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

Contenu

Introduction

Dans la plupart des scénarios de Réseau privé virtuel à accès commuté (VPDN), le client compose le serveur d'accès à distance (NAS). Le NAS initie alors le protocol (L2TP) de tunnel de la couche 2 VPDN ou le tunnel de protocole de l'expédition de la couche 2 (L2F) à la passerelle domestique (HGW). Ceci crée une connexion VPDN entre le NAS, qui est le point final de concentrateur d'accès L2TP (LAC), et le HGW, qui est le point final du serveur de réseau L2TP (LNS). Ceci signifie que seulement le lien entre le NAS et le HGW utilise L2TP, et que le tunnel n'inclut pas le lien du PC client au NAS. Cependant, les clients PC exécutant le système d'exploitation Windows 2000 peuvent maintenant devenir le LAC et initier un tunnel L2TP du PC, par le NAS et terminé sur le HGW/LNS. Cette configuration d'échantillon affiche comment vous pouvez configurer un tel tunnel.

Conditions préalables

Conditions requises

Avant de tenter cette configuration, assurez-vous que vous répondez à ces exigences :

- Connaissance de comprendre VPDN
- Connaissance de synthèse d'accès distant d'Access VPDN utilisant L2TP

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

Composants utilisés

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

- LNS : Version de logiciel 12.2(1) courante de Cisco IOS® de routeur de gamme Cisco 7200
- Client : PC de Windows 2000 avec un modem

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

La configuration pour le LNS inclus dans ce document n'est pas particularité de plate-forme et peut être appliquée à tout routeur VPDN-capable.

La procédure pour configurer le PC client de Windows 2000 s'applique seulement dans le Windows 2000 et pas à n'importe quel autre système d'exploitation.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Informations générales

Comme mentionné dans l'introduction, avec le Windows 2000 vous pouvez initier un tunnel L2TP du PC client et avoir le tunnel terminé n'importe où en réseau de fournisseur de services Internet (ISP). Utilisant la terminologie VPDN, cette installation désigné sous le nom d'un tunnel « client-initié ». Puisque les tunnels client-initiés sont des tunnels initiés par le logiciel client sur le PC, le PC prend le rôle du LAC. Puisque le client sera authentifié utilisant le Protocole point à point (PPP), le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol), ou le Password Authentication Protocol (PAP) de toute façon, le tunnel lui-même n'a pas besoin d'être authentifié.

Avantages et inconvénients d'utiliser les tunnels client-initiés

les tunnels Client-initiés ont des avantages et des inconvénients, certains dont sont tracés les grandes lignes ici :

Avantages :

- Il sécurise la connexion entière du client par le réseau partagé par ISP et au réseau d'entreprise.
- Il n'exige pas la configuration supplémentaire sur le réseau ISP. Sans tunnel client-initié, le NAS ISP ou son serveur Radius/TACACS+ doit être configuré pour initier le tunnel au HGW.

Par conséquent, l'entreprise doit être en pourparlers avec beaucoup d'ISP pour permettre à des utilisateurs pour percer un tunnel par leur réseau. Avec un tunnel client-initié, l'utilisateur final peut se connecter à n'importe quel ISP et manuellement puis initier le tunnel au réseau d'entreprise.

Inconvénients :

- Il n'est pas aussi extensible qu'un tunnel ISP-initié. Puisque les tunnels client-initiés créent différents tunnels pour chaque client, le HGW doit individuellement terminer un grand nombre de tunnels.
- Le client doit gérer le logiciel client utilisé pour initier le tunnel. C'est souvent une source des problèmes support support pour l'entreprise.
- Le client doit avoir un compte avec l'ISP. Puisque des tunnels client-initiés peuvent seulement être créés après qu'une connexion à l'ISP soit établie, le client doit avoir un compte à connecter au réseau ISP.

Comment cela fonctionne

Thjs est comment l'exemple dans ce document fonctionne :

1. Le PC client introduit dans le NAS, authentifie utilisant le compte ISP du client, et obtient une adresse IP de l'ISP.
2. Le client initie et établit le tunnel L2TP au serveur de réseau HGW (LNS) L2TP. Le client renégociera le protocole de contrôle IP (IPCP) et obtiendra une nouvelle adresse IP du LNS.

Configurez le client de Windows 2000 pour L2TP

Créez deux connexions (BRUNES GRISÂTRE) de réseau de connexion à distance :

- Une connexion BRUNE GRISÂTRE à l'accès distant à l'ISP. Référez-vous à votre ISP pour plus d'informations sur ce sujet.
- Des autres connexion BRUNE GRISÂTRE pour le tunnel L2TP.

Pour créer et configurer la connexion BRUNE GRISÂTRE pour L2TP, exécutez ces étapes sur le PC client de Windows 200 :

1. Dès le début le menu, le sélectionnez Settings **> le panneau de configuration > le réseau et des connexions de connexion à distance > établissent le nouveau rapport**.Utilisez l'assistant pour créer une connexion appelée le L2TP. Veillez à sélectionner **se connectent à un réseau privé par l'Internet** dans la fenêtre de **type de connexion réseau**. Vous devez également spécifier l'adresse IP ou le nom du LNS/HGW.
2. La nouvelle connexion (L2TP Désigné) apparaît dans la fenêtre de **connexions de réseau et de connexion à distance** sous le panneau de configuration. D'ici, clic droit pour éditer **Properties**.
3. Cliquez sur l'onglet Mise en réseau et assurez-vous que le **type de serveur que j'appelle** est placé à **L2TP**.
4. Si vous prévoyez d'allouer une adresse interne dynamique (de réseau d'entreprise) à ce client du HGW, par un groupe local ou le DHCP, **protocole TCP/IP** choisi. Assurez-vous que le client est configuré pour obtenir une adresse IP automatiquement. Vous pouvez également émettre les informations de système de noms de domaine (DN) automatiquement.**Le bouton avancé** te permet pour définir Windows Internet Naming Service

statique (WINS) et l'information DNS. L'onglet d'**options** te permet pour arrêter IPSec ou pour assigner une stratégie différente à la connexion. Sous l'onglet Sécurité, vous pouvez définir les paramètres d'authentification de l'utilisateur. Par exemple, PAP, CHAP, ou MS-CHAP, ou connexion de domaine windows. Consultez l'administrateur du système de réseau pour les informations sur les paramètres qui devraient être configurés sur le client.

5. Une fois que la connexion est configurée, vous pouvez la double-cliquer pour s'afficher l'écran de connexion, et puis vous connectez.

Remarques complémentaires

Si votre tunnel L2TP utilise la sécurité IP (IPSec) et/ou le cryptage point par point de Microsoft (MPPE), alors vous devez définir cette commande sous la configuration de modèle virtuel sur le LNS/HGW.

```
ppp encrypt mppe 40
```

Maintenez dans l'esprit que ceci exige l'ensemble de caractéristiques chiffré de logiciel de Cisco IOS (au moins l'ensemble de caractéristiques d'IPSec ou l'IPSec avec 3DES).

Par défaut, IPSec est activé sur le Windows 2000. Si vous voulez le désactiver, vous devez modifier le registre de Windows utilisant Registry Editor :

Débronchement IPSec sur un PC Win2K

Avertissement : Prenez les précautions adéquates (telles que sauvegarder le registre) avant de modifier le registre. Vous devriez également se référer au site Web de Microsoft pour que la procédure correcte modifie le registre.

Pour ajouter la valeur de registre de ProhibitIpSec à votre ordinateur de Windows 2000-based, utilisation Regedt32.exe de 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 de Windows 2000-based pour que les modifications les prennent effet. Veuillez se référer à ces articles de Microsoft pour d'autres détails.

- Q258261 - Désactivant la stratégie IPSec utilisée avec L2TP
- Q240262- Comment configurer une connexion L2TP/IPSec utilisant une clé pré-partagée

Pour une installation plus complexe utilisant le Windows 2000, référez-vous à configurer le Cisco IOS et les clients de Windows 2000 pour L2TP utilisant Microsoft IAS.

Configurez

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

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

Le schéma de réseau ci-dessous affiche les diverses négociations qui se produisent parmi le PC client, le NAS ISP, et l'entreprise HGW. L'exemple de débogage dans la section de dépannage dépeint ces transactions aussi bien.

Configurations

Ce document utilise la configuration suivante :

- fifi (VPDN LNS/HGW)

Remarque: Seulement la section afférente 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
```

Vérifiez

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 au sujet de tunnel actif et d'identificateurs de message L2x dans un VPDN.

- **fenêtre de show vpdn session** — Affiche des informations sur la fenêtre pour la session VPDN.
- **utilisateur d'exposition** — Fournit une liste complète de tous les utilisateurs connectés au routeur.
- **détail de** *nom d'utilisateur d'***utilisateur de show caller** — Pour afficher des paramètres pour l'utilisateur particulier, tel que le Link Control Protocol (LCP), états de NCP et IPCP, aussi bien que l'adresse IP assignée, paramètres d'ensemble de PPP et de PPP, et ainsi de suite.

```
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
```

Dépannez

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 de **débogage**, référez-vous aux informations importantes sur des commandes de debug.

- **debug ppp negotiation** — Affiche des informations sur le trafic PPP et des échanges tout en négociant les composants de PPP comprenant LCP, authentification, et NCP. Une négociation PPP réussie d'abord ouvre l'état LCP, puis authentifie, et négocie finalement le NCP (habituellement IPCP).
- **événement de debug vpdn** — Affiche des messages au sujet des événements qui sont partie de l'établissement normal d'un tunnel ou arrêt.
- **erreur de debug vpdn** — Affiche les erreurs qui empêchent un tunnel d'être établi ou les erreurs qui causent un tunnel établi d'être fermé.
- **debug vpdn l2x-event** — Affiche des messages au sujet des événements qui sont partie de

l'établissement normal d'un tunnel ou arrêt pour L2x.

- **debug vpdn l2x-error** — Affiche les erreurs de protocole L2x qui empêchent l'établissement L2x ou empêchent son fonctionnement normal.

Remarque: Certaines de ces lignes de **sortie de débogage** sont divisées en plusieurs lignes pour des raisons d'impression.

Activez les commandes de **débogage** spécifiées ci-dessus sur le LNS et initiez un appel du PC client de Windows 2000. Met au point ici l'exposition la demande de tunnel du client, de l'établissement du tunnel, de l'authentification du client, et de 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.*

Cette sortie de débogage sur le LNS affiche le client de Windows 2000 déconnectant l'appel. Notez les divers messages où le LNS identifie le débranchement et exécute 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
- Configurer un serveur d'accès avec PRIs pour l'asynchrone entrant et les appels RNIS
- Pages d'assistance sur la technologie de numérotation
- Support technique - Cisco Systems