Configuration de la tunnellisation L2TP à l'initiative du client avec un PC Windows 2000

Contenu

Introduction

Dans la plupart des scénarios VPDN, le client compose le numéro du serveur d'accès au réseau (NAS). Le NAS lance ensuite le protocole L2TP (Layer 2 Tunnel Protocol) VPDN ou le tunnel de protocole L2F (Layer 2 Forwarding) vers la passerelle domestique (HGW). Cela crée une connexion VPDN entre le NAS, qui est le point de terminaison du concentrateur d'accès L2TP (LAC), et le HGW, qui est le point de terminaison du serveur de réseau L2TP (LNS). Cela signifie que seule la liaison entre le NAS et le HGW utilise L2TP et que le tunnel n'inclut pas la liaison entre le PC client et le NAS. Cependant, les clients PC exécutant le système d'exploitation Windows 2000 peuvent désormais devenir le LAC et initier un tunnel L2TP à partir du PC, via le NAS et se terminer sur le HGW/LNS. Cet exemple de configuration montre comment configurer un tel tunnel.

Conditions préalables

Conditions requises

Avant d'essayer cette configuration, assurez-vous de respecter les conditions suivantes :

- Connaissance de VPDN
- Familiarité avec le résumé de la connexion à distance VPDN d'accès à l'aide du protocole

L2TP

Remarque : la configuration NAS n'est pas incluse dans ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- LNS : Routeur de la gamme Cisco 7200 exécutant le logiciel Cisco IOS® Version 12.2(1)
- Client : PC Windows 2000 avec modem

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.

Produits connexes

La configuration du LNS incluse dans ce document n'est pas spécifique à la plate-forme et peut être appliquée à n'importe quel routeur compatible VPDN.

La procédure de configuration du PC client Windows 2000 s'applique uniquement à Windows 2000 et non à aucun autre système d'exploitation.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Informations générales

Comme indiqué dans l'Introduction, avec Windows 2000, vous pouvez lancer un tunnel L2TP à partir du PC client et faire terminer le tunnel n'importe où dans le réseau du fournisseur d'accès Internet (FAI). En utilisant la terminologie VPDN, cette configuration est appelée tunnel initié par le client. Puisque les tunnels initiés par le client sont des tunnels initiés par le logiciel client sur le PC, le PC prend le rôle de BAC. Puisque le client sera authentifié à l'aide du protocole PPP (Point-to-Point Protocol), du protocole CHAP (Challenge Handshake Authentication Protocol) ou du protocole PAP (Password Authentication Protocol), le tunnel lui-même n'a pas besoin d'être authentifié.

Avantages et inconvénients de l'utilisation de tunnels initiés par le client

Les tunnels initiés par le client présentent à la fois des avantages et des inconvénients, dont certains sont décrits ci-dessous :

Avantages :

- Elle sécurise l’intégralité de la connexion du client via le réseau partagé ISP et vers le réseau d’entreprise.
- Il *ne* nécessite *pas* de configuration supplémentaire sur le réseau du FAI. Sans tunnel initié par le client, le NAS du FAI ou son serveur Radius/TACACS+ doit être configuré pour initier le

tunnel vers le HGW. Par conséquent, l'entreprise doit négocier avec de nombreux FAI pour permettre aux utilisateurs de passer par tunnel sur leur réseau. Avec un tunnel initié par le client, l'utilisateur final peut se connecter à n'importe quel FAI, puis lancer manuellement le tunnel vers le réseau de l'entreprise.

Inconvénients :

- Il n'est pas aussi évolutif qu'un tunnel initié par un FAI. Puisque les tunnels initiés par le client créent des tunnels individuels pour chaque client, le HGW doit terminer individuellement un grand nombre de tunnels.
- Le client doit gérer le logiciel client utilisé pour lancer le tunnel. Il s'agit souvent d'une source de problèmes liés à l'assistance pour l'entreprise.
- Le client doit avoir un compte auprès du FAI. Puisque les tunnels initiés par le client ne peuvent être créés qu'après l'établissement d'une connexion au FAI, le client doit avoir un compte pour se connecter au réseau du FAI.

Comment ça fonctionne

Voici comment fonctionne l'exemple de ce document :

1. Le PC client compose le numéro du NAS, s'authentifie à l'aide du compte FAI du client et obtient une adresse IP du FAI.
2. Le client initie et construit le tunnel L2TP vers le serveur réseau L2TP HGW (LNS). Le client renégociera le protocole IPCP (IP Control Protocol) et obtiendra une nouvelle adresse IP auprès du LNS.

Configuration du client Windows 2000 pour L2TP

Créez deux connexions réseau commutées (DUN) :

- Une connexion DUN pour la connexion directe au FAI. Reportez-vous à votre FAI pour plus d'informations sur ce sujet.
- Une autre connexion DUN pour le tunnel L2TP.

Pour créer et configurer la connexion DUN pour L2TP, procédez comme suit sur le PC client Windows 200 :

1. Dans le menu Démarrer, sélectionnez **Paramètres > Panneau de configuration > Connexions réseau et accès à distance > Créer une connexion**.Utilisez l'Assistant pour créer une connexion appelée L2TP. Veillez à sélectionner **Connexion à un réseau privé via Internet** dans la fenêtre **Type de connexion réseau**. Vous devez également spécifier l'adresse IP ou le nom du LNS/HGW.
2. La nouvelle connexion (appelée L2TP) apparaît dans la fenêtre **Connexions réseau et accès à distance** sous Panneau de configuration. À partir d'ici, cliquez avec le bouton droit de la souris pour modifier les **propriétés**.
3. Cliquez sur l'onglet Mise en réseau et assurez-vous que le **type de serveur que j'appelle** est défini sur **L2TP**.
4. Si vous prévoyez d'allouer une adresse interne dynamique (réseau d'entreprise) à ce client à partir de HGW, via un pool local ou DHCP, sélectionnez le protocole **TCP/IP**. Assurez-vous que le client est configuré pour obtenir automatiquement une adresse IP. Vous pouvez également émettre automatiquement des informations DNS (Domain Naming System).Le

bouton **Avancé** vous permet de définir des informations WINS (Windows Internet Naming Service) et DNS statiques. L'onglet **Options** vous permet de désactiver IPSec ou d'affecter une autre stratégie à la connexion. Sous l'onglet Sécurité, vous pouvez définir les paramètres d'authentification des utilisateurs. Par exemple, PAP, CHAP, MS-CHAP ou ouverture de session de domaine Windows. Pour plus d'informations sur les paramètres à configurer sur le client, contactez l'administrateur système du réseau.

5. Une fois la connexion configurée, vous pouvez double-cliquer dessus pour afficher l'écran de connexion, puis vous connecter.

Remarques supplémentaires

Si votre tunnel L2TP utilise IP Security (IPSec) et/ou Microsoft Point-to-Point Encryption (MPPE), vous devez définir cette commande sous la configuration de modèle virtuel sur le LNS/HGW.

```
ppp encrypt mppe 40
```

Gardez à l'esprit que cela nécessite l'ensemble de fonctionnalités cryptées du logiciel Cisco IOS (au moins l'ensemble de fonctionnalités IPSec ou IPSec avec 3DES).

Par défaut, IPSec est activé sous Windows 2000. Si vous voulez le désactiver, vous devez modifier le Registre Windows à l'aide de l'Éditeur du Registre :

Désactiver IPSec sur un PC Win2K

Avertissement : Prenez les précautions nécessaires (comme la sauvegarde du Registre) avant de modifier le Registre. Vous devez également consulter le site Web de Microsoft pour connaître la procédure appropriée pour modifier le Registre.

Pour ajouter la valeur de Registre ProhibitIpSec à votre ordinateur Windows 2000, utilisez Regedt32.exe pour localiser cette clé dans le Registre :

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

Ajoutez cette valeur de registre à la clé :

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

Remarque : Vous devez redémarrer votre ordinateur Windows 2000 pour que les modifications prennent effet. Pour plus de détails, reportez-vous aux articles de Microsoft.

- Q258261 - Désactivation de la stratégie IPSec utilisée avec L2TP
- Q240262 - Configuration d'une connexion L2TP/IPSec à l'aide d'une clé pré-partagée

Pour une configuration plus complexe utilisant Windows 2000, référez-vous à Configuration de clients Cisco IOS et Windows 2000 pour L2TP à l'aide de Microsoft IAS.

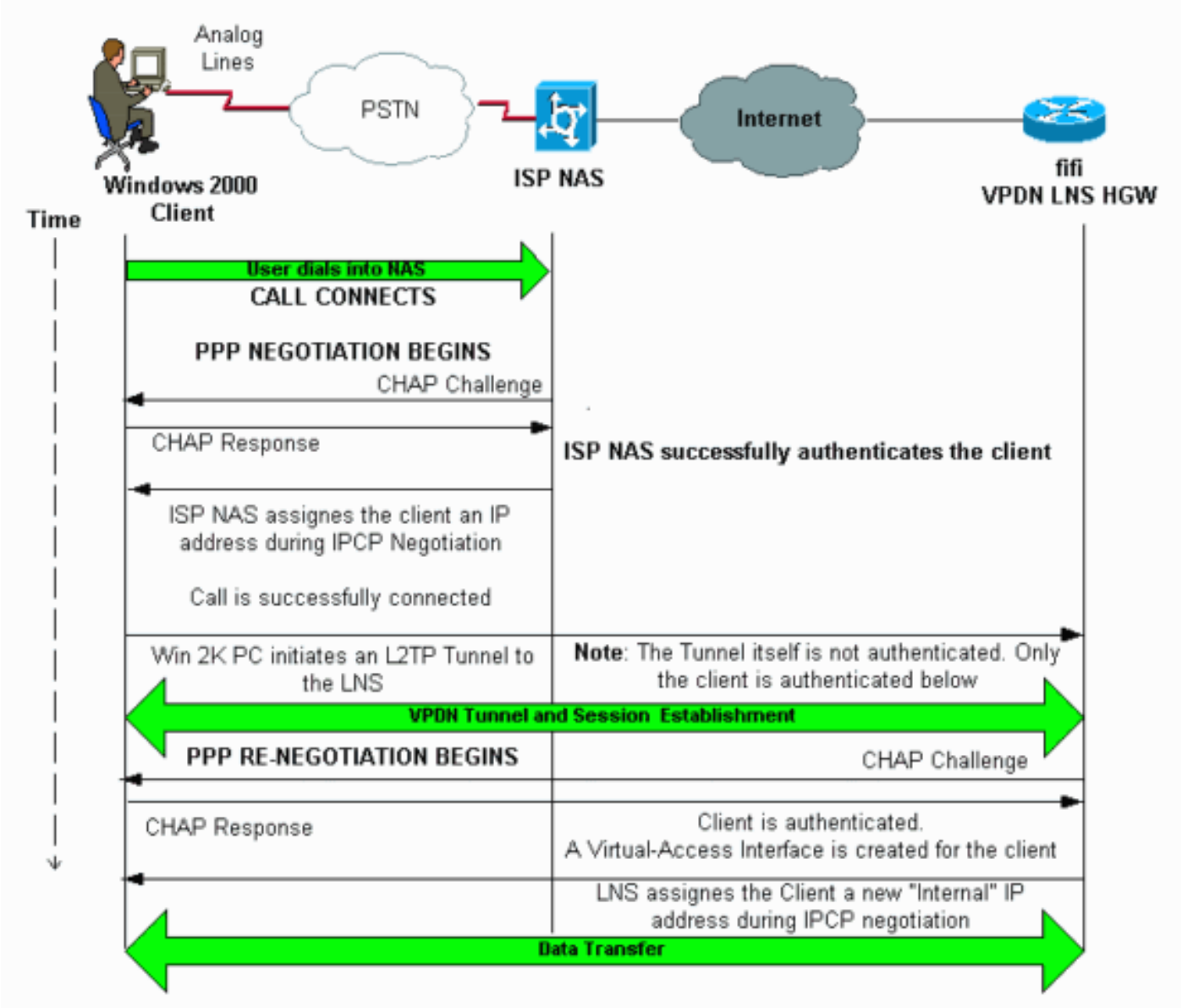
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Diagramme du réseau

Le schéma de réseau ci-dessous présente les différentes négociations qui ont lieu entre le PC client, le NAS du FAI et le HGW d'entreprise. L'exemple de débogage de la section Dépannage illustre également ces transactions.



Configurations

Ce document utilise la configuration suivante :

- fifi (VPDN LNS/HGW)

Remarque : Seule la section pertinente de la configuration LNS est incluse.

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
```

Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show vpdn** : affiche des informations sur le tunnel L2x actif et les identificateurs de message dans un VPDN.
- **show vpdn session window** : affiche des informations sur la fenêtre de la session VPDN.
- **show user** : fournit une liste complète de tous les utilisateurs connectés au routeur.
- **show caller user user *username* detail** : pour afficher les paramètres de l'utilisateur particulier, tels que les états LCP (Link Control Protocol), NCP et IPCP, ainsi que l'adresse IP attribuée, les paramètres PPP et PPP, 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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque : avant d'émettre des commandes **debug**, reportez-vous à Informations importantes sur les commandes de débogage.

- **debug ppp negotiation** - Affiche des informations sur le trafic et les échanges PPP lors de la négociation des composants PPP, y compris LCP, Authentication et NCP. Une négociation

PPP réussie ouvre d'abord l'état LCP, puis s'authentifie et négocie finalement NCP (généralement IPCP).

- **debug vpdn event** : affiche des messages sur les événements qui font partie de l'établissement ou de l'arrêt normal du tunnel.
- **debug vpdn error** - Affiche les erreurs qui empêchent l'établissement d'un tunnel ou les erreurs qui provoquent la fermeture d'un tunnel établi.
- **debug vpdn l2x-event** : affiche des messages sur les événements qui font partie de l'établissement ou de l'arrêt normal du tunnel pour L2x.
- **debug vpdn l2x-error** - Affiche les erreurs de protocole L2x qui empêchent l'établissement de L2x ou empêchent son fonctionnement normal.

Remarque : Certaines de ces lignes de **débogage** sont divisées en plusieurs lignes à des fins d'impression.

Activez les commandes **debug** spécifiées ci-dessus sur le LNS et lancez un appel à partir du PC client Windows 2000. Les débogages ici montrent la demande de tunnel du client, l'établissement du tunnel, l'authentification du client et la renégociation de l'adresse 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.
```

Ce résultat de débogage sur le LNS montre le client Windows 2000 qui déconnecte l'appel. Notez les différents messages dans lesquels le LNS reconnaît la déconnexion et effectue un arrêt propre du 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
```

Informations connexes

- Configuration des clients Cisco IOS et Windows 2000 pour L2TP à l'aide de Microsoft IAS
- Présentation de VPDN
- Configuration VPDN sans AAA
- Configuration de l'authentification du protocole L2TP (Layer 2 Tunnel Protocol) avec RADIUS
- Configuration d'un serveur d'accès avec des PRI pour les appels asynchrones et RNIS entrants
- Pages d'assistance sur la technologie de numérotation
- Support technique - Cisco Systems