L2TP Tunnel Setup and Teardown

Document ID: 23980

Contents

Introduction

This document discusses the Layer Two Tunneling Protocol (L2TP) tunnel setup and teardown. The document also gives a summary of PPP and L2TP.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco IOS® Software Releases 12.0(1)T and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

PPP

PPP is a symmetrical peer−to−peer protocol that transports L2 and Layer 3 (L3) traffic over point−to−point links. There are three main components:

- Encapsulation

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

Datagrams are encapsulated in PPP. The LCP allows for the negotiation of configuration options to allow link establishment. NCPs are negotiated for each of the L3 protocols that runs on the link.

During the life of a PPP session, the link goes though four distinct phases:

- Link establishing As part of the link establishing phase, PPP uses an LCP function that must be completed and declared open before the link enters the authentication phase, if applicable, and negotiates the opening of the network layer. LCP is also used to terminate the PPP link.
- Authentication The authentication phase is implementation−specific and is not a mandatory requirement for a move from LCP to NCP. If negotiated and agreed upon during the LCP phase, the remote peer must identify itself and pass the agreed authentication method before PPP moves to the network layer.
- Network layer NCP negotiation ensures that both peers agree on the characteristics of the L3 protocol. In the case of IP, the control protocol is called IP Control Protocol (IPCP). In addition to the negotiation between peers, there is also an element of assignment. This is common with Microsoft Windows−type remote−access clients who have no allocated IP address and rely on the service provider to allocate the IP address upon connection.
- Link termination The link termination phase can be entered at any time during the life cycle of the call. LCP is used to deliver the termination request.

L2TP

L2TP extends the point−to−point nature of PPP. L2TP provides an encapsulation method for the transmit of tunneled PPP frames, which allows the PPP endpoints to be tunneled over a packet−switched network. L2TP is most commonly deployed in remote−access−type scenarios that use the Internet to offer intranet−type services. The concept is that of a Virtual Private Network (VPN).

The two primary physical elements of L2TP are the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS):

- LAC The LAC is a peer to the LNS that acts as one side of the tunnel endpoint. The LAC terminates the remote PPP connection and sits between the remote and the LNS. Packets are forwarded to and from the remote connection over the PPP connection. Packets to and from the LNS are forwarded over the L2TP tunnel.
- LNS The LNS is a peer to the LAC that acts as one side of the tunnel endpoint. The LNS is the termination point for the LAC PPP tunneled sessions. This is used to aggregate the multiple LAC−tunneled PPP sessions and ingress into the private network.

There are two different message types that L2TP uses:

- Control messages L2TP passes control and data messages over separate control and data channels. The in−band control channel passes sequenced control connection management, call management, error reporting, and session control messages. Initiation of the control connection is not specific to either the LAC or the LNS but, rather, the tunnel originator and receiver that has relevance in the control connection establishment. A shared−secret challenge authentication method is used between the tunnel endpoints.
- Data messages Data messages are used to encapsulate the PPP frames that are sent into the L2TP tunnel.

L2TP uses the registered User Datagram Protocol (UDP) port 1701, and the whole L2TP packet is

encapsulated within the UDP datagram. As per normal UDP operation, the tunnel initiator selects an available UDP port and sends port number 1701 to the UDP destination. In the reply, the destination port number is the same as the source port number that is used in the incoming UDP header. The source port is set on the basis of any free port that is found. After the source and destination ports are established, the ports must remain the same for the duration of the tunnel. In Cisco IOS Software, the source and destination port numbers are always set to UDP port number 1701.

Note: Layer 2 Forwarding (L2F) Protocol and L2TP share the same UDP port number. The Version field in the header enables you to discriminate between the two protocols. A value of 1 indicates L2F, and a value of 2 indicates L2TP.

PPP and L2TP Flow Summary

Establishment of the control connection and session must occur before PPP frames can be forwarded through the tunnel.

After successful establishment of the control channel, sessions are created for each PPP connection. Session establishment is directional, in relation to the LAC and LNS. For incoming calls, the LAC requests the LNS to accept the session. For outgoing calls, the LNS asks the LAC to accept the session.

The PPP/L2TP Connection Sequence section of this document details the PPP and L2TP call setup when a remote−access user places a call into the LAC. This example uses the dialed number identification service (DNIS) in order to initiate the L2TP tunnel, although you can also use the domain name for this purpose. The sequence shows the start of the PPP session from a SOHO 2500 router, the LCP negotiation between the remote−access user and LAC, and the partial authentication. The LAC then proceeds to establish the L2TP tunnel and session within the tunnel. A session is established for each PPP connection between the LAC and LNS. L2TP uses the peer tunnel and session identifiers in all outgoing messages in order to multiplex and demultiplex PPP connections. These identifiers are assigned and exchanged during the respective control connection and session establishment phases. The tunnel and session IDs have local significance only. The tunnel endpoints have different identifiers for the same tunnel and session.

Note: The value 0 has unique significance and is only used when the tunnel and session identifier have yet to be assigned.

After establishment of the tunnel, the PPP authentication process completes between the remote−access user and the LNS. The LAC continues to receive PPP frames. The link framing and cyclic redundancy check (CRC) are removed, encapsulated into LT2P, and forwarded into the tunnel to the LNS. There, the L2TP packet is received and treated as if it were terminated on a local PPP interface. The negotiation of PPP NCP occurs, and then IPCP is declared open. The connection is complete.

The PPP/L2TP Connection Sequence

This is the connection sequence of events:

1. The remote user initiates a PPP connection. The LAC accepts the connection. A PPP link is established.
2. LCP is negotiated between the remote user and LAC. The LAC issues a Challenge Handshake Authentication Protocol (CHAP) challenge in order to perform a partial authentication of the remote user. The reply is sent to the LNS during session establishment. The reply is sent as attribute−value pair (AVP) 33 proxy authentication response in the Incoming−Call−Connected (ICCN).
3. The DNIS is used to determine whether the user is a virtual private dial−up network (VPDN) client.
4. Because there is no existing tunnel for the dialed number (614629), creation of a new tunnel is necessary. RADIUS is queried and the tunnel information is downloaded to the LAC.

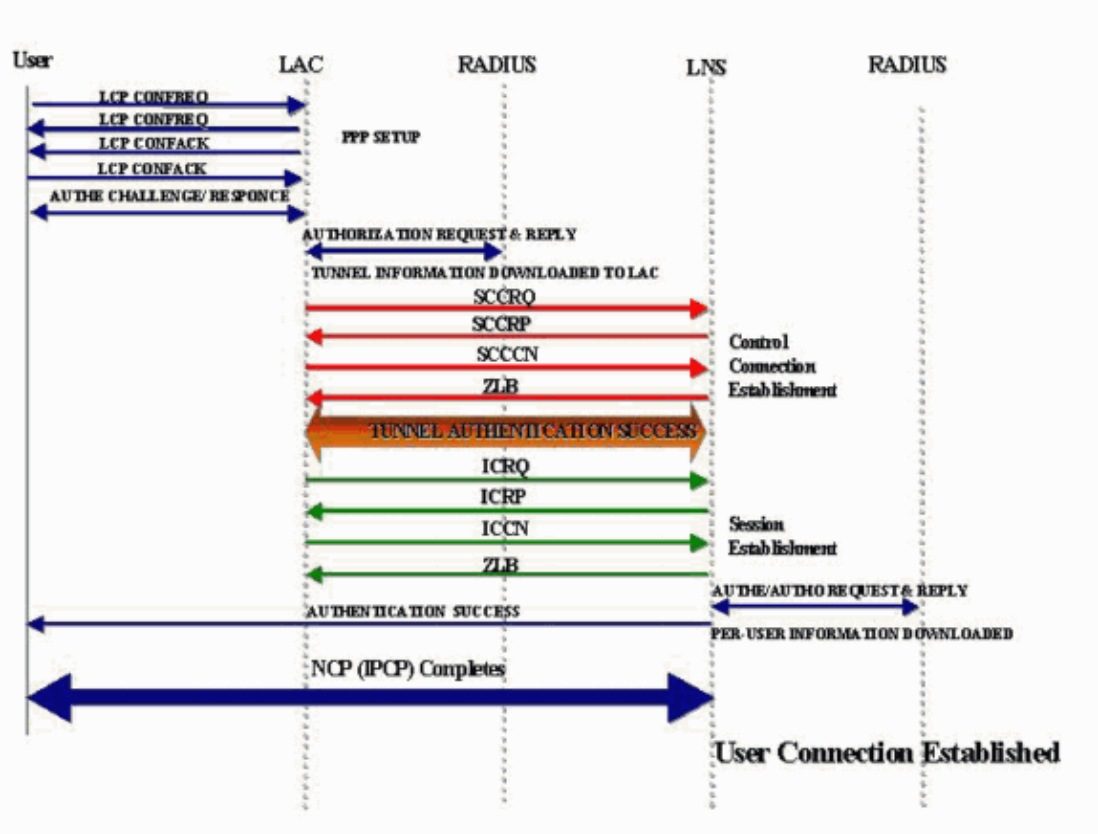
5. The control connection is started. The tunnel is in an IDLE state:

    - The tunnel initiator (in this case, the LAC) sends a Start−Control−Connection−Request (SCCRQ) to the LNS. The SCCRQ contains an AVP 11 challenge, which indicates that the LAC wants to authenticate the tunnel with use of a CHAP−style authentication. The same secret is known to both tunnel endpoints. The tunnel is now in a WAIT−CTL−REPLY state.
    - The LNS can bring up the tunnel, so the LNS replies with a Start−Control−Connection−Reply (SCCRP). The SCCRP contains an AVP 11 challenge and an AVP 13 challenge response in reply to the SCCRQ. The tunnel is now in a WAIT−CTL−REPLY state.
    - The LAC responds with a Start−Control−Connection−Connected (SCCCN) message. The SCCCN contains an AVP 13 in reply to the SCCRP. The tunnel is now in an Established state.
    - The LNS sends a Zero−Length Body (ZLB) message to the LAC. The ZLB message is a sequenced acknowledgement. The tunnel is now in an Established state.
6. The tunnel authentication is now complete and the tunnel is established. The session is now in an IDLE state.
7. Now that the tunnel exists, a three−way exchange for session establishment within the tunnel is performed:

    - The LAC sends an Incoming−Call−Request (ICRQ) with the parameter information for the session. The session is now in a Wait Reply state.
    - The LNS sends an Incoming−Call−Reply (ICRP) that contains the session ID. The session is now in a Wait Connect state.
    - The LAC sends an ICCN and provides the LNS with additional information for the answered call. This information includes the LCP information from the negotiation that the LAC and remote user performed. The session is now in an Established state.
    - The LNS sends a ZLB message, which is a sequenced acknowledgement, to the LAC. The session is now in an Established state.
8. After establishment of the session, a virtual access interface is created on the LNS. The LCP configuration information that was delivered in the ICCN is forced onto the virtual access interface PPP stack. This information includes the partial authentication information.
9. The LNS generates an authentication challenge. The proxy authentication response AVP 33, which was delivered in the ICCN, is replayed.
10. Normal authentication, authorization, and accounting (AAA) or PPP authentication and authorization takes place.
11. A RADIUS Access−Request is sent for per−user authentication and authorization.
12. A RADIUS Access−Accept is received.

    Note: RADIUS has been configured to allow the IP address that the remote user has offered in the incoming IPCP Configure−Request.
13. A CHAP success message is sent to the remote user.
14. PPP IPCP negotiation completes and is declared OPEN. A host route is installed to the remote interface. The remote user is now connected, and traffic flow can commence.

PPP and L2TP Connection Call Flow



Debug Taken from LAC That Shows PPP and L2TP Call Establishment

```
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 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 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 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/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
```

Debug Taken from LNS That Shows PPP and L2TP Call Establishment

```
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
```

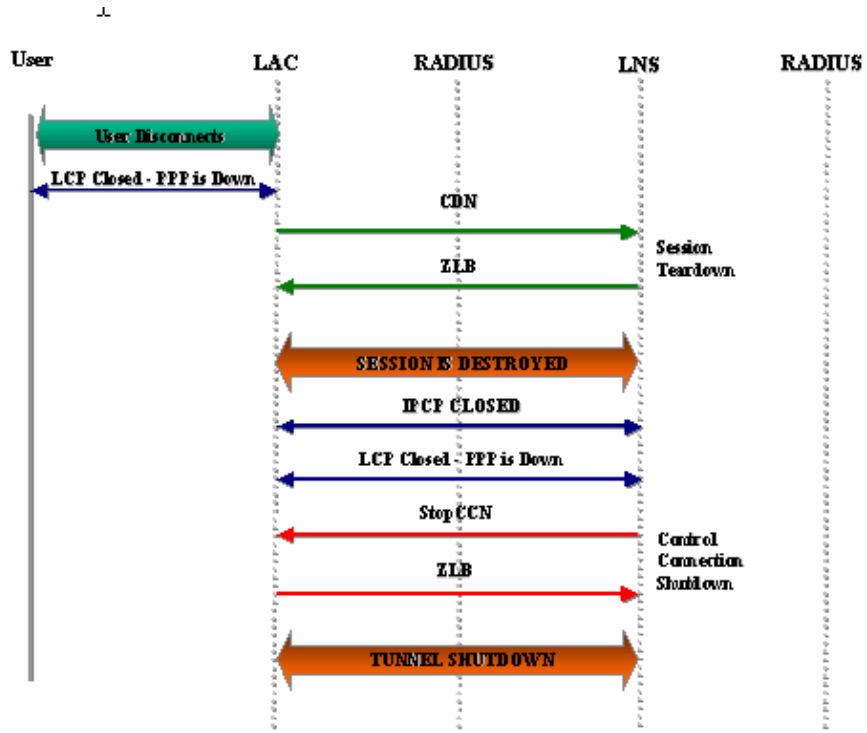
```
Jan  1 00:04:13.233: Vi4 IPCP:    Address 10.10.53.2 (0x03060A0A3502)
Jan  1 00:04:13.233: Vi4 IPCP: State is Open
Jan  1 00:04:13.261: Vi4 IPCP: Install route to 10.10.53.2
Jan  1 00:04:14.015: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Virtual-Access4, changed state to up
```

The PPP/L2TP Disconnect Sequence

1. The remote user drops the ISDN link in order to drop the call to the LAC.
2. The LAC PPP state machine terminates and the LCP state is Closed.
3. In order to notify the LNS of the disconnection of the session, the LAC sends a Call−Disconnect−Notify (CDN) and destroys the session. The CDN contains an AVP 1 result code, which has "Loss of carrier" as the reason for the disconnect. The session is now in an IDLE state.
4. The LNS sends a ZLB message, which is a sequenced acknowledgement, and destroys the session. The session is now in an IDLE state.
5. The LNS takes down the local PPP interface. The virtual access interface changes state to Down:

    - IPCP is closed, LCP is closed, and the PPP state machine is declared Down.
    - The host route to the remote user is removed from the LNS routing table.
    - The tunnel state is now No−Sessions−Left on both the LAC and the LNS.
6. Because this is the last session within the tunnel, the control connection can now be shut down. The default timers for tunnel shutdown are 10 seconds for the LNS and 15 seconds for the LAC.
7. The LNS sends a Stop−Control−Connection−Notification (Stop−CCN) to the LAC in order to close down the control connection and tunnel. The Stop−CCN contains the reason for the tunnel shutdown, which is "Request to clear control connection". The tunnel is now in an IDLE state.
8. The LAC sends a ZLB message, which is a sequenced acknowledgement, to the LNS. The tunnel is now in an IDLE state.
9. The tunnel is now shut down.

Note: Either the LAC or LNS can initiate the session and control connection teardown. It is not necessary to clear the sessions within the tunnel before the tunnel can be shut down.



Debug Taken from LAC That Shows PPP and L2TP Disconnect

```
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/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 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 Taken from LNS That Shows PPP and L2TP Disconnect

```
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
```

Related Information

- **Dial and Access Technology Support Pages**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jan 29, 2008 Document ID: 23980