Configuración de la tunelización iniciada con L2TP Client con Windows 2000 PC

Contenido

Introducción

En la mayoría de los escenarios de red de acceso telefónico privada virtual (VPDN), el cliente marca el servidor de acceso a la red (NAS). A continuación, el NAS inicia el protocolo de túnel de capa 2 (L2TP) de VPDN o el túnel de protocolo de reenvío de capa 2 (L2F) en la puerta de enlace doméstica (HGW). Esto crea una conexión VPDN entre el NAS, que es el terminal del concentrador de acceso L2TP (LAC), y el HGW, que es el terminal del servidor de red L2TP (LNS). Esto significa que solamente el link entre el NAS y el HGW utiliza L2TP, y ese túnel no incluye el link del equipo cliente al NAS. Sin embargo, los clientes PC que ejecutan el sistema operativo Windows 2000 ahora pueden convertirse en el LAC e iniciar un túnel L2TP desde el PC, a través del NAS y terminados en el HGW/LNS. Esta configuración de ejemplo muestra cómo se puede configurar dicho túnel.

Prerequisites

Requirements

Antes de utilizar esta configuración, asegúrese de que cumple con estos requisitos:

- Familiaridad con Comprensión de VPDN
- Familiaridad con Sinopsis de Acceso VPDN Dial-In Usando L2TP

Nota: La configuración NAS no se incluye en este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- LNS: Cisco 7200 Series Router que ejecuta Cisco IOS® Software Release 12.2(1)
- Cliente: PC con Windows 2000 y módem

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.

Productos Relacionados

La configuración para el LNS incluida en este documento no es específica de la plataforma y se puede aplicar a cualquier router con capacidad para VPDN.

El procedimiento para configurar el equipo cliente de Windows 2000 sólo se aplica a Windows 2000 y no a ningún otro sistema operativo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Antecedentes

Como se menciona en la Introducción, con Windows 2000 puede iniciar un túnel L2TP desde el equipo cliente y hacer que el túnel termine en cualquier lugar de la red del proveedor de servicios de Internet (ISP). Con la terminología VPDN, esta configuración se denomina túnel "iniciado por el cliente". Dado que los túneles iniciados por el cliente son túneles iniciados por el software del cliente en la PC, la PC asume la función de LAC. Dado que el cliente se autenticará de todos modos mediante el protocolo punto a punto (PPP), el protocolo de autenticación por desafío mutuo (CHAP) o el protocolo de autenticación de contraseña (PAP), el túnel en sí no necesita autenticación.

Ventajas y desventajas del uso de túneles iniciados por el cliente

Los túneles iniciados por el cliente tienen ventajas y desventajas, algunas de las cuales se describen aquí:

Ventajas:

- Protege toda la conexión del cliente a través de la red compartida ISP y a la red empresarial.
- *No* requiere configuración adicional en la red ISP. Sin un túnel iniciado por el cliente, el ISP NAS o su servidor Radius/TACACS+ debe configurarse para iniciar el túnel al HGW. Por lo tanto, la empresa debe negociar con muchos ISP para permitir que los usuarios tunelicen a través de su red. Con un túnel iniciado por el cliente, el usuario final puede conectarse a

cualquier ISP y luego iniciar manualmente el túnel a la red empresarial.

Desventajas:

- No es tan escalable como un túnel iniciado por ISP. Dado que los túneles iniciados por el cliente crean túneles individuales para cada cliente, el HGW debe terminar individualmente un gran número de túneles.
- El cliente debe administrar el software cliente utilizado para iniciar el túnel. Esto suele ser una fuente de problemas relacionados con el soporte para la empresa.
- El cliente debe tener una cuenta con el ISP. Dado que los túneles iniciados por el cliente sólo se pueden crear después de establecer una conexión con el ISP, el cliente debe tener una cuenta para conectarse a la red ISP.

Cómo funciona

Así funciona el ejemplo de este documento:

1. El equipo cliente marca en el NAS, autentica usando la cuenta ISP del cliente y obtiene una dirección IP del ISP.
2. El cliente inicia y genera el túnel L2TP en el servidor de red L2TP HGW (LNS). El cliente renegociará el protocolo de control IP (IPCP) y obtendrá una nueva dirección IP del LNS.

Configure el Cliente de Windows 2000 para L2TP

Cree dos conexiones de red de acceso telefónico (DUN):

- Una conexión DUN para marcar al ISP. Consulte el ISP para obtener más información sobre este tema.
- Otra conexión DUN para el túnel L2TP.

Para crear y configurar la conexión DUN para L2TP, realice estos pasos en el equipo cliente Windows 200:

1. En el menú Inicio, elija **Settings > Control Panel > Network and Dial-up Connections > Make New Connection**.Utilice el asistente para crear una conexión llamada L2TP. Asegúrese de seleccionar **Connect to a private network through the Internet** in the **Network Connection Type** window. También debe especificar la dirección IP o el nombre del LNS/HGW.
2. La nueva conexión (denominada L2TP) aparece en la ventana **Conexiones de red y acceso telefónico** en Panel de control. Desde aquí, haga clic con el botón derecho para editar las **propiedades**.
3. Haga clic en la ficha Networking (Redes) y asegúrese de que el **tipo de servidor al que llamo** esté configurado en **L2TP**.
4. Si planea asignar una dirección interna dinámica (red empresarial) a este cliente desde el HGW, a través de un conjunto local o DHCP, seleccione el protocolo **TCP/IP**. Asegúrese de que el cliente esté configurado para obtener una dirección IP automáticamente. También puede emitir automáticamente información del sistema de nombres de dominio (DNS).El botón **Avanzado** permite definir información estática de Windows Internet Naming Service (WINS) y DNS. La ficha **Opciones** permite desactivar IPSec o asignar una política diferente a la conexión. En la ficha Seguridad, puede definir los parámetros de autenticación de usuario. Por ejemplo, PAP, CHAP o MS-CHAP, o inicio de sesión de dominio de Windows. Consulte al administrador de sistemas de red para obtener información sobre los parámetros que se

deben configurar en el cliente.

5. Una vez configurada la conexión, puede hacer doble clic en ella para abrir la pantalla de inicio de sesión y, a continuación, conectarse.

Comentarios adicionales

Si el túnel L2TP utiliza seguridad IP (IPSec) o cifrado punto a punto (MPPE) de Microsoft, debe definir este comando en la configuración de plantilla virtual en el LNS/HGW.

```
ppp encrypt mppe 40
```

Tenga en cuenta que esto requiere el conjunto de funciones de Cisco IOS Software cifrado (al menos el conjunto de funciones IPSec o IPSec con 3DES).

De forma predeterminada, IPSec está habilitado en Windows 2000. Si desea desactivarla, debe modificar el Registro de Windows mediante el Editor del Registro:

Inhabilitar IPSec en un PC Win2K

Advertencia: Tome las precauciones adecuadas (como hacer copia de seguridad del registro) antes de modificar el registro. También debe consultar el sitio Web de Microsoft para obtener el procedimiento correcto para modificar el registro.

Para agregar el valor del Registro ProhibitIpSec al equipo basado en Windows 2000, utilice Regedt32.exe para buscar esta clave en el Registro:

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

Agregue este valor de registro a la clave:

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

Nota: Debe reiniciar el equipo basado en Windows 2000 para que los cambios surtan efecto. Consulte estos artículos de Microsoft para obtener más información.

- Q258261 - Inhabilitación de la Política IPSec Utilizada con L2TP
- Q240262- Cómo configurar una conexión L2TP/IPSec mediante una clave previamente compartida

Para una configuración más compleja usando Windows 2000, refiérase a Configuración de Clientes de Cisco IOS y Windows 2000 para L2TP Usando Microsoft IAS.

Configurar

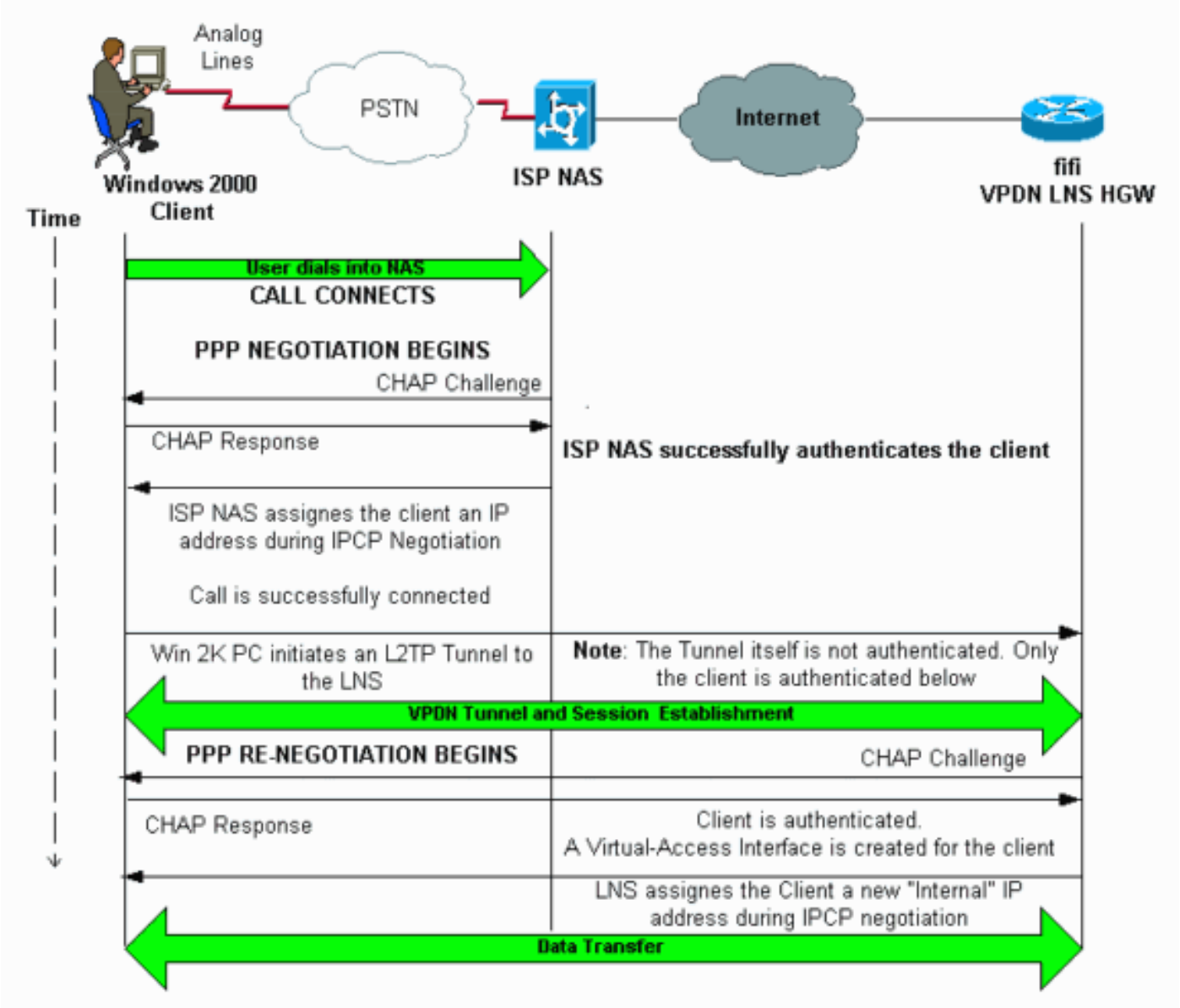
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice

la Command Lookup Tool (sólo clientes registrados) .

Diagrama de la red

El siguiente diagrama de red muestra las diversas negociaciones que se producen entre el PC cliente, ISP NAS y Enterprise HGW. El ejemplo de depuración de la sección Solución de problemas describe estas transacciones también.



Configuraciones

Este documento usa esta configuración:

- fifi (VPDN LNS/HGW)

Nota: Sólo se incluye la sección relevante de la configuración de 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
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show vpdn**—Muestra información sobre el túnel L2x activo y los identificadores de mensaje en una VPDN.
- **show vpdn session window**—Muestra información en la ventana de la sesión VPDN.
- **show user**: proporciona una lista completa de todos los usuarios conectados al router.
- **show caller user *username* detail**: para mostrar parámetros para el usuario en particular, como los estados Link Control Protocol (LCP), NCP e IPCP, así como la dirección IP asignada, los parámetros PPP y PPP bundle, etc.

```
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
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: Antes de ejecutar un comando **debug**, consulte Información Importante sobre Comandos Debug.

- **debug ppp negotiation**: muestra información sobre el tráfico PPP y los intercambios mientras negocia los componentes PPP, incluidos LCP, Authentication y NCP. Una negociación PPP exitosa primero abre el estado LCP, luego autentica y finalmente negocia NCP (normalmente IPCP).

- **debug vpdn event — Muestra mensajes relativos a eventos que forman parte del establecimiento o cierre normal del túnel.**
- **debug vpdn error — Muestra errores que evitan que se establezca un túnel o errores que provocan que un túnel establecido se cierre.**
- **debug vpdn l2x-event**: muestra mensajes acerca de eventos que forman parte del establecimiento normal del túnel o del cierre para L2x.
- **debug vpdn l2x-error—Muestra errores de protocolo L2x que impiden el establecimiento de L2x o su funcionamiento normal.**

Nota: Algunas de estas líneas de la salida **debug** se dividen en varias líneas con fines de impresión.

Habilite los comandos **debug** especificados anteriormente en el LNS e inicie una llamada desde el equipo cliente de Windows 2000. Las depuraciones aquí muestran la solicitud de túnel del cliente, el establecimiento del túnel, la autenticación del cliente y la renegociación de la dirección 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.
```

Esta salida de depuración en el LNS muestra al cliente de Windows 2000 desconectando la llamada. Observe los diversos mensajes donde el LNS reconoce la desconexión y realiza un apagado limpio del túnel:

```
*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
```

Información Relacionada

- Configuración de clientes IOS de Cisco y Windows 2000 para L2TP por medio de Microsoft IAS
- Introducción a VPDN'
- Configuración de VPDN sin AAA
- Configuración de Capa 2 de autenticación de protocolo de túnel mediante servidor RADIUS
- Configuración del servidor de acceso con PRI para las llamadas ISDN y asíncronas entrantes
- Páginas de soporte de la tecnología de marcación
- Soporte Técnico - Cisco Systems