP: State is Open
*Mar 12 23:10:57.332: Vi1 IPCP: Install route to 172.16.10.1
*Mar 12 23:10:57.904: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
*Mar 12 23:11:06.324: Vi1 LCP: I ECHOREP [Open] id 1 len 12 magic
0x595E7636
*Mar 12 23:11:06.324: Vi1 LCP: Received id 1, sent id 1, line up
```

```
angela#show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions
8663  5     RSHANMUG-W2K1.c est    192.168.1.56    1701  1
LocID RemID TunID Intf     Username      State  Last Chg Fastswitch
44    1     8663  Vi1      tac           est    00:00:18 enabled
%No active L2F tunnels
%No active PPTP tunnels
%No active PPPoE tunnels
*Mar 12 23:11:16.332: Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic
0x595E7636
*Mar 12 23:11:16.332: Vi1 LCP: Received id 2, sent id 2, line upsh caller
ip
Line          User       IP Address      Local Number    Remote Number   <->
Vi1           tac        172.16.10.1     -               -               in

angela#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 10.200.20.1 to network 0.0.0.0
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.10.0/24 is directly connected, Loopback0
```

```
C       172.16.10.1/32 is directly connected, Virtual-Access1
10.0.0.0/24 is subnetted, 1 subnets
C       10.200.20.0 is directly connected, Ethernet0/0
S    192.168.1.0/24 [1/0] via 10.200.20.250
S*   0.0.0.0/0 [1/0] via 10.200.20.1


*Mar 12 23:11:26.328: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic
0x595E7636
*Mar 12 23:11:26.328: Vi1 LCP: Received id 3, sent id 3, line up172.16.10.1

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 = 156/160/168 ms
```

To Enable Encryption

Add the **ppp encrypt mppe 40** command under **interface virtual–template 1**. Make sure that encryption is selected in the Microsoft client as well.

```
*Mar 12 23:27:36.608: L2TP: I SCCRQ from  RSHANMUG-W2K1.cisco.com tnl 13
*Mar 12 23:27:36.608: Tnl 31311 L2TP: New tunnel created for remote
RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:27:36.608: Tnl 31311 L2TP: O SCCRP  to  RSHANMUG-W2K1.cisco.com
tnlid 13
*Mar 12 23:27:36.612: Tnl 31311 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Mar 12 23:27:36.772: Tnl 31311 L2TP: I SCCCN from  RSHANMUG-W2K1.cisco.com
tnl 13
*Mar 12 23:27:36.772: Tnl 31311 L2TP: Tunnel state change from
wait-ctl-reply to established
*Mar 12 23:27:36.776: Tnl 31311 L2TP: SM State established
*Mar 12 23:27:36.780: Tnl 31311 L2TP: I ICRQ from  RSHANMUG-W2K1.cisco.com
tnl 13
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: Session FS enabled
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: Session state change from idle
to wait-connect
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: New session created
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: O ICRP to
RSHANMUG-W2K1.cisco.com 13/1
*Mar 12 23:27:36.924: Tnl/Cl 31311/52 L2TP: I ICCN from
RSHANMUG-W2K1.cisco.com tnl 13, cl 1
*Mar 12 23:27:36.928: Tnl/Cl 31311/52 L2TP: Session state change from
wait-connect to established
*Mar 12 23:27:36.928: Vi1 VPDN: Virtual interface created for
*Mar 12 23:27:36.928: Vi1 PPP: Phase is DOWN, Setup [0 sess, 0 load]
*Mar 12 23:27:36.928: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
*Mar 12 23:27:36.972: Tnl/Cl 31311/52 L2TP: Session with no hwidb
*Mar 12 23:27:36.976: %LINK-3-UPDOWN: Interface Virtual-Access1, changed
state to up
*Mar 12 23:27:36.976: Vi1 PPP: Using set call direction
*Mar 12 23:27:36.976: Vi1 PPP: Treating connection as a callin
*Mar 12 23:27:36.976: Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess,
0 load]
*Mar 12 23:27:36.976: Vi1 LCP: State is Listen
*Mar 12 23:27:36.976: Vi1 VPDN: Bind interface direction=2
*Mar 12 23:27:38.976: Vi1 LCP: TIMEout: State Listen
*Mar 12 23:27:38.976: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Mar 12 23:27:38.976: Vi1 LCP: O CONFREQ [Listen] id 1 len 15
*Mar 12 23:27:38.976: Vi1 LCP:    AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:27:38.976: Vi1 LCP:    MagicNumber 0x4E2A5593 (0x05064E2A5593)
*Mar 12 23:27:38.984: Vi1 LCP: I CONFREQ [REQsent] id 1 len 44
*Mar 12 23:27:38.984: Vi1 LCP:    MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:38.984: Vi1 LCP:    PFC (0x0702)
```

```
*Mar 12 23:27:38.984: Vi1 LCP:    ACFC (0x0802)
*Mar 12 23:27:38.984: Vi1 LCP:    Callback 6  (0x0D0306)
*Mar 12 23:27:38.984: Vi1 LCP:    MRRU 1614 (0x1104064E)
*Mar 12 23:27:38.984: Vi1 LCP:    EndpointDisc 1 Local
*Mar 12 23:27:38.984: Vi1 LCP:     (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:27:38.984: Vi1 LCP:     (0x10D0AC0000000A)
*Mar 12 23:27:38.984: Vi1 LCP: O CONFREJ [REQsent] id 1 len 34
*Mar 12 23:27:38.984: Vi1 LCP:    Callback 6  (0x0D0306)
*Mar 12 23:27:38.984: Vi1 LCP:    MRRU 1614 (0x1104064E)
*Mar 12 23:27:38.984: Vi1 LCP:    EndpointDisc 1 Local
*Mar 12 23:27:38.988: Vi1 LCP:     (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:27:38.988: Vi1 LCP:     (0x10D0AC0000000A)
*Mar 12 23:27:39.096: Vi1 LCP: I CONFACK [REQsent] id 1 len 15
*Mar 12 23:27:39.096: Vi1 LCP:    AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:27:39.096: Vi1 LCP:    MagicNumber 0x4E2A5593 (0x05064E2A5593)
*Mar 12 23:27:39.128: Vi1 LCP: I CONFREQ [ACKrcvd] id 2 len 14
*Mar 12 23:27:39.128: Vi1 LCP:    MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:39.128: Vi1 LCP:    PFC (0x0702)
*Mar 12 23:27:39.128: Vi1 LCP:    ACFC (0x0802)
*Mar 12 23:27:39.128: Vi1 LCP: O CONFACK [ACKrcvd] id 2 len 14
*Mar 12 23:27:39.128: Vi1 LCP:    MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:39.128: Vi1 LCP:    PFC (0x0702)
*Mar 12 23:27:39.128: Vi1 LCP:    ACFC (0x0802)
*Mar 12 23:27:39.128: Vi1 LCP: State is Open
*Mar 12 23:27:39.128: Vi1 PPP: Phase is AUTHENTICATING, by this end [0
sess, 0 load]
*Mar 12 23:27:39.128: Vi1 MS-CHAP: O CHALLENGE id 32 len 21 from angela
*Mar 12 23:27:39.260: Vi1 LCP: I IDENTIFY [Open] id 3 len 18 magic
0x4B4817ED MSRASV5.00
*Mar 12 23:27:39.288: Vi1 LCP: I IDENTIFY [Open] id 4 len 27 magic
0x4B4817ED MSRAS-1- RSHANMUG-W2K1
*Mar 12 23:27:39.296: Vi1 MS-CHAP: I RESPONSE id 32 len 57 from tac
*Mar 12 23:27:39.296: AAA: parse name=Virtual-Access1 idb type=21 tty=-1
*Mar 12 23:27:39.296: AAA: name=Virtual-Access1 flags=0x11 type=5 shelf=0
slot=0 adapter=0 port=1 channel=0
*Mar 12 23:27:39.296: AAA/MEMORY: create_user (0x6273D528) user='tac'
ruser='' port='Virtual-Access1' rem_addr='' authen_type=MSCHAP service=PPP
priv=1
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): port='Virtual-Access1'
list='' action=LOGIN service=PPP
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): using default list
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): Method=radius (radius)
*Mar 12 23:27:39.296: RADIUS: ustruct sharecount=0
*Mar 12 23:27:39.300: RADIUS: Initial Transmit Virtual-Access1 id 181
10.200.20.245:1645, Access-Request, len 129
*Mar 12 23:27:39.300:        Attribute 4 6 0AC81402
*Mar 12 23:27:39.300:        Attribute 5 6 00000001
*Mar 12 23:27:39.300:        Attribute 61 6 00000001
*Mar 12 23:27:39.300:        Attribute 1 5 7461631A
*Mar 12 23:27:39.300:        Attribute 26 16 000001370B0AFC72
*Mar 12 23:27:39.300:        Attribute 26 58 0000013701342001
*Mar 12 23:27:39.300:        Attribute 6 6 00000002
*Mar 12 23:27:39.300:        Attribute 7 6 00000001
*Mar 12 23:27:39.312: RADIUS: Received from id 181 10.200.20.245:1645,
Access-Accept, len 116
*Mar 12 23:27:39.312:        Attribute 7 6 00000001
*Mar 12 23:27:39.312:        Attribute 6 6 00000002
*Mar 12 23:27:39.312:        Attribute 25 32 502E05AE
*Mar 12 23:27:39.312:        Attribute 26 40 000001370C225042
*Mar 12 23:27:39.312:        Attribute 26 12 000001370A06204E
*Mar 12 23:27:39.312: AAA/AUTHEN (2410248116): status = PASS
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.316: AAA/AUTHOR/LCP: Vi1 (2365724222) user='tac'
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): send AV service=ppp
```

```
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): send AV protocol=lcp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): found list default
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): Method=radius
(radius)
*Mar 12 23:27:39.316: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR (2365724222): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Processing AV service=ppp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.316: Vi1 MS-CHAP: O SUCCESS id 32 len 4
*Mar 12 23:27:39.316: Vi1 PPP: Phase is UP [0 sess, 0 load]
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/FSM: (0): Can we start IPCP?
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.320: AAA/AUTHOR/FSM: Vi1 (1499311111) user='tac'
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): send AV service=ppp
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): send AV protocol=ip
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): found list default
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): Method=radius
(radius)
*Mar 12 23:27:39.320: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR (1499311111): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM: We can start IPCP
*Mar 12 23:27:39.320: Vi1 IPCP: O CONFREQ [Closed] id 1 len 10
*Mar 12 23:27:39.320: Vi1 IPCP:    Address 172.16.10.100 (0x0306AC100A64)
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM: (0): Can we start CCP?
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (327346364):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.324: AAA/AUTHOR/FSM: Vi1 (327346364) user='tac'
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): send AV service=ppp
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): send AV protocol=ccp
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): found list default
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): Method=radius
(radius)
*Mar 12 23:27:39.324: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR (327346364): Post authorization status
= PASS_REPL
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM: We can start CCP
*Mar 12 23:27:39.324: Vi1 CCP: O CONFREQ [Closed] id 1 len 10
*Mar 12 23:27:39.324: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.460: Vi1 CCP: I CONFREQ [REQsent] id 5 len 10
*Mar 12 23:27:39.460: Vi1 CCP:    MS-PPC supported bits 0x01000001
(0x120601000001)
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar 12 23:27:39.464: Vi1 CCP: O CONFNAK [REQsent] id 5 len 10
*Mar 12 23:27:39.464: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.472: Vi1 IPCP: I CONFREQ [REQsent] id 6 len 34
*Mar 12 23:27:39.472: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Mar 12 23:27:39.472: Vi1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:27:39.472: Vi1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:27:39.472: Vi1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:27:39.472: Vi1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
```

```
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:27:39.472: Vi1 IPCP: Pool returned 172.16.10.1
*Mar 12 23:27:39.476: Vi1 IPCP: O CONFREJ [REQsent] id 6 len 28
*Mar 12 23:27:39.476: Vi1 IPCP:     PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:27:39.476: Vi1 IPCP:     PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:27:39.476: Vi1 IPCP:     SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:27:39.476: Vi1 IPCP:     SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:27:39.480: Vi1 IPCP: I CONFACK [REQsent] id 1 len 10
*Mar 12 23:27:39.484: Vi1 IPCP:     Address 172.16.10.100 (0x0306AC100A64)
*Mar 12 23:27:39.488: Vi1 CCP: I CONFACK [REQsent] id 1 len 10
*Mar 12 23:27:39.488: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 CCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar 12 23:27:39.596: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar 12 23:27:39.596: Vi1 CCP: O CONFACK [ACKrcvd] id 7 len 10
*Mar 12 23:27:39.596: Vi1 CCP:    MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 CCP: State is Open
*Mar 12 23:27:39.600: Vi1 MPPE: Generate keys using RADIUS data
*Mar 12 23:27:39.600: Vi1 MPPE: Initialize keys
*Mar 12 23:27:39.600: Vi1 MPPE: [40 bit encryption]  [stateless mode]
*Mar 12 23:27:39.620: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar 12 23:27:39.620: Vi1 IPCP:     Address 0.0.0.0 (0x030600000000)
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0, we
want 172.16.10.1
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0, we
want 172.16.10.1
*Mar 12 23:27:39.624: Vi1 IPCP: O CONFNAK [ACKrcvd] id 8 len 10
*Mar 12 23:27:39.624: Vi1 IPCP:     Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.756: Vi1 IPCP: I CONFREQ [ACKrcvd] id 9 len 10
*Mar 12 23:27:39.756: Vi1 IPCP:     Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP: Start.  Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.756: AAA/AUTHOR/IPCP: Vi1 (2840659706) user='tac'
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV service=ppp
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV protocol=ip
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV
addr*172.16.10.1
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): found list
default
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): Method=radius
(radius)
*Mar 12 23:27:39.756: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR (2840659706): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP: Reject 172.16.10.1, using
172.16.10.1
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV addr*172.16.10.1
```

```
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Done.  Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:27:39.760: Vi1 IPCP: O CONFACK [ACKrcvd] id 9 len 10
*Mar 12 23:27:39.760: Vi1 IPCP:    Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.760: Vi1 IPCP: State is Open
*Mar 12 23:27:39.764: Vi1 IPCP: Install route to 172.16.10.1
*Mar 12 23:27:40.316: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
*Mar 12 23:27:46.628: Vi1 LCP: I ECHOREP [Open] id 1 len 12 magic
0x4B4817ED
*Mar 12 23:27:46.628: Vi1 LCP: Received id 1, sent id 1, line up
*Mar 12 23:27:56.636: Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic
0x4B4817ED
*Mar 12 23:27:56.636: Vi1 LCP: Received id 2, sent id 2, line upcaller ip
Line           User        IP Address     Local Number    Remote Number   <->
Vi1            tac         172.16.10.1    -               -               in

angela#show ppp mppe virtual-Access 1
Interface Virtual-Access1 (current connection)
Software encryption, 40 bit encryption, Stateless mode
packets encrypted = 0        packets decrypted  = 16
sent CCP resets   = 0        receive CCP resets = 0
next tx coherency = 0        next rx coherency  = 16
tx key changes    = 0        rx key changes     = 16
rx pkt dropped    = 0        rx out of order pkt= 0
rx missed packets = 0
*Mar 12 23:28:06.604: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic
0x4B4817ED
*Mar 12 23:28:06.604: Vi1 LCP: Received id 3, sent id 3, 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 = 188/196/204 ms

angela#show ppp mppe virtual-Access 1
Interface Virtual-Access1 (current connection)
Software encryption, 40 bit encryption, Stateless mode
packets encrypted = 5        packets decrypted  = 22
sent CCP resets   = 0        receive CCP resets = 0
next tx coherency = 5        next rx coherency  = 22
tx key changes    = 5        rx key changes     = 22
rx pkt dropped    = 0        rx out of order pkt= 0
rx missed packets = 0

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 = 184/200/232 ms
angela#ping 172.16.10.1sh ppp mppe virtual-Access 1
Interface Virtual-Access1 (current connection)
Software encryption, 40 bit encryption, Stateless mode
packets encrypted = 10       packets decrypted  = 28
sent CCP resets   = 0        receive CCP resets = 0
next tx coherency = 10       next rx coherency  = 28
tx key changes    = 10       rx key changes     = 28
rx pkt dropped    = 0        rx out of order pkt= 0
rx missed packets = 0
angela#
```

debug and show Commands

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

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

If things do not work, minimal **debug** includes these 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, which includes 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 Microsoft Point−to−Point Encryption (MPPE) encryption, use one of these commands:

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

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

Split Tunneling

Assume that the gateway router is an Internet Service Provider (ISP) router. When the Point−to−Point Tunneling Protocol (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. In order to remedy this, modify the Microsoft routing to delete the default and reinstall the default route (this required knowing the IP address the PPTP client was assigned; for the current example, this is 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
```

Troubleshoot

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

Problem 1: IPSec Not Disabled

Symptom

The PC user sees this message:

```
Error connecting to L2TP:
Error 781: The encryption attempt failed because
no valid certificate was found.
```

Solution

Go to the **Properties** section of the **Virtual Private Connection** window and click on the **Security** tab. Disable the **Require Data Encryption** option.

Problem 2: Error 789

Symptom

The L2TP connection attempt fails because the security layer encountered a processing error during initial negotiations with the remote computer.

The Microsoft Remote Access and Policy Agent services create a policy that is used for L2TP traffic because L2TP does not provide encryption. This is applicable for the Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Server and Microsoft Windows 2000 Professional.

Solution

Use the Registry Editor (Regedt32.exe) to add the new registry entry to disable IPSec. Refer to Microsoft's documentation or the Microsoft help topic for Regedt32.exe.

You must add the ProhibitIpSec registry value to each Windows 2000–based endpoint computer of an L2TP or IPSec connection to prevent the automatic filter for L2TP and IPSec traffic from being created. When the ProhibitIpSec registry value is set to one, your Windows 2000–based computer does not create the automatic filter that uses CA authentication. Instead, it checks for a local or Active Directory IPSec policy. In order to add the ProhibitIpSec registry value to your Windows 2000–based computer, use Regedt32.exe to locate this key in the registry:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

Add this registry value to this key:

```
Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1
```

Note: You must restart your Windows 2000–based computer for the changes to take effect.

Problem 3: Problem with Tunnel Authentication

Users are authenticated at the NAS or LNS before the tunnel is established. This is not required for client–initiated tunnels like L2TP from a Microsoft client.

The PC user sees this message:

```
Connecting to 10.200.20.2..
Error 651: The modem(or other connecting device) has reported an error.
Router debugs:

*Mar 12 23:03:47.124: L2TP: I SCCRQ from  RSHANMUG-W2K1.cisco.com tnl 1
*Mar 12 23:03:47.124: Tnl 30107 L2TP: New tunnel created for remote
RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:03:47.124: Tnl 30107 L2TP: O SCCRP  to  RSHANMUG-W2K1.cisco.com
tnlid 1
*Mar 12 23:03:47.124: Tnl 30107 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Mar 12 23:03:47.308: Tnl 30107 L2TP: I SCCCN from  RSHANMUG-W2K1.cisco.com
tnl 1
*Mar 12 23:03:47.308: Tnl 30107 L2TP: Got a Challenge Response in SCCCN
from  RSHANMUG-W2K1.cisco.com
*Mar 12 23:03:47.308: AAA: parse name= idb type=-1 tty=-1
*Mar 12 23:03:47.308: AAA/MEMORY: create_user (0x6273D528) user='angela'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): port='' list='default'
action=SENDAUTH service=PPP
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): found list default
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): Method=radius (radius)
*Mar 12 23:03:47.308: AAA/AUTHEN/SENDAUTH (4077585132): no authenstruct
hwidb
*Mar 12 23:03:47.308: AAA/AUTHEN/SENDAUTH (4077585132): Failed sendauthen
for angela
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = FAIL
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): Method=LOCAL
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): SENDAUTH no password for
angela
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = ERROR
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): no methods left to try
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = ERROR
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): failed to authenticate
*Mar 12 23:03:47.308: VPDN: authentication failed, couldn't find user
information for angela
*Mar 12 23:03:47.308: AAA/MEMORY: free_user (0x6273D528) user='angela'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
*Mar 12 23:03:47.312: Tnl 30107 L2TP: O StopCCN  to
RSHANMUG-W2K1.cisco.com tnlid 1
*Mar 12 23:03:47.312: Tnl 30107 L2TP: Tunnel state change from
wait-ctl-reply to shutting-down
*Mar 12 23:03:47.320: Tnl 30107 L2TP: Shutdown tunnel
*Mar 12 23:03:47.320: Tnl 30107 L2TP: Tunnel state change from
shutting-down to idle
*Mar 12 23:03:47.324: L2TP: Could not find tunnel for tnl 30107, discarding
ICRQ ns 3 nr 1
*Mar 12 23:03:47.448: L2TP: Could not find tunnel for tnl 30107, discarding
ICRQ ns 3 nr 2
```

Related Information

- **Layer Two Tunneling Protocol (L2TP)**
- **L2TP Over IPsec Between Windows 2000 and VPN 3000 Concentrator Using Digital Certificates Configuration Example**
- **Configuring L2TP Over IPSec Between PIX Firewall and Windows 2000 PC Using Certificates**
- **Layer 2 Tunnel Protocol**
- **Configuring Virtual Private Networks**
- **Configuring Layer 2 Tunnel Protocol Authentication with RADIUS**
- **Technical Support & Documentation – Cisco Systems**