

LAYER 2 TUNNEL PROTOCOL

OVERVIEW

L2TP is one of the key building blocks for virtual private networks in the dial access space and is endorsed by Cisco and other internetworking industry leaders. It combines the best of Cisco's Layer 2 Forwarding (L2F) protocol and Microsoft's Point-to-Point Tunneling Protocol (PPTP).

PURPOSE

The purpose of this document is to give an overview of what L2TP IOS[®] configuration commands are used in the L2TP tunneling process and what communication processes go on between network access devices.

KEY L2TP TERMS

CHAP: Challenge Handshake Authentication Protocol. A PPP authentication protocol.

L2TP Access Concentrator (LAC): An LAC can be a Cisco network access server connected to the public switched telephone network (PSTN). The LAC need only implement media for operation over L2TP. An LAC can connect to the LNS using a local-area network or wide-area network such as public or private Frame Relay. The LAC is the initiator of incoming calls and the receiver of outgoing calls.

L2TP Network Server (LNS): Most any Cisco router connected to a local-area network or wide-area network, such as public or private Frame Relay, can act as an LNS. It is the server side of the L2TP protocol and must operate on any platform that terminates PPP sessions. The LNS is the initiator of outgoing calls and the receiver of incoming calls. Figure 1 depicts the call routine between the LAC and LNS.

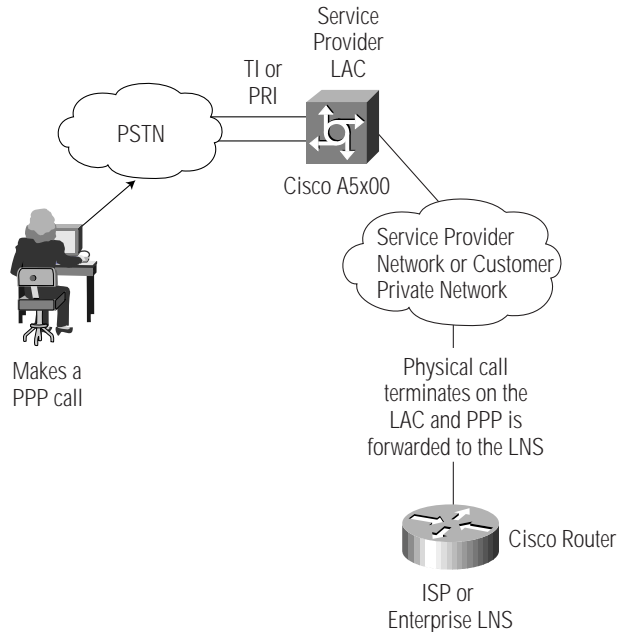
Virtual Private Dial Network (VPDN): A type of access VPN that uses PPP to deliver the service.

VPDN L2TP MODEL

Many different scenarios apply to the L2TP model. The most basic model is one in which a client initiates a call using a PC configured for PPP to his or her Internet service provider (ISP). With a wholesale dial model, an ISP outsources dial access to a service provider (SP). This paper examines L2TP behavior in the context of the wholesale dial model using VPDN, AAA, RADIUS, and L2TP. Figure 1 depicts a typical wholesale dial model. Dial access using an asynchronous or synchronous connection is assumed from the client to the SP.

Figure 1

L2TP LAC and LNS call routine. The physical call is terminated on the LAC while the PPP session is forwarded to the LNS.



WHOLESALE DIAL SCENARIO—L2TP COMMUNICATION PROCESSES

1.0 START PPP SESSION ON THE LAC

1.1 PPP Challenge and Response

A client at home initiates a PPP session to the service provider's access server, called SP_LAC. The SP_LAC challenges the remote user using Challenge Handshake Authentication Protocol (CHAP). We will call this user `sydnee@isp.com`.

Review the following debug from the LAC:

```
debug ppp negotiation
debug ppp authentication
Interface Async3, changed state to up
As3 PPP: Treating connection as a dedicated line
As3 PPP: Phase is ESTABLISHING, Active Open
As3 LCP: O CONFREQ [REQsent] id 2 len 25
As3 LCP: I CONFACK [REQsent] id 2 len 25
As3 LCP: I CONFREQ [ACKrcvd] id 3 len 20
As3 LCP: O CONFACK [ACKrcvd] id 3 len 20
As3 LCP: State is Open
As3 PPP: Phase is AUTHENTICATING, by this end
As3 CHAP: O CHALLENGE id 1 len 27 from "SP_LAC"
As3 CHAP: I RESPONSE id 1 len 35 from "sydnee@isp.com"
As3 PPP: Phase is FORWARDING
```

Notice the CHAP challenge from SP_LAC and the CHAP response from `sydnee@isp.com`. This is typical of any ppp initiated call. The domain name is important here because it signals the LAC to determine whether the user is a VPDN client. At this point the LAC begins searching for a tunnel to route `sydnee@isp.com`. You will see,

```
As3 VPDN: Looking for tunnel -- isp.com -
```

in the debug indicating the LAC is searching for a tunnel to isp.com. If no tunnel exists, the LAC will begin the sequence to build the tunnel. If DNIS was used the LAC will search for a tunnel based on DNIS. Now let's examine what the configuration of the LAC must look like to enable this service.

2.0 CONFIGURE THE LAC FOR L2TP

Cisco's IOS® allows you to configure L2TP locally on the access server or remotely using RADIUS.

2.1 Local Configuration on the LAC

Whether or not you use Radius, you must first configure VPDN locally on the LAC. The LAC is configured locally for VPDN services using the following command set:

```
vpdn enable
!
vpdn search-order domain dnis
```

Notice the vpdn search-order command. The vpdn search-order command tells the LAC how to perform VPDN tunnel authorization. The service provider can select a specific vpdn tunnel using either the Dialed Number Information Service (DNIS) or domain name. DNIS provides additional flexibility to service providers who offer VPDN services and to enterprises that use the service. An enterprise can provide multiple specific telephone numbers for users to dial into a service provider. When using DNIS, the user does not have to enter "@isp.com" in her username. So DNIS allows the VPDN service to be transparent to the end user. The default is to search using DNIS first and domain name second when the vpdn search-order command is not used.

2.2 Adding AAA for a locally configured LAC

Next we'll configure AAA to tell the LAC to use the local router configuration for tunnel authentication and authorization.

```
AAA configurations
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
```

You will also need to define a local username database on the LAC which will be used during tunnel authentication. This might look something like:

```
username sp_lac password 7 104D000A0618
username lns password 7 104D000A0618
```

(note that when entering the password you do NOT enter the "7", you simply use the format "username foo password bar". The numbers you see in the above output are generated automatically by the routers encryption algorithm).

2.3 Adding Tunnel Authorization Attributes locally on the LAC

Now add the attributes needed to find the LNS for the given domain name (or DNIS). You need to tell the LAC to use "L2TP" (or "any" if you wish to support both "L2F" and "L2TP"). You need to enter the LNS's IP address. You need to identify the domain name (or DNIS). Optionally you may enter a "local name" for the LAC, which will be used during tunnel authentication. If you do not enter the local name, the routers host name will be used instead.

```
vpdn-group 1
request dialin l2tp ip 172.22.66.25 domain isp.com
local name sp_lac
```

2.4 Adding RADIUS to the LAC Configuration

In this example, RADIUS is used to gather tunnel information. If no “VPDN group” is configured locally on the LAC, an AAA server must be used to retrieve the tunnel attributes. The LAC, using AAA, must get authorization information from RADIUS (or TACACS+) to begin building the tunnel between the LAC and LNS. This document only covers RADIUS.

(For all requests requiring network-related services, such as PPP, the AAA command `aaa authorization network default radius` is used. The configuration on the LAC might look something like:

```
aaa new-model
aaa authentication login default local
aaa authentication ppp default radius local
aaa authorization network default radius
aaa accounting network default start-stop radius
```

2.5 Configure the RADIUS Server Address

The following commands must be configured on both the LAC and LNS to enable communication to the RADIUS server (usually these will be two different RADIUS servers, one at the SP site and one at the ISP site, but they may be the same. A service provider offering a managed service may administer both the LAC and the LNS.

```
radius-server host 172.22.66.16 auth-port 1645 acct-port 1646
radius-server key cisco
```

3.0 RADIUS PROFILE FOR USE BY THE LAC

Certain information must be present before L2TP tunnels are built. A RADIUS profile must exist that contains information about the specific L2TP tunnel attributes (TACACS+ may also be used, and its configuration is similar, but this document only covers RADIUS). The profile contains information for the domain (in this case `isp.com`), such as the IP address for the LNS (where the tunnel is going), the tunnel ID (in this case, `sp_lac`), the tunnel type, and the tunnel password.

When the LAC asks the RADIUS server for these tunnel attributes, the LAC uses a special hard-coded password of “cisco” because the RADIUS protocol requires a requester to authenticate before any authorization attributes are given. Because the LAC must authenticate to access the tunnel attributes used to open the tunnel, the LAC must use a password. This profile will also be set to a service type of “outbound user.” This prevents a malicious user from logging in to the router as `username=isp.com, password=cisco`.

An example of a RADIUS profile for use by the LAC:

```
isp.com password="cisco" user_service_type= outbound-user,
cisco-avp="vpdn:ip-addresses=10.1.1.1,
cisco-avp="vpdn:tunnel-id=sp_lac",
cisco-avp="vpdn:tunnel-type=l2tp",
cisco-avp="vpdn:l2tp-tunnel-password=foobar"
```

Note: The RADIUS protocol does not support outbound authentication.

3.1 LNS Load Balancing

It is possible to configure the LACs to perform round robin load sharing across 2 or more LNSs. To do this you simply define more than one IP address (or DNS hostname) for the destination LNSs and comma delimit them. For example, you could modify the above example to support two additional LNSs:

```
cisco-avp="vpdn:ip-addresses=10.1.1.1, 10.2.2.2, 10.3.3.3",
```

3.2 LNS Backup

Similarly, you can specify a backup LNS or LNSs that will be used if all primary servers go down or do not respond. To do this, use the same syntax as above except use “/” as the delimiter. For example, the following configuration says to load balance across 10.1.1.1 and 10.2.2.2, but if both of these servers stop responding, use 10.3.3.3 and 10.4.4.4 as backup servers (and round-robin load balance across them):

```
cisco-avp="vpdn:ip-addresses=10.1.1.1, 10.2.2.2/10.3.3.3, 10.4.4.4",
```

4.0 SEQUENCE OF EVENTS ON THE LAC USING RADIUS

The vpdn enable command signals AAA to query the RADIUS daemon for attributes associated with VPDN services. This debug trace showing the flow:

```
debug aaa authentication
debug aaa authorization
debug radius
```

```
AAA/AUTHEN: create_user (0x60F1613C) user='isp.com' ruser=''
port='Async2' rem_addr='' authen_type=NONE service=LOGIN priv=0
AAA/AUTHOR/VPDN (721948876): Port='Async2' list='default' service=NET
AAA/AUTHOR/VPDN: (721948876) send AV service=ppp
AAA/AUTHOR/VPDN: (721948876) send AV protocol=vpdn
AAA/AUTHOR/VPDN (721948876) found list "default"
AAA/AUTHOR/VPDN: (721948876) Method=RADIUS
```

A series of RADIUS events occur between the LAC and the RADIUS server. Ultimately, RADIUS returns the following to the LAC:

```
RADIUS: cisco AVPair "vpdn:ip-addresses= 172.22.66.25"
RADIUS: cisco AVPair "vpdn:tunnel-id=sp_lac"
RADIUS: cisco AVPair "vpdn:tunnel-type=l2tp"
RADIUS: cisco AVPair "vpdn:tunnel-password= cisco"
AAA/AUTHOR (3804680290): Post authorization status = PASS_REPL
AAA/AUTHOR/VPDN: Processing AV ip-addresses=172.22.66.25
AAA/AUTHOR/VPDN: Processing AV tunnel-id=sp_lac
AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp (Tunnel Info)
AAA/AUTHOR/VPDN: Processing AV tunnel-password=cisco
As3 VPDN: Get tunnel info for isp.com with LAC sp_lac, IP 172.22.66.25
AAA/AUTHEN: free_user (0x60F19D98) user='isp.com' ruser='' port='Async3' rem_addr=''
authen_type=NONE service=LOGIN priv=0
As3 VPDN: Forward to address 172.22.66.25
AAA/AUTHEN: create_user(0x60EEE724)user='sydnee@isp.com'
```

The debug shows that AAA now has the information it needs to begin building the tunnel.

5.0 CONFIGURE THE LNS FOR L2TP

5.1 Local Configuration Needed when Configuring the LNS for L2TP

You must define the attributes for the LNS to know how to handle an incoming tunnel request. First, you enable the VPDN with the vpdn enable command. Enter the tunnel attributes in the vpdn-group. Note that in current versions of Cisco IOS software [through 12.0(3)T], you cannot configure tunnel attributes for the LNS through RADIUS or TACACS+.

The following configuration tells the LNS to “accept” inbound L2TP tunnels with the “sp_lac” tunnel ID. Note that the tunnel ID is often shown as an NAS name, but the tunnel ID should be a common name across all the SP NASs. There may be thousands of NASs, but they should all share a common ISP tunnel ID. You also must point this

incoming tunnel session to a “virtual template interface”; the PPP session that the LAC is forwarding to the LNS also needs an interface to terminate. The virtual template is used as a configuration repository from which virtual access interfaces “clone” their configurations. A virtual access interface is brought up dynamically when an incoming PPP session is forwarded across the L2TP tunnel. The virtual template interface contains all PPP and network layer configurations and appears as any other access interface type.

VPDN COMMANDS FOR THE LNS

```
vpdn enable
!
vpdn-group 1
accept dialin l2tp virtual-template 1 remote sp_lac
local name lns
```

VIRTUAL-TEMPLATE COMMANDS FOR THE LNS

```
interface Virtual-Template1
ip unnumbered FastEthernet0/0
no ip directed-broadcast
peer default ip address pool default
ppp authentication chap vpdn
ppp multilink
```

5.2 Adding RADIUS to the LNSs Configuration

The LNS will have a similar AAA configuration that will appear like this:

```
AAA LNS configuration:
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
aaa authentication ppp vpdn radius
aaa authorization network default radius
aaa accounting network default start-stop radius
```

You will also need to define a local username database on the LNS. This might look something like this:

```
username sp_lac password 7 104D000A0618
username lns password 7 104D000A0618
```

Because RADIUS does not support outbound authentication, Cisco maintains a special requirement for the LNS configuration. Use local authentication for the tunnel authentication, but use RADIUS authentication for user authentication. So create two PPP authentication methods: a “default” method used for tunnel authentication, and the VPDN for the virtual template interface. The default method uses local authentication. The VPDN method uses RADIUS. Because the VPDN method is bound to the virtual template, all inbound user authentication will be conducted through RADIUS.

5.3 Configure the RADIUS Server Address

The following commands must be configured on both the LAC and LNS to enable communication to the RADIUS server (usually these will be two different RADIUS servers, one at the SP site and one at the ISP site, but they may be the same. A service provider offering a managed service may administer both the LAC and the LNS.

```
radius-server host 172.22.66.16 auth-port 1645 acct-port 1646
radius-server key cisco
```

6.0 REVIEW OF THE ENTIRE PROCESS

6.1 Local Configurations if Not Using RADIUS

Once the tunnel information is gathered, the LAC has the necessary information to start building the tunnel. VPDN requests L2TP to open a tunnel connection to 172.22.66.25 domain isp.com. Recall the following configuration on the LAC:

```
vpdn enable
!
vpdn search-order domain dnis
vpdn-group 1
request dialin l2tp ip 172.22.66.25 domain isp.com
local name sp_lac
```

The request dialin l2tp ip 172.22.66.25 domain isp.com command string initiates a tunnel request to the LNS (172.22.66.25) for domain name isp.com. User sydney@isp.com is a VPDN client and either wants to be routed over an existing tunnel or a tunnel built to be routed to isp.com. The key here is the domain name isp.com.

The tunnel will use the command string local name sp_lac to identify itself.

The LNS configuration is similar:

```
vpdn enable
!
vpdn-group 1
accept dialin l2tp virtual-template 1 remote sp_lac
local name lns
```

You will also need to configure local username database entries for the LAC and LNS. The entries are used during the tunnel authentication process. The following is an example of these entries:

```
username sp_lac password 7 104D000A0618
username lns password 7 01100F175804
```

Remember, when using a RADIUS server to assist in building a L2TP tunnel, tunnel information requested by the LAC from RADIUS (RADIUS profile) is used to build the tunnel. VPDN, through the vpdn enable command is what initiates the request for L2TP tunneling to the LNS.

You may also build L2TP tunnels using local VPDN commands. For the LAC, attributes used to build the tunnel come from two places, local VPDN configuration commands and a local username database. For the LNS, attributes used to assist in building the tunnel come from local VPDN configurations and local username database period.

The benefit of using RADIUS is scalability. This makes it easier for service providers to scale L2TP to hundreds of L2TP access concentrators by maintaining a central place for defining tunnel attributes.

6.2 Tunnel Creation

Recall that the vpdn enable command is what kicks off tunnel creation. This subtle process occurs just before tunnel authentication begins and is shown in the following debugs for the LAC and LNS:

LAC Perspective:

```
As2 VPDN: Bind interface direction=1 (VPDN kick-off)
Tnl/Cl 1/1 L2TP: Session FS enabled
Tnl/Cl 1/1 L2TP: Session state change from idle to wait-for-tunnel
```

LNS Perspective:

```
L2TP: I SCCRQ from lac tnl 1
Tnl 4 L2TP: New tunnel created for remote sp_lac, address 172.22.66.23
```

6.3 Tunnel Authentication

Regardless of whether you're using RADIUS or local configurations, tunnel authentication begins with a series of communication process between the LAC and LNS. The following debug shows this process from the LAC perspective:

```
Tnl/C1 2/1 L2TP: Session FS enabled
Tnl/C1 2/1 L2TP: Session state change from idle to wait-for-tunnel
As3 2/1 L2TP: Create session
Tnl 2 L2TP: SM State idle
Tnl 2 L2TP: O SCCRQ
Tnl 2 L2TP: Tunnel state change from idle to wait-ctl-reply
Tnl 2 L2TP: SM State wait-ctl-reply
As3 VPDN: sydnee@isp.com is forwarded
Tnl 2 L2TP: I SCCRQ from lns
Tnl 2 L2TP: Got a challenge from remote peer, lns
Tnl 2 L2TP: Got a response from remote peer, lns
Tnl 2 L2TP: Tunnel Authentication success
Tnl 2 L2TP: Tunnel state change from wait-ctl-reply to established
Tnl 2 L2TP: O SCCCN to lns tnlid 5
Tnl 2 L2TP: SM State established
```

Notice the first line of the debug. "Session FS enabled" means that fast switching is in use and is on by default to improve performance. L2TP uses the well-known UDP port 1701. The entire L2TP packet is encapsulated in a UDP datagram.

6.4 Start Control and Incoming Messages

Figure 4 depicts how tunnel authentication is achieved during the start control message process between the LAC and LNS. During this process, the LAC and LNS exchange information about themselves—mainly identity and password.

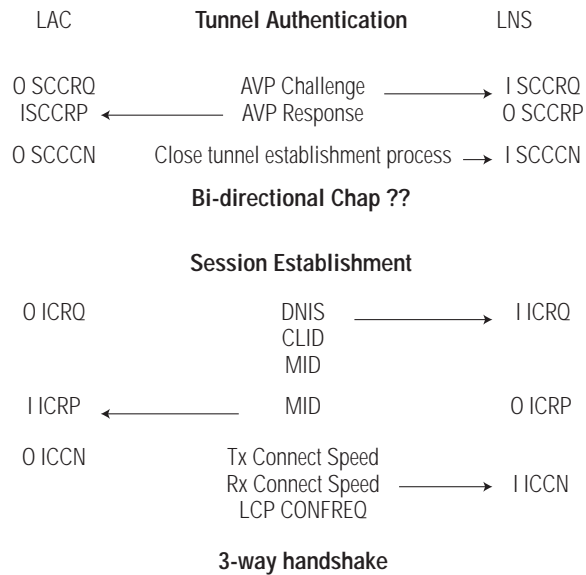
The first line in the below debug is the incoming start control connect request (I SCCRQ) from LAC. The second line indicates that a new tunnel was created from remote LAC sp_lac, and its IP address is provided. The following LNS debug shows the tunnel authentication process:

```
L2TP: I SCCRQ from lac tnl 1
Tnl 4 L2TP: New tunnel created for remote sp_lac, address 172.22.66.23
Tnl 4 L2TP: Got a challenge in SCCRQ, sp_lac
Tnl 4 L2TP: O SCCRQ to sp_lac tnlid 1
Tnl 4 L2TP: Tunnel state change from idle to wait-ctl-reply
Tnl 4 L2TP: I SCCCN from sp_lac tnl 1
Tnl 4 L2TP: Got a Challenge Response in SCCCN from lac
Tnl 4 L2TP: Tunnel Authentication success (LOOK HERE!)
Tnl 4 L2TP: Tunnel state change from wait-ctl-reply to established
Tnl 4 L2TP: SM State established
Tnl 4 L2TP: I ICRQ from sp_lac tnl 1
Tnl/C1 4/1 L2TP: Session FS enabled
Tnl/C1 4/1 L2TP: Session state change from idle to wait-for-tunnel
Tnl/C1 4/1 L2TP: New session created
Tnl/C1 4/1 L2TP: O ICRP to sp_lac 1/1
```

```
Tnl/Cl 4/1 L2TP: Session state change from wait-for-tunnel to wait-connect
Tnl/Cl 4/1 L2TP: I ICCN from sp_lac tnl 1, cl 1
Tnl/Cl 4/1 L2TP: Session state change from wait-connect to established
```

The debug line that read, “Tnl 4 L2TP: Tunnel Authentication success?” indicates that tunnel authentication was successful.

Figure 2
Start Control and Incoming Message Process



6.5 Session Establishment

Refer to Figure 4 again. The LAC and LNS negotiate session creation. This is the start of the three-way handshake beginning with the incoming call request (O ICRQ) from the LAC. The session is created and a reply (O ICRP) was sent back to the LAC. The incoming call connect message (I ICCN) is the last step in the three-way handshake process, and the session is established.

6.6 The PPP Session Starts up on the LNS

The LNS debug shows the virtual-access interface being created:

```
debug vtemplate
debug aaa authentication
debug aaa authorization
debug ppp negotiation
debug ppp authentication
Vi1 VPDN: Virtual interface created for sydney@isp.com
Vi1 VPDN: Set to Async interface
Vi1 PPP: Phase is DOWN, Setup
Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
Vi1 VTEMPLATE: Has a new cloneblk vtemplate, now it has vtemplate
Vi1 VTEMPLATE: *** CLONE VACCESS1 *****
Vi1 VTEMPLATE: Clone from Virtual-Templat1
```

```

interface Virtual-Access1
default ip address
ip unnumbered FastEthernet0/0
no ip directed-broadcast
peer default ip address pool default
ppp authentication chap
ppp multilink
ppp authen chap vpdn
end
Virtual Access Interface is up
4d08h: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
Vil PPP: Treating connection as a dedicated line
Vil PPP: Phase is ESTABLISHING, Active Open (PPP is up)
Vil AAA/AUTHOR/FSM: (0): LCP succeeds trivially
Vil LCP: O CONFREQ [Closed] id 1 len 37
Vil LCP:   ACCM 0x000A0000 (0x0206000A0000)
Vil LCP:   AuthProto CHAP (0x0305C22305)
Vil LCP:   MagicNumber 0x67525FF6 (0x050667525FF6)
Vil LCP:   PFC (0x0702)
Vil LCP:   ACFC (0x0802)
Vil LCP:   MRRU 1524 (0x110405F4)
EndpointDisc 1 Local (0x1308016867772D32)
Vil VPDN: Bind interface direction=2
Vil PPP: Treating connection as a dedicated line
Vil LCP: I FORCED CONFREQ len 21
Vil LCP:   ACCM 0x000A0000 (0x0206000A0000)
Vil LCP:   AuthProto CHAP (0x0305C22305)
Vil LCP:   MagicNumber 0x108AC65D (0x0506108AC65D)
Vil LCP:   PFC (0x0702)
Vil LCP:   ACFC (0x0802)
Vil VPDN: PPP LCP accepted rcv CONFACK
Vil VPDN: PPP LCP accepted sent CONFACK
Vil PPP: Phase is AUTHENTICATING, by this end
Vil CHAP: O CHALLENGE id 2 len 26 from "lns"
Vil CHAP: I RESPONSE id 1 len 35 from "sydnee@isp.com"
AAA: parse name=Virtual-Access1 idb type=21 tty=-1
AAA: name=Virtual-Access1 flags=0x11 type=5 shelf=0 slot=0
adapter=0 port=1 channel=0
AAA/AUTHEN: create_user (0x612B8150) user='sydnee@isp.com'
ruser='' port='Virtual-Access1' rem_addr='' authen_type=CHAP service=PPP priv=1
AAA/AUTHEN/START (2492784487): port='Virtual-Access1' list
='vpdn' action=LOGIN service=PPP
AAA/AUTHEN/START (2492784487): found list vpdn
AAA/AUTHEN/START (2492784487): Method=RADIUS

```

Notice the virtual-access interface was cloned from the virtual-template. Also, notice that the virtual-access interface state is changed to “up” and the PPP session is “active open.”

You will also notice in the debug that the LCP configuration was forced. This means that whatever LCP configurations were negotiated between the LAC and the client were forced to the virtual-access interface. Lastly, per-user authentication now takes place on the LNS.

The original per-user authentication process had been suspended until the tunnel and the virtual-access interface are created.

7.0 INSTALL ROUTE

7.1 Affirmation

Some debug clues indicate a successful VPDN L2TP call. Once the process starts the IPCP phase (L2TP/VPDN/PPP/ IPCP), you may begin.

```
Vil PPP: Phase is UP
```

```
AAA/AUTHOR/FSM: (0): Can we start IPCP?
```

```
Vil IPCP: State is Open
```

Problems that may occur after this point are likely to be standard PPP/AAA problems, and not specific to L2TP. When you see this you are successful:

```
Vil IPCP: Install route to 10.1.1.1 (This is your BIGGEST clue!)
```

```
lns-2#ping 10.1.1.1
```

```
!!!!
```

Don't forget to ping the client so you know your route to the client works.

8.0 USEFUL DEBUG COMMANDS

Helpful Hint: Activate on millisecond time stamping when in debug mode with the global command "service timestamps debug datetime msec."

8.1 For the LNS

```
debug ppp negotiation
```

```
debug ppp authentication
```

```
debug vtemplate
```

```
debug vpdn event
```

```
debug AAA authentication
```

```
debug AAA authorization
```

```
debug radius
```

```
debug vtemplate
```

8.2 For the LAC:

```
debug ppp negotiation
```

```
debug ppp authentication
```

```
debug vpdn event
```

```
debug AAA authentication
```

```
debug AAA authorization
```

```
debug radius
```

```
debug isdn q931
```

9.0 OTHER USEFUL COMMANDS

9.1 show vpdn session

The show vpdn session command displays information about active L2TP sessions in a VPDN environment.

9.2 show vpdn tunnel

The show vpdn tunnel command displays information about active L2TP tunnel information in a VPDN environment.

10.0 SAMPLE CONFIGURATIONS

10.1 LAC Configuration

```
SP_LAC#
SP_LAC#wr t
Building configuration...
Current configuration:
!
version 11.3
service timestamps debug datetime msec
service timestamps log uptime
service password-encryption
!
hostname SP_LAC
!
aaa new-model
aaa authentication login default local
aaa authentication login con local
aaa authentication ppp default radius
aaa authorization network default radius
aaa accounting network default start-stop radius
enable secret 5 $1$9.Cr$681eBZWHyPu2IaFODQLbA.
!
username sp_lac password 7 104D000A0618
username lns password 7 01100F175804
vpdn enable
!
vpdn search-order domain dnis
vpdn-group 1
request dialin l2tp ip 172.22.66.25 domain isp.com
local name sp_lac
!
...
!
radius-server host 172.22.66.16 auth-port 1645 acct-port 1646
radius-server key cisco
end
```

10.2 LNS Configuration

```
lns#wr t
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug datetime msec
service timestamps log uptime
service password-encryption
!
hostname lns
!
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
aaa authentication ppp vpdn radius
aaa authorization network default radius
aaa accounting network default start-stop radius
!
```

```

username sp_lac password 7 104D000A0618
username lns password 7 060506324F41
!
vpdn enable
!
vpdn-group 1
accept dialin l2tp virtual-template 1 remote sp_lac
local name lns
!
async-bootp dns-server 1.1.1.1 2.2.2.2
async-bootp nbns-server 8.8.8.8 9.9.9.9
!
!
interface FastEthernet0/0
ip address 172.22.66.25 255.255.255.192
no ip directed-broadcast
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered FastEthernet0/0
no ip directed-broadcast
peer default ip address pool default
ppp authentication chap vpdn
ppp multilink
!
ip local pool default 10.1.1.1 10.1.1.16
...
!
radius-server host 172.22.66.16 auth-port 1645 acct-port 1646
radius-server key cisco
end

```

11.0 SUMMARY

In the context of a wholesale dial model and VPDN, L2TP is straightforward. Understanding the basic communication processes of PPP session establishment, gathering tunnel information, building the tunnel, VPDN interworking, and debug events will not only help you configure L2TP but aid in the troubleshooting process.

Sources and References:

Layer 2 Tunnel Protocol Fact Sheet

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/l2tun_ds.htm

Layer 2 Tunnel Protocol

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/l2tpt.htm>

VPDN Configuration Guide

http://www.cisco.com/en/US/tech/tk801/tk703/technologies_tech_note09186a0080094586.shtml

VPDN Configuration and Troubleshooting

http://www-tac.cisco.com/Support_Library/Internetworking/VPDN/vpdn_config.0.html

Security Configuration Guide

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/index.htm

RADIUS Configuration Guide

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt2/index.htm

APPENDIX A: L2TP MULTIHOP CONFIGURATION

A router may operate as both an LNS to given set of LACs and simultaneously as an LAC to a given LNS. When configured to operate in this way, the router is considered to be configured for “VPDN multihop.” This model may be used in a clearinghouse, where the router is redirecting tunnels on behalf of client LACs and LNSs.

The following is a sample multihop configuration that shows a router configured to accept inbound tunnel requests from an LAC using tunnel ID “cs1”: The tunnel is terminated locally using virtual template 1. If the destination domain is “cisco.com,” a new tunnel is opened to the LNS at 10.1.1.1

```
vpdn enable
vpdn multihop
!
vpdn-group 1
accept dialin l2tp virtual-template 1 remote cs1
local name cs2
!
vpdn-group 2
request dialin l2tp ip 10.1.1.1 domain cisco.com
local name cs2
```

Note that only one IDB is used for both inbound and outbound sessions. Inbound and outbound sessions use the same virtual access interface, and the virtual access interface has the intelligence to establish the direction.

APPENDIX B: LNS STACK GROUP CONFIGURATION

Two or more LNSs may be placed into a Multichassis Multilink PPP “stack group” using the Stack Group Bidding Protocol (SGBP). This allows for arbitrarily large groupings of LNSs into a single logical unit. The main benefit of this approach, compared with load balancing across two or more LNSs, is that with a stack group, the LNSs can terminate Multilink PPP links for the same bundle across multiple LNS chassis.

To configure a stack group of LNSs, enable the “vpdn multihop” feature discussed above in Appendix A, and configure the LNSs to an SGBP stack group. The “vpdn multihop” command enables the LNSs to forward links that belong to the same Multilink PPP bundle to the LNS that owns bundles for that Multilink PPP session. See the Cisco IOS documentation for more information about SGBP and Multichassis Multilink PPP.

The following is a sample configuration excerpt for an LNS belonging to an L2TP stack group. You configure your LNS to know the name of the stack group, and configure the members of the stack group with their IP addresses. The stack group members will authenticate each other using normal CHAP-like authentication, so you will either need a local username for the stack group name or AAA. See the Cisco IOS documentation for SGBP for details. Only the specific commands for the stack group are shown; the rest of the LNS configuration must also be in place.

```
hostname LNS1
!
username LNSstack password 7 00071A150754
!
multilink virtual-template 1
!
sgbp group LNSstack
sgbp member LNS2 10.1.1.2
sgbp member LNS3 10.1.1.3
sgbp member LNS4 10.1.1.4
!
vpdn multihop
```

APPENDIX C ADVANCED RADIUS OPTIONS

RADIUS Hosted IP Pools

This is not an L2TP feature, but it may be useful for scaling large LNS installations.

To host IP pools on a RADIUS server, a special RADIUS user is defined. The user is predefined to be "pools- <Home Gateway Name>". You may choose a different name, but the HGW will need to be configured with the Cisco IOS command:

```
aaa configuration config-username <YourPoolName>
```

A sample pools definition on the Radius server follows. The following syntax is used for CiscoSecure ACS for Unix, but exactly the same attributes apply for other Radius syntaxes.

```
user = pools-lns01 {
radius=Cisco {
Check Items= {
Password=cisco
User Service Type=Outbound User
}
Reply_Attributes= {
cisco-avpair="ip:pool-def#1=one 1.1.1.1 1.1.1.48"
cisco-avpair="ip:pool-def#2=two 2.2.2.1 2.2.2.48"
cisco-avpair="ip:pool-def#3=three 3.3.3.1 3.3.3.48"
}
}
}
```

The router will ask for the pools, the pools will be downloaded to the router, and they will then appear to be "dynamically" downloaded local pools:

```
hgw01#sh ip local pool
Pool      Begin      End          Free InUse
default  172.16.2.1  172.16.2.48  48    0
one      1.1.1.1    1.1.1.48    48    0    (dynamic)
two      2.2.2.1    2.2.2.48    47    1    (dynamic)
three    3.3.3.1    3.3.3.48    48    0    (dynamic)
```



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0403R) 204044_ETMG_SH_07.04