

# Einrichtung und Entfernung von L2TP-Tunneln

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[PPP](#)

[L2TP](#)

[PPP und L2TP Flow Summary](#)

[Die PPP/L2TP-Verbindungssequenz](#)

[Debugging aus LAC, das PPP- und L2TP-Anrufaufbau zeigt](#)

[Debugging aus LNS, das PPP- und L2TP-Anrufaufbau zeigt](#)

[Die PPP/L2TP-Trennungssequenz](#)

[Debugging aus LAC, das PPP- und L2TP-Trennung anzeigt](#)

[Debugging aus LNS, das die PPP- und L2TP-Trennung anzeigt](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird die Einrichtung und Außerbetriebnahme des Layer-2-Tunneling-Protokolls (L2TP) erläutert. Das Dokument enthält auch eine Zusammenfassung von PPP und L2TP.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Cisco IOS® Software-Versionen 12.0(1)T und höher.

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

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

## PPP

PPP ist ein symmetrisches Peer-to-Peer-Protokoll, das L2- und L3-Datenverkehr über Punkt-zu-Punkt-Verbindungen transportiert. Es gibt drei Hauptkomponenten:

- Kapselung
- Link Control Protocol (LCP)
- Network Control Protocol (NCP)

Datagramme sind in PPP gekapselt. Das LCP ermöglicht die Aushandlung von Konfigurationsoptionen, um das Herstellen von Verbindungen zu ermöglichen. NCP werden für jedes L3-Protokoll ausgehandelt, das auf der Verbindung ausgeführt wird.

Während einer PPP-Sitzung wird die Verbindung in vier verschiedenen Phasen unterteilt:

- Link-Einrichtung - Im Rahmen der Verbindungsphase verwendet PPP eine LCP-Funktion, die abgeschlossen und für offen erklärt werden muss, bevor die Verbindung gegebenenfalls in die Authentifizierungsphase eintritt, und handelt die Öffnung der Netzwerkschicht aus. LCP wird auch zum Terminieren der PPP-Verbindung verwendet.
- Authentication (Authentifizierung): Die Authentifizierungsphase ist implementierungsspezifisch und nicht zwingend erforderlich, um von LCP auf NCP umzustellen. Wenn der Remote-Peer während der LCP-Phase ausgehandelt und vereinbart wurde, muss er sich identifizieren und die vereinbarte Authentifizierungsmethode durchlaufen, bevor PPP zur Netzwerkebene wechselt.
- Network Layer - Bei der NCP-Aushandlung wird sichergestellt, dass beide Peers die Eigenschaften des L3-Protokolls einverstanden sind. Bei IP wird das Steuerungsprotokoll als IP Control Protocol (IPCP) bezeichnet. Neben den Verhandlungen zwischen Peers gibt es auch ein Element der Zuweisung. Dies ist bei Remotezugriffsclients vom Typ Microsoft Windows üblich, die über keine zugewiesene IP-Adresse verfügen und bei der Verbindung auf den Dienstanbieter angewiesen sind, die IP-Adresse zuzuweisen.
- Verbindungsbeendigung - Die Verbindungsperiode kann während des Lebenszyklus des Anrufs jederzeit eingegeben werden. LCP wird zur Übermittlung der Terminierungsanfrage verwendet.

## L2TP

L2TP erweitert den Point-to-Point-Charakter von PPP. L2TP bietet eine Kapselungsmethode für die Übertragung von getunnelten PPP-Frames, mit der die PPP-Endpunkte über ein paketvermittelltes Netzwerk getunnelt werden können. L2TP wird in der Regel in Szenarien mit Remote-Zugriff bereitgestellt, die das Internet verwenden, um Intranet-Dienste anzubieten. Das Konzept ist ein Virtual Private Network (VPN).

Die beiden primären physischen Elemente von L2TP sind der L2TP Access Concentrator (LAC) und der L2TP Network Server (LNS):

- LAC - Die LAC ist ein Peer zum LNS, der als eine Seite des Tunnelendpunkts fungiert. Die LAC terminiert die Remote-PPP-Verbindung und befindet sich zwischen der Remote-Verbindung und dem LNS. Pakete werden über die PPP-Verbindung an die Remote-Verbindung und von dieser an die PPP-Verbindung weitergeleitet. Pakete an das und vom LNS werden über den L2TP-Tunnel weitergeleitet.
- LNS - Das LNS ist ein Peer der LAC, der als eine Seite des Tunnelendpunkts fungiert. Das LNS ist der Terminationspunkt für die PPP-Sitzungen des LAC. Diese Funktion dient zum Aggregieren mehrerer PPP-Sitzungen mit LAC-Tunneling und zum Eindringen in das private Netzwerk.

L2TP verwendet zwei verschiedene Meldungstypen:

- Kontrollnachrichten - L2TP übergibt Kontroll- und Datennachrichten über separate Steuerungs- und Datenkanäle. Der In-Band-Steuerungskanal leitet sequenzielle Nachrichten für das Management von Steuerungsverbindungen, Anrufverwaltung, Fehlerberichte und Sitzungssteuerung weiter. Die Initiierung der Steuerungsverbindung ist nicht spezifisch für die LAC oder das LNS, sondern vielmehr für den Tunneloriginator und -empfänger, der für die Einrichtung der Steuerungsverbindung relevant ist. Zwischen den Tunnelendpunkten wird eine Authentifizierungsmethode für die gemeinsam genutzte geheime Herausforderung verwendet.
- Datenmeldungen - Datenmeldungen werden verwendet, um die PPP-Frames zu kapseln, die in den L2TP-Tunnel gesendet werden.

L2TP verwendet den registrierten UDP-Port 1701 (User Datagram Protocol), und das gesamte L2TP-Paket wird in das UDP-Datagramm eingekapselt. Im normalen UDP-Betrieb wählt der Tunnelinitiator einen verfügbaren UDP-Port aus und sendet die Portnummer 1701 an das UDP-Ziel. In der Antwort entspricht die Ziel-Portnummer der Quell-Portnummer, die im eingehenden UDP-Header verwendet wird. Der Quellport wird auf Basis eines freien Ports festgelegt, der gefunden wird. Nachdem die Quell- und Zielports eingerichtet wurden, müssen die Ports für die Dauer des Tunnels gleich bleiben. In der Cisco IOS Software sind die Quell- und Ziel-Portnummern immer auf die UDP-Portnummer 1701 eingestellt.

**Hinweis:** Das Layer 2 Forwarding (L2F)-Protokoll und L2TP verwenden dieselbe UDP-Portnummer. Mit dem Feld Version im Header können Sie zwischen den beiden Protokollen unterscheiden. Ein Wert von 1 steht für L2F, ein Wert von 2 für L2TP.

## [PPP und L2TP Flow Summary](#)

Bevor PPP-Frames durch den Tunnel weitergeleitet werden können, müssen Steuerungsverbindungen und -sitzungen eingerichtet werden.

Nach der erfolgreichen Einrichtung des Steuerungskanals werden Sitzungen für jede PPP-Verbindung erstellt. Die Sitzungseinrichtung ist in Bezug auf die LAC und das LNS richtungsgerichtet. Bei eingehenden Anrufen fordert die LAC das LNS auf, die Sitzung zu akzeptieren. Bei ausgehenden Anrufen bittet das LNS die LAC, die Sitzung zu akzeptieren.

[Im Abschnitt "PPP/L2TP Connection Sequence"](#) dieses Dokuments wird die Einrichtung von PPP- und L2TP-Anrufen beschrieben, wenn ein Benutzer mit Remotezugriff einen Anruf in der LAC tätigt. In diesem Beispiel wird der Dienst zur Rufnummernerkennung (DNIS) verwendet, um den L2TP-Tunnel zu initiieren. Sie können jedoch auch den Domännennamen für diesen Zweck verwenden. Die Sequenz zeigt den Start der PPP-Sitzung von einem SOHO 2500-Router aus, die

LCP-Aushandlung zwischen dem Remote-Zugriffsbenutzer und der LAC sowie die teilweise Authentifizierung. Die LAC setzt dann den L2TP-Tunnel und die Sitzung innerhalb des Tunnels ein. Für jede PPP-Verbindung zwischen LAC und LNS wird eine Sitzung eingerichtet. L2TP verwendet den Peer-Tunnel und die Sitzungs-IDs in allen ausgehenden Nachrichten, um die PPP-Verbindungen zu multiplizieren und zu demultiplizieren. Diese Identifikatoren werden während der jeweiligen Kontroll-, Verbindungs- und Sitzungs-Einrichtungsphase zugewiesen und ausgetauscht. Tunnel- und Sitzungs-IDs haben nur lokale Bedeutung. Die Tunnel-Endpunkte verfügen über verschiedene IDs für denselben Tunnel und dieselbe Sitzung.

**Hinweis:** Der Wert 0 hat eine einzigartige Bedeutung und wird nur verwendet, wenn Tunnel- und Sitzungsbezeichner noch nicht zugewiesen werden müssen.

Nach der Einrichtung des Tunnels wird der PPP-Authentifizierungsprozess zwischen dem Remote-Benutzer und dem LNS abgeschlossen. Die LAC empfängt weiterhin PPP-Frames. Die Link-Framing- und CRC-Prüfung (zyklische Redundanzprüfung) werden entfernt, in L2TP eingekapselt und in den Tunnel an das LNS weitergeleitet. Dort wird das L2TP-Paket empfangen und behandelt, als ob es auf einer lokalen PPP-Schnittstelle terminiert würde. Die Aushandlung von PPP-NCP erfolgt, und anschließend wird IPCP als offen erklärt. Die Verbindung ist abgeschlossen.

## Die PPP/L2TP-Verbindungssequenz

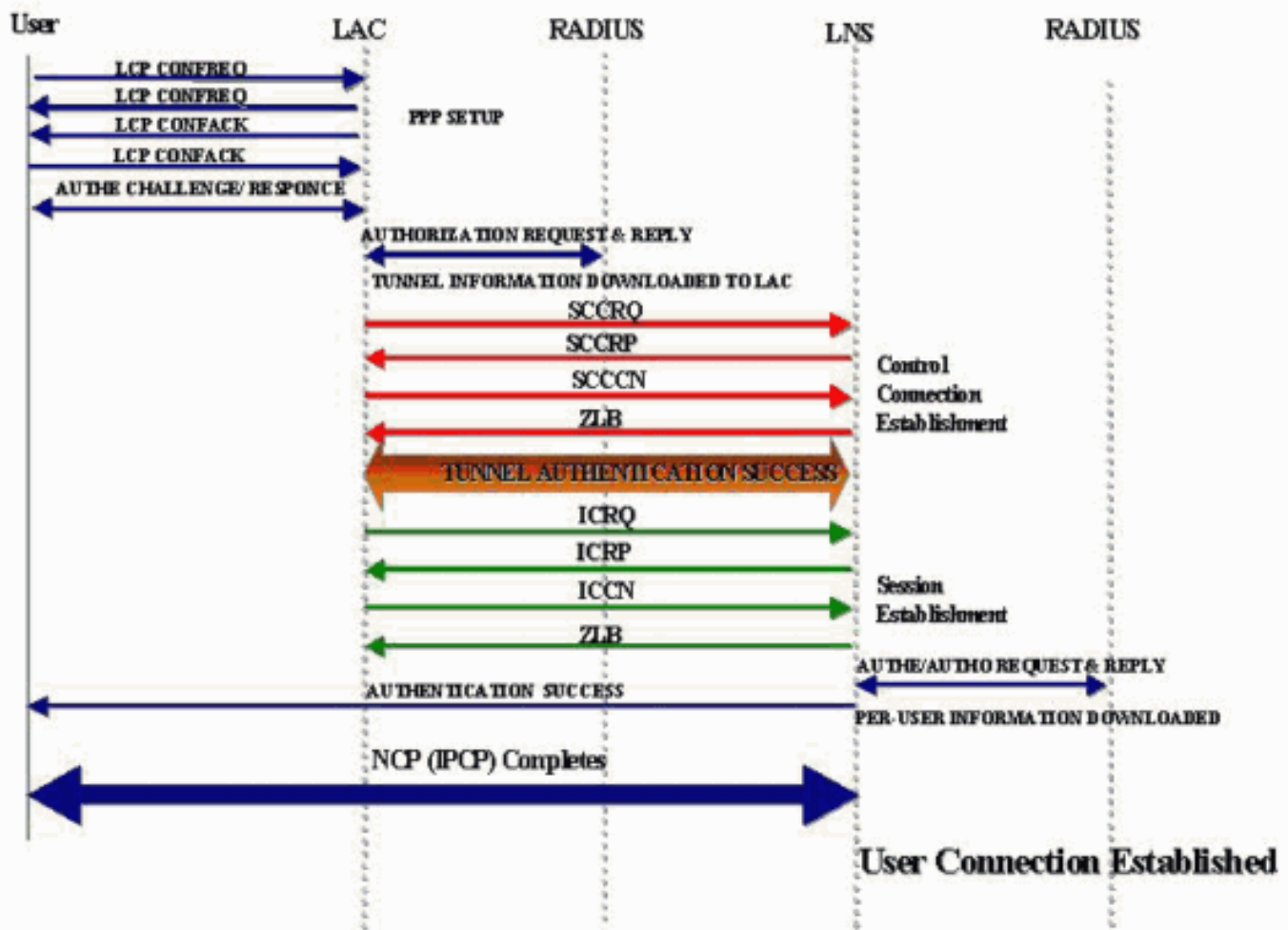
Dies ist die Verbindungssequenz der Ereignisse:

1. Der Remote-Benutzer initiiert eine PPP-Verbindung. Die LAC akzeptiert die Verbindung. Es wird eine PPP-Verbindung hergestellt.
2. LCP wird zwischen dem Remote-Benutzer und der LAC ausgehandelt. Die LAC stellt eine Challenge Handshake Authentication Protocol (CHAP)-Herausforderung aus, um eine teilweise Authentifizierung des Remote-Benutzers durchzuführen. Die Antwort wird während der Sitzungserstellung an das LNS gesendet. Die Antwort wird als AVP-33-Proxy-Authentifizierungsantwort in der ICCN (Incoming-Call-Connected) gesendet.
3. Mit dem DNIS wird bestimmt, ob es sich bei dem Benutzer um einen Virtual Private Dial-up Network (VPDN)-Client handelt.
4. Da für die gewählte Nummer (614629) kein Tunnel vorhanden ist, ist die Erstellung eines neuen Tunnels erforderlich. RADIUS wird abgefragt, und die Tunnelinformationen werden in die LAC heruntergeladen.
5. Die Steuerungsverbindung wird gestartet. Der Tunnel befindet sich im IDLE-Status: Der Tunnelinitiator (in diesem Fall die LAC) sendet eine Start-Control-Connection-Request (SCCRQ) an das LNS. Das SCCRQ enthält eine AVP 11-Herausforderung, die anzeigt, dass die LAC den Tunnel mithilfe einer CHAP-artigen Authentifizierung authentifizieren möchte. Das gleiche Geheimnis ist beiden Tunnelendpunkten bekannt. Der Tunnel befindet sich jetzt im Status WAIT-CTL-REPLY. Das LNS kann den Tunnel aufrufen, sodass das LNS mit einer Start-Control-Connection-Reply (SCCRP) antwortet. Das SCCRP enthält eine AVP 11-Herausforderung und eine AVP 13-Herausforderung-Antwort als Antwort auf das SCCRQ. Der Tunnel befindet sich jetzt im Status WAIT-CTL-REPLY. Die LAC reagiert mit einer SCCCN-Nachricht (Start-Control-Connection-Connected). Das SCCCN enthält einen AVP 13 als Antwort auf das SCCRP. Der Tunnel befindet sich jetzt in einem etablierten Zustand. Das LNS sendet eine ZLB-Nachricht (Zero Length Body) an die LAC. Die ZLB-Nachricht ist eine sequenzielle Bestätigung. Der Tunnel befindet sich jetzt in einem etablierten Zustand.
6. Die Tunnelauthentifizierung ist nun abgeschlossen, und der Tunnel ist eingerichtet. Die

Sitzung befindet sich jetzt im IDLE-Status.

7. Nachdem der Tunnel vorhanden ist, wird ein Dreiwege-Austausch zur Sitzungseinrichtung im Tunnel durchgeführt: Die LAC sendet eine ICRQ (Incoming Call Request) mit Parameterinformationen für die Sitzung. Die Sitzung befindet sich jetzt im Zustand "Wait Reply" (Antworten warten). Das LNS sendet eine eingehende Anrufantwort (Incoming Call Reply, ICRP), die die Sitzungs-ID enthält. Die Sitzung befindet sich jetzt im Zustand Wait Connect. Die LAC sendet eine ICCN und stellt dem LNS zusätzliche Informationen für den angenommenen Anruf zur Verfügung. Diese Informationen enthalten die LCP-Informationen aus der Aushandlung, die die LAC und der Remote-Benutzer durchgeführt haben. Die Sitzung befindet sich jetzt in einem etablierten Zustand. Das LNS sendet eine ZLB-Nachricht, eine sequenzierte Bestätigung, an die LAC. Die Sitzung befindet sich jetzt in einem etablierten Zustand.
8. Nach Einrichtung der Sitzung wird auf dem LNS eine virtuelle Zugriffsschnittstelle erstellt. Die im ICCN bereitgestellten LCP-Konfigurationsinformationen werden in den PPP-Stack der virtuellen Zugriffsschnittstelle gezwungen. Diese Informationen enthalten Informationen zur teilweisen Authentifizierung.
9. Das LNS erzeugt eine Authentifizierungsproblem. Die Proxy-Authentifizierungsantwort AVP 33, die im ICCN bereitgestellt wurde, wird erneut abgespielt.
10. Die normale Authentifizierung, Autorisierung und Abrechnung (AAA) oder PPP-Authentifizierung und -Autorisierung erfolgt.
11. Eine RADIUS-Zugriffsanfrage wird für eine benutzerspezifische Authentifizierung und Autorisierung gesendet.
12. Es wird eine RADIUS Access-Accept-Nachricht empfangen. **Hinweis:** RADIUS wurde so konfiguriert, dass die IP-Adresse, die der Remote-Benutzer in der eingehenden IPCP-Konfigurationsanforderung angegeben hat, zugelassen wird.
13. Eine CHAP-Erfolgsmeldung wird an den Remote-Benutzer gesendet.
14. Die PPP-IPCP-Aushandlung ist abgeschlossen und wird für OPEN erklärt. Eine Hostroute wird auf der Remote-Schnittstelle installiert. Der Remote-Benutzer ist nun verbunden, und der Datenverkehrsfluss kann beginnen.

## Anrufablauf der PPP- und L2TP-Verbindung



## Debugging aus LAC, das PPP- und L2TP-Anrufaufbau zeigt

```

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 CONFREQ [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 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 00:04:10.567: 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 SCCR
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 SCCR
Jan 1 00:04:10.659: Tnl 17688 L2TP: I SCCR, flg TLS, ver 2,
len 154, tnl 17688, cl 0, ns 0, nr 1
      C8 02 00 9A 45 18 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 SCCR 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 SCCR to l2tp-gw tnlid 55270
Jan 1 00:04:10.663: Tnl 17688 L2TP: O SCCR, 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/Cl 17688/7 L2TP: Session FS enabled
Jan 1 00:04:10.663: Tnl/Cl 17688/7 L2TP: Session state change from idle
to wait-for-tunnel
Jan 1 00:04:10.663: Se0:0 Tnl/Cl 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 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 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

```

## [Debugging aus LNS, das PPP- und L2TP-Anrufaufbau zeigt](#)

```

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 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 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 00:04:11.003: 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 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 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 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 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-Template1
interface Virtual-Access4
default ip address
no ip address
encap 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):

```

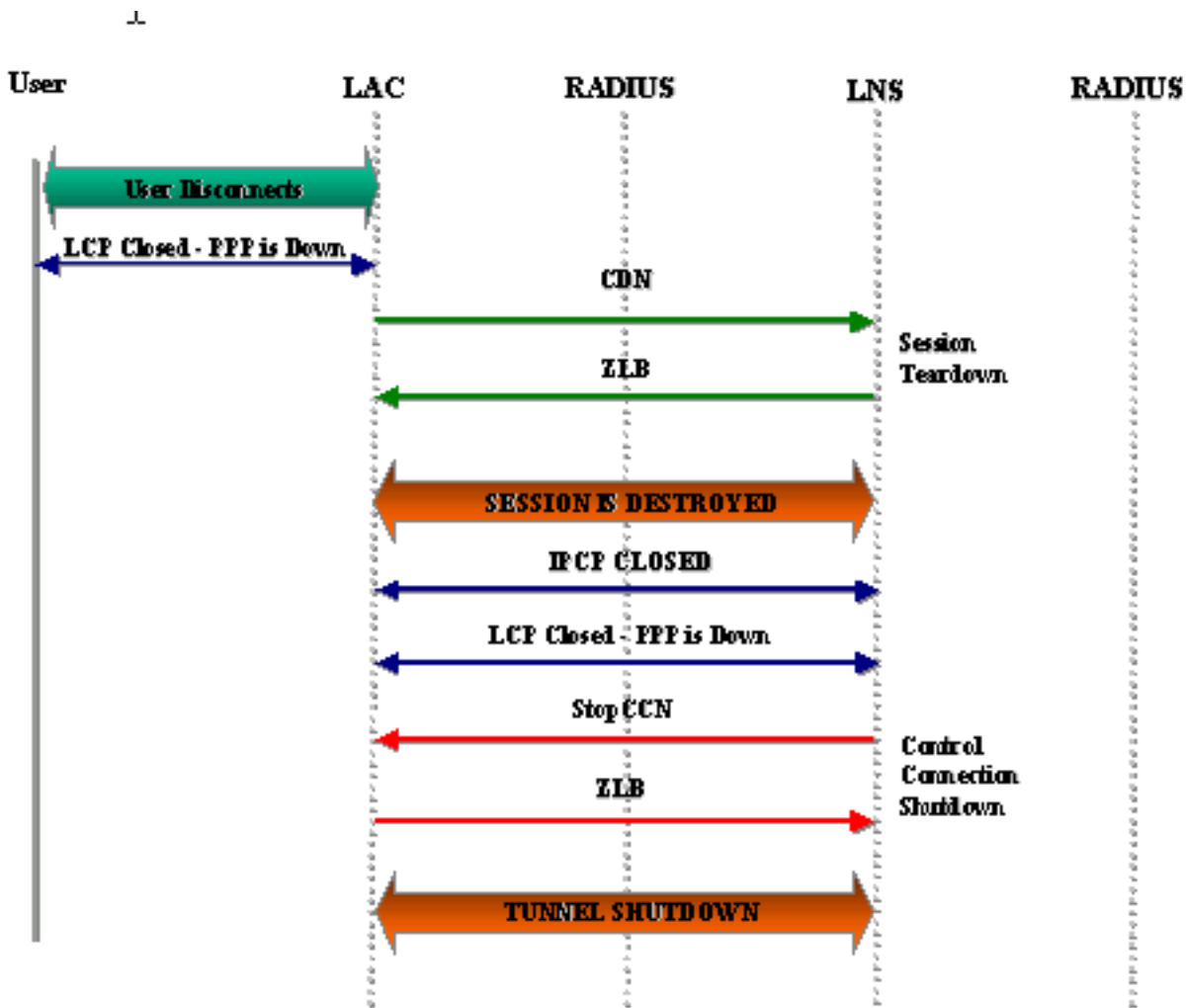
Post authorization status = PASS_REPL
Jan  1 00:04:13.146: Vi4 AAA/AUTHOR/IPCP: Processing AV service=ppp
Jan  1 00:04:13.146: Vi4 AAA/AUTHOR/IPCP: Processing AV addr=10.10.53.2
Jan  1 00:04:13.150: Vi4 AAA/AUTHOR/IPCP: Authorization succeeded
Jan  1 00:04:13.150: Vi4 AAA/AUTHOR/IPCP: Done.  Her address 10.10.53.2,
we want 10.10.53.2
Jan  1 00:04:13.154: Vi4 IPCP: O CONFREJ [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

```

## Die PPP/L2TP-Trennungssequenz

1. Der Remote-Benutzer verwirft die ISDN-Verbindung, um den Anruf an die LAC zu verwerfen.
2. Der LAC PPP-Statuscomputer wird beendet, und der LCP-Status ist "Closed" (geschlossen).
3. Um das LNS über die Trennung der Sitzung zu informieren, sendet die LAC eine CDN (Call-Disconnect-Notify) und zerstört die Sitzung. Das CDN enthält einen AVP 1-Ergebniscode, bei dem der Grund für die Trennung "Carrier-Verlust" ist. Die Sitzung befindet sich jetzt im IDLE-Status.
4. Das LNS sendet eine ZLB-Nachricht, die eine sequenzierte Bestätigung ist, und zerstört die Sitzung. Die Sitzung befindet sich jetzt im IDLE-Status.
5. Das LNS deaktiviert die lokale PPP-Schnittstelle. Die virtuelle Zugriffsschnittstelle ändert den Status auf "Down": IPCP wird geschlossen, LCP wird geschlossen, und das PPP-Statussystem wird als Down deklariert. Die Hostroute zum Remote-Benutzer wird aus der LNS-Routing-Tabelle entfernt. Der Tunnelstatus ist jetzt No-Sessions-Left (Keine Sitzungen) auf der LAC und dem LNS.
6. Da dies die letzte Sitzung im Tunnel ist, kann die Steuerungsverbindung jetzt geschlossen werden. Die Standard-Timer für die Tunnelabschaltung sind 10 Sekunden für das LNS und 15 Sekunden für die LAC.
7. Das LNS sendet eine Stopp-Control-Connection-Notification (Stopp-CCN) an die LAC, um die Steuerverbindung und den Tunnel zu schließen. Der Befehl Stopp-CCN enthält den Grund für das Herunterfahren des Tunnels, d. h. die Anforderung, die Steuerungsverbindung zu löschen. Der Tunnel befindet sich jetzt im IDLE-Zustand.
8. Die LAC sendet eine ZLB-Nachricht (eine sequenzierte Bestätigung) an das LNS. Der Tunnel befindet sich jetzt im IDLE-Zustand.
9. Der Tunnel ist jetzt geschlossen.

**Hinweis:** Entweder das LAC- oder das LNS kann die Sitzung und das Beenden der Steuerverbindung initiieren. Die Sitzungen im Tunnel müssen nicht gelöscht werden, bevor der Tunnel geschlossen werden kann.



## Debugging aus LAC, das PPP- und L2TP-Trennung anzeigt

```

Jan  1 00:04:27.375: %ISDN-6-DISCONNECT: Interface Serial0:0
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/C1 17688/7 L2TP: 0 CDN to l2tp-gw 55270/45
Jan  1 00:04:27.387: Se0:0 Tnl/C1 17688/7 L2TP: 0 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/C1 17688/7 L2TP:
Destroying session
Jan  1 00:04:27.387: Se0:0 Tnl/C1 17688/7 L2TP: Session state change
from established to idle
Jan  1 00:04:27.387: Se0:0 Tnl/C1 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 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

```

## [Debugging aus LNS, das die PPP- und L2TP-Trennung anzeigt](#)

```

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 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
```

## [Zugehörige Informationen](#)

- [Support-Seiten für die Dial- und Access-Technologie](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)