Konfigurieren des L2TP-Client-Initiated Tunneling mit Windows 2000 PC

Inhalt

Einführung

In den meisten VPDN-Szenarien (Virtual Private Dial-up Network) wählt der Client den Netzwerkzugriffsserver (NAS). Das NAS-Gerät initiiert dann den VPDN Layer 2 Tunnel Protocol (L2TP)- oder Layer 2 Forwarding (L2F)-Protokolltunnel zum Home Gateway (HGW). Dadurch wird eine VPDN-Verbindung zwischen dem NAS-Gerät, dem LAC-Endpunkt (L2TP Access Concentrator), und dem HGW, dem Endpunkt des L2TP-Netzwerkservers (LNS), hergestellt. Dies bedeutet, dass nur die Verbindung zwischen dem NAS-Gerät und dem HGW L2TP verwendet und dieser Tunnel die Verbindung vom Client-PC zum NAS nicht beinhaltet. PC-Clients, die das Windows 2000-Betriebssystem ausführen, können nun die LAC werden und vom PC über das NAS-Gerät einen L2TP-Tunnel initiieren, der auf dem HGW/LNS terminiert wird. Diese Beispielkonfiguration zeigt, wie Sie einen solchen Tunnel konfigurieren können.

Voraussetzungen

Anforderungen

Stellen Sie vor dem Versuch dieser Konfiguration sicher, dass Sie die folgenden Anforderungen erfüllen:

- Vertrautheit mit VPDN

- Vertrautheit mit der Synopsis of Access VPDN Dial-In mithilfe von L2TP

Hinweis: Die NAS-Konfiguration ist in diesem Dokument nicht enthalten.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- LNS: Cisco Router der Serie 7200 mit Cisco IOS® Software, Version 12.2(1)
- Kunde: Windows 2000 PC mit Modem

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Die in diesem Dokument enthaltene Konfiguration für das LNS ist nicht plattformspezifisch und kann auf jeden VPDN-fähigen Router angewendet werden.

Das Verfahren zur Konfiguration des Windows 2000 Client-PCs gilt nur für Windows 2000 und nicht für jedes andere Betriebssystem.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

Hintergrundinformationen

Wie in der Einführung erwähnt, können Sie mit Windows 2000 einen L2TP-Tunnel vom Client-PC aus initiieren und den Tunnel an einer beliebigen Stelle im Internet Service Provider (ISP)-Netzwerk terminieren lassen. Mithilfe der VPDN-Terminologie wird diese Konfiguration als "Client-Initiated" Tunnel bezeichnet. Da Client-initiierte Tunnel Tunnels sind, die von Client-Software auf dem PC initiiert werden, übernimmt der PC die Rolle der LAC. Da der Client ohnehin mithilfe von Point-to-Point Protocol (PPP), Challenge Handshake Authentication Protocol (CHAP) oder Password Authentication Protocol (PAP) authentifiziert wird, muss der Tunnel selbst nicht authentifiziert werden.

Vorteile und Nachteile der Verwendung von Client-initiierten Tunneln

Client-gesteuerte Tunnel haben sowohl Vor- als auch Nachteile, einige davon sind hier aufgeführt:

Vorteile:

- Sie sichert die gesamte Verbindung vom Client über das gemeinsam genutzte ISP-Netzwerk und zum Unternehmensnetzwerk.
- Es ist *keine* zusätzliche Konfiguration im ISP-Netzwerk erforderlich. Ohne Client-initiierten Tunnel muss der ISP-NAS- oder dessen Radius/TACACS+-Server konfiguriert werden, um

den Tunnel zum HGW zu initiieren. Daher muss das Unternehmen mit vielen ISPs verhandeln, um Benutzern die Tunnelung über ihr Netzwerk zu ermöglichen. Mit einem Client-initiierten Tunnel kann der Endbenutzer eine Verbindung zu einem beliebigen ISP herstellen und den Tunnel zum Unternehmensnetzwerk manuell initiieren.

Nachteile:

- Sie ist nicht so skalierbar wie ein vom ISP initiierter Tunnel. Da Client-initiierte Tunnel individuelle Tunnel für jeden Client erstellen, muss das HGW eine große Anzahl von Tunneln einzeln terminieren.
- Der Client muss die Client-Software verwalten, die zum Initiieren des Tunnels verwendet wird. Dies ist häufig eine Ursache für Support-bezogene Probleme des Unternehmens.
- Der Kunde muss über ein Konto beim ISP verfügen. Da Client-initiierte Tunnel erst erstellt werden können, nachdem eine Verbindung zum ISP hergestellt wurde, muss der Client über ein Konto für die Verbindung mit dem ISP-Netzwerk verfügen.

Funktionsweise

So funktioniert das Beispiel in diesem Dokument:

1. Der Client-PC wählt sich in das NAS-Gerät ein, authentifiziert sich über das ISP-Konto des Clients und erhält eine IP-Adresse vom ISP.
2. Der Client initiiert und erstellt den L2TP-Tunnel zum L2TP-Netzwerkserver HGW (LNS). Der Client handelt das IP Control Protocol (IPCP) neu aus und erhält eine neue IP-Adresse vom LNS.

Konfigurieren des Windows 2000-Clients für L2TP

Erstellen Sie zwei DFÜ-Netzwerkverbindungen (DUN):

- Eine DUN-Verbindung zum Einwählen beim ISP. Weitere Informationen zu diesem Thema erhalten Sie von Ihrem ISP.
- Eine weitere DUN-Verbindung für den L2TP-Tunnel.

So erstellen und konfigurieren Sie die DUN-Verbindung für L2TP auf dem Windows 200 Client-PC:

1. Wählen Sie im Startmenü **Einstellungen > Systemsteuerung > Netzwerk- und DFÜ-Verbindungen > Neue Verbindung herstellen aus**.Verwenden Sie den Assistenten, um eine Verbindung mit dem Namen L2TP zu erstellen. Wählen Sie **im** Fenster **Netzwerkverbindungstyp die** Option **Verbindung mit einem privaten Netzwerk über das Internet herstellen aus**. Sie müssen auch die IP-Adresse oder den Namen des LNS/HGW angeben.
2. Die neue Verbindung (L2TP genannt) wird im Fenster **Netzwerk- und DFÜ-Verbindungen** unter Systemsteuerung angezeigt. Klicken Sie hier mit der rechten Maustaste, um die **Eigenschaften** zu bearbeiten.
3. Klicken Sie auf die Registerkarte Netzwerk, und stellen Sie sicher, dass der **Typ des Servers, den ich anrufe,** auf **L2TP** festgelegt ist.
4. Wenn Sie planen, diesem Client vom HGW entweder über einen lokalen Pool oder DHCP eine dynamische interne (Enterprise Network)-Adresse zuzuweisen, wählen Sie **TCP/IP-**Protokoll. Stellen Sie sicher, dass der Client so konfiguriert ist, dass er automatisch eine IP-

Adresse bezieht. Sie können auch DNS-Informationen (Domain Naming System) automatisch ausgeben.Mit der **Schaltfläche Erweitert** können Sie statische Windows Internet Naming Service (WINS)- und DNS-Informationen definieren. Mit dem Register **Optionen** können Sie IPSec deaktivieren oder der Verbindung eine andere Richtlinie zuweisen. Auf der Registerkarte Sicherheit können Sie die Parameter für die Benutzerauthentifizierung festlegen. Beispiel: Anmeldung bei PAP-, CHAP- oder MS-CHAP- oder Windows-Domänen. Weitere Informationen zu den Parametern, die auf dem Client konfiguriert werden sollen, erhalten Sie vom Netzwerksystemadministrator.

5. Nach der Konfiguration der Verbindung können Sie auf diese doppelklicken, um den Anmeldebildschirm anzuzeigen und dann eine Verbindung herzustellen.

Weitere Anmerkungen

Wenn Ihr L2TP-Tunnel IP Security (IPSec) und/oder Microsoft Point-to-Point Encryption (MPPE) verwendet, müssen Sie diesen Befehl unter der Konfiguration der virtuellen Vorlage auf dem LNS/HGW definieren.

```
ppp encrypt mppe 40
```

Beachten Sie, dass dafür das verschlüsselte Feature-Set der Cisco IOS Software erforderlich ist (mindestens das IPSec-Feature-Set oder IPSec mit 3DES).

IPSec ist in Windows 2000 standardmäßig aktiviert. Wenn Sie diese deaktivieren möchten, müssen Sie die Windows-Registrierung mit dem Registrierungs-Editor ändern:

Deaktivieren Sie IPSec auf einem Win2K-PC.

Warnung: Nehmen Sie vor dem Ändern der Registrierung angemessene Vorsichtsmaßnahmen (z. B. zur Sicherung der Registrierung) vor. Sie sollten auch auf der Microsoft-Website nachlesen, wie Sie die Registrierung ändern können.

Um dem Windows 2000-basierten Computer den Registrierungswert ProhibitIpSec hinzuzufügen, suchen Sie diesen Schlüssel mithilfe von Regedt32.exe in der Registrierung:

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

Fügen Sie diesen Registrierungswert dem Schlüssel hinzu:

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

Hinweis: Sie müssen Ihren Windows 2000-basierten Computer neu starten, damit die Änderungen wirksam werden. Weitere Informationen finden Sie in diesen Microsoft-Artikeln.

- Q258261 - Deaktivieren der IPSec-Richtlinie für L2TP
- Q240262 - Konfigurieren einer L2TP/IPSec-Verbindung mithilfe eines vorinstallierten Schlüssels

Eine komplexere Konfiguration unter Windows 2000 finden Sie unter Konfigurieren von Cisco IOS-

und Windows 2000-Clients für L2TP mithilfe von Microsoft IAS.

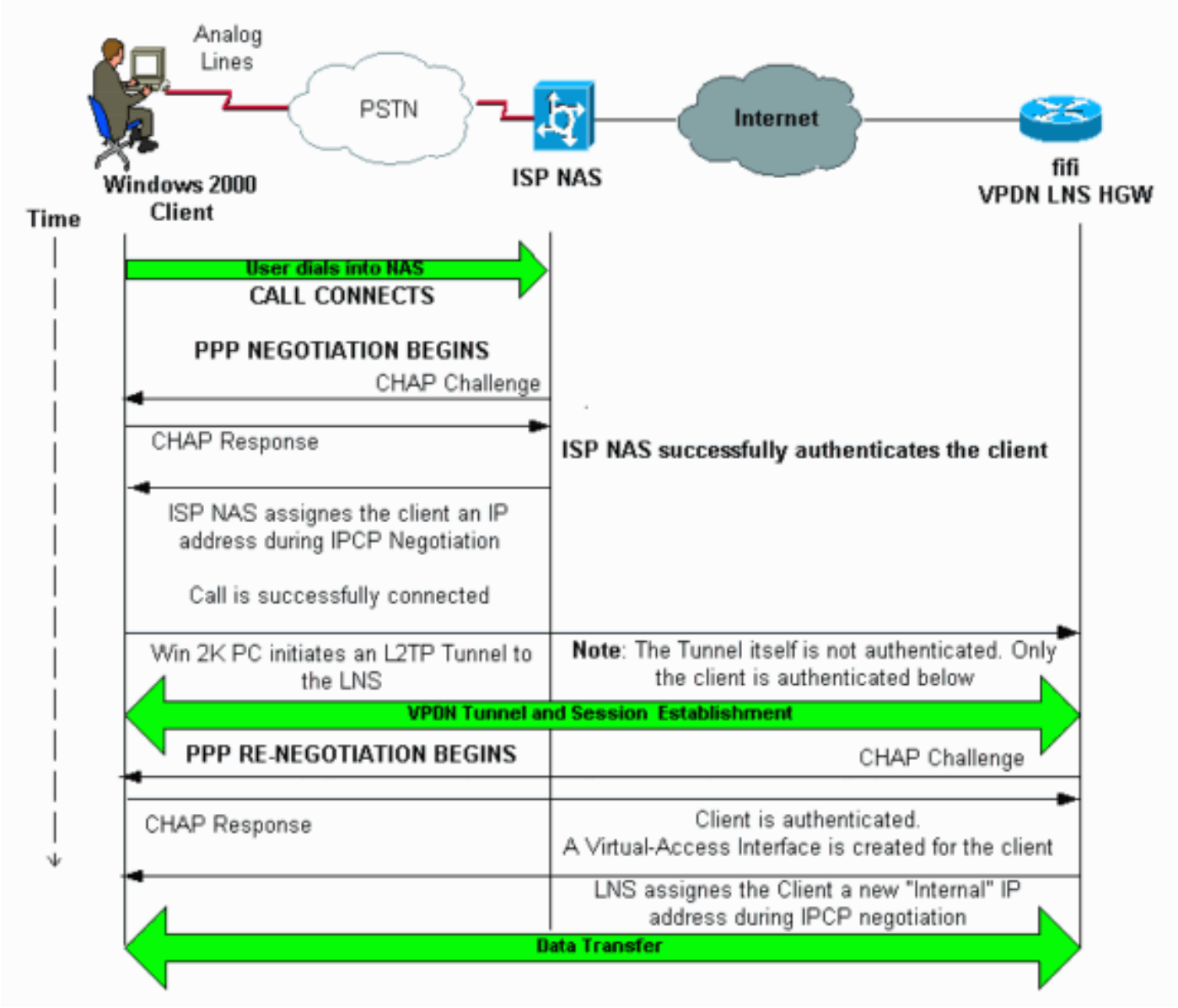
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Netzwerkdiagramm

Das folgende Netzwerkdiagramm zeigt die verschiedenen Aushandlungen, die zwischen dem Client-PC, ISP NAS und Enterprise HGW auftreten. Im Debugbeispiel im Abschnitt Problembehandlung werden diese Transaktionen ebenfalls dargestellt.



Konfigurationen

In diesem Dokument wird diese Konfiguration verwendet:

- fünfzig (VPDN LNS/HGW)

Hinweis: Nur der entsprechende Abschnitt der LNS-Konfiguration ist enthalten.

fünfzig (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
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show vpdn**: Zeigt Informationen über den aktiven L2x-Tunnel und die Nachrichtenbezeichner in einem VPDN an.
- **show vpdn session window**: Zeigt Informationen zum Fenster der VPDN-Sitzung an.
- **show user** - Bietet eine umfassende Liste aller Benutzer, die mit dem Router verbunden sind.
- **Details zum *Benutzernamen des* Anrufers anzeigen** - Zum Anzeigen von Parametern für den jeweiligen Benutzer, z. B. Link Control Protocol (LCP), NCP- und IPCP-Status, zugewiesene IP-Adresse, PPP- und PPP-Paketparameter usw.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-

Befehle.

- **debug ppp negotiation**: Zeigt Informationen über PPP-Datenverkehr und -Datenaustausch während der Aushandlung der PPP-Komponenten wie LCP, Authentifizierung und NCP an. Eine erfolgreiche PPP-Aushandlung öffnet zuerst den LCP-Status, authentifiziert dann den Status und handelt schließlich NCP (normalerweise IPCP) aus.
- **debug vpdn event** (**vpdn-Ereignis debug**): Zeigt Meldungen über Ereignisse an, die Teil der normalen Tunneleinrichtung oder -abschaltung sind.
- **debug vpdn error** (**vpdn-Fehler debug**): Zeigt Fehler an, die das Herstellen eines Tunnels verhindern oder Fehler, die das Schließen eines etablierten Tunnels verursachen.
- **debug vpdn l2x-event**: Zeigt Meldungen über Ereignisse an, die Teil der normalen Tunneleinrichtung oder des Herunterfahrens für L2x sind.
- **debug vpdn l2x-error**: Zeigt L2x-Protokollfehler an, die eine L2x-Einrichtung verhindern oder deren normalen Betrieb verhindern.

Hinweis: Einige dieser Zeilen der **Debugausgabe** werden zu Druckzwecken in mehrere Zeilen aufgeteilt.

Aktivieren Sie die oben im LNS angegebenen **Debug-**Befehle, und initiieren Sie einen Aufruf vom Windows 2000-Client-PC. Die hier gezeigten Debugging-Meldungen zeigen die Tunnelanforderung des Clients, die Einrichtung des Tunnels, die Authentifizierung des Clients und die Neuverhandlung der IP-Adresse:

```
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.

Diese Debug-Ausgabe im LNS zeigt an, dass der Windows 2000-Client den Anruf trennt. Beachten Sie die verschiedenen Meldungen, bei denen das LNS die Trennung erkennt und eine saubere Abschaltung des Tunnels durchführt:

```
*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
```

Zugehörige Informationen

- Konfigurieren von Cisco IOS- und Windows 2000-Clients für L2TP mithilfe von Microsoft IAS
- VPDN im Überblick
- VPDN-Konfiguration ohne AAA
- Konfigurieren der Layer-2-Tunnelprotokollauthentifizierung mit RADIUS
- Konfigurieren eines Zugangs-Servers mit PRIs für eingehende Async- und ISDN-Anrufe
- Support-Seiten für Wähltechnologie
- Technischer Support - Cisco Systems