Configurazione del tunneling avviato dal client L2TP con Windows 2000 PC

Sommario

Introduzione

Nella maggior parte degli scenari VPDN (Virtual Private Dial-up Network), il client chiama il server di accesso alla rete (NAS). Il server NAS avvia quindi il protocollo VPDN Layer 2 Tunnel Protocol (L2TP) o il tunnel di protocollo Layer 2 Forwarding (L2F) sul gateway principale (HGW). In questo modo viene creata una connessione VPDN tra il server NAS, che è l'endpoint L2TP access concentrator (LAC), e il server HGW, che è l'endpoint L2TP network server (LNS). Ciò significa che solo il collegamento tra il NAS e l'HGW utilizza L2TP e che tale tunnel non include il collegamento dal PC client al NAS. Tuttavia, i client PC che eseguono il sistema operativo Windows 2000 possono ora diventare LAC e avviare un tunnel L2TP dal PC, attraverso il NAS e terminato su HGW/LNS. In questa configurazione di esempio viene mostrato come configurare un tunnel di questo tipo.

Prerequisiti

Requisiti

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti requisiti:

- Familiarità con la VPDN
- Familiarità con la sinossi di Access VPDN Dial-In tramite L2TP

Nota: la configurazione NAS non è inclusa in questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- LNS: Cisco serie 7200 router con software Cisco IOS® versione 12.2(1)
- Cliente: Windows 2000 PC con modem

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

La configurazione dell'LNS inclusa in questo documento non è specifica della piattaforma e può essere applicata a qualsiasi router compatibile con VPDN.

La procedura di configurazione del PC client Windows 2000 è applicabile solo a Windows 2000 e non ad altri sistemi operativi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Come indicato nell'introduzione, con Windows 2000 è possibile avviare un tunnel L2TP dal PC client e terminare il tunnel in qualsiasi punto della rete del provider di servizi Internet (ISP). Utilizzando la terminologia VPDN, questa configurazione viene definita "tunnel avviato dal client". Poiché i tunnel avviati dal client sono tunnel avviati dal software client sul PC, quest'ultimo svolge il ruolo di LAC. Poiché il client verrà autenticato comunque tramite il protocollo PPP (Point-to-Point Protocol), il protocollo CHAP (Challenge Handshake Authentication Protocol) o il protocollo PAP (Password Authentication Protocol), non è necessario autenticare il tunnel.

Vantaggi e svantaggi dell'utilizzo di tunnel avviati dal client

I tunnel avviati dal client presentano sia vantaggi che svantaggi, alcuni dei quali sono descritti di seguito:

Vantaggi:

- Protegge l'intera connessione dal client attraverso la rete condivisa dell'ISP e la rete aziendale.
- *Non* è necessaria alcuna configurazione aggiuntiva sulla rete ISP. Senza un tunnel avviato dal client, è necessario configurare l'ISP NAS o il relativo server Radius/TACACS+ per avviare il tunnel verso l'HGW. Pertanto, l'azienda deve negoziare con molti ISP per consentire agli

utenti di eseguire il tunnel attraverso la rete. Con un tunnel avviato dal client, l'utente finale può connettersi a qualsiasi ISP e quindi avviare manualmente il tunnel alla rete aziendale.

Svantaggi:

- Non è scalabile come un tunnel avviato dall'ISP. Poiché i tunnel avviati dal client creano singoli tunnel per ciascun client, l'HGW deve terminare individualmente un elevato numero di tunnel.
- Il client deve gestire il software client utilizzato per avviare il tunnel. Ciò è spesso fonte di problemi legati al supporto per l'azienda.
- Il client deve disporre di un account con l'ISP. Poiché i tunnel avviati dal client possono essere creati solo dopo la connessione all'ISP, il client deve disporre di un account per connettersi alla rete dell'ISP.

Come funziona

Ecco come funziona l'esempio di questo documento:

1. Il PC client effettua la connessione al NAS, esegue l'autenticazione utilizzando l'account ISP del client e ottiene un indirizzo IP dall'ISP.
2. Il client avvia e crea il tunnel L2TP per il server di rete L2TP HGW (LNS). Il client rinegozierà il protocollo IPCP (IP Control Protocol) e otterrà un nuovo indirizzo IP dal DNS.

Configurazione del client Windows 2000 per L2TP

Creare due connessioni remote (DUN):

- Una connessione DUN per la connessione remota all'ISP. Per ulteriori informazioni su questo argomento, rivolgersi al proprio ISP.
- Un'altra connessione DUN per il tunnel L2TP.

Per creare e configurare la connessione DUN per L2TP, eseguire la procedura seguente sul PC client Windows 2000:

1. Dal menu Start, scegliere **Impostazioni > Pannello di controllo > Rete e connessioni remote > Crea nuova connessione**.Utilizzare la procedura guidata per creare una connessione denominata L2TP. Assicurarsi di selezionare **Connetti a una rete privata tramite Internet** nella finestra **Tipo di connessione di rete**. Specificare inoltre l'indirizzo IP o il nome del server LNS/HGW.
2. La nuova connessione (denominata L2TP) viene visualizzata nella finestra **Rete e connessioni remote** nel Pannello di controllo. Fare clic con il pulsante destro del mouse per modificare le **proprietà**.
3. Fare clic sulla scheda Rete e verificare che il **tipo di server chiamato** sia impostato su **L2TP**.
4. Se si intende allocare un indirizzo dinamico interno (rete aziendale) a questo client dall'HGW, tramite un pool locale o DHCP, selezionare **TCP/IP** protocol. Verificare che il client sia configurato in modo da ottenere automaticamente un indirizzo IP. È inoltre possibile utilizzare automaticamente le informazioni DNS (Domain Naming System).Il pulsante **Avanzate** consente di definire informazioni statiche WINS (Windows Internet Naming Service) e DNS. La scheda **Opzioni** consente di disattivare IPSec o assegnare un criterio diverso alla connessione. Nella scheda Protezione è possibile definire i parametri di autenticazione utente. Ad esempio, PAP, CHAP o MS-CHAP o accesso al dominio Windows. Consultare

l'amministratore dei sistemi di rete per informazioni sui parametri da configurare sul client.
5. Una volta configurata la connessione, è possibile fare doppio clic su di essa per visualizzare la schermata di accesso e quindi connettersi.

Ulteriori osservazioni

Se il tunnel L2TP utilizza IP Security (IPSec) e/o Microsoft Point-to-Point Encryption (MPPE), è necessario definire questo comando nella configurazione del modello virtuale su LNS/HGW.

```
ppp encrypt mppe 40
```

Tenere presente che questa operazione richiede un gruppo di funzionalità del software Cisco IOS crittografato (almeno il gruppo di funzionalità IPSec o IPSec con 3DES).

Per impostazione predefinita, IPSec è attivato in Windows 2000. Se si desidera disattivarlo, è necessario modificare il Registro di sistema di Windows utilizzando l'Editor del Registro di sistema:

Disabilitare IPSec in un PC Win2K

Avviso: adottare le precauzioni appropriate, ad esempio eseguire il backup del Registro di sistema, prima di modificare il Registro di sistema. È inoltre consigliabile visitare il sito Web Microsoft per informazioni sulla procedura corretta per la modifica del Registro di sistema.

Per aggiungere il valore ProhibitIpSec al Registro di sistema del computer Windows 2000, utilizzare Regedt32.exe per individuare la chiave nel Registro di sistema:

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

Aggiungere il valore del Registro di sistema alla chiave:

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

Nota: per rendere effettive le modifiche è necessario riavviare il computer con sistema operativo Windows 2000. Per ulteriori informazioni, fare riferimento a questi articoli Microsoft.

- Q258261 - Disabilitazione dei criteri IPSec utilizzati con L2TP
- Q240262- Come configurare una connessione L2TP/IPSec utilizzando una chiave già condivisa

Per informazioni su una configurazione più complessa con Windows 2000, vedere Configurazione dei client Cisco IOS e Windows 2000 per L2TP con Microsoft IAS.

Configurazione

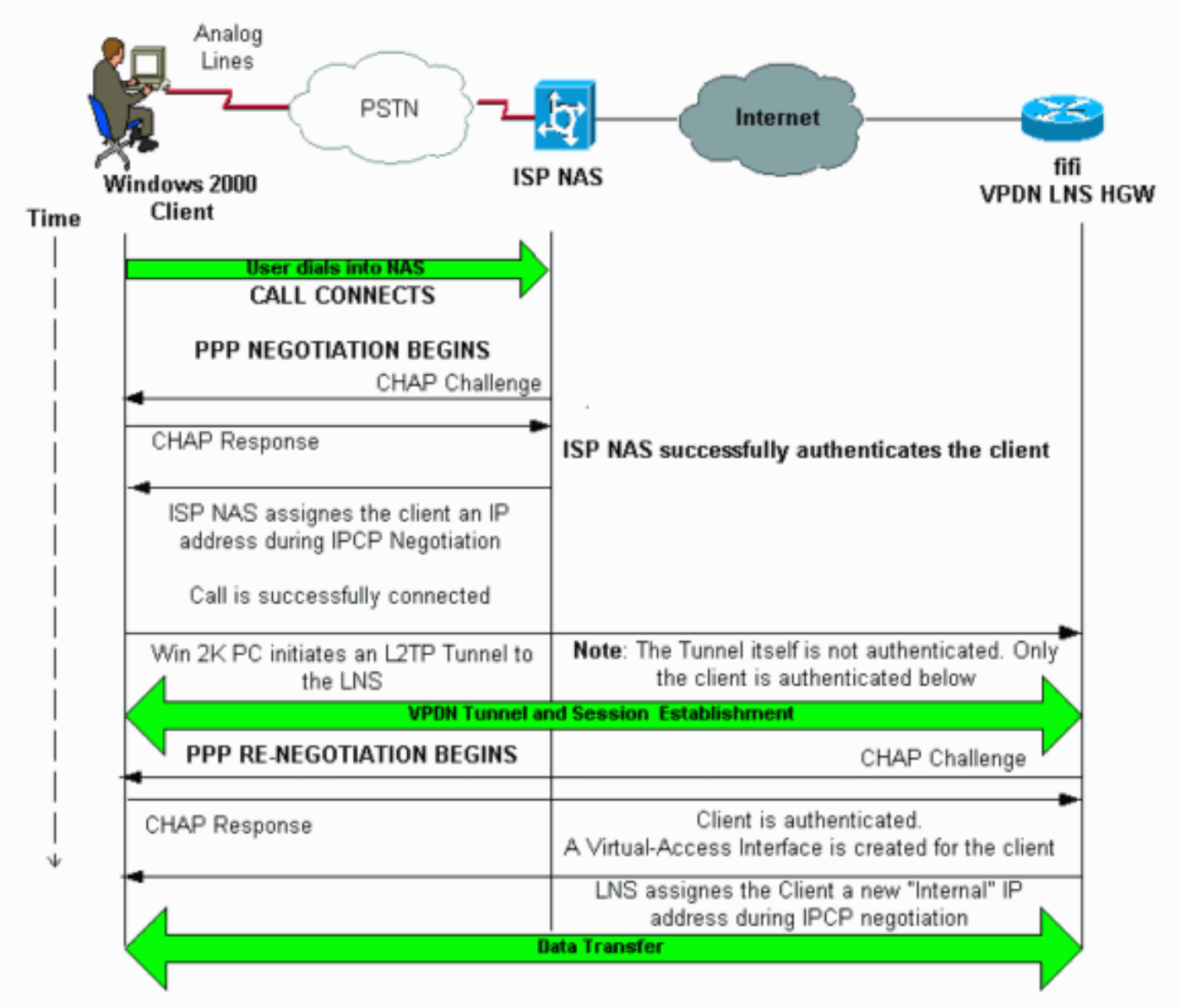
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di

ricerca dei comandi (solo utenti registrati).

Esempio di rete

Il diagramma di rete seguente mostra le varie negoziazioni che si verificano tra il PC client, il NAS ISP e l'HGW aziendale. L'esempio di debug nella sezione Risoluzione dei problemi descrive anche queste transazioni.



Configurazioni

Nel documento viene usata questa configurazione:

- fifi (VPDN LNS/HGW)

Nota: è inclusa solo la sezione pertinente della configurazione LNS.

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
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show.**

- **show vpdn**: visualizza le informazioni sul tunnel L2x attivo e gli identificatori di messaggio in una VPDN.
- **show vpdn session window**: visualizza le informazioni sulla finestra per la sessione VPDN.
- **show user**: fornisce un elenco completo di tutti gli utenti connessi al router.
- **show caller user *username* detail**: consente di visualizzare i parametri di un utente specifico, ad esempio gli stati LCP (Link Control Protocol), NCP e IPCP, nonché l'indirizzo IP assegnato, i parametri del bundle PPP e PPP e così via.

```
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
  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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Alcuni comandi **show** sono supportati dallo strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

- **debug ppp negotiation**: visualizza le informazioni sul traffico e gli scambi PPP durante la negoziazione dei componenti PPP, inclusi LCP, Autenticazione e NCP. Una negoziazione PPP riuscita apre innanzitutto lo stato LCP, quindi autentica e infine negozia NCP (generalmente IPCP).

- **debug vpdn event**: visualizza i messaggi relativi agli eventi che fanno parte della normale creazione del tunnel o del normale arresto.
- **debug vpdn error**: visualizza gli errori che impediscono di stabilire un tunnel o gli errori che causano la chiusura di un tunnel stabilito.
- **debug vpdn l2x-event**: visualizza i messaggi relativi agli eventi che fanno parte della normale definizione del tunnel o dell'arresto per L2x.
- **debug vpdn l2x-error**: visualizza gli errori del protocollo L2x che impediscono la creazione di L2x o il suo normale funzionamento.

Nota: alcune delle righe dell'output del **comando debug** sono suddivise in più righe per la stampa.

Abilitare i comandi di **debug** sopra specificati sull'LNS e avviare una chiamata dal PC client Windows 2000. I debug qui mostrano la richiesta del tunnel dal client, la creazione del tunnel, l'autenticazione del client e la rinegoziazione dell'indirizzo IP:

```
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.
```

Questo output di debug sul server LNS visualizza la disconnessione della chiamata da parte del client Windows 2000. Annotare i vari messaggi in cui l'LNS riconosce la disconnessione ed esegue un arresto corretto del 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
```

Informazioni correlate

- Configurazione dei client Cisco IOS e Windows 2000 per L2TP con Microsoft IAS
- Informazioni sulla VPDN
- Configurazione VPDN senza AAA
- Configurazione dell'autenticazione Layer 2 Tunnel Protocol con RADIUS
- Configurazione di un server di accesso con PRI per le chiamate asincrone e ISDN in arrivo
- Pagine di supporto per la tecnologia di composizione
- Supporto tecnico – Cisco Systems