Configuring L2TP Client Inititiated Tunnelling with Windows 2000 PC

Document ID: 21381

Contents

Introduction

In most virtual private dial−up network (VPDN) scenarios, the client dials the network access server (NAS). The NAS then initiates the VPDN Layer 2 Tunnel Protocol (L2TP) or the Layer 2 Forwarding (L2F) protocol tunnel to the Home Gateway (HGW). This creates a VPDN connection between the NAS, which is the L2TP access concentrator (LAC) endpoint, and the HGW, which is the L2TP network server (LNS) endpoint. This means that only the link between the NAS and the HGW uses L2TP, and that tunnel does not include the link from the client PC to the NAS. However, PC clients running the Windows 2000 operating system are now able to become the LAC and initiate an L2TP tunnel from the PC, through the NAS and terminated on the HGW/LNS. This sample configuration shows how you can configure such a tunnel.

Prerequisites

Requirements

Before attempting this configuration, ensure that you meet these requirements:

- Familiarity with Understanding VPDN
- Familiarity with Synopsis of Access VPDN Dial−In Using L2TP

Note: The NAS configuration is not included in this document.

Components Used

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

- LNS: Cisco 7200 Series router running Cisco IOS® Software Release 12.2(1)
- Client: Windows 2000 PC with a modem

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.

Related Products

The configuration for the LNS included in this document is not platform specific and can be applied to any VPDN−capable router.

The procedure to configure the Windows 2000 client PC is applicable only to Windows 2000 and not to any other operating system.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Background Information

As mentioned in the Introduction, with Windows 2000 you can initiate an L2TP tunnel from the client PC and have the tunnel terminated anywhere in the Internet service provider (ISP) network. Using VPDN terminology, this setup is referred to as a "client−initiated" tunnel. Since client−initiated tunnels are tunnels initiated by client software on the PC, the PC takes on the role of the LAC. Since the client will be authenticated using Point−to−Point Protocol (PPP), Challenge Handshake Authentication Protocol (CHAP), or Password Authentication Protocol (PAP) anyway, the tunnel itself does not need to be authenticated.

Advantages and Disadvantages of using client−initiated tunnels

Client−initiated tunnels have both advantages and disadvantages, some of which are outlined here:

Advantages:

- It secures the entire connection from the client through the ISP shared network and to the enterprise network.
- It does *not* require additional configuration on the ISP network. Without a client−initiated tunnel, the ISP NAS or its Radius/TACACS+ server needs to be configured to initiate the tunnel to the HGW. Therefore, the enterprise must negotiate with many ISPs to allow users to tunnel through their network. With a client−initiated tunnel, the end user can connect to any ISP and then manually initiate the tunnel to the enterprise network.

Disadvantages:

- It is not as scalable as an ISP−initiated tunnel. Since client−initiated tunnels create individual tunnels for each client, the HGW must individually terminate a large number of tunnels.
- The client must manage the client software used to initiate the tunnel. This is often a source of support−related problems for the enterprise.
- The client must have an account with the ISP. Since client−initiated tunnels can only be created after a connection to the ISP is established, the client must have an account to connect to the ISP network.

How it works

Thjs is how the example in this document works:

1. The client PC dials into the NAS, authenticates using the client's ISP account, and obtains an IP address from the ISP.
2. The client initiates and builds the L2TP tunnel to the L2TP network server HGW (LNS). The client will renegotiate IP Control Protocol (IPCP) and will obtain a new IP address from the LNS.

Configure the Windows 2000 Client For L2TP

Create two dial−up networking (DUN) connections:

- One DUN connection to dial−in to the ISP. Refer to your ISP for more information on this subject.
- Another DUN connection for the L2TP tunnel.

To create and configure the DUN connection for L2TP, perform these steps on the Windows 200 client PC:

1. From the Start Menu, choose **Settings > Control Panel > Network and Dial−up Connections > Make New Connection**.

   Use the Wizard to create a connection called L2TP. Make sure to select **Connect to a private network through the Internet** in the **Network Connection Type** window. You must also specify the IP address or name of the LNS/HGW.
2. The new connection (named L2TP) appears in the **Network and Dial−up Connections** window under Control Panel. From here, right−click to edit the **Properties**.
3. Click the Networking tab and make sure that the **Type Of Server I Am Calling** is set to **L2TP**.
4. If you plan to allocate a dynamic internal (enterprise network) address to this client from the HGW, through either a local pool or DHCP, select **TCP/IP** protocol. Make sure that the client is configured to obtain an IP address automatically. You may also issue Domain Naming System (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. Under the Security Tab, you can define the user authentication parameters. For example, PAP, CHAP, or MS−CHAP, or Windows domain logon. Consult the network systems administrator for information on the parameters that should be configured on the client.
5. Once the connection is configured, you can double−click it to pop up the login screen, and then connect.

Additional Remarks

If your L2TP tunnel uses IP Security (IPSec) and/or Microsoft Point−to−Point Encryption (MPPE), then you must define this command under the virtual−template configuration on the LNS/HGW.

```
ppp encrypt mppe 40
```

Keep in mind that this requires the encrypted Cisco IOS Software feature set (at least the IPSec feature set or IPSec with 3DES).

By default, IPSec is enabled on Windows 2000. If you want to disable it, you must modify the Windows Registry using the Registry Editor:

Disable IPSec on a Win2K PC

Warning: Take adequate precautions (such as backing up the registry) prior to modifying the registry.

You should also refer to the Microsoft web site for the correct procedure to modify the registry.

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 the key:

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

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

For a more complex setup using Windows 2000, refer to Configuring Cisco IOS and Windows 2000 Clients for L2TP Using Microsoft IAS.
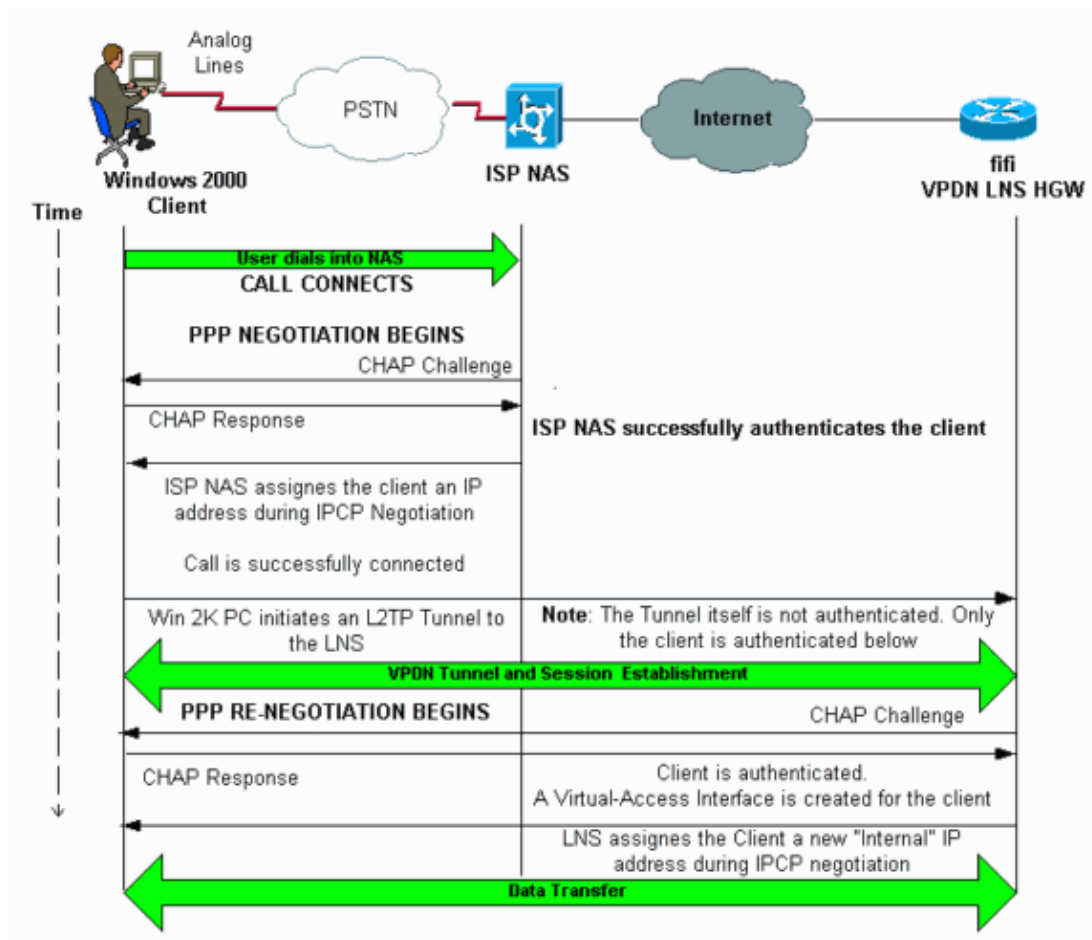
Configure

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 Command Lookup Tool (registered customers only) .

Network Diagram

The network diagram below shows the various negotiations that occur among the client PC, ISP NAS, and Enterprise HGW. The debug example in the Troubleshoot section depicts these transactions as well.

Analog Lines

PSTN

Internet

ISP NAS

fifi
VPDN LNS HGW

Windows 2000 Client

Time

User dials into NAS
CALL CONNECTS

PPP NEGOTIATION BEGINS
CHAP Challenge

CHAP Response

ISP NAS successfully authenticates the client

ISP NAS assignes the client an IP address during IPCP Negotiation

Call is successfully connected

Win 2K PC initiates an L2TP Tunnel to the LNS

Note: The Tunnel itself is not authenticated. Only the client is authenticated below

VPDN Tunnel and Session Establishment

PPP RE-NEGOTIATION BEGINS
CHAP Challenge

CHAP Response

Client is authenticated.
A Virtual-Access Interface is created for the client

LNS assignes the Client a new "Internal" IP address during IPCP negotiation

Data Transfer

Configurations

This document uses this configuration:

- fifi (VPDN LNS/HGW)

Note: Only the relevant section of the LNS configuration is included.

fifi (VPDN LNS/HGW)

```
hostname fifi
!
username l2tp-w2k password 0 ww

!--- This is the password for the Windows 2000 client.
!--- With AAA, the username and password can be offloaded to the external
!--- AAA server.

!
vpdn enable

!--- Activates VPDN.

!
vpdn-group l2tp-w2k

!--- This is the default L2TP VPDN group.

 accept-dialin
  protocol l2tp
```

```
  !--- This allows L2TP on this VPDN group.

  virtual-template 1

  !--- Use virtual-template 1 for the virtual-interface configuration.

 no l2tp tunnel authentication

 !--- The L2TP tunnel is not authenticated.


 !--- Tunnel authentication is not needed because the client will be
 !--- authenticated using PPP CHAP/PAP. Keep in mind that the client is the
 !--- only user of the tunnel, so client authentication is sufficient.

!
interface loopback 0
 ip address 1.1.1.1 255.255.255.255
!
interface Ethernet1/0
 ip address 200.0.0.14 255.255.255.0
 ip router isis
 duplex half
 tag-switching ip
!
interface Virtual-Template1

!--- Virtual-Template interface specified in the vpdn-group configuration.

 ip unnumbered Loopback0
 peer default ip address pool pptp

 !--- IP address for the client obtained from IP pool named pptp (defined below).

 ppp authentication chap
!
ip local pool pptp 1.100.0.1 1.100.0.10

!--- This defines the "Internal" IP address pool (named pptp) for the client.

ip route 199.0.0.0 255.255.255.0 200.0.0.45
```

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 (registered customers only) , which allows you to view an analysis of **show** command output.

- **show vpdn** Displays information about active L2x tunnel and message identifiers in a VPDN.
- **show vpdn session window** Displays information on the window for the VPDN session.
- **show user** Provides a comprehensive listing of all users connected to the router.
- **show caller user** *username* **detail** To show parameters for the particular user, such as the Link Control Protocol (LCP), NCP and IPCP states, as well as the IP address assigned, PPP and PPP bundle parameters, and so on.

```
show vpdn
---------

L2TP Tunnel and Session Information Total tunnels 1 sessions 1
```

```
LocID RemID Remote Name   State  Remote Address  Port  Sessions
25924 1     JVEYNE-W2K1.c est    199.0.0.8       1701  1
```

```
LocID RemID TunID Intf         Username      State  Last Chg Fastswitch
2     1     25924 Vi1          l2tp-w2k      est    00:00:13 enabled
```

```
%No active L2F tunnels

%No active PPTP tunnels

%No active PPPoE tunnels
```

show vpdn session window

```
L2TP Session Information Total tunnels 1 sessions 1

LocID RemID TunID ZLB-tx  ZLB-rx  Rbit-tx Rbit-rx WSize MinWS Timeouts Qsize
2     1     25924 0       0       0       0       0     0     0        0

%No active L2F tunnels

%No active PPTP tunnels

%No active PPPoE tunnels
```

show user

```
    Line        User       Host(s)             Idle        Location
*  0 con 0                  idle                00:00:00

  Interface     User       Mode               Idle        Peer Address
   Vi1          l2tp-w2k   Virtual PPP (L2TP ) 00:00:08
```

show caller user l2tp-w2k detail

```
  User: l2tp-w2k, line Vi1, service PPP L2TP
        Active time 00:01:08, Idle time 00:00:00
  Timeouts:           Absolute  Idle
      Limits:         -         -
      Disconnect in:  -         -
  PPP: LCP Open, CHAP (<- local), IPCP
```

```
  LCP: -> peer, AuthProto, MagicNumber
```

```
          <- peer, MagicNumber, EndpointDisc
    NCP: Open IPCP

    !--- The IPCP state is Open.

    IPCP: <- peer, Address
          -> peer, Address
    IP: Local 1.1.1.1, remote 1.100.0.2

    !--- The IP address assigned to the client is 1.100.0.2 (from the IP pool
    !--- on the LNS).

    VPDN: NAS , MID 2, MID Unknown
          HGW , NAS CLID 0, HGW CLID 0, tunnel open

    !--- The VPDN tunnel is open.

    Counts: 48 packets input, 3414 bytes, 0 no buffer
            0 input errors, 0 CRC, 0 frame, 0 overrun
            20 packets output, 565 bytes, 0 underruns
            0 output errors, 0 collisions, 0 interface resets
```

Troubleshoot

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

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, refer to Important Information on Debug Commands.

- **debug ppp negotiation** Displays information on PPP traffic and exchanges while negotiating the PPP components including LCP, Authentication, and NCP. A successful PPP negotiation first opens the LCP state, then authenticates, and finally negotiates NCP (usually IPCP).
- **debug vpdn event** Displays messages about events that are part of normal tunnel establishment or shutdown.
- **debug vpdn error** Displays errors that prevent a tunnel from being established or errors that cause an established tunnel to be closed.
- **debug vpdn l2x–event** Displays messages about events that are part of normal tunnel establishment or shutdown for L2x.
- **debug vpdn l2x–error** Displays L2x protocol errors that prevent L2x establishment or prevent its normal operation.

Note: Some of these lines of **debug** output are broken into multiple lines for printing purposes.

Enable the **debug** commands specified above on the LNS and initiate a call from the Windows 2000 client PC. The debugs here show the tunnel request from the client, the establishment of the tunnel, the authentication of the client, and the renegotiation of the IP address:

```
    LNS: Incoming session from PC Win2K :
    ====================================

    *Jun  6 04:02:05.174: L2TP: I SCCRQ from JVEYNE-W2K1.cisco.com tnl 1

    !--- This is the incoming tunnel initiation request from the client PC.

    *Jun  6 04:02:05.178: Tnl 25924 L2TP: New tunnel created for remote
```

JVEYNE-W2K1.cisco.com, address 199.0.0.8

!--- The tunnel is created. Note that the client IP address is the one
!--- assigned by the NAS.
!--- This IP address will be renegotiatied later.

```
*Jun  6 04:02:05.178: Tnl 25924 L2TP: O SCCRP  to JVEYNE-W2K1.cisco.com tnlid 1
*Jun  6 04:02:05.178: Tnl 25924 L2TP: Tunnel state change from idle to wait-ctl-reply
*Jun  6 04:02:05.346: Tnl 25924 L2TP: I SCCCN from JVEYNE-W2K1.cisco.com tnl 1
*Jun  6 04:02:05.346: Tnl 25924 L2TP: Tunnel state change from wait-ctl-reply
   to established
```

!--- The tunnel is now established.

```
*Jun  6 04:02:05.346: Tnl 25924 L2TP: SM State established
*Jun  6 04:02:05.358: Tnl 25924 L2TP: I ICRQ from JVEYNE-W2K1.cisco.com tnl 1
*Jun  6 04:02:05.358: Tnl/Cl 25924/2 L2TP: Session FS enabled
*Jun  6 04:02:05.358: Tnl/Cl 25924/2 L2TP: Session state change from idle to
   wait-connect
*Jun  6 04:02:05.358: Tnl/Cl 25924/2 L2TP: New session created
*Jun  6 04:02:05.358: Tnl/Cl 25924/2 L2TP: O ICRP to JVEYNE-W2K1.cisco.com 1/1
*Jun  6 04:02:05.514: Tnl/Cl 25924/2 L2TP: I ICCN from JVEYNE-W2K1.cisco.com tnl 1,
   cl 1
```

!--- The LNS receives ICCN (Incoming Call coNnected). The VPDN session is up, then
!--- the LNS receives the LCP layer along with the username and CHAP password
!--- of the client. A virtual-access will be cloned from the virtual-template 1.

```
*Jun  6 04:02:05.514: Tnl/Cl 25924/2 L2TP: Session state change from wait-connect
   to established
```

!--- A VPDN session is being established within the tunnel.

```
*Jun  6 04:02:05.514: Vi1 VPDN: Virtual interface created for
*Jun  6 04:02:05.514: Vi1 PPP: Phase is DOWN, Setup [0 sess, 0 load]
*Jun  6 04:02:05.514: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
*Jun  6 04:02:05.566: Tnl/Cl 25924/2 L2TP: Session with no hwidb
*Jun  6 04:02:05.570: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Jun  6 04:02:05.570: Vi1 PPP: Using set call direction
*Jun  6 04:02:05.570: Vi1 PPP: Treating connection as a callin
*Jun  6 04:02:05.570: Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0 load]
*Jun  6 04:02:05.570: Vi1 LCP: State is Listen
*Jun  6 04:02:05.570: Vi1 VPDN: Bind interface direction=2
*Jun  6 04:02:07.546: Vi1 LCP: I CONFREQ [Listen] id 1 len 44
```

!--- LCP negotiation begins.

```
*Jun  6 04:02:07.546: Vi1 LCP:    MagicNumber 0x21A20F49 (0x050621A20F49)
*Jun  6 04:02:07.546: Vi1 LCP:    PFC (0x0702)
*Jun  6 04:02:07.546: Vi1 LCP:    ACFC (0x0802)
*Jun  6 04:02:07.546: Vi1 LCP:    Callback 6  (0x0D0306)
*Jun  6 04:02:07.546: Vi1 LCP:    MRRU 1614 (0x1104064E)
*Jun  6 04:02:07.546: Vi1 LCP:    EndpointDisc 1 Local
*Jun  6 04:02:07.546: Vi1 LCP:     (0x131701708695CDF2C64730B5B6756CE8)
*Jun  6 04:02:07.546: Vi1 LCP:     (0xB1AB1600000001)
*Jun  6 04:02:07.550: Vi1 LCP: O CONFREQ [Listen] id 1 len 19
*Jun  6 04:02:07.550: Vi1 LCP:    MRU 1460 (0x010405B4)
*Jun  6 04:02:07.550: Vi1 LCP:    AuthProto CHAP (0x0305C22305)
*Jun  6 04:02:07.550: Vi1 LCP:    MagicNumber 0xFA95EEC3 (0x0506FA95EEC3)
*Jun  6 04:02:07.550: Vi1 LCP: O CONFREJ [Listen] id 1 len 11
*Jun  6 04:02:07.550: Vi1 LCP:    Callback 6  (0x0D0306)
*Jun  6 04:02:07.550: Vi1 LCP:    MRRU 1614 (0x1104064E)
*Jun  6 04:02:07.710: Vi1 LCP: I CONFNAK [REQsent] id 1 len 8
*Jun  6 04:02:07.710: Vi1 LCP:    MRU 1514 (0x010405EA)
*Jun  6 04:02:07.710: Vi1 LCP: O CONFREQ [REQsent] id 2 len 15
*Jun  6 04:02:07.710: Vi1 LCP:    AuthProto CHAP (0x0305C22305)
```

```
*Jun  6 04:02:07.710: Vi1 LCP:    MagicNumber 0xFA95EEC3 (0x0506FA95EEC3)
*Jun  6 04:02:07.718: Vi1 LCP: I CONFREQ [REQsent] id 2 len 37
*Jun  6 04:02:07.718: Vi1 LCP:    MagicNumber 0x21A20F49 (0x050621A20F49)
*Jun  6 04:02:07.718: Vi1 LCP:    PFC (0x0702)
*Jun  6 04:02:07.718: Vi1 LCP:    ACFC (0x0802)
*Jun  6 04:02:07.718: Vi1 LCP:    EndpointDisc 1 Local
*Jun  6 04:02:07.718: Vi1 LCP:     (0x131701708695CDF2C64730B5B6756CE8)
*Jun  6 04:02:07.718: Vi1 LCP:     (0xB1AB1600000001)
*Jun  6 04:02:07.718: Vi1 LCP: O CONFACK [REQsent] id 2 len 37
*Jun  6 04:02:07.718: Vi1 LCP:    MagicNumber 0x21A20F49 (0x050621A20F49)
*Jun  6 04:02:07.718: Vi1 LCP:    PFC (0x0702)
*Jun  6 04:02:07.718: Vi1 LCP:    ACFC (0x0802)
*Jun  6 04:02:07.718: Vi1 LCP:    EndpointDisc 1 Local
*Jun  6 04:02:07.718: Vi1 LCP:     (0x131701708695CDF2C64730B5B6756CE8)
*Jun  6 04:02:07.718: Vi1 LCP:     (0xB1AB1600000001)
*Jun  6 04:02:07.858: Vi1 LCP: I CONFACK [ACKsent] id 2 len 15
*Jun  6 04:02:07.858: Vi1 LCP:    AuthProto CHAP (0x0305C22305)
*Jun  6 04:02:07.858: Vi1 LCP:    MagicNumber 0xFA95EEC3 (0x0506FA95EEC3)
*Jun  6 04:02:07.858: Vi1 LCP: State is Open
```

!--- LCP negotiation is complete.

```
*Jun  6 04:02:07.858: Vi1 PPP: Phase is AUTHENTICATING, by this end [0 sess, 0 load]
*Jun  6 04:02:07.858: Vi1 CHAP: O CHALLENGE id 5 len 25 from "fifi"
*Jun  6 04:02:07.870: Vi1 LCP: I IDENTIFY [Open] id 3 len 18 magic 0x21A20F49
   MSRASV5.00
*Jun  6 04:02:07.874: Vi1 LCP: I IDENTIFY [Open] id 4 len 27 magic 0x21A20F49
   MSRAS-1-JVEYNE-W2K1
*Jun  6 04:02:08.018: Vi1 CHAP: I RESPONSE id 5 len 29 from "l2tp-w2k"
*Jun  6 04:02:08.018: Vi1 CHAP: O SUCCESS id 5 len 4
```

!--- CHAP authentication is successful. If authentication fails, check the
!--- username and password on the LNS.

```
*Jun  6 04:02:08.018: Vi1 PPP: Phase is UP [0 sess, 0 load]
*Jun  6 04:02:08.018: Vi1 IPCP: O CONFREQ [Closed] id 1 len 10
*Jun  6 04:02:08.018: Vi1 IPCP:    Address 1.1.1.1 (0x030601010101)
*Jun  6 04:02:08.158: Vi1 CCP: I CONFREQ [Not negotiated] id 5 len 10
*Jun  6 04:02:08.158: Vi1 CCP:    MS-PPC supported bits 0x01000001 (0x120601000001)
*Jun  6 04:02:08.158: Vi1 LCP: O PROTREJ [Open] id 3 len 16 protocol CCP
  (0x80FD0105000A120601000001)
*Jun  6 04:02:08.170: Vi1 IPCP: I CONFREQ [REQsent] id 6 len 34
*Jun  6 04:02:08.170: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Jun  6 04:02:08.170: Vi1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Jun  6 04:02:08.170: Vi1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Jun  6 04:02:08.170: Vi1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Jun  6 04:02:08.170: Vi1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Jun  6 04:02:08.170: Vi1 IPCP: Pool returned 1.100.0.2
```

!--- This is the new "Internal" IP address for the client returned by the
!--- LNS IP address pool.

```
*Jun  6 04:02:08.170: Vi1 IPCP: O CONFREJ [REQsent] id 6 Len 28
*Jun  6 04:02:08.170: Vi1 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
*Jun  6 04:02:08.170: Vi1 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
*Jun  6 04:02:08.170: Vi1 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
*Jun  6 04:02:08.170: Vi1 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
*Jun  6 04:02:08.174: Vi1 IPCP: I CONFACK [REQsent] id 1 Len 10
*Jun  6 04:02:08.174: Vi1 IPCP:    Address 1.1.1.1 (0x030601010101)
*Jun  6 04:02:08.326: Vi1 IPCP: I CONFREQ [ACKrcvd] id 7 Len 10
*Jun  6 04:02:08.326: Vi1 IPCP:    Address 0.0.0.0 (0x030600000000)
*Jun  6 04:02:08.326: Vi1 IPCP: O CONFNAK [ACKrcvd] id 7 Len 10
*Jun  6 04:02:08.330: Vi1 IPCP:    Address 1.100.0.2 (0x030601640002)
*Jun  6 04:02:08.486: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 Len 10
*Jun  6 04:02:08.486: Vi1 IPCP:    Address 1.100.0.2 (0x030601640002)
*Jun  6 04:02:08.486: Vi1 IPCP: O CONFACK [ACKrcvd] id 8 Len 10
```

```
*Jun  6 04:02:08.490: Vi1 IPCP:    Address 1.100.0.2 (0x030601640002)
*Jun  6 04:02:08.490: Vi1 IPCP: State is Open
*Jun  6 04:02:08.490: Vi1 IPCP: Install route to 1.100.0.2
*Jun  6 04:02:09.018: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
    changed state to up
```

!--- The interface is up.

This debug output on the LNS shows the Windows 2000 client disconnecting the call. Note the various messages where the LNS recognizes the disconnect and performs a clean shutdown of the tunnel:

```
*Jun  6 04:03:25.174: Vi1 LCP: I TERMREQ [Open] id 9 Len 16
    (0x21A20F49003CCD7400000000)
```

!--- This is the incoming session termination request. This means that the client
!--- disconnected the call.

```
*Jun  6 04:03:25.174: Vi1 LCP: O TERMACK [Open] id 9 Len 4
*Jun  6 04:03:25.354: Vi1 Tnl/Cl 25924/2 L2TP: I CDN from JVEYNE-W2K1.cisco.com
    tnl 1, CL 1
*Jun  6 04:03:25.354: Vi1 Tnl/CL 25924/2 L2TP: Destroying session
*Jun  6 04:03:25.358: Vi1 Tnl/CL 25924/2 L2TP: Session state change from established
    to idle
*Jun  6 04:03:25.358: Vi1 Tnl/CL 25924/2 L2TP: Releasing idb for LAC/LNS tunnel
    25924/1 session 2 state idle
*Jun  6 04:03:25.358: Vi1 VPDN: Reset
*Jun  6 04:03:25.358: Tnl 25924 L2TP: Tunnel state change from established to
    no-sessions-left
*Jun  6 04:03:25.358: Tnl 25924 L2TP: No more sessions in tunnel, shutdown (likely)
    in 10 seconds
```

!--- Because there are no more calls in the tunnel, it will be shut down.

```
*Jun  6 04:03:25.362: %LINK-3-UPDOWN: Interface Virtual-Access1,
    changed state to down
*Jun  6 04:03:25.362: Vi1 LCP: State is Closed
*Jun  6 04:03:25.362: Vi1 IPCP: State is Closed
*Jun  6 04:03:25.362: Vi1 PPP: Phase is DOWN [0 sess, 0 load]
*Jun  6 04:03:25.362: Vi1 VPDN: Cleanup
*Jun  6 04:03:25.362: Vi1 VPDN: Reset
*Jun  6 04:03:25.362: Vi1 VPDN: Unbind interface
*Jun  6 04:03:25.362: Vi1 VPDN: Unbind interface
*Jun  6 04:03:25.362: Vi1 VPDN: Reset
*Jun  6 04:03:25.362: Vi1 VPDN: Unbind interface
*Jun  6 04:03:25.362: Vi1 IPCP: Remove route to 1.100.0.2
*Jun  6 04:03:25.514: Tnl 25924 L2TP: I StopCCN from JVEYNE-W2K1.cisco.com tnl 1
*Jun  6 04:03:25.514: Tnl 25924 L2TP: Shutdown tunnel
```

!--- The tunnel is shut down.

```
*Jun  6 04:03:25.514: Tnl 25924 L2TP: Tunnel state change from no-sessions-left
    to idle
*Jun  6 04:03:26.362: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
    changed state to down
```

Related Information

- **Configuring Cisco IOS and Windows 2000 Clients for L2TP Using Microsoft IAS**
- **Understanding VPDN**
- **VPDN Configuration Without AAA**
- **Configuring Layer 2 Tunnel Protocol Authentication with RADIUS**
- **Configuring an Access Server with PRIs for Incoming Async and ISDN Calls**

- **Dial Technology Support Pages**
- **Technical Support – Cisco Systems**

Updated: Feb 04, 2010   Document ID: 21381