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

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Productos Relacionados](#)
[Convenciones](#)
[Antecedentes](#)
[Configure al cliente del Windows 2000 para el L2TP](#)
[Configurar](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Verificación](#)
[Troubleshooting](#)
[Comandos para resolución de problemas](#)
[Información Relacionada](#)

Introducción

En la mayoría de los escenarios del Virtual Private Dialup Network (VPDN), el cliente marca al servidor de acceso a la red (NAS). El NAS entonces inicia el Tunnel Protocol de la capa 2 VPDN (L2TP) o el túnel de protocolo de la expedición de la capa 2 (L2F) al gateway de inicio (HGW). Esto crea una conexión VPDN entre el NAS, que es el punto final del L2TP Access Concentrator (LAC), y el HGW, que es el punto final del L2TP Network Server (LNS). Esto significa que solamente el link entre el NAS y el HGW utiliza el L2TP, y que el túnel no incluye el link del PC del cliente al NAS. Sin embargo, los PC cliente que funcionan con el sistema operativo del Windows 2000 pueden ahora hacer el LAC e iniciar un túnel L2TP del PC, con el NAS y terminado en el HGW/LNS. Esta configuración de muestra muestra cómo usted puede configurar tal túnel.

prerrequisitos

Requisitos

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

- Familiaridad con la comprensión del VPDN
- Familiaridad con la sinopsis del dial-in del acceso VPDN usando el L2TP

Nota: La Configuración de 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 funciona con el Software Release 12.2(1) de Cisco IOS®
- Cliente: Windows 2000 PC con un módem

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

La configuración para el LNS incluido en este documento no es plataforma específica y se puede aplicar a cualquier router apto para VPDN.

El procedimiento para configurar el Windows 2000 PC del cliente es aplicable solamente al Windows 2000 y no a cualquier 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 el Windows 2000 usted puede iniciar un túnel L2TP del PC del cliente y tener el túnel terminada dondequiera en la red de Proveedor de servicios de Internet (ISP). Usando la terminología VPDN, se refiere esta configuración como un túnel “iniciado por el cliente”. Puesto que los túneles iniciados por el cliente son túneles iniciados por el software de cliente en el PC, el PC adquiere el papel del LAC. Puesto que autenticarán al cliente usando el Point-to-Point Protocol (PPP), el Challenge Handshake Authentication Protocol (CHAP), o el protocolo password authentication (PAP) de todos modos, el túnel sí mismo no necesita ser autenticado.

Ventajas y desventajas de usar los túneles iniciados por el cliente

Los túneles iniciados por el cliente tienen ambas ventajas y desventajas, algunos de los cuales se delinean aquí:

Ventajas:

- Asegura la conexión entera del cliente a través de la red compartida ISP y a la red para empresas.
- No requiere la configuración adicional en la red ISP. Sin un túnel iniciado por el cliente, el ISP NAS o su servidor Radius/TACACS+ necesita ser configurado para iniciar el túnel al HGW. Por lo tanto, la empresa debe negociar con muchos ISP para permitir que los usuarios hagan un túnel a través de su red. Con un túnel iniciado por el cliente, el usuario final puede

conectar con cualquier ISP y después iniciar manualmente el túnel a la red para empresas.

Desventajas:

- No es tan scalable como un túnel ISP-iniciado. Puesto que los túneles iniciados por el cliente crean los túneles individuales para cada cliente, el HGW debe terminar individualmente un gran número de túneles.
- El cliente debe manejar el software de cliente usado para iniciar el túnel. Ésta es a menudo una fuente de problemas soporte-relacionados para la empresa.
- El cliente debe tener una cuenta con el ISP. Puesto que los túneles iniciados por el cliente pueden ser creados solamente después de que una conexión al ISP se establezca, el cliente debe tener una cuenta a conectar con la red ISP.

Cómo trabaja

Thjs es cómo el ejemplo en este documento trabaja:

1. PC del cliente marca en el NAS, autentica usando la cuenta ISP del cliente, y obtiene una dirección IP del ISP.
2. El cliente inicia y construye el túnel L2TP al L2TP Network Server HGW (LNS). El cliente renegociará el IP Control Protocol (IPCP) y obtendrá una nueva dirección IP del LNS.

Configure al cliente del Windows 2000 para el L2TP

Cree dos conexiones del dial-up networking (DUN):

- Una conexión DUN a acceder telefónicamente al ISP. Refiera a su ISP para más información sobre este tema.
- Otra conexión DUN para el túnel L2TP.

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

1. Desde el principio el menú, elige el **Settings (Configuración) > Control Panel (Panel de control) > Network and dial-up connections (Conexiones de red y de marcado manual) > el Make New Connection**.Utilice al Asisitente para crear una conexión llamada L2TP. Aseegurese seleccionar **conectan con una red privada a través de Internet** en la ventana del **tipo de conexión de red**. Usted debe también especificar la dirección IP o el nombre del LNS/HGW.
2. La nueva conexión (L2TP Nombrado) aparece en la ventana de la **red y de las conexiones por línea telefónica** bajo el panel de control. De aquí, click derecho para editar las **propiedades**.
3. Haga clic la ficha de interconexión de redes y aseegurese que el **Type of Server I Am Calling** está fijado al **L2TP**.
4. Si usted planea afectar un aparato un direccionamiento interno dinámico (de la red para empresas) a este cliente del HGW, con una agrupación local o el DHCP, seleccione el protocolo **TCP/IP**. Aseegurese que configuran al cliente para obtener una dirección IP automáticamente. Usted puede también publicar la información del Domain Naming System (DNS) automáticamente.**El botón Advanced** permite que usted defina el Windows Internet Naming Service estático (TRIUNFOS) y la información DNS. La lengueta de las **opciones** permite que usted apague el IPSec o que asigne una diversa directiva a la conexión.

Conforme a la ficha de seguridad, usted puede definir los parámetros de autenticación de usuario. Por ejemplo, PAP, GRIETA, o MS-CHAP, o inicio del Dominio de Windows. Consulte al administrador para información de los sistemas de red en los parámetros que se deben configurar en el cliente.

5. Una vez que se configura la conexión, usted puede hacerla doble clic para surgir a la pantalla de inicio de sesión, y después conecta.

Observaciones adicionales

Si su túnel L2TP utiliza la seguridad IP (IPSec) y/o el Microsoft Point-to-Point Encryption (MPPE), después usted debe definir este comando bajo configuración de plantilla virtual en el LNS/HGW.

```
ppp encrypt mppe 40
```

Tenga presente que esto requiere el conjunto cifrado de la característica del Cisco IOS Software (por lo menos el conjunto de características del IPSec o IPSec con el 3DES).

Por abandono, el IPSec se habilita en el Windows 2000. Si usted quiere inhabilitarlo, usted debe modificar el registro de Windows usando el Editor de registro:

IPSec de la neutralización en un win2k PC

Advertencia: Tome las precauciones adecuadas (tales como respaldo del registro) antes de modificar el registro. Usted debe también referir al sitio Web de Microsoft para que el procedimiento correcto modifique el registro.

Para agregar el valor de registro de ProhibitIpSec a su ordenador de Windows 2000-based, utilice el regedt32.exe para localizar 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: Usted debe reiniciar su ordenador de Windows 2000-based para que los cambios tomen el efecto. Refiera por favor a estos artículos de Microsoft para otros detalles.

- Q258261 - Inhabilitando la política IPSec usada con el L2TP
- Q240262- Cómo configurar una conexión del L2TP/IPSec usando una clave previamente compartida

Para una configuración más compleja usando el Windows 2000, refiera a configurar el Cisco IOS y a los clientes del Windows 2000 para el L2TP usando el Microsoft IAS.

Configurar

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

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento,

use la Command Lookup Tool (solo para clientes registrados).

Diagrama de la red

El diagrama de la red abajo muestra las diversas negociaciones que ocurren entre PC del cliente, ISP NAS, y la empresa HGW. El ejemplo del debug en la sección del Troubleshooting representa estas transacciones también.

Configuraciones

Este documento usa esta configuración:

- fifi (VPDN LNS/HGW)

Nota: Solamente la sección pertinente de la configuración LNS es incluida.

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.

- **vpdn de la demostración** — Información de las visualizaciones sobre el túnel y los identificadores de mensajes activos del l2x en un VPDN.

- **show vpdn session window** — Visualiza la información sobre la ventana para la sesión de VPDN.
- **usuario de la demostración** — Proporciona un anuncio completo de todos los usuarios conectados con el router.
- **show caller user username detail** — Para mostrar los parámetros para el usuario determinado, tal como los estados del (LCP), NCP y IPCP del Link Control Protocol, así como la dirección IP asignada, parámetros de agrupamiento PPP y PPP, y así sucesivamente.

```
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
```

Troubleshooting

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 de depuración, consulte Información importante sobre comandos de depuración.

- **haga el debug de la negociación ppp** — Visualiza la información sobre el tráfico y los intercambios PPP mientras que negocia a los componentes PPP incluyendo el LCP, la autenticación, y el NCP. Una negociación PPP satisfactoria primero abre el estado LCP, después autentica, y finalmente negocia NCP (generalmente 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** — Visualiza los mensajes sobre los eventos que son parte del

establecimiento normal de túneles o apagan para el 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 **salida de los debugs** están rotas en las líneas múltiples para los propósitos de la impresión.

Habilite los **comandos debug** especificados arriba en el LNS e inicie una llamada del Windows 2000 PC del cliente. Los debugs aquí muestran la petición del túnel del cliente, del establecimiento del túnel, de la autenticación del cliente, y de 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 los debugs en el LNS muestra al cliente del Windows 2000 que desconecta la llamada. Observe los diversos mensajes donde el LNS reconoce la desconexión y realiza un limpio apaga 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