

Configuration et désinstallation du tunnel L2TP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[PPP](#)

[L2TP](#)

[Le PPP et les L2TP circulent le résumé](#)

[L'ordre de connexion PPP/L2TP](#)

[Debug pris du LAC qui établissement affiche de PPP et L2TP appel](#)

[Debug pris du LNS qui établissement affiche de PPP et L2TP appel](#)

[L'ordre de débranchement PPP/L2TP](#)

[Debug pris du LAC qui affiche le débranchement de PPP et L2TP](#)

[Debug pris du LNS qui affiche le débranchement de PPP et L2TP](#)

[Informations connexes](#)

Introduction

Ce document discute l'installation et la désinstallation de tunnel de protocole (L2TP) de perçage d'un tunnel de la couche deux. Le document fournit également un résumé de PPP et de L2TP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur des versions de logiciel 12.0(1)T et ultérieures de Cisco IOS®.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

PPP

Le PPP est un protocole peer-to-peer symétrique qui transporte le trafic L2 et de couche 3 (L3) au-dessus des liens point par point. Il y a trois composants principaux :

- Encapsulation
- Link Control Protocol (LCP)
- Protocole de contrôle de réseau (NCP)

Des datagrammes sont encapsulés dans le PPP. Le LCP tient compte de la négociation des options de configuration de permettre l'établissement d'une liaison. NCPs sont négociés pour chacun des protocoles L3 qui fonctionne sur le lien.

Pendant la vie d'une session PPP, le lien va cependant quatre phases distinctes :

- Établissement de lien — En tant qu'élément du lien établissant la phase, le PPP utilise une fonction LCP qui doit être terminée et ouvert avoué avant que le lien entre dans la phase d'authentification, si c'est approprié, et négocie l'ouverture de la couche réseau. LCP est également utilisé pour terminer le lien de PPP.
- Authentification — La phase d'authentification est implémentation-particularité et n'est pas une condition obligatoire pour un mouvement de LCP au NCP. Si négocié et convenu pendant la phase LCP, le pair distant doit s'identifier et passer la méthode d'authentification convenue avant que le PPP se déplace à la couche réseau.
- Couche réseau — La négociation de NCP s'assure que les deux pairs conviennent sur les caractéristiques du protocole L3. Dans le cas de l'IP, le protocole de contrôle s'appelle le protocole de contrôle IP (IPCP). En plus de la négociation entre les pairs, il y a également un élément d'affectation. C'est commun avec les clients de remote-access de Windows-type de Microsoft qui n'ont aucune adresse IP allouée et comptent sur le fournisseur de services pour allouer l'adresse IP sur la connexion.
- Arrêt de lien — La phase de terminaison de lien peut être écrite à tout moment pendant le cycle de vie de l'appel. LCP est utilisé pour fournir la demande d'arrêt.

L2TP

L2TP étend la nature point par point du PPP. L2TP fournit une méthode d'encapsulation pour la transmission des trames PPP percées un tunnel, qui permet les points finaux de PPP à percer un tunnel au-dessus d'un réseau de commutation de paquets. L2TP le plus généralement est déployé dans les scénarios de distant-Access-type qui emploient l'Internet pour offrir des services d'intranet-type. Le concept est celui d'un réseau privé virtuel (VPN).

Les deux éléments physiques primaires de L2TP sont le concentrateur L2TP Access (LAC) et le serveur de réseau L2TP (LNS) :

- LAC — Le LAC est un pair au LNS qui agit en tant qu'un côté du périphérique du tunnel. Le LAC termine la connexion PPP distante et se repose entre le distant et le LNS. Des paquets sont expédiés à et de la connexion distante au-dessus de la connexion PPP. Des paquets à

et du LNS sont expédiés au-dessus du tunnel L2TP.

- LNS — Le LNS est un pair au LAC qui agit en tant qu'un côté du périphérique du tunnel. Le LNS est le point d'arrêt pour les sessions percées un tunnel par PPP de LAC. Ceci est utilisé pour agréger les sessions PPP et le d'entrée LAC-percés un tunnel par multiple dans le réseau privé.

Il y a deux types de message différents que L2TP utilise :

- Messages de contrôle — L2TP passe des messages de contrôle et de données au-dessus du contrôle et des voies de transmission de données distincts. Le canal de contrôle d'intrabande passe la Gestion ordonnancée de connexion de contrôle, le programme de maintenance, le rapport d'erreurs, et les messages de Contrôle de session. L'initiation de la connexion de contrôle n'est pas spécifique au LAC ou au LNS mais, plutôt, au créateur de tunnel et au récepteur qui a la pertinence dans l'établissement de la connexion de contrôle. Une méthode d'authentification de défi de partager-secret est utilisée entre les périphériques du tunnel.
- Messages de données — Des messages de données sont utilisés pour encapsuler les trames PPP qui sont envoyées dans le tunnel L2TP.

L2TP utilise le port enregistré 1701 de Protocole UDP (User Datagram Protocol), et le paquet entier L2TP est encapsulé dans le datagramme UDP. Selon l'exécution normale d'UDP, le demandeur de tunnel sélectionne un port UDP disponible et envoie le numéro de port 1701 à la destination d'UDP. Dans la réponse, le nombre de destination port est identique que le numéro de port de source qui est utilisé dans l'en-tête entrante d'UDP. Le port de source est placé sur la base de n'importe quel port franc qui est trouvé. Après la source et les destinations port sont établis, les ports doit rester les mêmes pour la durée du tunnel. En logiciel de Cisco IOS, la source et les nombres de destination port sont toujours placés au numéro de port UDP 1701.

Remarque: Posez 2 (L2F) Protocol de transmission et L2TP partagent le même numéro de port UDP. Le champ de version dans l'en-tête te permet de distinguer entre les deux protocoles. Une valeur de 1 indique L2F, et une valeur de 2 indique L2TP.

[Le PPP et les L2TP circulent le résumé](#)

L'établissement de la connexion et de la session de contrôle doit se produire avant que des trames PPP puissent être expédiées par le tunnel.

Après l'établissement réussi du canal de contrôle, des sessions sont créées pour chaque connexion PPP. L'établissement de session est directionnel, par rapport au LAC et au LNS. Pour des appels entrant, le LAC invite le LNS pour recevoir la session. Pour des appels sortants, le LNS demande au LAC pour recevoir la session.

La section d'[ordre de connexion PPP/L2TP de](#) ce document détaille l'établissement d'appel de PPP et L2TP quand un utilisateur de remote-access place un appel dans le LAC. Cet exemple emploie le Service d'identification du numéro composé réacheminé (RDNIS) afin d'initier le tunnel L2TP, bien que vous puissiez également utiliser le nom de domaine à cet effet. L'ordre affiche le début de la session PPP d'un routeur SOHO 2500, de la négociation LCP entre l'utilisateur de remote-access et le LAC, et de l'authentification partielle. Le LAC poursuit alors pour établir le tunnel L2TP et la session dans le tunnel. Une session est établie pour chaque connexion PPP entre le LAC et le LNS. L2TP utilise le tunnel de pair et les identifiants de session dans tous les messages sortants afin de multiplexer et démultiplexer des connexions PPP. Ces identifiants sont assignés et permutés pendant la connexion et les phases d'établissement de session respectives de contrôle. Les id de tunnel et de session ont la portée locale seulement. Les périphériques du

tunnel ont différents identifiants pour le mêmes tunnel et session.

Remarque: La valeur 0 a la seule importance et est seulement utilisée quand le tunnel et l'identifiant de session ont pour être assignés encore.

Après l'établissement du tunnel, la procédure d'authentification de PPP se termine entre l'utilisateur de remote-access et le LNS. Le LAC continue à recevoir des trames PPP. Le tramage et le contrôle de redondance cyclique (CRC) de lien sont retirés, encapsulés dans L2TP, et expédiés dans le tunnel au LNS. Là, le paquet L2TP est reçu et traité comme si il ont été terminés sur une interface locale de PPP. La négociation du NCP de PPP se produit, et alors IPCP est ouvert avoué. La connexion est complète.

L'ordre de connexion PPP/L2TP

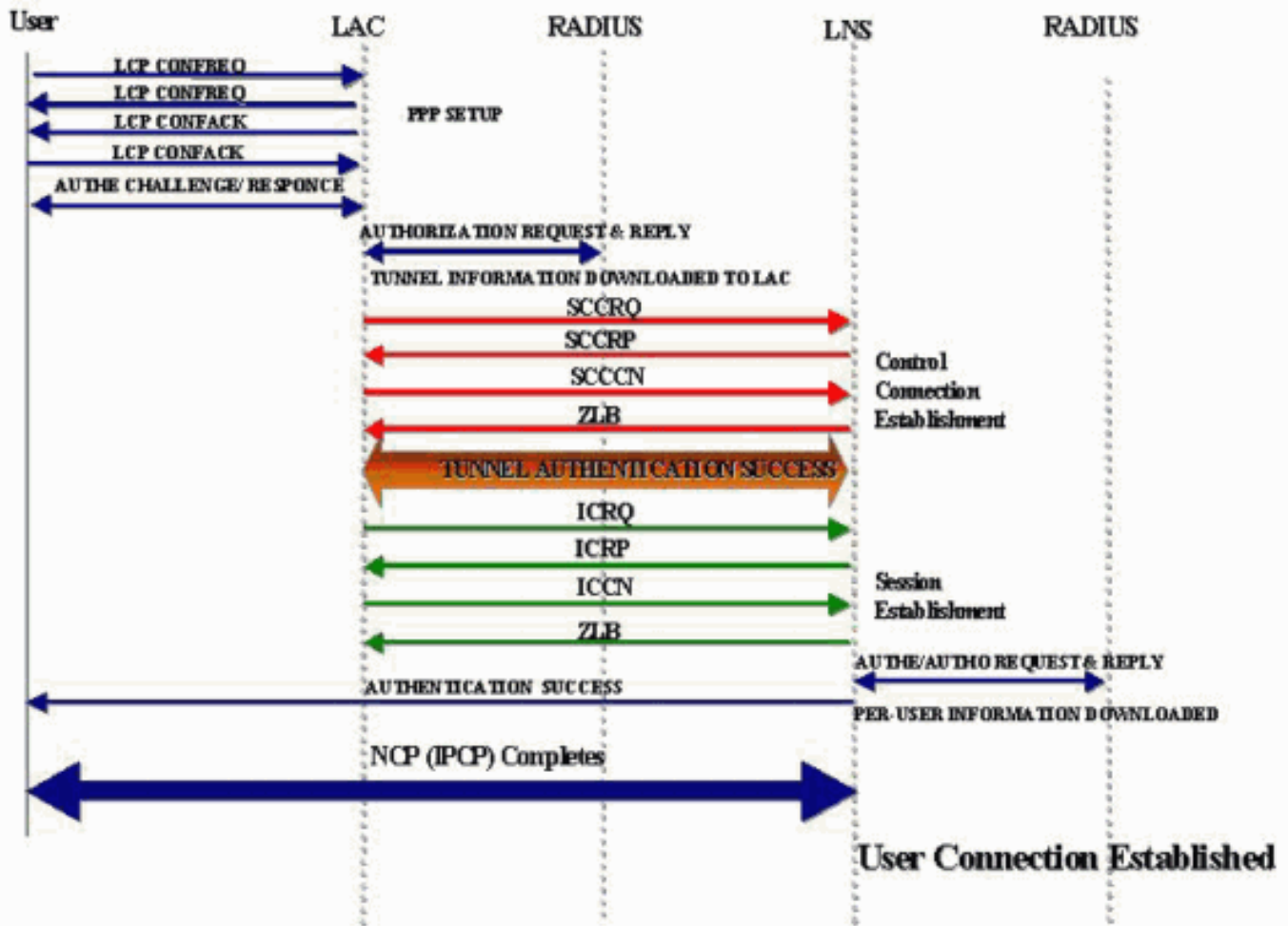
C'est la séquence de connexion d'opérations :

1. L'utilisateur distant initie une connexion PPP. Le LAC reçoit la connexion. Un lien de PPP est établi.
2. LCP est négocié entre l'utilisateur distant et le LAC. Le LAC émet un défi de protocole d'authentification CHAP (Challenge Handshake Authentication Protocol) afin d'exécuter une authentification partielle de l'utilisateur distant. La réponse est envoyée au LNS pendant l'établissement de session. La réponse est envoyée en tant que réponse de l'authentification de proxy 33 de la paire de valeurs d'attribut (AVP) dans Entrant-Appel-connecté (ICCN).
3. Le DNIS est utilisé pour déterminer si l'utilisateur est un client de Réseau privé virtuel à accès commuté (VPDN).
4. Puisqu'il n'y a aucun tunnel existant pour le numéro composé (614629), la création d'un nouveau tunnel est nécessaire. Le RAYON est questionné et les informations de tunnel sont téléchargées au LAC.
5. La connexion de contrôle est commencée. Le tunnel est dans un état libre :Le demandeur de tunnel (dans ce cas, le LAC) envoie une Commencement-Contrôle-Connexion-demande (SCCRQ) au LNS. Le SCCRQ contient un défi AVP 11, qui indique que le LAC veut authentifier le tunnel avec l'utilisation d'une authentification de style de la CHAP. Le même secret est connu aux deux périphériques du tunnel. Le tunnel est maintenant dans un état WAIT-CTL-REPLY.Le LNS peut évoquer le tunnel, ainsi les réponses LNS avec une Commencement-Contrôle-Connexion-réponse (SCCRP). Le SCCRP contient un défi AVP 11 et une réponse de défi AVP 13 en réponse au SCCRQ. Le tunnel est maintenant dans un état WAIT-CTL-REPLY.Le LAC répond avec un message (SCCCN) Commencement-Contrôle-Connexion-connecté. Le SCCCN contient un AVP 13 en réponse au SCCRP. Le tunnel est maintenant dans un état établi.Le LNS envoie un message du corps de Zéro-longueur (ZLB) au LAC. Le message ZLB est un accusé de réception ordonnancé. Le tunnel est maintenant dans un état établi.
6. L'authentification de tunnel est maintenant complète et le tunnel est établi. La session est maintenant dans un état libre.
7. Maintenant que le tunnel existe, un échange à trois voies pour l'établissement de session dans le tunnel est exécuté :Le LAC envoie une Entrant-Appel-demande (ICRQ) avec les informations de paramètre pour la session. La session est maintenant dans un état de réponse d'attente.Le LNS envoie une Entrant-Appel-réponse (I'ICRP) qui contient l'ID de session. La session est maintenant dans une attente connectent l'état.Le LAC envoie un ICCN et fournit au LNS les informations complémentaires pour l'appel répondu. Ces

informations incluent les informations LCP de la négociation que le LAC et l'utilisateur distant ont exécutée. La session est maintenant dans un état établi. Le LNS envoie un message ZLB, qui est un accusé de réception ordonnancé, au LAC. La session est maintenant dans un état établi.

8. Après l'établissement de la session, une interface d'accès virtuelle est créée sur le LNS. Les informations de configuration LCP qui ont été fournies dans l'ICCN sont forcées sur la pile virtuelle de PPP d'interface d'accès. Ces informations incluent les informations d'authentification partielles.
9. Le LNS génère un défi d'authentification. La réponse AVP 33 d'authentification de proxy, qui a été fournie dans l'ICCN, est rejouée.
10. L'Authentification, autorisation et comptabilité (AAA) ou l'authentification et l'autorisation normal de PPP a lieu.
11. Une Access-demande de RAYON est envoyée pour l'authentification et l'autorisation de par-utilisateur.
12. UN RAYON Access-Recevoir est reçu. **Remarque:** Le RAYON a été configuré pour permettre l'adresse IP que l'utilisateur distant a offerte dans la Configurer-demande entrante IPCP.
13. Un message de succès de CHAP est envoyé à l'utilisateur distant.
14. La négociation de PPP IPCP se termine et est OUVRETE avoué. Une route hôte est installée sur l'interface distante. L'utilisateur distant est maintenant connecté, et la circulation peut débuter.

Écoulement d'appel de connexion de PPP et L2TP



Debug pris du LAC qui établissement affiche de PPP et L2TP appel

```

Jan 1 00:04:10.235: %LINK-3-UPDOWN: Interface Serial0:0,
changed state to up
Jan 1 00:04:10.455: Se0:0 PPP: Treating connection as a callin
Jan 1 00:04:10.455: Se0:0 PPP: Phase is ESTABLISHING,
Passive Open [0 sess, 0 load]
Jan 1 00:04:10.455: Se0:0 CHAP: Using alternate hostname 5300-1
Jan 1 00:04:10.455: Se0:0 LCP: State is Listen Jan 1 00:04:10.455: Se0:0 LCP: I CONFREQ [Listen]
id 118 len 10 Jan 1 00:04:10.455: Se0:0 LCP: MagicNumber 0x6EE4E865 (0x05066EE4E865) Jan 1
00:04:10.455: Se0:0 CHAP: Using alternate hostname 5300-1 Jan 1 00:04:10.455: Se0:0 LCP: O
CONFREQ [Listen] id 11 len 28 Jan 1 00:04:10.455: Se0:0 LCP: AuthProto CHAP (0x0305C22305) Jan 1
00:04:10.455: Se0:0 LCP: MagicNumber 0x109D08F2 (0x0506109D08F2) Jan 1 00:04:10.455: Se0:0 LCP:
MRRU 1524 (0x110405F4) Jan 1 00:04:10.455: Se0:0 LCP: EndpointDisc 1 Local
(0x130901353330302D31) Jan 1 00:04:10.455: Se0:0 LCP: O CONFACK [Listen] id 118 len 10 Jan 1
00:04:10.455: Se0:0 LCP: MagicNumber 0x6EE4E865 (0x05066EE4E865) Jan 1 00:04:10.495: Se0:0 LCP:
I CONFREJ [ACKsent] id 11 len 17 Jan 1 00:04:10.495: Se0:0 LCP: MRRU 1524 (0x110405F4) Jan 1
00:04:10.495: Se0:0 LCP: EndpointDisc 1 Local (0x130901353330302D31) Jan 1 00:04:10.495: Se0:0
LCP: O CONFREQ [ACKsent] id 12 len 15 Jan 1 00:04:10.495: Se0:0 LCP: AuthProto CHAP
(0x0305C22305) Jan 1 00:04:10.495: Se0:0 LCP: MagicNumber 0x109D08F2 (0x0506109D08F2) Jan 1
00:04:10.527: Se0:0 LCP: I CONFACK [ACKsent] id 12 len 15 Jan 1 00:04:10.527: Se0:0 LCP:
AuthProto CHAP (0x0305C22305) Jan 1 00:04:10.527: Se0:0 LCP: MagicNumber 0x109D08F2
(0x0506109D08F2) Jan 1 00:04:10.527: Se0:0 LCP: State is Open Jan 1 00:04:10.527: Se0:0 PPP:
Phase is AUTHENTICATING, by this end [0 sess, 0 load] Jan 1 00:04:10.527: Se0:0 CHAP: Using
alternate hostname 5300-1 Jan 1 00:04:10.527: Se0:0 CHAP: O CHALLENGE id 6 len 27 from "5300-1"
Jan 1 00:04:10.555: Se0:0 CHAP: I RESPONSE id 6 len 27 from "2500-1" Jan 1 00:04:10.555: Se0:0
PPP: Phase is FORWARDING [0 sess, 0 load] Jan 1 00:04:10.555: Se0:0 VPDN: Got DNIS string 614629
Jan 1 00:04:10.555: Se0:0 VPDN: Looking for tunnel -- dnis:614629 -- Jan 1 00:04:10.555:
Serial0:0 AAA/AUTHOR/VPDN (1692520761): Port='Serial0:0' list='default' service=NET Jan 1

```

00:04:10.555: AAA/AUTHOR/VPDN: Serial0:0 (1692520761) user='dnis:614629' Jan 1 00:04:10.555: Serial0:0 AAA/AUTHOR/VPDN (1692520761): send AV service=ppp Jan 1 00:04:10.555: Serial0:0 AAA/AUTHOR/VPDN (1692520761): send AV protocol=vpdn Jan 1 00:04:10.555: Serial0:0 AAA/AUTHOR/VPDN (1692520761): found list "default" Jan 1 00:04:10.555: Serial0:0 AAA/AUTHOR/VPDN (1692520761): Method=NSA_LAB (radius) Jan 1 00:04:10.559: RADIUS: Initial Transmit Serial0:0 id 18 10.51.6.3:1645, Access-Request, len 112 Jan 1 00:04:10.559: Attribute 4 6 0A330644 Jan 1 00:04:10.559: Attribute 5 6 00000000 Jan 1 00:04:10.559: Attribute 26 17 00000009020B5365 Jan 1 00:04:10.559: Attribute 61 6 00000002 Jan 1 00:04:10.559: Attribute 1 13 646E6973 Jan 1 00:04:10.559: Attribute 30 8 36313436 Jan 1 00:04:10.559: Attribute 31 12 32303835 Jan 1 00:04:10.559: Attribute 2 18 D0A81832 Jan 1 00:04:10.559: Attribute 6 6 00000005 Jan 1 00:04:10.559: RADIUS: Received from id 18 10.51.6.3:1645, Access-Accept, len 156 Jan 1 00:04:10.559: Attribute 6 6 00000005 Jan 1 00:04:10.559: Attribute 26 29 0000000901177670 Jan 1 00:04:10.559: Attribute 26 26 0000000901147670 Jan 1 00:04:10.559: Attribute 26 36 00000009011E7670 Jan 1 00:04:10.559: Attribute 26 39 0000000901217670 Jan 1 00:04:10.563: RADIUS: saved authorization data for user 626A0C10 at 62258960 Jan 1 00:04:10.563: RADIUS: cisco AVPair "vpdn:tunnel-type=l2tp" Jan 1 00:04:10.563: RADIUS: cisco AVPair "vpdn:tunnel-id=hgw" Jan 1 00:04:10.563: RADIUS: cisco AVPair "vpdn:ip-addresses=10.51.6.82" Jan 1 00:04:10.563: RADIUS: cisco AVPair "vpdn:l2tp-tunnel-password=hello" Jan 1 00:04:10.563: AAA/AUTHOR (1692520761): Post authorization status = PASS_ADD Jan 1 00:04:10.563: AAA/AUTHOR/VPDN: Processing AV service=ppp Jan 1 00:04:10.563: AAA/AUTHOR/VPDN: Processing AV protocol=vpdn Jan 1 00:04:10.563: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp Jan 1 00:04:10.563: AAA/AUTHOR/VPDN: Processing AV tunnel-id=hgw Jan 1 00:04:10.563: AAA/AUTHOR/VPDN: Processing AV ip-addresses=10.51.6.82 Jan 1 00:04:10.563: AAA/AUTHOR/VPDN: Processing AV l2tp-tunnel-password=hello Jan 1 00:04:10.563: Se0:0 VPDN/RPMS/: Got tunnel info for dnis:614629 Jan 1 00:04:10.563: Se0:0 VPDN/RPMS/: LAC hgw Jan 1 00:04:10.563: Se0:0 VPDN/RPMS/: l2tp-busy-disconnect yes Jan 1 00:04:10.563: Se0:0 VPDN/RPMS/: l2tp-tunnel-password xxxxxx Jan 1 00:04:10.563: Se0:0 VPDN/RPMS/: IP 10.51.6.82 Jan 1 00:04:10.563: Se0:0 VPDN/: curlvl 1 Address 0: 10.51.6.82, priority 1 Jan 1 00:04:10.563: Se0:0 VPDN/: Select non-active address 10.51.6.82, priority 1 Jan 1 00:04:10.567: Tnl 17688 L2TP: SM State idle Jan 1 00:04:10.567: Tnl 17688 L2TP: O SCCRQ Jan 1 00:04:10.567: Tnl 17688 L2TP: O SCCRQ, flg TLS, ver 2, len 128, tnl 0, cl 0, ns 0, nr 0 C8 02 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 80 08 00 00 00 02 01 00 80 0A 00 00 00 03 00 00 00 03 80 0A 00 00 00 04 00 00 00 ... Jan 1 00:04:10.567: Tnl 17688 L2TP: Tunnel state change from idle to wait-ctl-reply Jan 1 00:04:10.567: Tnl 17688 L2TP: SM State wait-ctl-reply Jan 1 00:04:10.567: Se0:0 VPDN: Find LNS process created Jan 1 00:04:10.567: Se0:0 VPDN: Forward to address 10.51.6.82 Jan 1 00:04:10.567: Se0:0 VPDN: Pending Jan 1 00:04:10.567: Se0:0 VPDN: Process created Jan 1 00:04:10.655: Tnl 17688 L2TP: Parse AVP 0, len 8, flag 0x8000 (M) Jan 1 00:04:10.655: Tnl 17688 L2TP: Parse SCCRP Jan 1 00:04:10.655: Tnl 17688 L2TP: Parse AVP 2, len 8, flag 0x8000 (M) Jan 1 00:04:10.655: Tnl 17688 L2TP: Protocol Ver 256 Jan 1 00:04:10.655: Tnl 17688 L2TP: Parse AVP 3, len 10, flag 0x8000 (M) Jan 1 00:04:10.655: Tnl 17688 L2TP: Framing Cap 0x3 Jan 1 00:04:10.655: Tnl 17688 L2TP: Parse AVP 4, len 10, flag 0x8000 (M) Jan 1 00:04:10.655: Tnl 17688 L2TP: Bearer Cap 0x3 Jan 1 00:04:10.659: Tnl 17688 L2TP: Parse AVP 6, len 8, flag 0x0 Jan 1 00:04:10.659: Tnl 17688 L2TP: Firmware Ver 0x1120 Jan 1 00:04:10.659: Tnl 17688 L2TP: Parse AVP 7, len 13, flag 0x8000 (M) Jan 1 00:04:10.659: Tnl 17688 L2TP: Hostname l2tp-gw Jan 1 00:04:10.659: Tnl 17688 L2TP: Parse AVP 8, len 25, flag 0x0 Jan 1 00:04:10.659: Tnl 17688 L2TP: Vendor Name Cisco Systems, Inc. Jan 1 00:04:10.659: Tnl 17688 L2TP: Parse AVP 9, len 8, flag 0x8000 (M) Jan 1 00:04:10.659: Tnl 17688 L2TP: Assigned Tunnel ID 55270 Jan 1 00:04:10.659: Tnl 17688 L2TP: Parse AVP 10, len 8, flag 0x8000 (M) Jan 1 00:04:10.659: Tnl 17688 L2TP: Rx Window Size 300 Jan 1 00:04:10.659: Tnl 17688 L2TP: Parse AVP 11, len 22, flag 0x8000 (M) Jan 1 00:04:10.659: Tnl 17688 L2TP: Chlng 98B296C28429E7ADC767237A45F31040 Jan 1 00:04:10.659: Tnl 17688 L2TP: Parse AVP 13, len 22, flag 0x8000 (M) Jan 1 00:04:10.659: Tnl 17688 L2TP: Chlng Resp 7C358F7A7BA21957C07801195DCADFA6 Jan 1 00:04:10.659: Tnl 17688 L2TP: No missing AVPs in SCCRP Jan 1 00:04:10.659: Tnl 17688 L2TP: I SCCRP, flg TLS, ver 2, len 154, tnl 17688, cl 0, ns 0, nr 1 C8 02 00 9A 45 18 00 00 00 00 00 00 01 80 08 00 00 00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00 00 03 00 00 00 03 80 0A 00 00 00 04 00 00 00 ... Jan 1 00:04:10.659: Tnl 17688 L2TP: I SCCRP from l2tp-gw Jan 1 00:04:10.659: Tnl 17688 L2TP: Got a challenge from remote peer, l2tp-gw Jan 1 00:04:10.659: Tnl 17688 L2TP: Got a response from remote peer, l2tp-gw Jan 1 00:04:10.659: Tnl 17688 L2TP: Tunnel Authentication success Jan 1 00:04:10.659: Tnl 17688 L2TP: Tunnel state change from wait-ctl-reply to established Jan 1 00:04:10.663: Tnl 17688 L2TP: O SCCCN to l2tp-gw tnlid 55270 Jan 1 00:04:10.663: Tnl 17688 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl 55270, cl 0, ns 1, nr 1 C8 02 00 2A D7 E6 00 00 00 01 00 01 80 08 00 00 00 00 00 03 80 16 00 00 00 0D 96 39 53 18 41 AC 22 E3 10 3E 20 8E F7 D9 09 89 Jan 1 00:04:10.663: Tnl 17688 L2TP: SM State established Jan 1 00:04:10.663: Tnl/C1 17688/7 L2TP: Session FS enabled Jan 1 00:04:10.663: Tnl/C1 17688/7 L2TP: Session state change from idle to wait-for-tunnel Jan 1 00:04:10.663: Se0:0 Tnl/C1 17688/7 L2TP: Create session Jan 1 00:04:10.663: Tnl 17688 L2TP: SM State established Jan

1 00:04:10.663: Se0:0 Tnl/Cl 17688/7 L2TP: O ICRQ to l2tp-gw 55270/0 Jan 1 00:04:10.663: Se0:0 Tnl/Cl 17688/7 L2TP: O ICRQ, flg TLS, ver 2, len 91, tnl 55270, cl 0, ns 2, nr 1 C8 02 00 5B D7 E6 00 00 00 02 00 01 80 08 00 00 00 00 00 0A 80 08 00 00 00 0E 00 07 80 0A 00 00 00 0F D1 14 C7 C5 80 0A 00 00 00 12 00 00 00 ... Jan 1 00:04:10.667: Se0:0 Tnl/Cl 17688/7 L2TP: Session state change from wait-for-tunnel to wait-reply Jan 1 00:04:10.703: Tnl 17688 L2TP: I ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 17688, cl 0, ns 1, nr 2 Jan 1 00:04:10.795: Se0:0 Tnl/Cl 17688/7 L2TP: Parse AVP 0, len 8, flag 0x8000 (M) Jan 1 00:04:10.795: Se0:0 Tnl/Cl 17688/7 L2TP: Parse ICRP Jan 1 00:04:10.795: Se0:0 Tnl/Cl 17688/7 L2TP: Parse AVP 14, len 8, flag 0x8000 (M) Jan 1 00:04:10.795: Se0:0 Tnl/Cl 17688/7 L2TP: Assigned Call ID 45 Jan 1 00:04:10.795: Se0:0 Tnl/Cl 17688/7 L2TP: No missing AVPs in ICRP Jan 1 00:04:10.795: Se0:0 Tnl/Cl 17688/7 L2TP: I ICRP, flg TLS, ver 2, len 28, tnl 17688, cl 7, ns 1, nr 3 C8 02 00 1C 45 18 00 07 00 01 00 03 80 08 00 00 00 00 0B 80 08 00 00 00 0E 00 2D Jan 1 00:04:10.795: Se0:0 Tnl/Cl 17688/7 L2TP: O ICCN to l2tp-gw 55270/45 Jan 1 00:04:10.795: Se0:0 Tnl/Cl 17688/7 L2TP: O ICCN, flg TLS, ver 2, len 151, tnl 55270, cl 45, ns 3, nr 2 C8 02 00 97 D7 E6 00 2D 00 03 00 02 80 08 00 00 00 00 0C 80 0A 00 00 00 18 00 00 FA 00 00 0A 00 00 00 26 00 00 FA 00 80 0A 00 00 00 13 00 ... Jan 1 00:04:10.795: Se0:0 Tnl/Cl 17688/7 L2TP: Session state change from wait-reply to established Jan 1 00:04:10.899: Tnl 17688 L2TP: I ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 17688, cl 0, ns 2, nr 4 Jan 1 00:04:11.667: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0:0, changed state to up Jan 1 00:04:16.239: %ISDN-6-CONNECT: Interface Serial0:0 is now connected to 2085730592 2500-1

Debug pris du LNS qui établissement affiche de PPP et L2TP appel

Jan 1 00:04:10.916: L2X: Parse AVP 0, len 8, flag 0x0x8000 (M)
Jan 1 00:04:10.920: L2X: Parse SCCRQ
Jan 1 00:04:10.920: L2X: Parse AVP 2, len 8, flag 0x0x8000 (M)
Jan 1 00:04:10.924: L2X: Protocol Ver 256
Jan 1 00:04:10.924: L2X: Parse AVP 3, len 10, flag 0x0x8000 (M)
Jan 1 00:04:10.928: L2X: Framing Cap 0x0x3
Jan 1 00:04:10.928: L2X: Parse AVP 4, len 10, flag 0x0x8000 (M)
Jan 1 00:04:10.932: L2X: Bearer Cap 0x0x3
Jan 1 00:04:10.932: L2X: Parse AVP 6, len 8, flag 0x0x0
Jan 1 00:04:10.936: L2X: Firmware Ver 0x0x1130
Jan 1 00:04:10.936: L2X: Parse AVP 7, len 9, flag 0x0x8000 (M)
Jan 1 00:04:10.940: L2X: Hostname hgw
Jan 1 00:04:10.940: L2X: Parse AVP 8, len 25, flag 0x0x0
Jan 1 00:04:10.944: L2X: Vendor Name Cisco Systems, Inc.
Jan 1 00:04:10.948: L2X: Parse AVP 9, len 8, flag 0x0x8000 (M)
Jan 1 00:04:10.952: L2X: Assigned Tunnel ID 17688
Jan 1 00:04:10.952: L2X: Parse AVP 10, len 8, flag 0x0x8000 (M)
Jan 1 00:04:10.956: L2X: Rx Window Size 800
Jan 1 00:04:10.956: L2X: Parse AVP 11, len 22, flag 0x0x8000 (M)
Jan 1 00:04:10.960: L2X: Chlng 545A2343FBE20EA08BCA7B56E4A7D29E
Jan 1 00:04:10.964: L2X: No missing AVPs in SCCRQ
Jan 1 00:04:10.968: L2X: I SCCRQ, flg TLS, ver 2, len 128, tnl 0, cl 0, ns 0, nr 0 contiguous pak, size 128 C8 02 00 80 00 00 00 00 00 00 00 00 00 00 80 08 00 00 00 00 00 01 80 08 00 00 00 02 01 00 80 0A 00 00 00 03 00 00 00 03 80 0A 00 00 00 04 00 00 00 ... Jan 1 00:04:10.975: L2TP: I SCCRQ from hgw tnl 17688 Jan 1 00:04:10.983: Tnl 55270 L2TP: Got a challenge in SCCRQ, hgw Jan 1 00:04:10.983: Tnl 55270 L2TP: New tunnel created for remote hgw, address 10.51.6.68 Jan 1 00:04:10.987: Tnl 55270 L2TP: O SCCRP to hgw tnlid 17688 Jan 1 00:04:10.991: Tnl 55270 L2TP: O SCCRP, flg TLS, ver 2, len 154, tnl 17688, cl 0, ns 0, nr 1 Jan 1 00:04:10.999: contiguous buffer, size 154 C8 02 00 9A 45 18 00 00 00 00 00 01 80 08 00 00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00 00 03 00 00 00 03 80 0A 00 00 00 04 00 00 00 ... Jan 1 00:04:11.003: Tnl 55270 L2TP: Tunnel state change from idle to wait-ctl-reply Jan 1 00:04:11.019: Tnl 55270 L2TP: Parse AVP 0, len 8, flag 0x0x8000 (M) Jan 1 00:04:11.019: Tnl 55270 L2TP: Parse SCCCN Jan 1 00:04:11.023: Tnl 55270 L2TP: Parse AVP 13, len 22, flag 0x0x8000 (M) Jan 1 00:04:11.023: Tnl 55270 L2TP: Chlng Resp 9639531841AC22E3103E208EF7D90989 Jan 1 00:04:11.031: Tnl 55270 L2TP: No missing AVPs in SCCCN Jan 1 00:04:11.031: Tnl 55270 L2TP: I SCCCN, flg TLS, ver 2, len 42, tnl 55270, cl 0, ns 1, nr 1 contiguous pak, size 42 C8 02 00 2A D7 E6 00 00 00 01 00 01 80 08 00 00 00 00 03 80 16 00 00 00 0D 96 39 53 18 41 AC 22 E3 10 3E 20 8E F7 D9 09 89 Jan 1 00:04:11.043: Tnl 55270 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 17688, cl 0, ns 1, nr 2 Jan 1 00:04:11.047: contiguous buffer, size 12 C8 02 00 0C 45 18 00 00 00 01 00 02 Jan 1 00:04:11.051: Tnl 55270 L2TP: I SCCCN from hgw tnl 17688 Jan 1 00:04:11.055: Tnl 55270 L2TP: Got a Challenge Response in SCCCN from hgw Jan 1 00:04:11.055: Tnl 55270 L2TP: Tunnel Authentication

success Jan 1 00:04:11.059: Tnl 55270 L2TP: Tunnel state change from wait-ctl-reply to established Jan 1 00:04:11.063: Tnl 55270 L2TP: SM State established Jan 1 00:04:11.067: Tnl 55270 L2TP: Parse AVP 0, len 8, flag 0x0x8000 (M) Jan 1 00:04:11.071: Tnl 55270 L2TP: Parse ICRQ Jan 1 00:04:11.071: Tnl 55270 L2TP: Parse AVP 14, len 8, flag 0x0x8000 (M) Jan 1 00:04:11.075: Tnl 55270 L2TP: Assigned Call ID 7 Jan 1 00:04:11.075: Tnl 55270 L2TP: Parse AVP 15, len 10, flag 0x0x8000 (M) Jan 1 00:04:11.079: Tnl 55270 L2TP: Serial Number Jan 1 00:04:11.083: Tnl 55270 L2TP: Parse AVP 18, len 10, flag 0x0x8000 (M) Jan 1 00:04:11.083: Tnl 55270 L2TP: Bearer Type 1 Jan 1 00:04:11.087: Tnl 55270 L2TP: Parse AVP 22, len 16, flag 0x0x8000 (M) Jan 1 00:04:11.087: Tnl 55270 L2TP: Calling Number 2085730592 Jan 1 00:04:11.095: Tnl 55270 L2TP: Parse AVP 21, len 12, flag 0x0x8000 (M) Jan 1 00:04:11.095: Tnl 55270 L2TP: Called Number 614629 Jan 1 00:04:11.099: Tnl 55270 L2TP: Parse Cisco AVP 100, len 15, flag 0x0x0 Jan 1 00:04:11.102: Tnl 55270 L2TP: Client NAS Port Serial0:0 Jan 1 00:04:11.106: Tnl 55270 L2TP: No missing AVPs in ICRQ **Jan 1 00:04:11.106: Tnl 55270 L2TP: I ICRQ, flg TLS, ver 2, len 91, tnl 55270, cl 0, ns 2, nr 1 contiguous pak, size 91** C8 02 00 5B D7 E6 00 00 00 02 00 01 80 08 00 00 00 00 0A 80 08 00 00 00 0E 00 07 80 0A 00 00 00 0F D1 14 C7 C5 80 0A 00 00 00 12 00 00 00 ... Jan 1 00:04:11.118: Tnl 55270 L2TP: I ICRQ from hgw tnl 17688 Jan 1 00:04:11.122: Tnl/Cl 55270/45 L2TP: Session FS enabled Jan 1 00:04:11.126: Tnl/Cl 55270/45 L2TP: Session state change from idle to wait-connect Jan 1 00:04:11.126: Tnl/Cl 55270/45 L2TP: New session created Jan 1 00:04:11.130: Tnl/Cl 55270/45 L2TP: O ICRP to hgw 17688/7 **Jan 1 00:04:11.134: Tnl/Cl 55270/45 L2TP: O ICRP, flg TLS, ver 2, len 28, tnl 17688, cl 7, ns 1, nr 3** Jan 1 00:04:11.138: contiguous buffer, size 28 C8 02 00 1C 45 18 00 07 00 01 00 03 80 08 00 00 00 00 0B 80 08 00 00 00 0E 00 2D Jan 1 00:04:11.154: Tnl/Cl 55270/45 L2TP: Parse AVP 0, len 8, flag 0x0x8000 (M) Jan 1 00:04:11.158: Tnl/Cl 55270/45 L2TP: Parse ICCN Jan 1 00:04:11.162: Tnl/Cl 55270/45 L2TP: Parse AVP 24, len 10, flag 0x0x8000 (M) Jan 1 00:04:11.162: Tnl/Cl 55270/45 L2TP: Connect Speed 64000 Jan 1 00:04:11.166: Tnl/Cl 55270/45 L2TP: Parse AVP 38, len 10, flag 0x0x0 Jan 1 00:04:11.166: Tnl/Cl 55270/45 L2TP: Rx Speed 64000 Jan 1 00:04:11.170: Tnl/Cl 55270/45 L2TP: Parse AVP 19, len 10, flag 0x0x8000 (M) Jan 1 00:04:11.174: Tnl/Cl 55270/45 L2TP: Framing Type 2 Jan 1 00:04:11.174: Tnl/Cl 55270/45 L2TP: Parse AVP 27, len 17, flag 0x0x0 Jan 1 00:04:11.178: Tnl/Cl 55270/45 L2TP: Last Sent LCPREQ 0305C223050506109D08F2 Jan 1 00:04:11.182: Tnl/Cl 55270/45 L2TP: Parse AVP 28, len 12, flag 0x0x0 Jan 1 00:04:11.186: Tnl/Cl 55270/45 L2TP: Last Rx LCPREQ 05066EE4E865 Jan 1 00:04:11.190: Tnl/Cl 55270/45 L2TP: Parse AVP 31, len 22, flag 0x0x0 Jan 1 00:04:11.194: Tnl/Cl 55270/45 L2TP: Proxy Auth Chal 5D0D008CB1677CF8BC354556321A7A74 Jan 1 00:04:11.198: Tnl/Cl 55270/45 L2TP: Parse AVP 32, len 8, flag 0x0x0 Jan 1 00:04:11.202: Tnl/Cl 55270/45 L2TP: Proxy Auth ID 6 Jan 1 00:04:11.206: Tnl/Cl 55270/45 L2TP: Parse AVP 30, len 12, flag 0x0x0 Jan 1 00:04:11.206: Tnl/Cl 55270/45 L2TP: Proxy Auth Name 2500-1 Jan 1 00:04:11.210: Tnl/Cl 55270/45 L2TP: Parse AVP 33, len 22, flag 0x0x8000 (M) Jan 1 00:04:11.214: Tnl/Cl 55270/45 L2TP: Proxy Auth Resp CA1CC2E4FA6899E8DF1B695C0A80883E Jan 1 00:04:11.222: Tnl/Cl 55270/45 L2TP: Parse AVP 29, len 8, flag 0x0x0 Jan 1 00:04:11.222: Tnl/Cl 55270/45 L2TP: Proxy Auth Type 2 Jan 1 00:04:11.225: Tnl/Cl 55270/45 L2TP: No missing AVPs in ICCN **Jan 1 00:04:11.229: Tnl/Cl 55270/45 L2TP: I ICCN, flg TLS, ver 2, len 151, tnl 55270, cl 45, ns 3, nr 2 contiguous pak, size 151** C8 02 00 97 D7 E6 00 2D 00 03 00 02 80 08 00 00 00 00 0C 80 0A 00 00 00 18 00 00 FA 00 00 0A 00 00 00 26 00 00 FA 00 80 0A 00 00 00 13 00 ... **Jan 1 00:04:11.241: Tnl/Cl 55270/45 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 17688, cl 0, ns 2, nr 4** Jan 1 00:04:11.245: contiguous buffer, size 12 C8 02 00 0C 45 18 00 00 00 02 00 04 Jan 1 00:04:11.249: Tnl/Cl 55270/45 L2TP: I ICCN from hgw tnl 17688, cl 7 Jan 1 00:04:11.253: Tnl/Cl 55270/45 L2TP: Session state change from wait-connect to established Jan 1 00:04:11.257: Vi4 VTEMPLATE: Hardware address 0030.94fe.1bbf Jan 1 00:04:11.257: Vi4 VPDN: Virtual interface created for 2500-1 **Jan 1 00:04:11.261: Vi4 PPP: Phase is DOWN, Setup** Jan 1 00:04:11.261: Vi4 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking Jan 1 00:04:11.265: Vi4 VTEMPLATE: Has a new cloneblk vtemplate, now it has vtemplate Jan 1 00:04:11.269: Vi4 VTEMPLATE: ***** CLONE VACCESS4 ***** Jan 1 00:04:11.273: Vi4 VTEMPLATE: Clone from Virtual-Templatel interface Virtual-Access4 default ip address no ip address encaps ppp ip unnumbered Ethernet0 no peer default ip address ppp authentication chap vpdn ppp authorization vpdn peer default ip address pool default ppp mu end Jan 1 00:04:12.892: %LINK-3-UPDOWN: Interface Virtual-Access4, changed state to up Jan 1 00:04:12.908: Vi4 PPP: Using set call direction Jan 1 00:04:12.908: Vi4 PPP: Treating connection as a callin Jan 1 00:04:12.912: Vi4 PPP: Phase is ESTABLISHING, Passive Open **Jan 1 00:04:12.912: Vi4 LCP: State is Listen** Jan 1 00:04:12.920: **Vi4 LCP: I FORCED CONFREQ len 11** Jan 1 00:04:12.924: Vi4 LCP: AuthProto CHAP (0x0305C22305) Jan 1 00:04:12.924: Vi4 LCP: MagicNumber 0x109D08F2 (0x0506109D08F2) Jan 1 00:04:12.928: Vi4 VPDN: PPP LCP accepted rcv CONFACK Jan 1 00:04:12.928: Vi4 VPDN: PPP LCP accepted sent CONFACK **Jan 1 00:04:12.928: Vi4 PPP: Phase is AUTHENTICATING, by this end** Jan 1 00:04:12.932: **Vi4 CHAP: O CHALLENGE id 3 len 27 from "1600-3"** Jan 1 00:04:12.940: **Vi4 CHAP: I RESPONSE id 6 len 27 from "2500-1"** Jan 1 00:04:12.967: RADIUS: Initial Transmit Virtual-Access4 id 48 10.51.6.3:1645, Access-Request, len 97 Jan 1 00:04:12.971: Attribute 4 6 0A330652 Jan 1 00:04:12.975: Attribute 5 6 00000004 Jan 1

00:04:12.975: Attribute 61 6 00000005 Jan 1 00:04:12.975: Attribute 1 8 32353030 Jan 1
00:04:12.979: Attribute 30 8 36313436 Jan 1 00:04:12.979: Attribute 31 12 32303835 Jan 1
00:04:12.979: Attribute 3 19 06CA1CC2 Jan 1 00:04:12.983: Attribute 6 6 00000002 Jan 1
00:04:12.983: Attribute 7 6 00000001 Jan 1 00:04:12.987: RADIUS: Received from id 48
10.51.6.3:1645, Access-Accept, len 38 Jan 1 00:04:12.991: Attribute 6 6 00000002 Jan 1
00:04:12.991: Attribute 7 6 00000001 Jan 1 00:04:12.991: Attribute 8 6 FFFFFFFF Jan 1
00:04:12.999: AAA/AUTHEN (3530581085): status = PASS Jan 1 00:04:12.999: Vi4 AAA/AUTHOR/LCP:
Authorize LCP Jan 1 00:04:13.003: Vi4 AAA/AUTHOR/LCP (1947215169): Port='Virtual-Access4'
list='vpdn' service=NET Jan 1 00:04:13.003: AAA/AUTHOR/LCP: Vi4 (1947215169) user='2500-1' Jan 1
00:04:13.007: Vi4 AAA/AUTHOR/LCP (1947215169): send AV service=ppp Jan 1 00:04:13.007: Vi4
AAA/AUTHOR/LCP (1947215169): send AV protocol=lcp Jan 1 00:04:13.007: Vi4 AAA/AUTHOR/LCP
(1947215169): found list "vpdn" Jan 1 00:04:13.011: Vi4 AAA/AUTHOR/LCP (1947215169):
Method=radius (radius) Jan 1 00:04:13.015: Vi4 AAA/AUTHOR (1947215169): Post authorization
status = PASS_REPL Jan 1 00:04:13.015: Vi4 AAA/AUTHOR/LCP: Processing AV service=ppp **Jan 1**
00:04:13.019: Vi4 CHAP: O SUCCESS id 6 len 4 Jan 1 00:04:13.023: Vi4 PPP: Phase is UP Jan 1
00:04:13.027: Vi4 AAA/AUTHOR/FSM: (0): Can we start IPCP? Jan 1 00:04:13.027: Vi4 AAA/AUTHOR/FSM
(536495163): Port='Virtual-Access4' list='vpdn' service=NET Jan 1 00:04:13.031: AAA/AUTHOR/FSM:
Vi4 (536495163) user='2500-1' Jan 1 00:04:13.031: Vi4 AAA/AUTHOR/FSM (536495163): send AV
service=ppp Jan 1 00:04:13.035: Vi4 AAA/AUTHOR/FSM (536495163): send AV protocol=ip Jan 1
00:04:13.035: Vi4 AAA/AUTHOR/FSM (536495163): found list "vpdn" Jan 1 00:04:13.039: Vi4
AAA/AUTHOR/FSM (536495163): Method=radius (radius) **Jan 1 00:04:13.039: RADIUS: allowing**
negotiated framed address Jan 1 00:04:13.043: Vi4 AAA/AUTHOR (536495163): Post authorization
status = PASS_REPL Jan 1 00:04:13.043: Vi4 AAA/AUTHOR/FSM: We can start IPCP Jan 1 00:04:13.047:
Vi4 IPCP: O CONFREQ [Closed] id 1 len 10 Jan 1 00:04:13.051: Vi4 IPCP: Address 10.51.6.82
(0x03060A330652) Jan 1 00:04:13.102: Vi4 IPCP: I CONFREQ [REQsent] id 187 len 16 Jan 1
00:04:13.114: Vi4 IPCP: CompressType VJ 15 slots (0x0206002D0F00) Jan 1 00:04:13.118: Vi4 IPCP:
Address 10.10.53.2 (0x03060A0A3502) Jan 1 00:04:13.118: Vi4 AAA/AUTHOR/IPCP: Start. Her address
10.10.53.2, we want 0.0.0.0 Jan 1 00:04:13.122: Vi4 AAA/AUTHOR/IPCP (2669954081): Port='Virtual-
Access4' list='vpdn' service=NET Jan 1 00:04:13.126: AAA/AUTHOR/IPCP: Vi4 (2669954081)
user='2500-1' Jan 1 00:04:13.126: Vi4 AAA/AUTHOR/IPCP (2669954081): send AV service=ppp Jan 1
00:04:13.130: Vi4 AAA/AUTHOR/IPCP (2669954081): send AV protocol=ip Jan 1 00:04:13.130: Vi4
AAA/AUTHOR/IPCP (2669954081): send AV addr*10.10.53.2 Jan 1 00:04:13.134: Vi4 AAA/AUTHOR/IPCP
(2669954081): found list "vpdn" Jan 1 00:04:13.134: Vi4 AAA/AUTHOR/IPCP (2669954081):
Method=radius (radius) **Jan 1 00:04:13.138: RADIUS: allowing negotiated framed address 10.10.53.2**
Jan 1 00:04:13.142: Vi4 AAA/AUTHOR (2669954081): Post authorization status = PASS_REPL Jan 1
00:04:13.146: Vi4 AAA/AUTHOR/IPCP: Processing AV service=ppp Jan 1 00:04:13.146: Vi4
AAA/AUTHOR/IPCP: Processing AV addr=10.10.53.2 Jan 1 00:04:13.150: Vi4 AAA/AUTHOR/IPCP:
Authorization succeeded Jan 1 00:04:13.150: Vi4 AAA/AUTHOR/IPCP: Done. Her address 10.10.53.2,
we want 10.10.53.2 Jan 1 00:04:13.154: Vi4 IPCP: O CONFREQ [REQsent] id 187 len 10 Jan 1
00:04:13.154: Vi4 IPCP: CompressType VJ 15 slots (0x0206002D0F00) Jan 1 00:04:13.162: Vi4 IPCP:
I CONFACK [REQsent] id 1 len 10 Jan 1 00:04:13.162: Vi4 IPCP: Address 10.51.6.82
(0x03060A330652) Jan 1 00:04:13.213: Vi4 IPCP: I CONFREQ [ACKrcvd] id 188 len 10 Jan 1
00:04:13.217: Vi4 IPCP: Address 10.10.53.2 (0x03060A0A3502) Jan 1 00:04:13.217: Vi4
AAA/AUTHOR/IPCP: Start. Her address 10.10.53.2, we want 10.10.53.2 Jan 1 00:04:13.221: Vi4
AAA/AUTHOR/IPCP: Processing AV service=ppp Jan 1 00:04:13.221: Vi4 AAA/AUTHOR/IPCP: Processing
AV addr=10.10.53.2 Jan 1 00:04:13.225: Vi4 AAA/AUTHOR/IPCP: Authorization succeeded Jan 1
00:04:13.225: Vi4 AAA/AUTHOR/IPCP: Done. Her address 10.10.53.2, we want 10.10.53.2 Jan 1
00:04:13.229: Vi4 IPCP: O CONFACK [ACKrcvd] id 188 len 10 Jan 1 00:04:13.233: Vi4 IPCP: Address
10.10.53.2 (0x03060A0A3502) **Jan 1 00:04:13.233: Vi4 IPCP: State is Open Jan 1 00:04:13.261: Vi4**
IPCP: Install route to 10.10.53.2 Jan 1 00:04:14.015: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Virtual-Access4, changed state to up

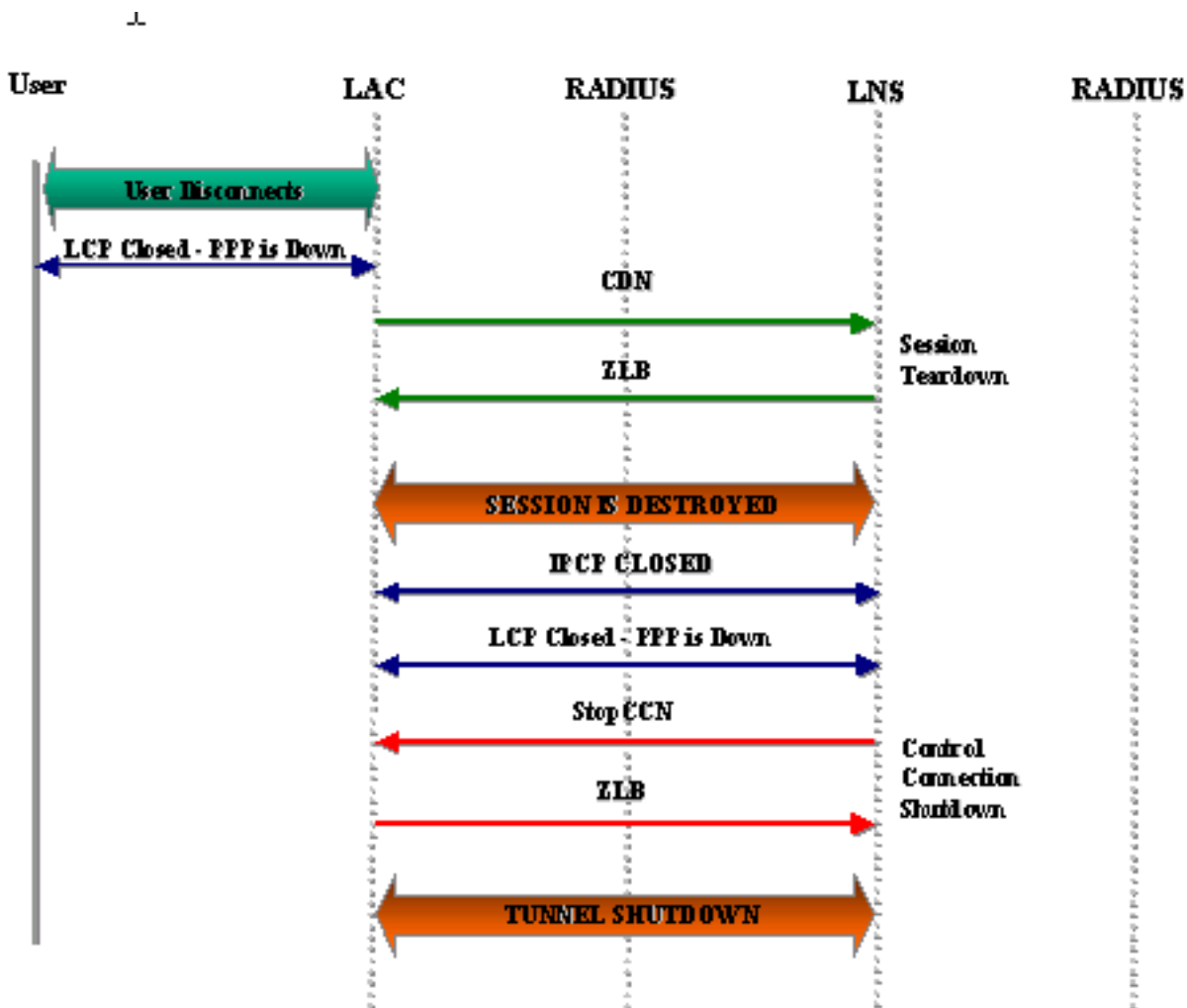
[L'ordre de débranchement PPP/L2TP](#)

1. L'utilisateur distant relâche la liaison RNIS afin de relâcher l'appel au LAC.
2. L'ordinateur d'état de PPP de LAC se termine et l'état LCP est fermé.
3. Afin d'informer le LNS de la déconnexion de la session, le LAC envoie une Appel-Débranchement-notification (CDN) et détruit la session. Le CDN contient un code de résultat AVP 1, qui a la « perte de transporteur » comme raison pour le débranchement. La session est maintenant dans un état libre.
4. Le LNS envoie un message ZLB, qui est un accusé de réception ordonnancé, et détruit la

session. La session est maintenant dans un état libre.

5. Le LNS prend vers le bas l'interface locale de PPP. L'interface d'accès virtuelle change l'état à vers le bas : IPCP est fermé, LCP est fermé, et l'ordinateur d'état de PPP est déclaré vers le bas. La route hôte à l'utilisateur distant est retirée de la table de routage LNS. L'état du tunnel NO--Session-est maintenant quitté sur le LAC et le LNS.
6. Puisque c'est la dernière session dans le tunnel, la connexion de contrôle peut maintenant être arrêtée. Les minuteurs par défaut pour l'arrêt de tunnel sont de 10 secondes pour le LNS et de 15 secondes pour le LAC.
7. Le LNS envoie une Arrêt-Contrôle-Connexion-notification (arrêt-CCN) au LAC afin de fermer la connexion et le tunnel de contrôle. L'arrêt-CCN contient la raison pour l'arrêt de tunnel, qui est « demande d'effacer la connexion de contrôle ». Le tunnel est maintenant dans un état libre.
8. Le LAC envoie un message ZLB, qui est un accusé de réception ordonnancé, au LNS. Le tunnel est maintenant dans un état libre.
9. Le tunnel est maintenant arrêté.

Remarque: Le LAC ou le LNS peut initier la désinstallation de session et de connexion de contrôle. Il n'est pas nécessaire d'effacer les sessions dans le tunnel avant que le tunnel puisse être arrêté.



[Debug pris du LAC qui affiche le débranchement de PPP et L2TP](#)

disconnected from 2085730592 2500-1, call lasted 17 seconds
Jan 1 00:04:27.387: %LINK-3-UPDOWN:
Interface Serial0:0, changed state to down
Jan 1 00:04:27.387: Se0:0 PPP: Phase is TERMINATING [0 sess, 0 load]
Jan 1 00:04:27.387: Se0:0 LCP: State is Closed Jan 1 00:04:27.387: Se0:0 PPP: Phase is DOWN [0
sess, 0 load] Jan 1 00:04:27.387: Se0:0 VPDN: Cleanup Jan 1 00:04:27.387: Se0:0 VPDN: Reset Jan
1 00:04:27.387: Se0:0 Tnl/Cl 17688/7 L2TP: O CDN to l2tp-gw 55270/45 **Jan 1 00:04:27.387: Se0:0
Tnl/Cl 17688/7 L2TP: O CDN, flg TLS, ver 2, len 38, tnl 55270, cl 45, ns 4, nr 2** C8 02 00 26 D7
E6 00 2D 00 04 00 02 80 08 00 00 00 00 00 0E 80 08 00 00 00 0E 00 07 80 0A 00 00 00 01 00 01 00
00 **Jan 1 00:04:27.387: Se0:0 Tnl/Cl 17688/7 L2TP: Destroying session** Jan 1 00:04:27.387: Se0:0
Tnl/Cl 17688/7 L2TP: Session state change from established to idle Jan 1 00:04:27.387: Se0:0
Tnl/Cl 17688/7 L2TP: VPDN: Releasing idb for LAC/LNS tunnel 17688/55270 session 7 state idle Jan
1 00:04:27.387: Tnl 17688 L2TP: Tunnel state change from established to no-sessions-left **Jan 1
00:04:27.387: Tnl 17688 L2TP: No more sessions in tunnel, shutdown (likely) in 15 seconds** Jan 1
**00:04:27.431: Tnl 17688 L2TP: I ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 17688, cl 0, ns 2, nr
5** Jan 1 00:04:28.387: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0:0, changed state
to down Jan 1 00:04:37.383: Tnl 17688 L2TP: Parse AVP 0, len 8, flag 0x8000 (M) Jan 1
00:04:37.383: Tnl 17688 L2TP: Parse StopCCN Jan 1 00:04:37.383: Tnl 17688 L2TP: Parse AVP 9, len
8, flag 0x8000 (M) Jan 1 00:04:37.383: Tnl 17688 L2TP: Assigned Tunnel ID 55270 Jan 1
00:04:37.383: Tnl 17688 L2TP: Parse AVP 1, len 8, flag 0x8000 (M) Jan 1 00:04:37.387: L2X:
Result code(1): 1: Request to clear control connection Jan 1 00:04:37.387: Error code(0): No
error Jan 1 00:04:37.387: Tnl 17688 L2TP: No missing AVPs in StopCCN **Jan 1 00:04:37.387: Tnl
17688 L2TP: I StopCCN, flg TLS, ver 2, len 36, tnl 17688, cl 0, ns 2, nr 5** C8 02 00 24 45 18 00
00 00 02 00 05 80 08 00 00 00 00 04 80 08 00 00 00 09 D7 E6 80 08 00 00 00 01 00 01 **Jan 1
00:04:37.387: Tnl 17688 L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 55270, cl 0, ns 5, nr
3** C8 02 00 0C D7 E6 00 00 00 05 00 03 Jan 1 00:04:37.387: Tnl 17688 L2TP: I StopCCN from l2tp-gw
tnl 55270 **Jan 1 00:04:37.387: Tnl 17688 L2TP: Shutdown tunnel** Jan 1 00:04:37.387: Tnl 17688
L2TP: Tunnel state change from no-sessions-left to idle

[Debug pris du LNS qui affiche le débranchement de PPP et L2TP](#)

Jan 1 00:04:27.740: Vi4 Tnl/Cl 55270/45 L2TP:
Parse AVP 0, len 8, flag 0x0x8000 (M)
Jan 1 00:04:27.740: Vi4 Tnl/Cl 55270/45 L2TP: Parse CDN
Jan 1 00:04:27.744: Vi4 Tnl/Cl 55270/45 L2TP:
Parse AVP 14, len 8, flag 0x0x8000 (M)
Jan 1 00:04:27.748: Vi4 Tnl/Cl 55270/45 L2TP: Assigned Call ID 7
Jan 1 00:04:27.752: Vi4 Tnl/Cl 55270/45 L2TP:
Parse AVP 1, len 10, flag 0x0x8000 (M)
Jan 1 00:04:27.752: Vi4 Tnl/Cl 55270/45 L2TP:
Result code(1): 1: Loss of carrier
Jan 1 00:04:27.756: Error code(0): No error
Jan 1 00:04:27.756: Vi4 Tnl/Cl 55270/45 L2TP:
No missing AVPs in CDN
**Jan 1 00:04:27.760: Vi4 Tnl/Cl 55270/45 L2TP: I CDN, flg TLS, ver 2, len 38, tnl 55270, cl 45,
ns 4, nr 2 contiguous pak, size 38** C8 02 00 26 D7 E6 00 2D 00 04 00 02 80 08 00 00 00 00 00 0E
80 08 00 00 00 0E 00 07 80 0A 00 00 00 01 00 01 00 00 **Jan 1 00:04:27.772: Vi4 Tnl/Cl 55270/45
L2TP: O ZLB ctrl ack, flg TLS, ver 2, len 12, tnl 17688, cl 0, ns 2, nr 5** Jan 1 00:04:27.776:
contiguous buffer, size 12 C8 02 00 0C 45 18 00 00 00 02 00 05 Jan 1 00:04:27.780: Vi4 Tnl/Cl
55270/45 L2TP: I CDN from hgw tnl 17688, cl 7 **Jan 1 00:04:27.780: Vi4 Tnl/Cl 55270/45 L2TP:
Destroying session** Jan 1 00:04:27.784: Vi4 Tnl/Cl 55270/45 L2TP: Session state change from
established to idle Jan 1 00:04:27.788: Vi4 Tnl/Cl 55270/45 L2TP: VPDN: Releasing idb for
LAC/LNS tunnel 55270/17688 session 45 state idle Jan 1 00:04:27.792: Vi4 VPDN: Reset Jan 1
00:04:27.792: Tnl 55270 L2TP: Tunnel state change from established to no-sessions-left **Jan 1
00:04:27.796: Tnl 55270 L2TP: No more sessions in tunnel, shutdown (likely) in 10 seconds** Jan 1
00:04:27.800: %LINK-3-UPDOWN: Interface Virtual-Access4, changed state to down **Jan 1
00:04:27.816: Vi4 IPCP: State is Closed** Jan 1 00:04:27.820: Vi4 PPP: Phase is TERMINATING **Jan 1
00:04:27.820: Vi4 LCP: State is Closed** Jan 1 00:04:27.824: Vi4 PPP: Phase is DOWN Jan 1
00:04:27.839: Vi4 IPCP: Remove route to 10.10.53.2 Jan 1 00:04:29.022: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Virtual-Access4, changed state to down Jan 1 00:04:37.720: Tnl 55270 L2TP:
O StopCCN to hgw tnlid 17688 **Jan 1 00:04:37.724: Tnl 55270 L2TP: O StopCCN, flg TLS, ver 2, len
36, tnl 17688, cl 0, ns 2, nr 5** Jan 1 00:04:37.728: contiguous buffer, size 36 C8 02 00 24 45 18
00 00 00 02 00 05 80 08 00 00 00 00 04 80 08 00 00 00 09 D7 E6 80 08 00 00 00 01 00 01 Jan 1
00:04:37.736: Tnl 55270 L2TP: Tunnel state change from no-sessions-left to shutting-down **Jan 1**

00:04:37.740: Tnl 55270 L2TP: Shutdown tunnel Jan 1 00:04:37.744: Tnl 55270 L2TP: Tunnel state change from shutting-down to idle

Informations connexes

- [Pages de support technologique de Composition et accès](#)
- [Support et documentation techniques - Cisco Systems](#)