

# L2TP-client geïnitieerde tunneling configureren met Windows 2000 PC

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[De Windows 2000-client configureren voor L2TP](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Opdrachten voor troubleshooting](#)

[Gerelateerde informatie](#)

## Inleiding

In de meeste VPDN-scenario's (Virtual Private dial-up Network) draait de client de netwerktoegangsserver (NAS). NAS start vervolgens de VPDN Layer 2 Tunnel Protocol (L2TP) of Layer 2 Forwarding (L2F) aan de Home Gateway (HGW). Dit creëert een VPDN-verbinding tussen de NAS, dat het L2TP-toegangsconcentrator (LAC)-eindpunt is, en de HGW, dat het L2TP-netwerkservereindpunt (LNS) is. Dit betekent dat alleen de verbinding tussen de NAS en de HGW L2TP gebruikt, en die tunnel omvat niet de verbinding van de client-PC naar de NAS. Desondanks zijn pc-klanten die het Windows 2000-besturingssysteem runnen nu in staat om de LAC te worden en een L2TP-tunnel te openen vanaf de PC, via het NAS en afgesloten op de HGW/LNS. Deze voorbeeldconfiguratie toont hoe je zo'n tunnel kunt configureren.

## Voorwaarden

### Vereisten

Zorg er voordat u deze configuratie probeert voor dat u aan deze vereisten voldoet:

- Bekendheid met [begrip van VPDN](#)
- Bekendheid met [Synthetisch van inbel-VPDN met gebruik van L2TP](#)

**Opmerking:** de NAS-configuratie is niet in dit document opgenomen.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- LNS: Cisco 7200 Series router met Cisco IOS®-software release 12.2(1)
- Cliënt: Windows 2000 PC met een modem

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Verwante producten

De configuratie voor de LNS die in dit document is opgenomen, is geen platform-specifiek en kan worden toegepast op elke VPDN-geschikte router.

De procedure om de Windows 2000 client-pc te configureren is alleen van toepassing op Windows 2000 en niet op een ander besturingssysteem.

## Conventies

Raadpleeg voor meer informatie over documentconventies de [technische Tips](#) van [Cisco](#).

## Achtergrondinformatie

Zoals in de [Inleiding](#) vermeld, kunt u met Windows 2000 een L2TP-tunnel van de client-PC openen en de tunnel overal in het netwerk van de Internet Service Provider (ISP) laten begaan. Gebruikmakend van de VPDN-terminologie wordt deze instelling aangeduid als een "client-geïnitieerde" tunnel. Aangezien tunnels die door client geïnitieerd worden tunnels zijn die door clientsoftware op de PC geïnitieerd worden, neemt de PC de rol van de LAC op zich. Aangezien de client beveiligd is met Point-to-Point Protocol (PPP), Challenge Handshake Authentication Protocol (CHAP) of Password Authentication Protocol (PAP), hoeft de tunnel zelf niet te worden geauthentiseerd.

### **Voordelen en nadelen van het gebruik van door cliënten geïnitieerde tunnels**

Door cliënten geïnitieerde tunnels hebben zowel voor- als nadelen, waarvan enkele hier worden beschreven:

#### **Voordelen:**

- Het waarborgt de gehele verbinding van de client via het ISP-gedeelde netwerk en het ondernemingsnetwerk.
- Er zijn *geen* extra configuratie nodig op het ISP-netwerk. Zonder een client-geïnitieerde tunnel moet NAS of de RADIUS/TACACS+ server van de ISP worden geconfigureerd om de tunnel naar de HGW te openen. Daarom moet de onderneming met veel ISP's onderhandelen om gebruikers door hun netwerk te laten tunnellen. Met een client-geïnitieerde tunnel kan de eindgebruiker verbinding maken met een willekeurige ISP en de tunnel vervolgens handmatig naar het ondernemingsnetwerk openen.

## Nadelen:

- Het is niet zo schaalbaar als een ISP-geïnitieerde tunnel. Aangezien tunnels die door een cliënt geïnitieerd worden afzonderlijke tunnels voor elke cliënt creëren, moet de HGW een groot aantal tunnels afzonderlijk beëindigen.
- De cliënt moet de clientsoftware beheren die gebruikt wordt om de tunnel te openen. Dit is vaak een bron van ondersteunende problemen voor de onderneming.
- De client moet een account bij de ISP hebben. Aangezien de client-geïnitieerde tunnels alleen kunnen worden gemaakt nadat een verbinding met de ISP is gerealiseerd, moet de client een account hebben om verbinding met het ISP-netwerk te maken.

## Hoe werkt het?

Zo werkt het voorbeeld in dit document:

1. De client-PC bellen in de NAS, bevestig het gebruik van de ISP-account van de client en krijgt een IP-adres van de ISP.
2. De client start en bouwt de L2TP-tunnel naar de L2TP-netwerkserver HGW (LNS). De client onderhandelt over IP Control Protocol (IPCP) en krijgt een nieuw IP-adres van de LNS.

## [De Windows 2000-client configureren voor L2TP](#)

Maak twee inbelnetwerken (DUN)-verbindingen:

- Eén VN-verbinding met de ISP. Raadpleeg uw ISP voor meer informatie over dit onderwerp.
- Een andere DUN-verbinding voor de L2TP-tunnel.

Om de DUN-verbinding voor L2TP te maken en te configureren voert u deze stappen uit op de Windows 2000 client-pc:

1. Kies in het menu Start **Instellingen > Configuratiescherm > Netwerk- en inbelverbindingen > Nieuwe verbinding maken**. Gebruik de Wizard om een verbinding te maken die L2TP wordt genoemd. Zorg ervoor dat u **verbinding maakt met een privénetwerk via het internet** in het venster **Network Connection Type**. U moet ook het IP-adres of de naam van de LNS/HGW specificeren.
2. De nieuwe verbinding (L2TP genaamd) verschijnt in het venster **Network and Dial-up Connections** onder Control Panel. Klik vanuit deze optie met de rechtermuisknop om de **eigenschappen** te bewerken.
3. Klik op het tabblad **Netwerk** en zorg ervoor dat het **type server dat ik bel** is ingesteld op **L2TP**.
4. Als u een dynamisch intern (ondernemingsnetwerk) adres aan deze client vanuit de HGW wilt toewijzen, via een lokale pool of DHCP, selecteert u **TCP/IP-protocol**. Zorg dat de client is geconfigureerd om automatisch een IP-adres te verkrijgen. U kunt DNS-informatie (Domain Naming System) ook automatisch uitgeven. Met de knop **Advanced** kunt u de statische Windows Internet Naming Service (WINS) en DNS-informatie definiëren. In het tabblad **Opties** kunt u IPsec uitschakelen of een ander beleid aan de verbinding toewijzen. Onder het tabblad **Beveiliging** kunt u de parameters voor de gebruikersverificatie definiëren. Bijvoorbeeld PAP, CHAP, of MS-CHAP, of de opening van een domeinaanmelding van Windows. Raadpleeg de systeembeheerder voor informatie over de parameters die op de client moeten worden ingesteld.

5. Nadat de verbinding is geconfigureerd kunt u dubbelklikken om op het inlogscherf te klikken en vervolgens verbinding te maken.

### Aanvullende opmerkingen

Als uw L2TP-tunnel IP-beveiliging (IPSec) en/of Microsoft Point-to-Point Encryption (MPPE) gebruikt, moet u deze opdracht definiëren onder de virtueel-sjabloon configuratie op de LNS/HGW.

```
ppp encrypt mppe 40
```

Houd in gedachten dat dit de gecodeerde Cisco IOS-software release vereist (ten minste de IPSec optie of IPSec met 3DES).

Standaard is IPSec ingeschakeld op Windows 2000. Als u deze wilt uitschakelen, moet u de Windows-registratie wijzigen met behulp van de Registratieeditor:

### Schakel IPSec uit op een Win2K-pc

**Waarschuwing:** neem adequate voorzorgsmaatregelen (zoals een back-up van het register) voordat u het register wijzigt. U dient ook de Microsoft website te raadplegen voor de juiste procedure om het register te wijzigen.

Om de registratiewaarde van ProhibitIpSec aan uw op Windows 2000 gebaseerde computer toe te voegen, gebruikt u Regedt32.exe om deze sleutel in het register te vinden:

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

Voeg deze registratiewaarde toe aan de toets:

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

**Opmerking:** U moet de op Windows 2000 gebaseerde computer opnieuw opstarten om de wijzigingen van kracht te laten worden. Raadpleeg deze Microsoft-artikelen voor meer informatie.

- Q2582-61 - IPSec-beleid uitschakelen met L2TP
- Q240-262-Hoe u een L2TP/IPSec-verbinding kunt configureren met behulp van een vooraf gedeelde sleutel

Voor een complexere installatie met Windows 2000 raadpleegt u [Cisco IOS en Windows 2000 Clients configureren voor L2TP met behulp van Microsoft IAS](#).

## Configureren

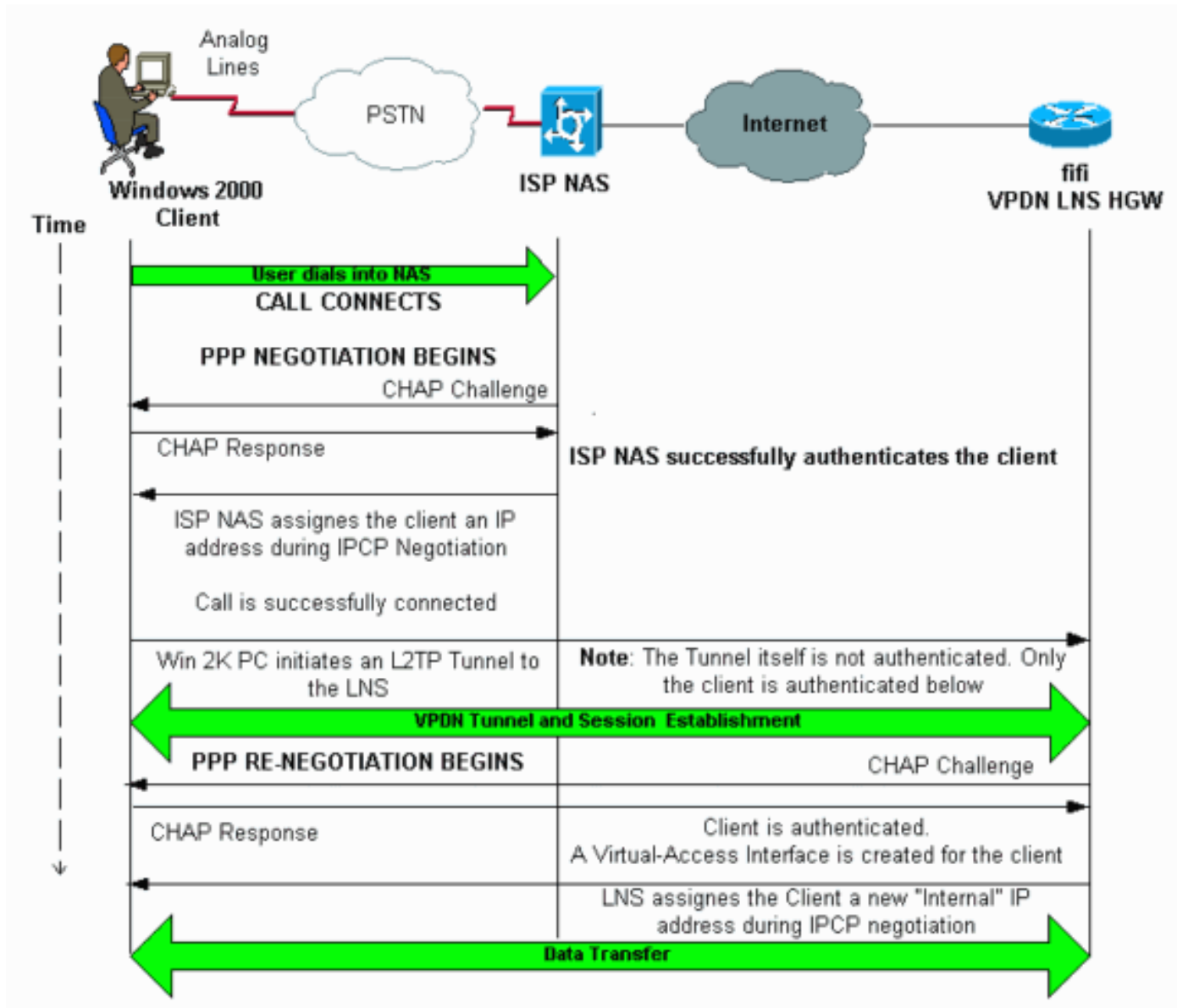
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

**N.B.:** Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het

[Opdrachtplanningprogramma](#) (alleen [geregistreerd](#) klanten).

## Netwerkdigram

In het onderstaande netwerkdigram worden de verschillende onderhandelingen weergegeven die plaatsvinden tussen de client-PC, ISP NAS en Enterprise HGW. Het debug voorbeeld in de sectie [Problemen oplossen](#) toont deze transacties ook.



## Configuraties

Dit document gebruikt deze configuratie:

- FIFI (VPDN LNS/HGW)

**Opmerking:** Alleen het relevante gedeelte van de LNS-configuratie is inbegrepen.

### 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

```

## Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show** worden ondersteund door de tool [Output Interpreter \(alleen voor geregistreerde klanten\)](#). Hiermee kunt u een analyse van de output van opdrachten met **show** genereren.

- **tonen vpdn**-Beeldinformatie over actieve L2x-tunnels en bericht herkenners in een VPDN.
- **Laat vpdn sessievenster**—informatie zien in het venster voor de VPDN-sessie.
- **Laat gebruiker-zien** biedt een uitgebreide lijst van alle gebruikers die op de router zijn aangesloten.
- **Geef de gebruikersnaam voor de beller detail**-Om parameters voor de specifieke gebruiker weer te geven, zoals de LCP-staten (Link Control Protocol), NCP- en IPCP-staten, evenals de IP-adressen, PPP- en PPP-bundelparameters enzovoort.

```
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	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
<b>Vi1</b>	<b>l2tp-w2k</b>	Virtual PPP ( <b>L2TP</b> )	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
```

## Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

### Opdrachten voor troubleshooting

Bepaalde opdrachten met **show** worden ondersteund door de tool [Output Interpreter \(alleen voor geregistreerde klanten\)](#). Hiermee kunt u een analyse van de output van opdrachten met **show** genereren.

**Opmerking:** Voordat u **debug**-opdrachten afgeeft, raadpleegt u [Belangrijke informatie over Debug Commands](#).

- **debug van PPP onderhandeling**-informatie over PPP verkeer en uitwisselingen tijdens het onderhandelen van de componenten PPP waaronder LCP, Verificatie, en NCP. Een succesvolle PPP-onderhandeling opent eerst de LCP-staat, authenticatie, en onderhandelt uiteindelijk over NCP (gewoonlijk IPCP).

- **debug van gebeurtenis-displays vpdn** over gebeurtenissen die deel uitmaken van de normale tunnelvestiging of sluiting.
- **debug VPDN fout-displays** die verhinderen dat een tunnel wordt aangelegd of fouten die veroorzaken dat een gevestigde tunnel wordt gesloten.
- **debug vpdn l2x-event-displays** over gebeurtenissen die deel uitmaken van de normale tunnelvestiging of shutdown voor L2x.
- **debug vpdn l2x-fout-displays** L2x protocolfouten die L2x-instelling verhinderen of de normale werking ervan verhinderen.

**Opmerking:** Sommige van deze regels **debug**-uitvoer worden voor afdrucken in meerdere regels verdeeld.

Schakel de hierboven gespecificeerde opdrachten in **en** open een oproep uit de Windows 2000 client-pc. De hier besproken punten tonen het tunnelverzoek van de cliënt, de totstandbrenging van de tunnel, de authenticatie van de cliënt, en de heronderhandeling van het IP-adres:

```
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:
```



```

Vil LCP: MRRU 1614 (0x1104064E) *Jun 6 04:02:07.710: Vil LCP: I CONFNAK [REQsent] id 1 len 8
*Jun 6 04:02:07.710: Vil LCP: MRU 1514 (0x010405EA) *Jun 6 04:02:07.710: Vil LCP: O CONFREQ
[REQsent] id 2 len 15 *Jun 6 04:02:07.710: Vil LCP: AuthProto CHAP (0x0305C22305) *Jun 6
04:02:07.710: Vil LCP: MagicNumber 0xFA95EEC3 (0x0506FA95EEC3) *Jun 6 04:02:07.718: Vil LCP: I
CONFREQ [REQsent] id 2 len 37 *Jun 6 04:02:07.718: Vil LCP: MagicNumber 0x21A20F49
(0x050621A20F49) *Jun 6 04:02:07.718: Vil LCP: PFC (0x0702) *Jun 6 04:02:07.718: Vil LCP: ACFC
(0x0802) *Jun 6 04:02:07.718: Vil LCP: EndpointDisc 1 Local *Jun 6 04:02:07.718: Vil LCP:
(0x131701708695CDF2C64730B5B6756CE8) *Jun 6 04:02:07.718: Vil LCP: (0xB1AB1600000001) *Jun 6
04:02:07.718: Vil LCP: O CONFACK [REQsent] id 2 len 37 *Jun 6 04:02:07.718: Vil LCP: MagicNumber
0x21A20F49 (0x050621A20F49) *Jun 6 04:02:07.718: Vil LCP: PFC (0x0702) *Jun 6 04:02:07.718: Vil
LCP: ACFC (0x0802) *Jun 6 04:02:07.718: Vil LCP: EndpointDisc 1 Local *Jun 6 04:02:07.718: Vil
LCP: (0x131701708695CDF2C64730B5B6756CE8) *Jun 6 04:02:07.718: Vil LCP: (0xB1AB1600000001) *Jun
6 04:02:07.858: Vil 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 PROTREJ [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.

```

Dit debug uitvoer op LNS toont de client van Windows 2000 die de verbinding van het gesprek afsluit. Let op de verschillende berichten waarin de LNS de verbroken verbinding herkent en een schone afsluiten van de tunnel uitvoert:

```

*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:

```

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

## [Gerelateerde informatie](#)

- [Cisco IOS en Windows 2000-clients configureren voor L2TP met Microsoft IAS](#)
- [Inzicht VPDN](#)
- [VPDN-configuratie zonder AAA](#)
- [Layer 2 Tunnel Protocol-verificatie met RADIUS](#)
- [Een toegangsserver met PRI's configureren voor inkomende asynchrone en ISDN-oproepen](#)
- [Ondersteuning van kiestechnologie](#)
- [Technische ondersteuning - Cisco-systemen](#)