

# Configuring L2TP Client Initiated Tunnelling with Windows 2000 PC (Configurando túneis iniciados por clientes L2TP com Windows 2000)

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar o cliente do Windows 2000 para o L2TP](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

## Introdução

Na maioria de encenações do Virtual Private Dial-up Network (VPDN), o cliente disca o servidor do acesso de rede (NAS). O NAS inicia então o protocolo de túnel da camada 2 VPDN (L2TP) ou o túnel de protocolo da transmissão da camada 2 (L2F) ao home gateway (HGW). Isto cria uma conexão de VPDN entre o NAS, que é o valor-limite do L2TP Access Concentrator (LAC), e o HGW, que é o valor-limite do L2TP Network Server (LNS). Isto significa que somente o link entre o NAS e o HGW usa o L2TP, e que o túnel não inclui o link do PC cliente ao NAS. Contudo, os clientes PC que executam o sistema operacional do Windows 2000 podem agora transformar-se o LAC e iniciar um túnel L2TP do PC, com o NAS e terminado no HGW/LNS. Esta configuração de exemplo mostra como você pode configurar tal túnel.

## Pré-requisitos

### Requisitos

Antes de tentar esta configuração, verifique se estes requisitos são atendidos:

- Familiaridade com a [compreensão do VPDN](#)

- Familiaridade com o [sumário do discado do acesso VPDN usando o L2TP](#)

**Nota:** A configuração de NAS não é incluída neste documento.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- LNS: Cisco 7200 Series Router que executa o Software Release 12.2(1) de Cisco IOS®
- Cliente: Windows 2000 PC com um modem

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Produtos Relacionados

A configuração para o LNS incluído neste documento não é plataforma específica e pode ser aplicada a todo o roteador capaz de VPDN.

O procedimento para configurar o PC cliente do Windows 2000 é aplicável somente ao Windows 2000 e não a todo o outro sistema operacional.

## Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

## Informações de Apoio

Como mencionado na [introdução](#), com Windows 2000 você pode iniciar um túnel L2TP do PC cliente e ter o túnel terminado em qualquer lugar na rede de provedor de serviço do Internet (ISP). Usando a terminologia VPDN, esta instalação é referida como “cliente-iniciou” o túnel. Desde que os túneis iniciados pelo cliente são túneis iniciados pelo software do cliente no PC, o PC toma no papel do LAC. Desde que o cliente será autenticado usando o Point-to-Point Protocol (PPP), o protocolo de autenticação de cumprimento do desafio (RACHADURA), ou o protocolo password authentication (PAP) de qualquer maneira, o túnel próprio não precisa de ser autenticado.

### **Vantagens e desvantagem de usar túneis iniciados pelo cliente**

Os túneis iniciados pelo cliente têm ambas as vantagens e desvantagem, alguns de que são esboçados aqui:

#### **Vantagens:**

- Fixa a conexão inteira do cliente através da rede compartilhada ISP e à rede de empreendimento.
- Não exige a configuração adicional na rede ISP. Sem um túnel iniciado pelo cliente, o ISP NAS ou seu server Radius/TACACS+ precisam de ser configurados para iniciar o túnel ao HGW. Consequentemente, a empresa deve negociar com muitos ISP para permitir que os

usuários escavam um túnel através de sua rede. Com um túnel iniciado pelo cliente, o utilizador final pode conectar a todo o ISP e então manualmente iniciar o túnel à rede de empreendimento.

### Desvantagens:

- Não é tão escalável como um túnel ISP-iniciado. Desde que os túneis iniciados pelo cliente criam túneis individuais para cada cliente, o HGW deve individualmente terminar um grande número túneis.
- O cliente deve controlar o software do cliente usado para iniciar o túnel. Esta é frequentemente uma fonte de problemas apoio-relacionados para a empresa.
- O cliente deve ter uma conta com o ISP. Desde que os túneis iniciados pelo cliente podem somente ser criados depois que uma conexão ao ISP é estabelecida, o cliente deve ter uma conta a conectar à rede ISP.

### Como trabalha

Thjs é como o exemplo neste documento trabalha:

1. O PC cliente disca no NAS, autentica usando a conta ISP do cliente, e obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT do ISP.
2. O cliente inicia e constrói o túnel L2TP ao L2TP Network Server HGW (LNS). O cliente renegociará o protocolo de controle de IP (IPCP) e obterá um endereço IP de Um ou Mais Servidores Cisco ICM NT novo do LNS.

### [Configurar o cliente do Windows 2000 para o L2TP](#)

Crie duas conexões da rede de comunicação dial-up (DUN):

- Uma conexão DUN ao discado ao ISP. Refira seu ISP para obter mais informações sobre deste assunto.
- Uma outra conexão DUN para o túnel L2TP.

Para criar e configurar a conexão DUN para o L2TP, execute estas etapas no PC cliente de Windows 200:

1. Desde o início o menu, escolhe o **Configurações > Painel de Controle > Conexões de Rede e de Dial-up > o Make New Connection**. Use o assistente para criar uma conexão chamada L2TP. Certifique-se selecionar **conectam a uma rede privada através do Internet no tipo de conexão de rede** indicador. Você deve igualmente especificar o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o nome do LNS/HGW.
2. A nova conexão (L2TP Nomeado) aparece no indicador da **rede e das conexões dial-up** sob o Control Panel. De aqui, clicar com o botão direito para editar as **propriedades**.
3. Clique a ABA de rede de comunicação e certifique-se de que o **Type of Server I Am Calling** está ajustado ao **L2TP**.
4. Se você planeia atribuir um endereço interno dinâmico (da rede de empreendimento) a este cliente do HGW, com um conjunto local ou o DHCP, selecione o protocolo **TCP/IP**. Certifique-se de que o cliente está configurado para obter automaticamente um endereço IP de Um ou Mais Servidores Cisco ICM NT. Você pode igualmente emitir a informação do Domain Naming System (DNS) automaticamente. O botão **Advanced** permite que você defina informações estáticas do Serviço de Cadastramento na Internet do Windows (WINS,

Windows Internet Naming Service) e do DNS. A guia **Options** permite que você desative o IPsec ou atribua uma política diferente à conexão. Na guia **Security**, você pode definir os parâmetros de autenticação de usuário. Por exemplo, PAP, RACHADURA, ou MS-CHAP, ou fazer logon do domínio do Windows. Consulte o administrador de sistemas de rede para obter informações sobre dos parâmetros que devem ser configurados no cliente.

5. Uma vez que a conexão é configurada, você pode fazer-la duplo clique para estalar acima a tela de login, e conecta então.

## Remarções adicionais

Se seu túnel L2TP usa a Segurança IP (IPsec) e/ou a criptografia Point-to-Point microsoft (MPPE), a seguir você deve definir este comando sob a configuração de molde virtual no LNS/HGW.

```
ppp encrypt mppe 40
```

Mantenha na mente que isto exige o grupo cifrado dos recursos do Cisco IOS Software (pelo menos o conjunto de recursos do IPsec ou o IPsec com 3DES).

À revelia, o IPsec é permitido no Windows 2000. Se você quer o desabilitar, você deve alterar o registro de Windows usando o editor de registro:

## **IPsec do desabilitação em Win2k PC**

**aviso:** Tome precauções adequadas (tais como a suportação do registro) antes de alterar o registro. Você deve igualmente referir a site do microsoft para que o procedimento correto altere o registro.

Para adicionar o valor de registro IPsec proibido a seu computador de Windows 2000-based, use Regedt32.exe para encontrar esta chave no registro:

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

Adicione este valor do Registro à chave:

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

**Nota:** Você deve recarregar seu computador de Windows 2000-based para que as mudanças tomem o efeito. Refira por favor estes artigos Microsoft para uns detalhes mais adicionais.

- Q258261 - Política de IPsec de desabilitação usada com L2TP
- Q240262- Como configurar uma conexão do L2TP/IPsec usando uma chave pré-compartilhada

Para uma instalação mais complexa usando o Windows 2000, refira [configurar o Cisco IOS e os clientes do Windows 2000 para o L2TP usando o Microsoft IAS](#).

## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Nota:** Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes [registrados](#)).

## [Diagrama de Rede](#)

O diagrama da rede abaixo mostra as várias negociações que ocorrem entre o PC cliente, o ISP NAS, e a empresa HGW. O exemplo debugar na seção da [pesquisa de defeitos](#) descreve estas transações também.

## [Configurações](#)

Este documento utiliza esta configuração:

- fifi (VPDN LNS/HGW)

**Nota:** Somente a seção relevante da configuração de LNS é incluída.

```
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
```

## [Verificar](#)

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool](#) ([somente clientes registrados](#)) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **vpdn da mostra** — Informação dos indicadores sobre o túnel e identificadores de mensagem ativos do L2x em um VPDN.

- **show vpdn session window** — Indica a informação no indicador para a sessão de VPDN.
- **usuário da mostra** — Fornece uma lista detalhada de todos os usuários conectados ao roteador.
- **show caller user username detail** — Para mostrar parâmetros para o usuário particular, tal como o protocolo de controle de link (LCP), estados NCP e IPCP, assim como o endereço IP de Um ou Mais Servidores Cisco ICM NT atribuído, parâmetros de pacote PPP e PPP, e assim por diante.

```
show vpdn ----- L2TP Tunnel and Session Information Total tunnels 1 sessions 1 !--- Note
that there is one tunnel and one session. LocID RemID Remote Name State Remote Address Port
Sessions 25924 1 JVEYNE-W2K1.c est 199.0.0.8 1701 1 !--- This is the tunnel information. !---
The Remote Name shows the client PC's computer name, as well as the !--- IP address that was
originally given to the client by the NAS. (This !--- address has since been renegotiated by the
LNS.) LocID RemID TunID Intf Username State Last Chg Fastswitch 2 1 25924 Vi1 l2tp-w2k est
00:00:13 enabled !--- This is the session information. !--- The username the client used to
authenticate is l2tp-w2k. %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 %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 !--- User l2tp-w2k is connected on
Virtual-Access Interface 1. !--- Also note that the connection is identified as an L2TP tunnel.
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 !--- The LCP state is Open. 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
```

## Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

### Comandos para Troubleshooting

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

**Nota:** [Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.](#)

- **debugar a negociação ppp** — Indica a informação no tráfego e nas trocas PPP ao negociar os componentes de PPP que incluem o LCP, a autenticação, e o NCP. Uma negociação de PPP bem-sucedida primeiramente abre o estado LCP, a seguir autentica, e negocia finalmente NCP (geralmente IPCP).
- **debug vpdn event** — Exibe mensagens sobre eventos que são parte do estabelecimento ou fechamento do túnel normal.
- **debug vpdn error** — Exibe erros que impedem que um túnel seja estabelecido ou erros que fazem com que o túnel estabelecido seja fechado.
- **debug vpdn l2x-event** — Indica mensagens sobre os eventos que são parte do

estabelecimento normal de túnel ou parada programada para o L2x.

- debug vpdn l2x-error—Exibe os erros do protocolo L2x que impedem seu estabelecimento ou sua operação normal.

**Nota:** Algumas destas linhas de **resultado do debug** são interrompidas em múltiplas linhas para fins de impressão.

Permita os **comandos debug** especificados acima no LNS e inicie um atendimento do PC cliente do Windows 2000. Debuga aqui a mostra a requisição de túnel do cliente, do estabelecimento do túnel, da autenticação do cliente, e da negociação nova do endereço IP de Um ou Mais Servidores Cisco ICM NT:

```
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  
renegotiated 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 CONFREQ [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: Vil LCP: AuthProto CHAP (0x0305C22305) *Jun 6 04:02:07.858: Vil LCP: MagicNumber
0xFA95EEC3 (0x0506FA95EEC3) *Jun 6 04:02:07.858: Vil LCP: State is Open !--- LCP negotiation is
complete. *Jun 6 04:02:07.858: Vil PPP: Phase is AUTHENTICATING, by this end [0 sess, 0 load]
*Jun 6 04:02:07.858: Vil CHAP: O CHALLENGE id 5 len 25 from "fifi" *Jun 6 04:02:07.870: Vil LCP:
I IDENTIFY [Open] id 3 len 18 magic 0x21A20F49 MSRASV5.00 *Jun 6 04:02:07.874: Vil LCP: I
IDENTIFY [Open] id 4 len 27 magic 0x21A20F49 MSRAS-1-JVEYNE-W2K1 *Jun 6 04:02:08.018: Vil CHAP:
I RESPONSE id 5 len 29 from "l2tp-w2k" *Jun 6 04:02:08.018: Vil 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: Vil PPP: Phase is UP [0 sess, 0 load] *Jun 6 04:02:08.018: Vil
IPCP: O CONFREQ [Closed] id 1 len 10 *Jun 6 04:02:08.018: Vil IPCP: Address 1.1.1.1
(0x030601010101) *Jun 6 04:02:08.158: Vil CCP: I CONFREQ [Not negotiated] id 5 len 10 *Jun 6
04:02:08.158: Vil CCP: MS-PPC supported bits 0x01000001 (0x120601000001) *Jun 6 04:02:08.158:
Vil LCP: O PROTREQ [Open] id 3 len 16 protocol CCP (0x80FD0105000A120601000001) *Jun 6
04:02:08.170: Vil IPCP: I CONFREQ [REQsent] id 6 len 34 *Jun 6 04:02:08.170: Vil IPCP: Address
0.0.0.0 (0x030600000000) *Jun 6 04:02:08.170: Vil IPCP: PrimaryDNS 0.0.0.0 (0x810600000000) *Jun
6 04:02:08.170: Vil IPCP: PrimaryWINS 0.0.0.0 (0x820600000000) *Jun 6 04:02:08.170: Vil IPCP:
SecondaryDNS 0.0.0.0 (0x830600000000) *Jun 6 04:02:08.170: Vil IPCP: SecondaryWINS 0.0.0.0
(0x840600000000) *Jun 6 04:02:08.170: Vil 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: Vil IPCP: O CONFREQ [REQsent] id 6 Len 28 *Jun 6 04:02:08.170: Vil IPCP:
PrimaryDNS 0.0.0.0 (0x810600000000) *Jun 6 04:02:08.170: Vil IPCP: PrimaryWINS 0.0.0.0
(0x820600000000) *Jun 6 04:02:08.170: Vil IPCP: SecondaryDNS 0.0.0.0 (0x830600000000) *Jun 6
04:02:08.170: Vil IPCP: SecondaryWINS 0.0.0.0 (0x840600000000) *Jun 6 04:02:08.174: Vil IPCP: I
CONFACK [REQsent] id 1 Len 10 *Jun 6 04:02:08.174: Vil IPCP: Address 1.1.1.1 (0x030601010101)
*Jun 6 04:02:08.326: Vil IPCP: I CONFREQ [ACKrcvd] id 7 Len 10 *Jun 6 04:02:08.326: Vil IPCP:
Address 0.0.0.0 (0x030600000000) *Jun 6 04:02:08.326: Vil IPCP: O CONFNAK [ACKrcvd] id 7 Len 10
*Jun 6 04:02:08.330: Vil IPCP: Address 1.100.0.2 (0x030601640002) *Jun 6 04:02:08.486: Vil IPCP:
I CONFREQ [ACKrcvd] id 8 Len 10 *Jun 6 04:02:08.486: Vil IPCP: Address 1.100.0.2
(0x030601640002) *Jun 6 04:02:08.486: Vil IPCP: O CONFACK [ACKrcvd] id 8 Len 10 *Jun 6
04:02:08.490: Vil IPCP: Address 1.100.0.2 (0x030601640002) *Jun 6 04:02:08.490: Vil IPCP: State
is Open *Jun 6 04:02:08.490: Vil 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.

```

Este resultado do debug no LNS mostra o cliente do Windows 2000 que desliga o atendimento. Note as várias mensagens onde o LNS reconhece a desconexão e executa uma parada programada limpa do túnel:

```

*Jun 6 04:03:25.174: Vil 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: Vil LCP: O TERMACK [Open] id 9 Len 4 *Jun 6 04:03:25.354: Vil
Tnl/Cl 25924/2 L2TP: I CDN from JVEYNE-W2K1.cisco.com tnl 1, CL 1 *Jun 6 04:03:25.354: Vil
Tnl/CL 25924/2 L2TP: Destroying session *Jun 6 04:03:25.358: Vil Tnl/CL 25924/2 L2TP: Session
state change from established to idle *Jun 6 04:03:25.358: Vil Tnl/CL 25924/2 L2TP: Releasing
idb for LAC/LNS tunnel 25924/1 session 2 state idle *Jun 6 04:03:25.358: Vil 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: Vil LCP: State
is Closed *Jun 6 04:03:25.362: Vil IPCP: State is Closed *Jun 6 04:03:25.362: Vil PPP: Phase is
DOWN [0 sess, 0 load] *Jun 6 04:03:25.362: Vil VPDN: Cleanup *Jun 6 04:03:25.362: Vil VPDN:
Reset *Jun 6 04:03:25.362: Vil VPDN: Unbind interface *Jun 6 04:03:25.362: Vil VPDN: Unbind
interface *Jun 6 04:03:25.362: Vil VPDN: Reset *Jun 6 04:03:25.362: Vil VPDN: Unbind interface
*Jun 6 04:03:25.362: Vil 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

```

## [Informações Relacionadas](#)

- [Configurando clientes Cisco IOS e Windows 2000 para L2TP usando Microsoft IAS](#)



- [Entendendo o VPDN](#)
- [Configuração VPDN sem AAA](#)
- [Configurando a autenticação do protocolo do túnel da camada 2 com RADIUS](#)
- [Configurando um servidor de acesso com PRIs para chamadas Asyn e ISDN recebidas](#)
- [Página de suporte da tecnologia de discagem](#)
- [Suporte Técnico - Cisco Systems](#)