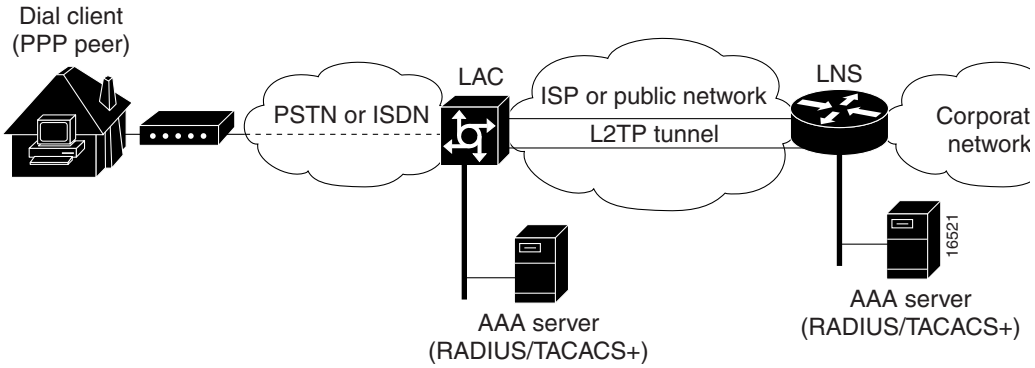
Layer 2 Tunnel Protocol

Feature Summary

The Layer 2 Tunnel Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. VPNs are cost-effective because users can connect to the Internet locally and tunnel back to connect to corporate resources. This not only reduces overhead costs associated with traditional remote access methods, but also improves flexibility and scalability.

Traditional dial-up networking services only support registered IP addresses, which limits the types of applications that are implemented over VPNs. L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. This allows the existing access infastructure, such as the Internet, modems, access servers, and ISDN terminal adapters (TAs), to be used. It also allows enterprise customers to outsource dialout support, thus reducing overhead for hardware maintenance costs and 800 number fees, and allows them to concentrate corporate gateway resources. Figure 1 shows the L2TP architecture in a typical dial up environment.

Figure 1 L2TP Architecture



L2TP offers the same full-range spectrum of features as L2F, but offers additional functionality. A L2TP-capable home gateway will work with an existing L2F network access server and will concurrently support upgraded components running L2TP. LNSs do not require reconfiguration each time an individual LAC is upgraded from L2F to L2TP. Table 1 offers a comparison of L2F and L2TP feature components.

Table 1 L2F and L2TP Feature Comparison

Function	L2F	L2TP
Flow Control	No	Yes
AVP hiding	No	Yes
Home gateway load sharing	Yes	Yes
Home gateway stacking	Yes	Yes
Home gateway primary and secondary backup	Yes	Yes
DNS name support	Yes	Yes
Domain name flexibility	Yes	Yes
Idle and absolute timeout	Yes	Yes
Multilink PPP support	Yes	Yes
Multichassis Multilink PPP support	Yes	Yes
Multihop support	Yes	Yes
Security	• All security benefits of PPP, including multiple per-user authentication options (CHAP, MS-CHAP, PAP). • Tunnel authentication mandatory	• All security benefits of PPP, including multiple per user authentication options (CHAP, MS-CHAP, PAP). • Tunnel authentication optional

Benefits

L2TP offers the following benefits:

- Vendor interoperability.
- Can be used as part of the wholesale access solution, which allows ISPs to the telco or service providers offer VPNs to Internet Service Providers (ISPs) and other service providers.
- Can be operated as a client initiated VPN solution, where enterprise customers using a PC, can use the client initiated L2TP from a third party.
- All value-added features currently available with Cisco's L2F, such as load sharing and backup support, will be available in future IOS releases of L2TP.
- Supports Multihop, which enables Multichassis Multilink PPP in multiple home gateways. This allows you to stack home gateways so that they appear as a single entity.

List of Terms

attribute-value pair (AV pair)—A generic pair of values passed from a AAA server to a AAA client. For example, in the AV pair user = bill, "user" is the attribute and "bill" is the value.

calling line identification (CLID)— A unique number that informs the called party of the phone number identification of the calling party.

challenge handshake authentication protocol (CHAP)—A PPP cryptographic challenge/response authentication protocol in which the cleartext password is not passed over the line. This allows the secure exchange of a shared secret between the two endpoints of a connection.

client—Instigator of the PPP session. Also referred to as the PPP client, or PPP peer.

cloning—Creating and configuring a virtual access interface by applying a specific virtual template interface. The template is the source of the generic user information and router-dependent information. The result of cloning, is a virtual access interface configured with all the commands in the template.

control messages—Exchange messages between the LAC and LNS pairs, operating in-band within the tunnel protocol. Control messages govern the aspects of the tunnel and sessions within the tunnel.

dial user—An end system or router attached to an on-demand PSTN or ISDN, which is either the initiator or recipient of a call. Also referred to as a dial-up or virtual dial-up client.

Dialed Number identification Service (DNIS)—The called party number. Typically, this is a number used by call centers or a central office where different numbers are each assigned to a specific service.

Integrated Services Digital Network (ISDN)—Communication protocols offered by telephone companies that permit telephone networks to carry date, voice, and other source traffic.

Layer 2 Tunnel Protocol (L2TP)—A Layer 2 tunneling protocol that is an extension to the PPP protocol used for Virtual Private Networks (VPNs). L2TP merges the best features of two existing tunneling protocols: Microsoft's PPTP and Cisco's L2F. It is the emerging IETF standard, currently being drafted by participants from Ascend, Cisco Systems, Copper Mountain Networks, IBM, Microsoft, and 3Com.

Link Control Protocol (**LCP)**—A protocol that establishes, configures, and tests data link connections used by PPP.

L2TP access concentrator (LAC)—An L2TP device that the client directly connects to and whereby PPP frames are tunneled to the L2TP network server (LNS). The LAC needs only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. It may tunnel any protocol carried within PPP. The LAC is the initiator of incoming calls and the receiver of outgoing calls. Analogous to the Layer 2 Forwarding (L2F) network access server (NAS).

L2TP network server (LNS)—Termination point for L2TP tunnel and access point where PPP frames are processed and passed to higher layer protocols. An LNS operates on any platform capable of PPP termination. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single media over which L2TP tunnels arrive. The LNS may have a single LAN or WAN interface, yet still be able to terminate calls arriving at any of the LACs full range of PPP interfaces (asynchronous, synchronous, ISDN, V.120, etc.). The LNS is the initiator of outgoing calls and the receiver of incoming calls. Analogous to the Layer 2 Forwarding (L2F) home gateway (HGW).

Multiplex Identifier (MID)—The number associated with a specific user's L2TP/L2F session.

Multilink PPP Protocol (MLP)—A protocol that provides the capability of splitting and recombining packets to a single end system across a logical pipe (also called a bundle) formed by multiple links. Multilink PPP provides bandwidth on demand and reduces transmission latency across WAN links.

Network Access Server (NAS)—A device providing temporary, on-demand network access to users. The access is point-to-point typically using PSTN or ISDN lines. A NAS may also serve as a LAC, LNS, or both. In Cisco's implementation for L2TP, the NAS serves as a LAC for incoming calls and serves as a LNS for outgoing calls. The NAS is synonymous with LAC.

Network Control protocol (NCP)—PPP protocol for negotiation of OSI Layer 3 (the network layer) parameters.

Password Authentication Protocol (PAP)—A simple PPP authentication mechanism in which a cleartext username and password are transmitted to prove identity. PAP is not as secure as CHAP because the password is passed in "cleartext."

point-of-presence (POP)—The access point to a service provider's network.

Point-to-Point Protocol (PPP)—A protocol that encapsulates network layer protocol information over point-to-point links. The RFC for PPP is RFC 1661.

Point-to-Point Tunneling Protocol (PPTP)—Microsoft's Point to Point Tunneling Protocol. Some of the features in L2TP were derived from PPTP.

public switched telephone network (PSTN)—Telephone networks and services in place worldwide.

session—A single, tunneled PPP session. Also referred to as a call.

tunnel—A virtual pipe between the LAC and LNS that can carry multiple PPP sessions.

tunnel ID—A two-octet value that denotes a tunnel between a LAC and LNS

virtual access interface—Instance of a unique virtual interface that is created dynamically and exists temporarily. Virtual access interfaces can be created and configured differently by different applications, such as virtual profiles and virtual private dialup networks.Virtual access interfaces are cloned from virtual template interfaces.

virtual template interface—A logical interface configured with generic configuration information for a specific purpose or configuration common to specific users, plus router-dependent information. The template takes the form of a list of Cisco IOS interface commands that are applied to virtual access interfaces, as needed.

Virtual Private Dialup Networking (VPDN)—A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPDNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the LNS, instead of the LAC.

zero length body message (ZLB)—A control or payload packet that only contains an L2TP header and does not contain any control message information or PPP payload. ZLB messages are used explicitly for acknowledging packets on the control or data channel.

Restrictions

The following restrictions apply to the L2TP feature:

- If flow control is enabled using the **l2tp flow-control receive-window** command with a value greater than zero, the switching path defaults to process level switching.
- Only dial in support currently exists.

Platforms

For 12.0T IOS Releases, L2TP is supported on the following platforms:

- Cisco 1003, Cisco 1004, and Cisco 1005
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 2800 series
- Cisco 2900 series
- Cisco 3600 series
- Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M)
- Cisco AS5200
- Cisco AS5300
- Cisco 6400 series
- Cisco 7200 series
- Cisco 7500 series

For 11.3AA IOS Releases, L2TP is supported on the following platforms:

- Cisco 7200 series
- Cisco AS5200
- Cisco AS5300
- Cisco AS5800

Prerequisites

A Cisco router or access server must be using a Cisco IOS software image that supports VPDN and the hardware platform you are using.

Supported MIBs and RFCs

L2TP is an emerging standard and currently supports the L2TP Internet Engineering Task Force (IETF) draft document.

Functional Description

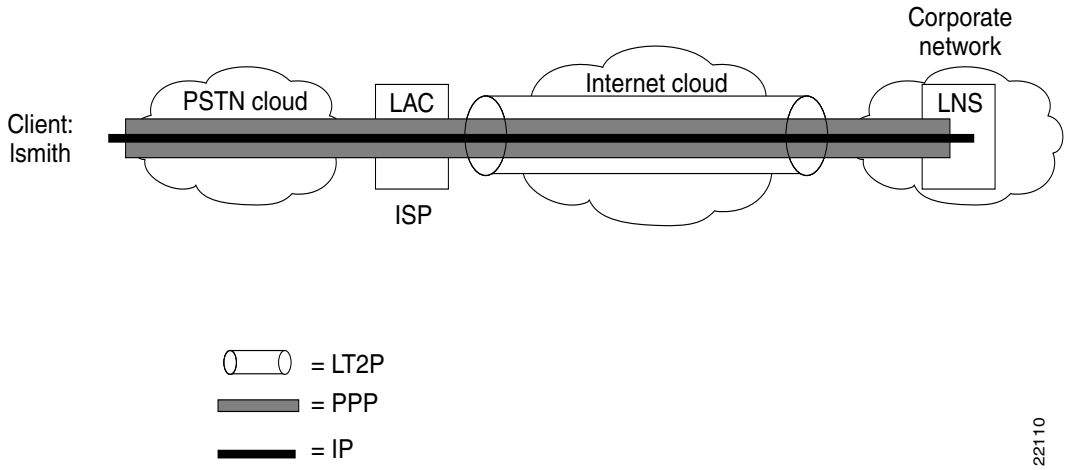
The following sections are included as part of the functional description:

- L2TP Overview
- Incoming Call Sequence
- LAC AAA Tunnel Definition Lookup

L2TP Overview

The following sections supply additional detail about the interworkings and Cisco's implementation of L2TP. Using L2TP tunneling, an Internet Service Provider (ISP), or other access service, can create a virtual tunnel to link customer's remote sites or remote users with corporate home networks. The L2TP access concentrator (LAC) located at the ISP's point of presence (POP) exchanges PPP messages with remote users and communicates by way of L2TP requests and responses with the customer's L2TP network server (LNS) to set up tunnels. L2TP passes protocol-level packets through the virtual tunnel between end points of a point-to-point connection. Frames from remote users are accepted by the ISP's POP, stripped of any linked framing or transparency bytes, encapsulated in L2TP and forwarded over the appropriate tunnel. The customer's home gateway accepts these L2TP frames, strips the L2TP encapsulation, and processes the incoming frames for the appropriate interface. Figure 2 shows the L2TP tunnel detail and how user "lsmith" connects to the LNS to access the designated corporate intranet.

Figure 2 L2TP Tunnel Structure



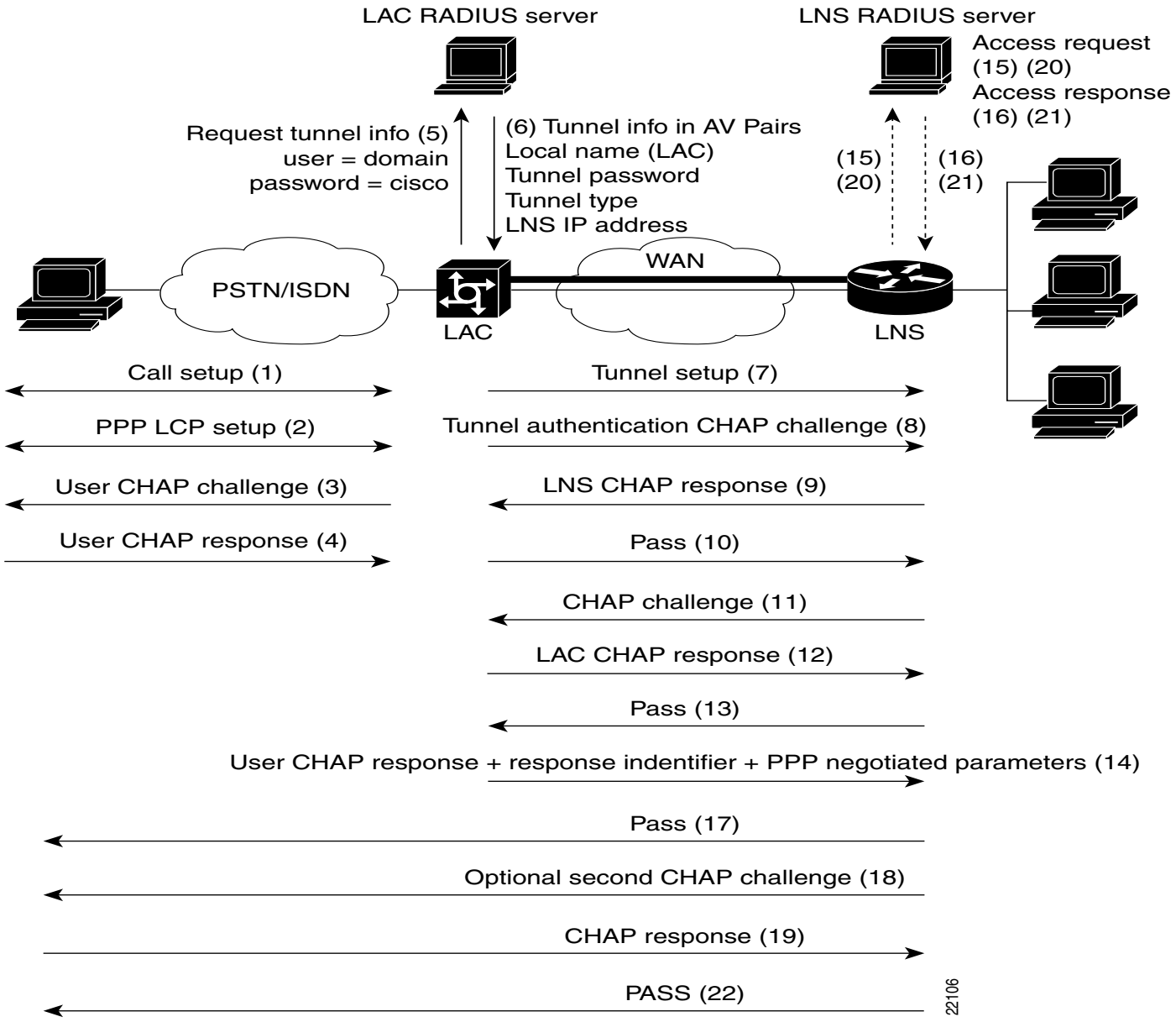
Incoming Call Sequence

A VPDN connection between a remote user, a LAC at the ISP point-of-presence (POP), and the LNS at the home LAN using an L2TP tunnel is accomplished as follows:

1. The remote user initiates a PPP connection to the ISP, using the analog telephone system or ISDN.
2. The ISP network LAC accepts the connection at the POP and the PPP link is established.
3. After the end user and LNS negotiate LCP, the LAC partially authenticates the end user with CHAP or PAP. The username, domain name, or DNIS is used to determine whether the user is a VPDN client. If the user is not a VPDN client, authentication continues, and the client will access the Internet or other contacted service. If the username is a VPDN client, the mapping will name a specific endpoint (the LNS).
4. The tunnel end points, the LAC and the LNS, authenticate each other before any sessions are attempted within a tunnel. Alternatively, the LNS can accept tunnel creation without any tunnel authentication of the LAC.
5. Once the tunnel exists, an L2TP session is created for the end user.
6. The LAC will propagate the LCP negotiated options and the partially authenticated CHAP/PAP information to the LNS. The LNS will funnel the negotiated options and authentication information directly to the virtual access interface. If the options configured on the virtual template interface does not match the negotiated options with the LAC, the connection will fail, and a disconnect is sent to the LAC.

The end result is that the exchange process appears to be between the dial-up client and the remote LNS exclusively, as if no intermediary device (the LAC) is involved. Figure 3 offers a pictorial account of the L2TP incoming call sequence with its own corresponding sequence numbers. Note the sequence numbers in figure 3 are not related to the sequence numbers described above.

Figure 3 L2TP Incoming Call Flow



LAC AAA Tunnel Definition Lookup

AAA tunnel definition look up allows the LAC to look up tunnel definitions using key words. Two new Cisco AV pairs are added to support LAC tunnel definition lookup: **tunnel type** and **l2tp-tunnel-password**. These AV pairs are configured on the Radius server. A description of the values are as follows:

tunnel type—Indicates the tunnel type is either L2F or L2TP. This is an optional AV pair and if not defined, reverts to L2F, the default value. If you want to configure an L2TP tunnel, you must use the L2TP AV pair value. This command is case sensitive.

l2tp-tunnel-password—This value is the secret (password) used for L2TP tunnel authentication and L2TP AV pair hiding. This is an optional AV pair value; however, if it is not defined, the secret will default to the password associated with the local name on the LAC local username-password database. This AV pair is analogous to the **l2tp local secret** CLI command. For example:

```
request dialin l2tp ip 172.21.9.13 domain cisco.com
l2tp local name dustie
l2tp local secret partner
```

is equivalent to the following RADIUS server configuration:

```
cisc.com Password = "cisco"
cisco-avpair = "vpdn: tunnel-id=dustie",
cisco-avpair = "vpdn: tunnel-type=l2tp",
cisco-avpair = "vpdn: l2tp-tunnel-password=partner',
cisco-avpair = "vpdn: ip-addresses=172.21.9.13"
```

Before You Begin

Before you configure your router or access server for VPDN using L2TP, you should proceed in one of two ways:

- Configure VPDN using local authentication by using the **hostname** command and verify peer-to-peer connectivity.

or

- Configure security attributes using AAA, TACACS+, or RADIUS and confirm peer-to-peer connectivity before configuring the LAC and LNS for VPDN.

Frequently problems arise when too many components are configured simultaneously and deciphering problems can become convoluted. Therefore, you should configure components independently and confirm connectivity before adding another component.

Authentication commands that are frequently used with VPDN are listed below. Use these commands to enable the AAA access control system and to define login and PPP access:

Step	Command	Purpose
1	**aaa new-model**	Enables the AAA access control system.
2	**aaa authentication login default local**	Enables AAA authentication at login and use the local username database for authentication.
3	**aaa authentication ppp default local**	Enables AAA authentication on serial interfaces running Point-to-Point Protocol (PPP) and use the local username database for authentication.

Note Refer to the Cisco IOS *Security Configuration Guide* for a complete list of commands and configurable options for security and AAA implementation.

Configuration Tasks

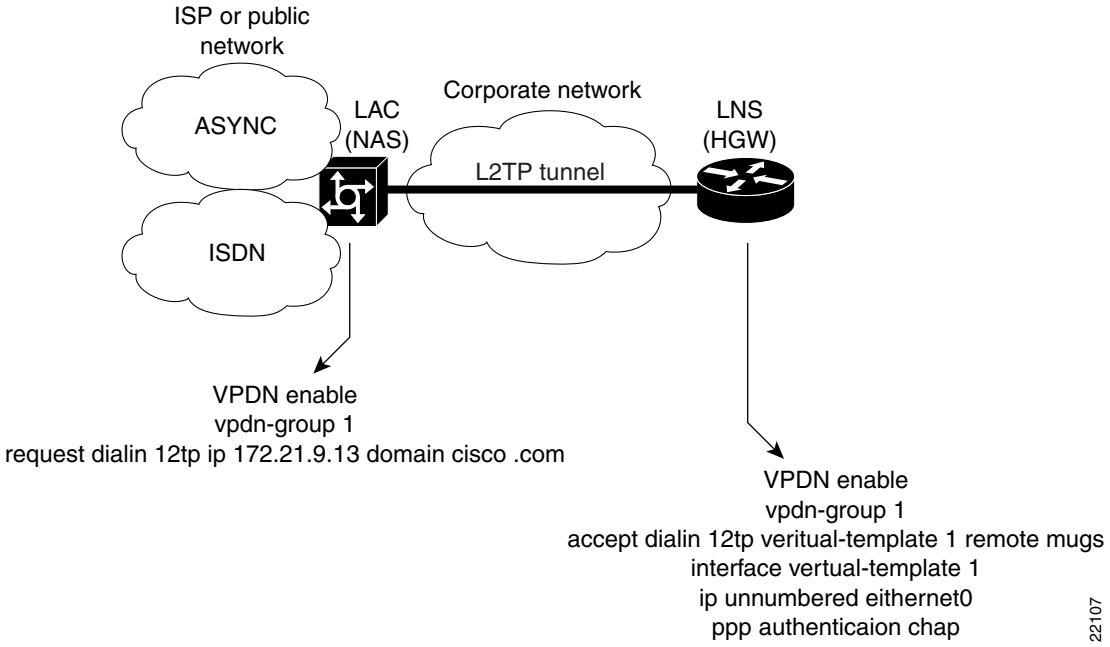
The three primary components involved in implementing VPDN are:

1. Enable VPDN on the LAC and LNS.
2. Define a VPDN group, to which you will apply all VPDN attributes for the LAC and LNS.
3. Enable the LAC and LNS to request and receive L2TP tunnels.

Subsequently, you can configure a virtual template interface, which applies defined attributes to virtual access interfaces, which will then pass link-layer frames over the L2TP tunnel.

Figure 4 shows the basic commands required for VPDN. Additional VPDN and L2TP commands can be applied as needed, in order to fine-tune parameters to suit your network characteristics.

Figure 4 VPDN Configuration Commands



To configure, monitor, and troubleshoot VPDN, perform the tasks in the following sections:

- Configure VPDN on the L2TP Access Concentrator (LAC)
- Configure VPDN on a L2TP Network Server (LNS)
- Monitor and Troubleshooting VPDN and L2TP

Configure VPDN on the L2TP Access Concentrator (LAC)

The LAC is a device that is typically (although not always) located at a service provider's POP and initial configuration and ongoing management is done by the service provider. Use the following commands to enable VPDN on a LAC using L2TP beginning in global configuration mode:

Step	Command	Purpose
1	**vpdn enable**	Enables VPDN and inform the router to look for tunnel definitions from an LNS.

Step	Command	Purpose
2	**vpdn group** *group-number*	Defines a local group number identifier for which other VPDN variables can be assigned.Valid group numbers range between 1 and 3000.
3	**request dialin** [**l2f** | **l2tp**] **ip** *ip-address* {**domain** *domain-name* | **dnis** *dialed-number*}	Enables the router to request a dial in tunnel to an IP address, if the dial in user belongs to a specific domain or the dial in user dialed a specific DNIS.

Configure VPDN on a L2TP Network Server (LNS)

The LNS is the termination point for an L2TP tunnel. The LNS initiates outgoing calls and receives incoming calls from the LAC. To configure the LNS to initiate and receive calls, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	**vpdn enable**	Enables VPDN and inform the router to look for tunnel definitions from an LNS.
2	**vpdn group** *group-number*	Defines a local group number identifier for which other VPDN variables can be assigned.Valid group numbers range between 1 and 3000.
3	**accept dialin** [**l2f** | **l2tp** | **any**] **virtual-template** *virtual-template number* **remote** *remote-peer-name*	Allows the LNS to accept an open tunnel request from the specified remote peer, define the Layer 2 protocol to use for the tunnel, and identify the virtual template to use for cloning virtual access interfaces.

At this point, you can configure the virtual template interface with configuration parameters you want applied to virtual access interfaces. A virtual template interface is a logical entity configured for a serial interface. The virtual template interface is not tied to any physical interface and is applied dynamically, as needed. Virtual access interfaces are *cloned* from a virtual template interface, used on demand, and then freed when no longer needed. Use the following commands to create and configure a virtual template interface beginning in global configuration mode:

Step	Command	Purpose
1	**interface virtual-template** *number*	Creates a virtual template interface, and enter interface configuration mode.
2	**ip unnumbered ethernet 0**	Enables IP without assigning a specific IP address on the LAN.
3	**encapsulation ppp**	Enables PPP encapsulation on the virtual template interface, which will be applied to virtual access interfaces.
4	**ppp authentication pap** | **chap**	Enables PAP or CHAP authentication on the virtual template interface, which will be applied to virtual access interfaces.

Optionally, you can configure other commands for the virtual template interface. For information about configuring virtual template interfaces, see the “Configuring Virtual Template Interfaces” chapter in the *Dial Solutions Configuration Guide*.

Review the "Command Reference" section in this document to learn about commands you can use to scale and enhance VPDN and L2TP features.

Monitor and Troubleshooting VPDN and L2TP

Troubleshooting components in VPDN is not always straightforward because there are multiple technologies and OSI layers involved. The following EXEC commands will help you isolate and identify problems on VPDNs using L2TP tunnels:

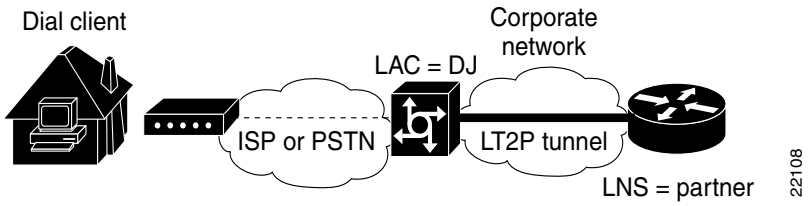
Command	Purpose
clear vpdn tunnel [**l2f** [**nas-name** | **hgw-name**] | **l2tp** [**remote-name** | **local-name**]]	Shuts down a specific tunnel and all the sessions within the tunnel.
debug ppp negotiation	Displays information about packets transmitted during PPP start-up and detailed PPP negotiation options.
debug ppp chap	Displays CHAP packet exchanges.
debug vpdn event [**protocol** | **flow-control**]	Displays VPDN errors and basic events within the protocol (such as L2TP, L2F, PPTP) and errors associated with flow control. Flow control is only possible if you are using L2TP and the remote peer "receive window" is configured for a value greater than zero.
debug vpdn packet [**control** | **data**] [**detail**]	Displays protocol-specific packet header information, such as sequence numbers if present, such as flags and length.
show interface virtual access *number*	Displays information about the virtual access interface, LCP, protocol states, and interface statistics. The status of the virtual access interface should be: "`Virtual-Access3 is up, line protocol is up`"
show vpdn session [**all** [**interface** | **tunnel** | **username**] | **packets** | **sequence** | **state** | **timers** | **window**]	Displays VPDN session information including interface, tunnel, username, packets, status, and window statistics.
show vpdn tunnel [**all** [**id** | **local-name** | **remote-name**] | **packets** | **state** | **summary** | **transport**]	Displays VPDN tunnel information including tunnel protocol, id, local and remote tunnel names, packets sent and received, tunnel, and transport status.

See the "Debug Examples" section in this document for sample output for the commands listed above.

Configuration Examples

- LAC Configuration Example
- LNS Configuration Example

Figure 5 Topology Configuration for Configuration Examples



LAC Configuration Example

The following is a basic L2TP configuration for the LAC for the topology shown in Figure 5. The local name is not defined so the hostname used as the local name. Because the L2TP tunnel password is not defined, the username password, DJ, is used.

```
! Enable AAA globally
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
authentication
aaa authentication ppp default local
! Define the username as "DJ"
username DJ password 7 030C5E070A00781B
! Enable VPDN
vpdn enable
! Define VPDN group number 1
vpdn-group 1
! Allow the LAC to respond to dialin requests using L2TP from IP address 172.21.9.13
  domain "cisco.com"
request dialin l2tp ip 172.21.9.13 domain cisco.com
```

LNS Configuration Example

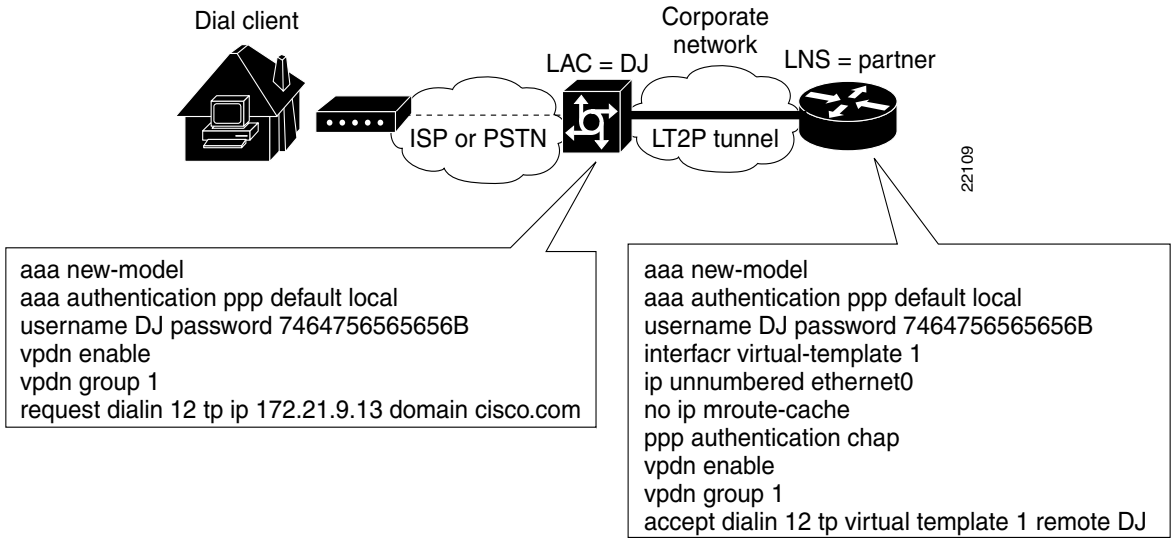
The following is a basic L2TP configuration example with corresponding comments on the LNS for the topology shown in Figure 5.

```
! Enable AAA globally
aaa new-model
! Enable AAA authentication for PPP and list the default method to use for PPP
authentication
aaa authentication ppp default local
! Define the username as "partner"
username partner password 7 030C5E070A00781B
! create virtual-template 1 and assign all values for virtual access interfaces
interface Virtual-Template1
! Borrow the IP address from interface ethernet 1
 ip unnumbered Ethernet0
! Disable multicast fast switching
 no ip mroute-cache
! Use CHAP to authenticate PPP
 ppp authentication chap
! Enable VPDN
vpdn enable
! Create vpdn-group number 1
vpdn-group 1
! Accept all dialin l2tp tunnels from virtual-template 1 from remote peer DJ
accept dialin l2tp virtual-template 1 remote DJ
```

Debug Examples

- LAC Debug Example
- LAC Problem Debug
- LNS Debug Example
- Debug PPP Negotiation Example
- Debug PPP Chap Example
- Debug VPDN Events Examples
- Show Interface Virtual Access Example
- Show VPDN Session Examples
- Show VPDN Tunnel Examples

Figure 6 Topology Diagram for Debug Example



LAC Debug Example

The following is a successful debug example for the topology shown in Figure 6.

```
DJ# show debug

VPDN events debugging is on
VPDN protocol events debugging is on
DJ#
20:47:33: %LINK-3-UPDOWN: Interface Async7, changed state to up
20:47:35: As7 VPDN: Looking for tunnel -- cisco.com --
20:47:35: As7 VPDN: Get tunnel info for cisco.com with NAS DJ, IP 172.21.9.13
20:47:35: As7 VPDN: Forward to address 172.21.9.13
20:47:35: As7 VPDN: Forwarding...
20:47:35: As7 VPDN: Bind interface direction=1
20:47:35: Tnl/Cl 8/1 L2TP: Session FS enabled
20:47:35: Tnl/Cl 8/1 L2TP: Session state change from idle to wait-for-tunnel
20:47:35: As7 8/1 L2TP: Create session
20:47:35: Tnl 8 L2TP: SM State idle
20:47:35: Tnl 8 L2TP: Tunnel state change from idle to wait-ctl-reply
20:47:35: Tnl 8 L2TP: SM State wait-ctl-reply
20:47:35: As7 VPDN: kath@cisco.com is forwarded
20:47:35: Tnl 8 L2TP: Got a challenge from remote peer, DJ
20:47:35: Tnl 8 L2TP: Got a response from remote peer, DJ
20:47:35: Tnl 8 L2TP: Tunnel Authentication success
20:47:35: Tnl 8 L2TP: Tunnel state change from wait-ctl-reply to established
20:47:35: Tnl 8 L2TP: SM State established
20:47:35: As7 8/1 L2TP: Session state change from wait-for-tunnel to wait-reply
20:47:35: As7 8/1 L2TP: Session state change from wait-reply to established
20:47:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async7, changed state to up
```

The following is output from the **show vpdn** command for the LAC (DJ):

```
show vpdn

L2TP Tunnel and Session Information (Total tunnels=1 sessions=1)
LocID RemID Remote Name   State  Remote Address  Port  Sessions
8     7     Partner       est    172.21.9.13     1701  1

LocID RemID TunID Intf    Username      State  Last Chg
1     1     8     As7     kath@cisco.com est    00:00:37
```

LAC Problem Debug

The following example assumes that you suspect an error in parsing control packets. You can use the **debug vpdn packet** using the **control** keyword to verify control packet information.

```
debug vpdn packet control

20:50:27: %LINK-3-UPDOWN: Interface Async7, changed state to up
20:50:29: Tnl 9 L2TP: O SCCRQ
20:50:29: Tnl 9 L2TP: O SCCRQ, flg TLF, ver 2, len 131, tnl 0, cl 0, ns 0, nr 0
20:50:29: contiguous buffer, size 131
         C8 02 00 83 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 ...
20:50:29: Tnl 9 L2TP: Parse AVP 0, len 8, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Parse SCCRP
20:50:29: Tnl 9 L2TP: Parse AVP 2, len 8, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Protocol Ver 256
20:50:29: Tnl 9 L2TP: Parse AVP 3, len 10, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Framing Cap 0x0x3
20:50:29: Tnl 9 L2TP: Parse AVP 4, len 10, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Bearer Cap 0x0x3
20:50:29: Tnl 9 L2TP: Parse AVP 6, len 8, flag 0x0x0
20:50:29: Tnl 9 L2TP: Firmware Ver 0x0x1120
20:50:29: Tnl 9 L2TP: Parse AVP 7, len 12, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Hostname DJ
20:50:29: Tnl 9 L2TP: Parse AVP 8, len 25, flag 0x0x0
20:50:29: Tnl 9 L2TP: Vendor Name Cisco Systems, Inc.
20:50:29: Tnl 9 L2TP: Parse AVP 9, len 8, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Assigned Tunnel ID 8
20:50:29: Tnl 9 L2TP: Parse AVP 10, len 8, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Rx Window Size 4
20:50:29: Tnl 9 L2TP: Parse AVP 11, len 22, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Chlng D807308D106259C5933C6162ED3A1689
20:50:29: Tnl 9 L2TP: Parse AVP 13, len 22, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Chlng Resp 9F6A3C70512BD3E2D44DF183C3FFF2D1
20:50:29: Tnl 9 L2TP: No missing AVPs in SCCRP
20:50:29: Tnl 9 L2TP: Clean Queue packet 0
20:50:29: Tnl 9 L2TP: I SCCRP, flg TLF, ver 2, len 153, tnl 9, cl 0, ns 0, nr 1
 contiguous pak, size 153
         C8 02 00 99 00 09 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
         00 03 00 00 00 03 80 0A 00 00 00 04 00 00 00 ...
20:50:29: Tnl 9 L2TP: I SCCRP from DJ
20:50:29: Tnl 9 L2TP: O SCCCN  to DJ tnlid 8
20:50:29: Tnl 9 L2TP: O SCCCN, flg TLF, ver 2, len 42, tnl 8, cl 0, ns 1, nr 1
20:50:29: contiguous buffer, size 42
         C8 02 00 2A 00 08 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 4B 2F A2 50 30 13
         E3 46 58 D5 35 8B 56 7A E9 85
20:50:29: As7 9/1 L2TP: O ICRQ to DJ 8/0
20:50:29: As7 9/1 L2TP: O ICRQ, flg TLF, ver 2, len 48, tnl 8, cl 0, ns 2, nr 1
20:50:29: contiguous buffer, size 48
         C8 02 00 30 00 08 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 08 00 00 00 0E 00 01 80 0A 00 00
         00 0F 00 00 00 04 80 0A 00 00 00 12 00 00 00 ...
20:50:29: Tnl 9 L2TP: Clean Queue packet 1
20:50:29: Tnl 9 L2TP: Clean Queue packet 2
20:50:29: Tnl 9 L2TP: I ZLB ctrl ack, flg TLF, ver 2, len 12, tnl 9, cl 0, ns 1, nr 2
 contiguous pak, size 12
         C8 02 00 0C 00 09 00 00 00 01 00 02
20:50:30: As7 9/1 L2TP: Parse AVP 0, len 8, flag 0x0x8000 (M)
20:50:30: As7 9/1 L2TP: Parse ICRP
20:50:30: As7 9/1 L2TP: Parse AVP 14, len 8, flag 0x0x8000 (M)
20:50:30: As7 9/1 L2TP: Assigned Call ID 1
```

```
20:50:30: As7 9/1 L2TP: No missing AVPs in ICRP
20:50:30: Tnl 9 L2TP: Clean Queue packet 2
20:50:30: As7 9/1 L2TP: I ICRP, flg TLF, ver 2, len 28, tnl 9, cl 1, ns 1, nr 3
 contiguous pak, size 28
         C8 02 00 1C 00 09 00 01 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 01
20:50:30: As7 9/1 L2TP: O ICCN to DJ 8/1
20:50:30: As7 9/1 L2TP: O ICCN, flg TLF, ver 2, len 203, tnl 8, cl 1, ns 3, nr 2
20:50:30: contiguous buffer, size 203
         C8 02 00 CB 00 08 00 01 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 00 00 DA C0 80 0A
         00 00 00 13 00 00 00 02 00 28 00 00 00 1B 02 ...
20:50:30: Tnl 9 L2TP: Clean Queue packet 3
20:50:30: As7 9/1 L2TP: I ZLB ctrl ack, flg TLF, ver 2, len 12, tnl 9, cl 1, ns 2, nr 4
 contiguous pak, size 12
         C8 02 00 0C 00 09 00 01 00 02 00 04
20:50:30: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async7, changed state to up
```

LNS Debug Example

The following is a successful debug example output from the LNS using the **debug vpdn protocol** command with the **events** keyword:

```
debug vpdn protocol events
20:19:17: L2TP: I SCCRQ from DJ tnl 8
20:19:17: L2X: Never heard of DJ
20:19:17: Tnl 7 L2TP: New tunnel created for remote DJ, address 172.21.9.4
20:19:17: Tnl 7 L2TP: Got a challenge in SCCRQ, DJ
20:19:17: Tnl 7 L2TP: Tunnel state change from idle to wait-ctl-reply
20:19:17: Tnl 7 L2TP: Got a Challenge Response in SCCCN from DJ
20:19:17: Tnl 7 L2TP: Tunnel Authentication success
20:19:17: Tnl 7 L2TP: Tunnel state change from wait-ctl-reply to established
20:19:17: Tnl 7 L2TP: SM State established
20:19:17: Tnl/Cl 7/1 L2TP: Session FS enabled
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from idle to wait-for-tunnel
20:19:17: Tnl/Cl 7/1 L2TP: New session created
20:19:17: Tnl/Cl 7/1 L2TP: O ICRP to DJ 8/1
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from wait-for-tunnel to wait-connect
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from wait-connect to established
20:19:17: Vi1 VPDN: Virtual interface created for kath@cisco.com
20:19:17: Vi1 VPDN: Set to Async interface
20:19:17: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
20:19:18: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
20:19:18: Vi1 VPDN: Bind interface direction=2
20:19:18: Vi1 VPDN: PPP LCP accepting rcv CONFACK
20:19:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed
state to up
```

The following is sample outpout on the LNS using the **show vpdn** command:

```
sh vpdn
L2TP Tunnel and Session Information (Total tunnels=1 sessions=1)
LocID RemID Remote Name   State  Remote Address  Port  Sessions
7     8     DJ            est    172.21.9.4      1701  1

LocID RemID TunID Intf    Username      State  Last Chg
1     1     7     Vi1     kath@cisco.com est    00:00:28
```

Debug PPP Negotiation Example

The following is sample output from the **debug ppp negotiation** command where the negotiated LCP options do not match between the LAC and the LNS. You may want to enable the **lcp renegotiation on-mismatch** command to enable the LNS to renegotiate LCP directly with the client.

```
Router# debug ppp nego
ppp: sending CONFREQ, type = 3 (CI_AUTHTYPE), value = C223/5
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 43C5B1AE
PPP BRI7: B-Channel 1: O LCP CONFREQ(1) id 44 (F) AUTHTYPE (5) 194 35 5
MAGICNUMBER (6) 67 197 177 174
PPP BRI7: B-Channel 1(i): pkt type 0xC021, datagramsize 34
PPP BRI7: B-Channel 1: I LCP CONFREQ(1) id 1 (1E) ?? (4) 0 0
MRU (4) 5 244
AUTHTYPE (5) 194 35 5
PPP BRI7: B-Channel 1(i): pkt type 0xC021, datagramsize 19
Type11 (4) 5 244
Type13 (9) 3 0 192 123 68 241 33
PPP BRI7: B-Channel 1: input(C021) state = REQSENT code = CONFREQ(1) id = 1
len = 30
ppp: received config for type = 0 (??)

ppp: rcvd unknown option 0 rejected
```

The **debug ppp negotiation** and **debug ppp chap** commands are enabled to decipher a CHAP negotiation problem. This is due to a connectivity problem between a Cisco and non-Cisco device. Also note that the **service-timestamps** command is enabled on the router. The **service-timestamps** command is helpful to decipher timing and keepalive issues and we recommend that you always enable this command.

```
Router# debug ppp nego chap
3:22:53: ppp: sending CONFREQ, type = 3 (CI_AUTHTYPE), value = C223/5
3:22:53: ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = C6091F.
3:22:55: ppp: sending CONFREQ, type = 3 (CI_AUTHTYPE), value = C223/5
3:22:55: ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = C6091F
3:22:55: PPP BRI0: B-Channel 1: received config for type = 0x0 (??)
3:22:55: PPP BRI0: B-Channel 1: rcvd unknown option 0x0 rejected
3:22:55: PPP BRI0: B-Channel 1: received config for type = 0x1 (MRU) value = 0x5
F4 rejected
3:22:55: PPP BRI0: B-Channel 1: received config for type = 0x3 (AUTHTYPE) value
= 0xC223 value = 0x5 acked
3:22:55: PPP BRI0: B-Channel 1: received config for type = 0x11 (MULTILINK_MRRU)
rejected
3:22:55: PPP BRI0: B-Channel 1: received config for type = 0x13 (UNKNOWN)
3:22:55: PPP BRI0: B-Channel 1: rcvd unknown option 0x13 rejected
3:22:55: ppp: config REJ received, type = 3 (CI_AUTHTYPE), value = C223/5
3:22:55: ppp: sending CONFREQ, type = 3 (CI_AUTHTYPE), value = C223/5
3:22:55: ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = C6091F
3:22:55: PPP BRI0: B-Channel 1: received config for type = 0x3 (AUTHTYPE) value
= 0xC2.
Success rate is 0 percent (0/5)
moog#23 value = 0x5 acked
3:22:55: ppp: config REJ received, type = 3 (CI_AUTHTYPE), value = C223/5

3:22:55: ppp: BRI0: B-Channel 1 closing connection because remote won't authenti
cate

3:22:55: ppp: sending CONFREQ, type = 3 (CI_AUTHTYPE), value = C223/5
3:22:55: ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = C6091F
3:22:55: %ISDN-6-DISCONNECT: Interface BRI0: B-Channel 1  disconnected from 0123
5820040 , call lasted 2 seconds
3:22:56: %LINK-3-UPDOWN: Interface BRI0: B-Channel 1, changed state to down
Indication:
```

Debug PPP Chap Example

The following **debug ppp chap** excerpt shows a CHAP authentication failure because a configuration mismatch between devices. Verifying and correcting any username and password mismatch should remedy this problem.

```
Router# debug ppp chap
ppp: received conf.ig for type = 5 (MAGICNUMBER) value = 1E24718 acked
PPP BRI0: B-Channel 1: state = ACKSENT fsm_rconfack(C021): rcvd id E6
ppp: config ACK received, type = 3 (CI_AUTHTYPE), value = C223
ppp: config ACK received, type = 5 (CI_MAGICNUMBER), value = 28CEF76C
BRI0: B-Channel 1: PPP AUTH CHAP input code = 1 id = 83 len = 16
BRI0: B-Channel 1: PPP AUTH CHAP input code = 2 id = 96 len = 28
BRI0: B-Channel 1: PPP AUTH CHAP input code = 4 id = 83 len = 21
BRI0: B-Channel 1: Failed CHAP authentication with remote.
Remote message is: MD compare failed
```

Debug VPDN Events Examples

The following is a debug trace on the LAC using the **debug vpdn event** command with the **protocol** keyword. The L2TP tunnel failure is caused by an error in the tunnel password.

```
Router# debug vpdn event protocol
%LINK-3-UPDOWN: Interface Async7, changed state to up
As7 VPDN: Looking for tunnel -- cisco.com --
As7 VPDN: Get tunnel info for cisco.com with NAS partner, IP 172.21.9.13
As7 VPDN: Forward to address 172.21.9.13
As7 VPDN: Forwarding...
As7 VPDN: Bind interface direction=1
Tnl/Cl 10/1 L2TP: Session FS enabled
Tnl/Cl 10/1 L2TP: Session state change from idle to wait-for-tunnel
As7 10/1 L2TP: Create session
Tnl 10 L2TP: SM State idle1
Tnl 10 L2TP: Tunnel state change from idle to wait-ctl-reply
Tnl 10 L2TP: SM State wait-ctl-reply
As7 VPDN: kath@cisco.com is forwarded
Tnl 10 L2TP:I SCCRP from stella

Tnl 10 L2TP: Tunnel Authentication fails for partner------>> TUNNEL FAILURE

Tnl 10 L2TP: Tunnel state change from wait-ctl-reply to shutting-down
Tnl 10 L2TP: Shutdown tunnel
As7 10/1 L2TP: Destroying session
As7 10/1 L2TP: Session state change from wait-for-tunnel to idle10
Tnl 10 L2TP: Tunnel state shutting-down while destroying session
Tnl 10 L2TP: Tunnel state change from shutting-down to idle
Mar  1 01:04:32: %LINK-3-UPDOWN: Interface Async7, changed state to down
As7 VPDN: Reset
A77 VPDN: Cleanup
As7 VPDN: Reset
As7 VPDN: Unbind interface
%LINK-5-CHANGED: Interface Async7, changed state to reset
%LINK-3-UPDOWN: Interface Async7, changed state to down
```

In this example, the **debug vpdn event protocol** command is enabled on the LNS. The LNS does not agree with the LCP CONFACK sent by the LAC to the client. The LAC has done LCP negotiation on behalf of the LNS and the CONFACK sent contained the LCP options that the LAC agreed on with the client (on behalf of the LNS). To remedy this problem you can do one of two things: check the configuration for the virtual-template on the LNS and the dialin interfaces on the

LAC to ensure they match, or use the **lcp renegotiation on-mismatch** command on the LNS. The **lcp-renegotiatoin on-mismatch** command forces renegotiation only if there is a mismatch between devices. Note that using the **lcp renegotiation on-mismatch** command will add a slight delay.

```
Router# debug vpdn event protocol
Tnl 12 L2TP: New tunnel created for remote partner, address 172.21.9.412
Tnl 12 L2TP: Tunnel state change from idle to wait-ctl-reply
Tnl 12 L2TP: Tunnel Authentication success
Tnl 12 L2TP: Tunnel state change from wait-ctl-reply to established
Tnl 12 L2TP: SM State established
Tnl/Cl 12/1 L2TP: Session FS enabled
Tnl/Cl 12/1 L2TP: Session state change from idle to wait-for-tunnel
Tnl/Cl 12/1 L2TP: New session created
Tnl/Cl 12/1 L2TP: Session state change from wait-for-tunnel to wait-connect
Tnl/Cl 12/1 L2TP: Session state change from wait-connect to established
Vi2 VPDN: Virtual interface created for kath@cisco.com
Vi2 VPDN: Set to Async interface
Vi2 VPDN: Clone from Vtemplate 1 filterPPP=1 blocking
%LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
Vi2 VPDN: Bind interface direction=2
Vi2 VPDN: PPP LCP accepted rcv CONFACK

VPDN: PPP LCP not accepting sent CONFACK

VPDN: Unbind interface
%LINK-3-UPDOWN: Interface Virtual-Access2, changed state to down
Vi2 VPDN: Cleanup
Vi2 VPDN: Reset
Vi2 VPDN: Unbind interface
Vi2 VPDN: Reset@cisco.com
Tnl 12/1 L2TP: ICCN Error getting virtual interface@cisco.com
Tnl 12/1 L2TP: Session state change from established to shutting-down bum1@cisco.com
Tnl 12/1 L2TP: Destroying session@cisco.com
Tn1 12/1 L2TP: Session state change from shutting-down to idle
Tnl 12 L2TP: Tunnel state change from established to no-sessions-left
Tnl 12 L2TP: No more sessions in tunnel, shutdown in 14 seconds
Tnl 12 L2TP: Shutdown tunnel
Tnl 12 L2TP: Tunnel state change from no-sessions-left to idle
```

Show Interface Virtual Access Example

The following is an example of the **show interface virtual access** command, which displays normal working status:

```
Router# show interface virtual-access 3
Virtual-Access3 is up, line protocol is up
   Hardware is Virtual Access interface
   MTU 1500 bytes, BW 128 Kbit, DLY 100000 usec, rely 255/255, load 1/255
   Encapsulation PPP, loopback not set, keepalive set (10 sec)
   DTR is pulsed for 5 seconds on reset
   LCP Open, multilink Open
   Open: IPCP
   Last input 00:02:30, output never, output hang never
   Last clearing of "show interface" counters 1d19h
   Queueing strategy: fifo
   Output queue 0/40, 0 drops; input queue 21/75, 0 drops
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
      55930 packets input, 3347967 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      105261 packets output, 9607052 bytes, 0 underruns
      0 output errors, 0 collisions, 0 interface resets
```

```
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Show VPDN Session Examples

By default, if the **show vpdn** command is used without any keywords or arguments, all tunnel and session information for all active sessions and tunnels is displayed:

```
Router# show vpdn
L2TP Tunnel and session Information (Total tunnels=1 sessions=1)
LocID RemID Remote Name   State  Remote Address  Port  Sessions
2     10    wander        est    172.21.9.13     1701  1
LocID RemID TunID Intf    Username      State  Last Chg
1     1     2     As7     kath@cisco.com est    00:23:01
L2F Tunnel and Session
 NAS CLID HGW CLID NAS Name        HGW Name        State
 10        2        stella          acadia          open
                    172.21.9.4      172.21.9.232
 CLID   MID    Username       Intf   State
 2      1      jdoe@hp.com     As6    open
```

The following is an example of the **show vpdn session** command, which summarizes status on all active tunnels:

```
Router# show vpdn session

L2TP Session Information (Total tunnels=1 sessions=1)

LocID RemID TunID Intf    Username      State  Last Chg
1     1     2     As7     bum1@cisco.co est    00:29:34

L2F Session

 CLID   MID    Username       Intf   State
 3      1      jdoe@hp.com     As6    open
```

Show VPDN Tunnel Examples

The following is sample output using the **show vpdn tunnel** command, which displays information about all active L2F and L2TP tunnels in summary-style format:

```
Router#sh vpdn tunnel

L2TP Tunnel Information (Total tunnels=1 sessions=1)
LocID RemID Remote Name   State  Remote Address  Port  Sessions
2     10    wander        est    172.21.9.13     1701  1
L2F Tunnel
 NAS CLID HGW CLID NAS Name        HGW Name        State
 9         1        stella          acadia          open
                    172.21.9.4      172.21.9.232
```

Use the **show vpdn tunnel** with the **all** keyword to display summary information about all active L2F and L2TP tunnels.

```
Router#show vpdn tunnel all
L2TP Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 2 is up, remote id is 10, 1 active session
  Tunnel state is established, time since change: 00:32:28
  Peer tunnel name is wander
    Internet Address: 172.21.9.13, port 1701
  Local tunnel name is stella
    Internet Address: 172.21.9.4, port 1701
```

```
  200 packets sent, 401 received, 5667 bytes sent, 11336 received
  Control Ss=4 Sr=2

L2F Tunnel
NAS name: stella
NAS CLID: 9
NAS IP address 172.21.9.4
Gateway name: acadia
Gateway CLID: 1
Gateway IP address 172.21.9.232
State: open
Packets out: 383
Bytes out: 8633
Packets in: 651
Bytes in: 29964
```

You can also use the **show vpdn session** command using the **all** and **username** keywords to display statistics about active L2F and L2TP tunnels. If there are no active tunnels, a "no active tunnel" message is displayed as seen below:

```
Router# show vpdn session all username bum1@cisco.com

L2TP Session Information (Total tunnels=1 sessions=1)
Call id 1 is up on tunnel id 2
Remote tunnel name is wander
  Internet Address: 172.21.9.13
  Session username is bum1@cisco.com, state is established
    Time since change: 00:34:28, Interface As7
    Remote call id: 1
    212 packets sent, 425 received, 6003 bytes sent, 12008 received
    Sequencing is on
      Ss=211 Sr=213  Remote Ns=212  Remote Nr=0  Out of order=0
      Remote has not requested congestion control

% No active L2F tunnels
```

The following output shows active L2F tunnel information for user kath@cisco.com and reports that there are no active L2TP tunnels:

```
Router#sh vpdn session all username kath@cisco.com

% No active L2TP tunnels

L2F Session
MID: 1
User: kath@cisco.com
Interface:  Async6
State:  open
Packets out: 139
Bytes out: 4518
Packets in: 422
Bytes in: 27013
```

Command Reference

This section documents new, existing, and modified commands that are used to configure, monitor, and troubleshoot L2TP and VPDNs:

- **accept dialin**
- **clear vpdn tunnel**

- **force-local-chap**
- **l2f ignore-mid-sequence**
- **l2f ignore-mid-sequence**
- **l2tp drop out-of-order**
- **l2tp flow-control backoff-queuesize**
- **l2tp flow-control maximum-ato**
- **l2tp flow-control receive-window**
- **l2tp flow-control static-rtt**
- **l2tp hidden**
- **l2tp ip udp checksum**
- **l2tp offset**
- **l2tp tunnel authentication**
- **l2tp tunnel hello**
- **l2tp tunnel password**
- **l2f ignore-mid-sequence**
- **local name**
- **lcp renegotiation**
- **show vpdn session**
- **show vpdn tunnel**
- **vpdn domain-delimiter**
- **vpdn enable**
- **vpdn-group**
- **show vpdn tunnel**
- **vpdn outgoing**
- **vpdn search-order**
- **vpdn source-ip**

See the Debug Commands section of this document for a complete list of deubg commands to use for isolating and troubleshooting L2TP problems.

accept dialin

To specify the local name to use for authenticating and the virtual template to use for cloning new virtual access interfaces when an incoming L2TP tunnel connection is requested from a specific peer, use the **accept dialin** VPDN group command. To disable authentication and virtual template cloning, use the **no** form of this command.

accept dialin [**l2f | l2tp | any**] **virtual-template** *number* [**remote** *remote-peer-name*]
no accept dialin [**l2f | l2tp | any**] **virtual-template** *number* [**remote** *remote-peer-name*]

Syntax Description

l2f | l2tp | any	(Optional) Indicates which Layer 2 tunnel protocol to use for a dialin tunnel. • **l2f**—Layer 2 forwarding protocol. • **l2tp**—Layer 2 tunnel protocol. • **any**—VPDN will use autodetect to determine which tunnel type to use, either l2f or l2tp.
virtual-template *number*	The virtual template interface that the new virtual access interface cloned from.
remote-peer-name	(Optoinal) Case-sensitive name that the remote peer will use for identification and tunnel authentication.

Default

Disabled

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

This command replies to a dial in L2F or L2TP tunnel open request from the specified peer. Once the LNS accepts the request from a LAC, it uses the specified virtual template to clone new virtual access interfaces. This command replaces the **vpdn incoming** command used in Cisco IOS Release 11.3. The user interface will automatically be upgraded when you reload the router with a 12.0 T or 11.3 AA image.

Default VPDN Group Configuration

Use the following command syntax to enable a default VPDN group configuration:

accept dialin l2tp virtual-template 1

Typically, you need one VPDN group for each LAC. For an LNS that services many LACs, the configuration can become cumbersome; however, you can use the default VPDN group configuration if all the LACs will share the same tunnel attributes. An example of this scenario

would be a LNS that services a large department with many Windows NT L2TP clients that are co-located with the LAC. Each of the Windows NT devices is an L2TP client as well as a LAC. Each of these devices will demand a tunnel to the LNS. If all the tunnels will share the same tunnel attributes you can use a default VPDN group configuration, which excels and simplifies the configuration process.

Note The **vpdn group** command must be configured with the **accept dialin** or **request dialin** command to be functional. The requester initiates a dial in tunnel. The acceptor accepts a request for a dial in tunnel.

Example

The following example allows the LNS to accept an L2TP type dial in tunnel. A virtual access interface will be cloned from virtual-template 1, from a remote peer named mugsy:

```
accept dialin l2tp virtual-template 1 remote mugsy
```

If you only use the **accept dialin** command with the **l2tp** and **virtual-template** keywords and omit the *remote-peer-name* argument, you automatically enable a default L2TP VPDN group, which allows all tunnels to share the same tunnel attributes:

```
vpdn-group 1
! Default L2TP VPDN group
 accept dialin l2tp virtual-template 1
```

Related Commands

vpdn incoming

clear vpdn tunnel

To shut down a specified tunnel and all sessions within the tunnel, use the **clear vpdn tunnel** EXEC command.

clear vpdn tunnel {l2f *nas-name hgw name* **| l2tp** [*remote name*] [*local name*]}

Syntax Description

l2f	Specifies the l2f tunnel protocol.
nas-hame	Name of the network access server at the far end of the tunnel.
hgw name	Host name of the home gateway at the local end of the tunnel.
l2tp	Specifies the l2tp tunnel protocol.
remote-name	(Optional) Host name of the tunnel peer. At the LNS, this is the name of the LAC; at the LAC, this is the name of the LNS.
local-name	(Optional) Local host name for the tunnel.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2

This command was modified with the **l2f** and **l2tp** keywords and options, in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

Use this command to clear a specific tunnel and all sessions within the tunnel.

Use this command to isolate problems by forcing a tunnel to come down without deconfiguring the tunnel (the tunnel can be restarted immediately by a user logging in).

If you are using the **l2tp** keyword, you can clear the tunnel by matching either the remote name or remote name and local name.

Example

The following example clears a tunnel to a remote peer named sophia:

```
clear vpdn tunnel l2tp mugsy sophia
```

force-local-chap

To force the LNS to reauthenticate the client, use the **force-local-chap** VPDN group command. To disable reauthentication, use the **no** form of this command.

force-local-chap
no force-local-chap

Syntax Description

This command has no arguments or keywords.

Default

CHAP authentication at the LNS is disabled; default authentication occurs at the LAC.

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

This command is only used if CHAP authentication is enabled for PPP (using the **ppp authentication chap** command). This command forces the LNS to reauthenticate the client in addition to the proxy authentication that occurs at the LAC. If the **force-local-chap** command is used, then the authentication challenge occurs twice. The first challenge comes from the LAC and the second challenge comes from the LNS. Some PPP clients may experience problems with double authentication. If this occurs, authentication challenge failures may be seen if the **debug ppp negotiation** command is enabled.

Example

The following example enables CHAP authentication at the LNS if a mismatch occurs between the client and the LAC:

```
force-local-chap on-mismatch
```

l2f ignore-mid-sequence

To ignore multiplex ID (MID) sequence numbers for sessions in an L2F tunnel, use the **l2f ignore-mid-sequence** VPDN group command. To remove the ability to ignore MID sequencing, use the **no** form of this command.

l2f ignore-mid-sequence
no l2f ignore-mid-sequence

Syntax Description

This command has no arguments or keywords.

Default

MID sequence number ignoring is disabled.

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release11.3(5)AA and 12.0(1)T.

This command applies only to L2F initiated tunnels and control packets for initial LCP tunnel negotiation.

This command is not required for Cisco-to-Cisco, LAC-to-LNS tunnel endpoints, and is only required if MID sequence numbering is not supported by a third-party hardware vendor.

Example

The following example ignores MID sequencing for L2F sessions between a Cisco router and a non-Cisco hardware device, which does not support MID sequencing:

```
l2f ignore-mid-sequence
```

l2tp drop out-of-order

To instruct a LAC or LNS using L2TP to drop packets that are received out of order, use the **l2tp drop out-of-order** VPDN group command. To disable dropping of out-of-sequence packets, use the **no** form of this command

l2tp drop out-of-order
no l2tp drop out-of-order

Syntax Description

This command has no keywords or arguments.

Default

Disabled

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release11.3(5)AA and 12.0(1)T.

This command is valid only for tunnels where sequencing is enabled.

Example

The following example causes the LAC or LNS to drop any packets that are received out of order:

```
l2tp drop out-of-order
```

l2tp flow-control backoff-queuesize

To define the maximum number of packets that can be queued locally for a session when a peer's receive window is full, use the **l2tp flow-control backoff-queuesize** VPDN group command. To change the value of the queue size simply reenter the command with the new queue size value. To remove a manually configured flow-control backoff value, use the **no** form of this command.

l2tp flow-control backoff-queuesize *queuesize*
no l2tp flow-control backoff-queuesize *queuesize*

Syntax Description

queuesize	Sets the queue size limit on a LAC or LNS so that when the remote peer's receive window is full, the LAC or LNS delays sending additional packets.

Default

L2tp flow control backoff queuing is enabled and uses a default value of 25.

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

This command is used for congestion control. This command will not appear as a valid option if the **l2tp flow-control receive-window** command is disabled, or the value is set to zero (for sequencing only).

Example

The following example uses the **l2tp flow-control receive-window** command option to 8, which in turn enables the **l2tp flow-control backoff-queuesize** command option. When the remote peer's receive window is full, the maximum number packets that can be queued locally for an L2TP session is 35.

```
l2tp flow-control receive-window 8
l2tp flow-control backoff-queuesize 35
```

Related Commands

l2tp flow-control maximum-ato
l2tp flow-control receive-window

l2tp flow-control maximum-ato

To define the maximum adaptive time-out for congestion control, use the **l2tp flow-control maximum-ato** VPDN group command. To reset the time-out to a new value, simply reenter the command with the new value. To remove a manually configured time-out value, use the **no** form of this command.

l2tp flow-control maximum-ato *milliseconds*
no l2tp flow-control maximum-ato *milliseconds*

Syntax Description

milliseconds	The wait time period, in milliseconds, before the LAC or LNS probes its remote peer's receive-window to resume sending packets.

Default

2000 milliseconds.

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

This command is used for congestion control between the LAC and LNS. This command will not appear as a valid option if the **l2tp flow-control receive-window** command is disabled or set to zero.

Example

The following example forces the LAC or LNS to wait 4000 milliseconds before attempting to probe the remote peer's receive status window again:

```
l2tp flow-control maximum-ato 4000
```

Related Commands

l2tp flow-control backoff-queuesize
l2tp flow-control receive-window

l2tp flow-control receive-window

To define the receive window on a LAC or LNS and enable either device to send sequence numbers, use the **l2tp flow-control receive-window** VPDN group command. To remove a flow-control receive-window value and disable sequencing, use the **no** form of this command.

l2tp flow-control receive-window *windowsize*
nol2tp flow-control receive-window *windowsize*

Syntax Description

windowsize	The number of packets that can be received by the remote end device before backoff queuing occurs.

Default

Receive window and sequence numbers are disabled.

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

If the receive-window value is set to zero, then sequence numbers are not sent, and congestion control is not enabled. Data zero length body (ZLB) acknowledgments are not sent when congestion control is disabled. If the receive-window value is greater than zero, then congestion control is enabled, and the value that is configured is sent to the L2TP receive window attribute value pair (AVP).

Using the **l2tp flow-control receive-window** command with a value greater than zero allows you to configure the following L2TP (optional) commands:

l2tp flow-control maximum-ato
l2tp flow-control backoff-queuesize

If the **l2tp flow-control receive-window** command is not enabled or the value is set to zero, then the **l2tp flow-control maximum-ato** and **2tp flow-control backoff-queuesize** commands will not appear as configurable options by the command parser.

Example

The following example configures a receive window value of 25 to be communicated to the remote peer and subsequently enables the configuration of the **l2tp flow-control maximum-ato** and **l2tp flow-control backoff-queuesize** commands.

```
l2tp flow-control receive-window 10
l2tp flow-control maximum-ato 15
l2tp flow-control backoff-queuesize 35
```

Related Commands

l2tp flow-control backoff-queuesize
l2tp flow-control maximum-ato

l2tp flow-control static-rtt

To define a static round-trip time for congestion control, use the **l2tp flow-control static-rtt** VPDN group command. To apply a different value, simply reenter the command with the new value. To disable a static round-trip time, use the **no** form of this command.

l2tp flow-control static-rtt *round-trip-time*
no l2tp flow-control static-rtt *round-trip-time*

Syntax Description

round-trip-time Sets the static round-trip time in milliseconds.

Default

Disabled; adaptive timeouts are used.

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release11.3(5)AA and 12.01(1)T.

If the LAC/LNS is configured to use a static round-trip time, then adaptive time-outs (ATO) are calculated on the fixed round-trip time value configured using the **l2tp flow-control static-rtt command**. If the device is not configured with the **l2tp flow-control static-rtt** command, then flow control is automatically calculated based on packet send and receive times.

Example

The following example sets a static round-trip delay of 15000 milliseconds, which in turn disables adaptive timeouts:

```
l2tp flow-control static-rtt 2500
```

Note You must have the **l2tp-flow control receive-window** command enabled with a value greater than zero in order to use the **l2tp flow-control maximum-ato** command.

Related Commands

l2tp flow-control backoff-queuesize
l2tp flow-control maximum-ato
l2tp flow-control receive-window

l2tp hidden

To enable L2TP AV pair hiding, which encrypts the AV pair "value," use the **l2tp hidden** VPDN group command. To disable L2TP AV pair value hiding, use the **no** form of this command.

l2tp hidden
no l2tp hidden

Syntax Description

This command has no keywords or arguments.

Default

L2TP AVP hiding is disabled.

Command Mode

VPDN group mode

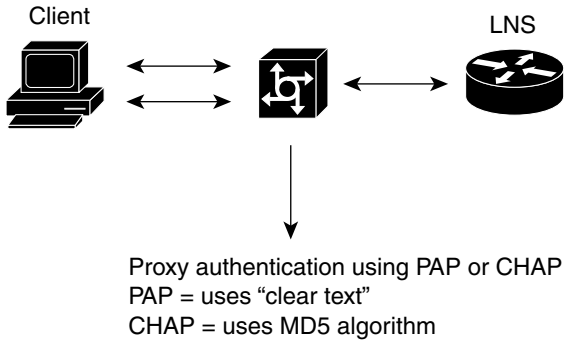
Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

This command is useful for additional security if PPP is using PAP or proxy authentication between the LAC and LNS. When AV pair hiding is enabled, then the L2TP hiding algorithm is executed, and sensitive passwords that are used between the L2TP AV pairs are encrypted during PAP or proxy authentication. This command is not required if one-time PAP password authentication is used.

In Figure 7, the client initiates a PPP session with the LAC, and tunnel authentication begins. The LAC in turn exchanges authentication requests with the LNS. Upon successful authentication between the LAC and LNS, a tunnel is created. Proxy authentication is done by the LAC, using either PAP or CHAP. Since PAP username and password information is exchanged between devices in clear-text, it is beneficial to use the **l2tp hidden** command where L2TP AV pair values are encrypted.

Figure 7 LAC-LNS Proxy authentication



Example

The following example encrypts the AV pair value exchanged between the LAC and LNS:

```
l2tp hidden
```

l2tp ip udp checksum

To enable IP User Data Protocol (UDP) checksums on L2TP payload packets, use the **l2tp ip udp checksum** VPDN group command. To disable IP UDP checksums, use the **no** form of this command.

l2tp ip udp checksum
no l2tp ip udp checksum

Syntax Description

There are no keywords or arguments for this command.

Default

Disabled

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

Enabling IP UDP checksum packets causes the switching path to revert to process-level switching, which results in slower performance.

Example

The following example enables IP UDP checksums on L2TP payload packets:

```
l2tp ip udp checksum
```

l2tp offset

To enable the offset field in L2TP payload packets, use the **l2tp offset** VPDN group command. To disable the offset field, use the **no** form of this command.

l2tp offset
no l2tp offset

Syntax Description

This command has no keywords or arguments.

Default

Enabled

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

Enabling the offset field forces longword header alignment in L2TP payload packets and may improve performance on some platforms (such as those using the 4k MIPS processor). However, this potentially increases the size of the packets. Use the **show version** command to determine if your Cisco router or access server has a 4k MIPS processor.

Note L2TP offset is enabled by default. Therefore, there is no need to enable this command unless it was previously disabled.

Example

The following example disables the offset field:

```
no l2tp offset
```

l2tp tunnel authentication

To enable L2TP tunnel authentication, use the **l2tp tunnel authentication** VPDN group command. To disable L2TP tunnel authentication, use the **no** form of this command.

l2tp tunnel authentication
no l2tp tunnel authentication

Syntax Description

This command has no keywords or arguments.

Default

Enabled

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

Example

The following example enables L2TP tunnel authentication:

```
l2tp tunnel authentication
```

Note L2TP tunnel authentication is enabled by default. Therefore, there is no need to enable this command unless it was previously disabled.

l2tp tunnel hello

To set the number of seconds between sending hello keepalive packets for a L2TP tunnel, use the **l2tp tunnel hello** command. To change the tunnel hello value, simply reenter the command with the new value. To disable the sending of hello keepalive packets, use the **no** form of this command.

l2tp tunnel hello *hello-interval*
no l2tp tunnel hello *hello-interval*

Syntax Description

hello-interval	The interval, in seconds, that the LAC and LNS wait before sending the next L2TP tunnel keepalive packet.

Default

60 seconds.

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

The L2TP tunnel keepalive timers do not have use the same value on both sides of the tunnel. For example, a LAC can use a keepalive value of 30 seconds, and an LNS can use the default value of 60 seconds.

Example

The following example sets the L2TP tunnel hello value to 90 seconds:

```
l2tp tunnel hello 90
```

l2tp tunnel password

To set the password that the router will use to authenticate the tunnel, use the **l2tp tunnel password** VPDN group command. To remove a previously configured password, use the **no** form of this command.

l2tp tunnel password *password*
no l2tp tunnel password *password*

Syntax Description

password	Identifies the password that the router will use for tunnel authentication.

Default

Disabled. If the **l2tp tunnel password** is not configured, the local password is used. If no local password is configured, the hostname is used.

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

The password defined with the **l2tp tunnel password** command is also used for AV pair hiding.

The password hierarchy sequence that is used for tunnel identification and, subsequently, tunnel authentication, is as follows:

- An L2TP tunnel password is used first (defined by the **l2tp tunnel password** command).
- If no L2TP tunnel password exists, the local name is used (defined by the **local name** command).
- If a local name does not exist, the hostname is used (defined by the **hostname** command).

Example

The following example configures the tunnel password, *dustie*, which will be used to authenticate the tunnel between local and remote peer:

```
l2tp tunnel password dustie
```

Related Commands

hostname
local name
l2tp hidden

lcp renegotiation

To allow the LNS to renegotiate the link control protocol (LCP) on dial in calls, using L2TP or L2F, use the **lcp renegotiation** VPDN group command. To remove LCP renegotiation, use the **no** form of this command.

lcp renegotiation
no lcp renegotiation

Syntax Description

always	Always renegotiates PPP LCP at the LNS.
on-mismatch	Renegotiates PPP LCP at the LNS only in the event of an LCP mismatch between the LAC and LNS.

Default

LCP renegotiation is disabled on the LNS.

Command Mode

VPDN group mode

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

This command is only valid at the LNS. This command is useful for an LNS that tunnels to a non-Cisco LAC, where the LAC may negotiate a different set of LCP options than what the LNS expects.

When a PPP session is started at the LAC, LCP parameters are negotiated, and a tunnel initiated, the LNS can either accept the LAC LCP negotiations or can request LCP renegotiation. Using the **lcp renegotiation always** command forces renegotiation to occur at the LNS. If **lcp renegotiation on-mismatch** is configured, then renegotiation will only occur if there is an LCP mismatch between the LNS and LAC.

Note Older PC PPP clients may experience a “lock up” during PPP LCP renegotiation.

Example

The following example configures the LNS to renegotiate PPP LCP with a non-Cisco LAC:

```
vpdn-group 1
 accept dialin l2tp virtual-template 1 remote pat
 lcp renegotiation on-mismatch
```

local name

To specify a local host name that the tunnel will use to identify itself, use the **local name** global configuration command. To remove a local name, use the **no** form of this command.

local name *name*
no local name *name*

Syntax Description

name	Local host name of the tunnel.

Default

Disabled. A local name must be explicitly configured.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

This command allows each VPDN group to use a unique and local name. The password hierarchy sequence that is used for tunnel identification and subsequently, tunnel authentication, is as follows:

- An L2TP tunnel password is used first (defined by the **l2tp tunnel password** command).
- If no L2TP tunnel password exists, the local name is used (defined by the **local name** command).
- If a local name does not exist, the hostname is used (defined by the **hostname** command).

Example

The following example configures the local host name of the tunnel as dustie:

```
local name dustie
```

Related Commands

hostname
l2tp tunnel password

request dialin

To specify a dial in L2F or L2TP tunnel to a remote peer if a dial in request is received for a caller belonging to a specified domain, or a specific Digital Number Information String (DNIS) is called, use the **request dialin** VPDN group command. To remove this function, use the **no** form of this command.

request dialin [**l2f | l2tp**] **ip** *ip-address* {**domain** *domain-name* | **dnis** *dialed-number*}
no request dialin [**l2f | l2tp**] **ip** *ip-address* {**domain** *domain-name* | **dnis** *dialed-number*}

Syntax Description

**l2f	l2tp**	L2F or L2TP tunnel protocol to be used.
ip *ip-address*	IP address of the remote peer (the other end of the tunnel).
domain *domain-name*	Case-sensitive domain name to which the caller must belong for tunneling to occur.
dnis *dialed-number*	Called number that indicates the calls should be tunneled.

Default

Disabled. No dial in is configured.

Command Mode

VPDN group mode

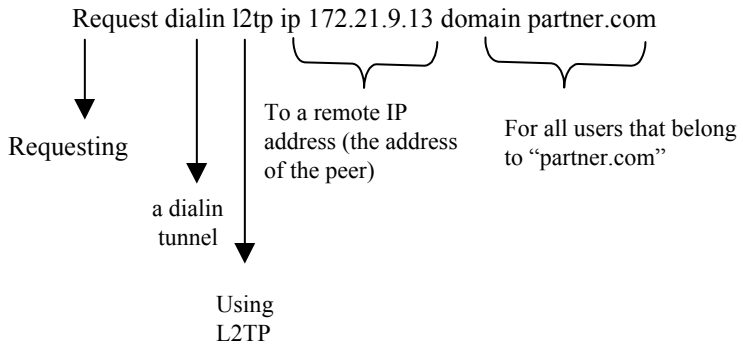
Usage Guidelines

This command first appeared in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

This command is used to initiate a tunnel to a remote peer at a specific IP address, if a dialin tunnel request is received for users under a specific domain name (cisco.com, for example), or if a specific DNIS is called (408-555-1234, for example).

Figure 8 shows a breakdown of the **request dialin** command.

Figure 8 Request Dialin Command Breakdown



Note The **vpdn group** command must be configured with the **accept dialin** command or the **request dialin** command in order to enable VPDN. The **request dialin** command initiates a dialing tunnel. The acceptor in turn, accepts a request for a dialin tunnel.

Example

The following example requests an L2TP dial in tunnel to a remote peer at IP address 172.17.33.125 for a user in the domain named partner.com:

```
request dialin l2tp ip 172.17.33.125 partner.com
```

Related Commands

accept dialin
vpdn incoming
vpdn outgoing

show vpdn session

To display information about activeL2TP or L2F sessions in a virtual private dialup network, use the **show vpdn session** EXEC command. If the **show vpdn** command is used without the **session** or **tunnel** keywords, both session and tunnel information is displayed by default.

show vpdn session [**all** [**interface | tunnel | username**] | **packets** | **sequence** | **state** | **timers** | **window**]

Syntax Description

all	(Optional) All session information for active sessions.
	(Optional) **interface** —Interface associated to a specific session.
	(Optional) **tunnel**—Tunnel attribute filter.
	(Optional) **username**—Username filter.
packets	(Optional) Packet/byte count.
sequence	(Optional) Sequence numbers.
state	(Optional) State of each session.
timers	(Optional) Timer information.
window	(Optional) Window information.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2. This command was modified for L2TP and L2F session and tunnel variables in Cisco IOS Release 11.3(5)AA and 12.0(1)T.

Sample Displays

This section shows sample displays from various **show vpdn** commands.

The following is sample output from the **show vpdn** command without any keywords or arguments. All session information is displayed by default.

```
Router# show vpdn

L2TP Tunnel and session Information (Total tunnels=1 sessions=1)

LocID RemID Remote Name   State  Remote Address  Port  Sessions
2     10    wander        est    172.21.9.13     1701  1

LocID RemID TunID Intf    Username       State  Last Chg
1     1     2     As7     bum1@cisco.com est    00:23:01

L2F Tunnel and Session
 NAS CLID HGW CLID NAS Name        HGW Name        State
 10        2        stella          acadia          open
                    172.21.9.4      172.21.9.232

 CLID   MID    Username       Intf   State
 2      1      jdoe@hp.com     As6    open
```

The following is sample output from the **show vpdn session** command:

```
Router# show vpdn session

L2TP Session Information (Total tunnels=1 sessions=1)

LocID RemID TunID Intf    Username      State  Last Chg
1     1     2     As7     bum1@cisco.co est    00:29:34
L2F Session

 CLID   MID    Username       Intf   State
 3      1      jdoe@hp.com     As6    open
```

The following sample output is from the **show vpdn** command with the **session**, **all**, and **username** keywords:

```
Router# sh vpdn session all username bum1@cisco.com
L2TP Session Information (Total tunnels=1 sessions=1)

Call id 1 is up on tunnel id 2
Remote tunnel name is wander
  Internet Address: 172.21.9.13
  Session username is bum1@cisco.com, state is established
    Time since change: 00:34:28, Interface As7
    Remote call id: 1
    212 packets sent, 425 received, 6003 bytes sent, 12008 received
    Sequencing is on
      Ss=211 Sr=213  Remote Ns=212  Remote Nr=0  Out of order=0
      Remote has not requested congestion control

% No active L2F tunnels

Router# sh vpdn session all username jdoe@hp.com

% No active L2TP tunnels

L2F Session
MID: 1
User:  jdoe@hp.com
Interface:  Async6
State:  open
Packets out: 139
Bytes out: 4518
Packets in: 422
Bytes in: 27013
```

Table 2 describes the fields shown in the **show vpdn session** display.

Table 2 Show VPDN Session Field Descriptions

Field	Description
L2TP Session Information	
Total tunnels	Number of active tunnels.
Total sessions	Number of active sessions.
LocID	A unique number that identifies the local id for the session.
RemID	A unique number that identifies the remote id for the session.
TunID	A unique number that identifies the tunnel.
Intf	The interface associated with a specific session.
Username	Username of the session.
State	Indicates status for the individual user in the tunnel. The states are: opening, open, closed, closing, and waiting_for_tunnel. The waiting_for_tunnel state means that the user connection is waiting until the main tunnel can be brought up before it moves to the opening state.
Last Chg	Last status change.
L2F Session	
CLID	?

Field	Description
MID	The multiplex identifier.
Username	Username from which a protocol message was forwarded over the tunnel.
Intf	Interface from which the protocol message was sent.
State	Indicates whether the tunnel is open, opening, closing, or closed.

Related Commands

show vpdn
show vpdn tunnel

show vpdn tunnel

To display information about active Layer 2 Tunneling Protocol (l2TP) or Level 2 Forwarding (L2F) tunnels in a virtual private dialup network, use the **show vpdn tunnel** EXEC command. If the **show vpdn** command is used without the **session** or **tunnel** keywords, both session and tunnel information is displayed by default.

show vpdn tunnel [**all** [**id** | **local-name** | **remote-name**] | **packets** | **state** | **summary** | **transport**]

Syntax Description

all	(Optional) All information for active tunnels.Options are: **id** —Local tunnel ID. **local-name**—Name of local end of tunnel. **remote-name**—Name of remote end of tunnel.
packets	Packet/byte count.
state	Tunnel state information.
summary	Tunnel information summary.
transport	Tunnel transport information.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2. This command was modified for l2TP and L2F session and tunnel variables in Cisco IOS Releases 11.3(5)AA and 12.0(1)T.

Sample Display

This section shows sample displays from vious **show vpdn** commands and keyword options. The following example displays the **show vpdn** command without any keywords or arguments:

```
Router# sh vpdn

L2TP Tunnel and session Information (Total tunnels=1 sessions=1)

LocID RemID Remote Name   State  Remote Address  Port  Sessions
2     10    wander        est    172.21.9.13     1701  1

LocID RemID TunID Intf    Username      State  Last Chg
1     1     2     As7     bum1@cisco.co est    00:23:01

L2F Tunnel and Session
 NAS CLID HGW CLID NAS Name        HGW Name        State
 10        2        stella          acadia          open
                    172.21.9.4      172.21.9.232

 CLID   MID    Username       Intf   State
 2      1      jdoe@hp.com     As6    open
```

The following is output from the **show vpdn tunnel** command:

```
Router# sh vpdn tunnel

L2TP Tunnel Information (Total tunnels=1 sessions=1)

LocID RemID Remote Name   State  Remote Address  Port  Sessions
2     10    wander        est    172.21.9.13     1701  1

L2F Tunnel

 NAS CLID HGW CLID NAS Name        HGW Name        State
 9         1        stella          acadia          open
                    172.21.9.4      172.21.9.232
```

Related Commands

show vpdn
show vpdn session

vpdn domain-delimiter

To specify the characters to be use to delimit the domain prefix or domain suffix, use the **vpdn domain-delimiter** global configuration command.

domain-delimiter *delimiter-characters* [**suffix | prefix**]

Syntax Description

delimiter-characters	One or more specific characters to be used as suffix or prefix diameters. Available characters are **%**, **–**, **@**, **** , **#**, and **/**. If a backslash (\) is the last delimiter in the command line, enter it as a double backslash (\\).
suffix | prefix	(Optional) Usage of the delimeter characters specified.

Default

This command is disabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

You can enter one **vpdn domain-delimiter** command to list the suffix delimiters and another **vpdn domain-delimiter** command to list the prefix delimiters. However, no character can be both a suffix delimiter and a prefix delimiter.

This command allows the network access server to parse a list of home gateway DNS domain names and addresses sent by an AAA server. The AAA server can store domain names or IP addresses in the following AV pair:

```
cisco-avpair = "lcp:interface-config=ip address 1.1.1.1 255.255.255.255.0",
cisco-avpair = "lcp:interface-config=ip address bigrouter@excellentinc.com,
```

Examples

The following example lists three suffix delimiters and three prefix delimiters:

```
vpdn domain-delimiter %-@ suffix
vpdn domain-delimiter #/\\ prefix
```

The following example allows the host name and domain name:

```
cisco.com#houstonddr
houstonddr@cisco.com
```

Related Commands

vpdn enable
vpdn search-order

vpdn enable

To enable VPDN on the router and inform the router to look for tunnel definitions in a local database and on a remote authorization server (LNS), if one is present, use the **vpdn enable** global configuration command. To disable VPDN, use the **no** form of this command.

vpdn enable
no vpdn enable

Syntax Description

This command has no keywords or arguments.

Default

Disabled

Command Mode

Global configuration.

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

Sample Display

The following example enables VPDN on the router:

```
vpdn enable
```

vpdn-group

To define a local, unique group number identifier, use the **vpdn-group** global configuration command. To remove a group number, use the **no** form of this command.

vpdn-group *group-number*
no vpdn-group *group-numbe***r**

Syntax Description

group-number	Local group number. Valid group numbers range between 1 and 3000.

Default

VPDN group number assignments are not defined.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release11.3(5)AA and 12.0(1)T.
The **vpdn-group number** command is a local, unique identifier for each VPDN group.

Example

The following example establishes local VPDN group number 1 for which other variables, such as force-local chap, can be assigned:

```
vpdn group-number 1
```

vpdn incoming

To specify the local name to use for authenticating, and the virtual template to use for building interfaces for incoming connections when a L2F connection is requested from a certain remote host, use the **vpdn incoming** global configuration command. To remove the local name for tunnel authentication, use the **no** form of this command.

vpdn incoming *remote-name local-name* **virtual-template** *number*

Syntax Description

remote-name	Case-sensitive name of the remote host requesting the connection.
local-name	Case-sensitive local name to use when authenticating back to the remote host.
virtual-template *number*	Virtual template to use for building interfaces for incoming calls.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

The **accept dialin** command will replace this command in future Cisco IOS Release.

The *remote-name* and *local-name* arguments are case sensitive.

This command is usually used on a home gateway, not on the network access server in the ISP or public data network.

Note The **vpdn incoming** command is still valid for defining tunnels; however, once the configuration is written to memory, the user interface will convert this command to the new syntax (the **accept dialin** command).

Example

The following partial example specifies use of local host go_blue and virtual template interface 6 for connections with remote host dallas_wan:

```
vpdn incoming dallas_wan go_blue virtual-template 6
```

vpdn outgoing

To specify use of a Dialed Number Information Service (DNIS) or use of a domain name when selecting a tunnel for forwarding traffic to the remote host (the home gateway) on a virtual private dialup network, use the **vpdn outgoing** global configuration command.

vpdn outgoing {**dnis** *dialed-number* | *domain-name*} *local-name* **ip** *ip-address*

Syntax Description

dnis *dialed-number*	Dialed number to be used for selecting a specific tunnel for forwarding traffic to a home gateway.
domain-name	Case-sensitive name of the domain to forward traffic to.
local-name	Case-sensitive local name to use when authenticating the tunnel to the remote host.
ip *ip-address*	IP address of the remote host (home gateway).

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

The **request dialin** command will replace this command in a future Cisco IOS Release.

The *domain-name* and *local-name* arguments are case sensitive.

This command is usually used on a network access server, not on a home gateway.

When DNIS is enabled and a dialed number is provided, the network service provider can use the dialed number to select a specific tunnel destination.

The domain name can be used to choose a tunnel destination. For example, if a user dials in as "joe@company-a.com," where joe is the username and "company-a.com" is the domain name, you can select a tunnel destination based on the domain (company-a.com).

If both DNIS information and a CHAP or PAP name map to a valid tunnel, the DNIS information is used.

If TACACS+ is used to get tunnel information, the string "dnis:" is prepended to the phone number before attempting to look up the information in AAA.

Note The **vpdn outgoing** command is still valid for defining tunnels; however, once the configuration is saved, the user interface will convert this command to the new syntax (the **request dialin** command).

Examples

The following example selects a tunnel destination based on the domain name:

```
vpdn outgoing chicago-main go-blue ip 172.17.33.125
```

The following example selects a tunnel destination based on the use of DNIS and a specific dialed number:

```
vpdn outgoing dnis 2387765 gocardinal ip 170.16.44.56
```

Related Commands

vpdn enable
vpdn history failure table-size

vpdn search-order

To specify how the service provider's network access server is to perform VPDN tunnel authorization searches, use the **vpdn search-order** global configuration command. To remove a prior specification, use the **no** form of the command.

vpdn search-order {**dnis domain | domain dnis | domain | dnis**}
no vpdn search-order

Syntax Description

dnis domain	Specidifes to search first on the Dialed Number Information Service (DNIS) information provided on ISDN lines and then on the domain name.
domain dnis	Specifies to search first on the domain name and then on the DNIS information.
domain	Specifies to search on the domain name only.
dnis	Specifies to earch on the DNIS information only.

Default

Search first on the DNIS information provided on ISDN lines and then search on the domain name. This is equivalent to using the **vpdn search-order dnis domain** command.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

VPDN authorization searches are performed only as specified.

The configuration shows the **vpdn search-order** command setting only if the command is explicitly configured.

Example

The following example configures a network access server to select a tunnel destination based on the use of DNIS and a specific dialed number and to perform tunnel authorization searches based on the DNIS information only.

```
vpdn enable
vpdn outgoing dnis 2387765 gocardinal ip 170.16.44.56
vpdn search-order dnis
```

vpdn source-ip

To set the source IP address of the network access server, use the **vpdn source-ip** global configuration command.

vpdn source-ip *address*

Syntax Description

address	IP address of the network access server.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

One source IP address is configured on the network access server. The source IP address is configured per network access server, not per domain.

Example

The following example enables VPDN on the network access server and sets an IP source address of 171.4.48.3.

```
vpdn enable
vpdn source-ip 171.4.48.3
```

Related Commands

vpdn enable

Debug Commands

Use the following new or modified commands to debug VPDN and L2TP tunnels:

- **debug vpdn event**
- **debug vpdn packet**

debug vpdn event

To display L2TP errors and events that are a part of normal tunnel establishment or shutdown for VPDNs, use the **debug vpdn event** command to display . To disable debugging errors and events, use the **no** form of this command to disable debugging output.

debug vpdn event [**protocol** | **flow-control**]
no debug vpdn event [**protocol** | **flow-control**]

Syntax Description

protocol	Displays all errors for the tunneling protocols used by VPDNs, such as L2TP, L2F, PPTP, and events within these protocols.
flow control	Displays L2TP flow control errors.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2(5)AA and 12.0(1)T.

Use this command to display VPDN errors and basic events within the protocol, such as state changes. This command does not include packet trace information or information about sent or received individual management packets.

Sample Display

The following is sample output for the natural sequence of events for an LNS named stella:

```
Router# debug vpdn event

20:47:33: %LINK-3-UPDOWN: Interface Async7, changed state to up
20:47:35: As7 VPDN: Looking for tunnel -- cisco.com --
20:47:35: As7 VPDN: Get tunnel info for cisco.com with NAS stella, IP 172.21.9.13
20:47:35: As7 VPDN: Forward to address 172.21.9.13
20:47:35: As7 VPDN: Forwarding...
20:47:35: As7 VPDN: Bind interface direction=1
20:47:35: Tnl/Cl 8/1 L2TP: Session FS enabled
20:47:35: Tnl/Cl 8/1 L2TP: Session state change from idle to wait-for-tunnel
20:47:35: As7 8/1 L2TP: Create session
20:47:35: Tnl 8 L2TP: SM State idle
20:47:35: Tnl 8 L2TP: Tunnel state change from idle to wait-ctl-reply
20:47:35: Tnl 8 L2TP: SM State wait-ctl-reply
20:47:35: As7 VPDN: bum1@cisco.com is forwarded
20:47:35: Tnl 8 L2TP: Got a challenge from remote peer, stella
20:47:35: Tnl 8 L2TP: Got a response from remote peer, stella
20:47:35: Tnl 8 L2TP: Tunnel Authentication success
20:47:35: Tnl 8 L2TP: Tunnel state change from wait-ctl-reply to established
20:47:35: Tnl 8 L2TP: SM State established
20:47:35: As7 8/1 L2TP: Session state change from wait-for-tunnel to wait-reply
20:47:35: As7 8/1 L2TP: Session state change from wait-reply to established
20:47:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async7, changed state to up
```

The following shows sample debug output on the LAC named stella:

```
Router# debug vpdn event

20:19:17: L2TP: I SCCRQ from stella tnl 8
20:19:17: L2X: Never heard of stella
20:19:17: Tnl 7 L2TP: New tunnel created for remote stella, address 172.21.9.4
20:19:17: Tnl 7 L2TP: Got a challenge in SCCRQ, stella
20:19:17: Tnl 7 L2TP: Tunnel state change from idle to wait-ctl-reply
20:19:17: Tnl 7 L2TP: Got a Challenge Response in SCCCN from stella
20:19:17: Tnl 7 L2TP: Tunnel Authentication success
20:19:17: Tnl 7 L2TP: Tunnel state change from wait-ctl-reply to established
20:19:17: Tnl 7 L2TP: SM State established
20:19:17: Tnl/Cl 7/1 L2TP: Session FS enabled
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from idle to wait-for-tunnel
20:19:17: Tnl/Cl 7/1 L2TP: New session created
20:19:17: Tnl/Cl 7/1 L2TP: O ICRP to stella 8/1
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from wait-for-tunnel to wait-connect
20:19:17: Tnl/Cl 7/1 L2TP: Session state change from wait-connect to established
20:19:17: Vi1 VPDN: Virtual interface created for bum1@cisco.com
20:19:17: Vi1 VPDN: Set to Async interface
20:19:17: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
20:19:18: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
20:19:18: Vi1 VPDN: Bind interface direction=2
20:19:18: Vi1 VPDN: PPP LCP accepting rcv CONFACK
20:19:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed
state to up
```

debug vpdn packet

To display L2TP errors and events that are a part of normal tunnel establishment or shutdown for VPDNs, use the **debug vpdn packet** command. To disable debugging output, use the **no** form of this command.

debug vpdn packet [**control | flow-control | control detail | data**]
no debug vpdn packet [**control | flow-control | control detail | data**]

Syntax Description

control	(Optional) Displays a one-line statement for each control packet sent, resent, or received.
flow-control	(Optional) Displays information about L2TP flow control.
control detail	(Optional) Displays detailed header field and AVP information, which is contained in control packets that are sent, resent, or received.
data	(Optional) Displays sequence numbers (if present), flags, length, and information about fast switching.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2(5)AA and 12.0(1)T.

Use this command with the following keywords:

- **control**—Use this command to debug to ensure control messages are sent, resent, or received correctly.
- **flow-control**—Use this command only when you want to debug L2TP flow control issues or where you suspect flow-control is problematic.
- **control detail**—Use this command when you suspect there is a problem parsing control packets. This command is particularly helpful for tunneling between a Cisco and non-Cisco device.
- **data**—Use this command when you want to debug the data path or determine the packet's switching path (fast switched or process switched).

Caution The **debug vpdn packet** command using the **data** keyword is CPU intensive and may decrease performance significantly.

Sample Display

The following is sample output from the **debug vpdn packet control** where VPDN event exchange is normal:

```
Router# debug vpdn event protocol

20:50:27: %LINK-3-UPDOWN: Interface Async7, changed state to up
20:50:29: Tnl 9 L2TP: O SCCRQ
20:50:29: Tnl 9 L2TP: O SCCRQ, flg TLF, ver 2, len 131, tnl 0, cl 0, ns 0, nr 0
20:50:29: contiguous buffer, size 131
         C8 02 00 83 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 ...
20:50:29: Tnl 9 L2TP: Parse AVP 0, len 8, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Parse SCCRP
20:50:29: Tnl 9 L2TP: Parse AVP 2, len 8, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Protocol Ver 256
20:50:29: Tnl 9 L2TP: Parse AVP 3, len 10, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Framing Cap 0x0x3
20:50:29: Tnl 9 L2TP: Parse AVP 4, len 10, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Bearer Cap 0x0x3
20:50:29: Tnl 9 L2TP: Parse AVP 6, len 8, flag 0x0x0
20:50:29: Tnl 9 L2TP: Firmware Ver 0x0x1120
20:50:29: Tnl 9 L2TP: Parse AVP 7, len 12, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Hostname stella
20:50:29: Tnl 9 L2TP: Parse AVP 8, len 25, flag 0x0x0
20:50:29: Tnl 9 L2TP: Vendor Name Cisco Systems, Inc.
20:50:29: Tnl 9 L2TP: Parse AVP 9, len 8, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Assigned Tunnel ID 8
20:50:29: Tnl 9 L2TP: Parse AVP 10, len 8, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Rx Window Size 4
20:50:29: Tnl 9 L2TP: Parse AVP 11, len 22, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Chlng D807308D106259C5933C6162ED3A1689
20:50:29: Tnl 9 L2TP: Parse AVP 13, len 22, flag 0x0x8000 (M)
20:50:29: Tnl 9 L2TP: Chlng Resp 9F6A3C70512BD3E2D44DF183C3FFF2D1
20:50:29: Tnl 9 L2TP: No missing AVPs in SCCRP
20:50:29: Tnl 9 L2TP: Clean Queue packet 0
20:50:29: Tnl 9 L2TP: I SCCRP, flg TLF, ver 2, len 153, tnl 9, cl 0, ns 0, nr 1
 contiguous pak, size 153
         C8 02 00 99 00 09 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
         00 03 00 00 00 03 80 0A 00 00 00 04 00 00 00 ...
20:50:29: Tnl 9 L2TP: I SCCRP from stella
20:50:29: Tnl 9 L2TP: O SCCCN  to stella tnlid 8
20:50:29: Tnl 9 L2TP: O SCCCN, flg TLF, ver 2, len 42, tnl 8, cl 0, ns 1, nr 1
20:50:29: contiguous buffer, size 42
         C8 02 00 2A 00 08 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 4B 2F A2 50 30 13
         E3 46 58 D5 35 8B 56 7A E9 85
20:50:29: As7 9/1 L2TP: O ICRQ to stella 8/0
20:50:29: As7 9/1 L2TP: O ICRQ, flg TLF, ver 2, len 48, tnl 8, cl 0, ns 2, nr 1
20:50:29: contiguous buffer, size 48
         C8 02 00 30 00 08 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 08 00 00 00 0E 00 01 80 0A 00 00
         00 0F 00 00 00 04 80 0A 00 00 00 12 00 00 00 ...
20:50:29: Tnl 9 L2TP: Clean Queue packet 1
20:50:29: Tnl 9 L2TP: Clean Queue packet 2
20:50:29: Tnl 9 L2TP: I ZLB ctrl ack, flg TLF, ver 2, len 12, tnl 9, cl 0, ns 1, nr 2
 contiguous pak, size 12
         C8 02 00 0C 00 09 00 00 00 01 00 02
20:50:30: As7 9/1 L2TP: Parse AVP 0, len 8, flag 0x0x8000 (M)
20:50:30: As7 9/1 L2TP: Parse ICRP
20:50:30: As7 9/1 L2TP: Parse AVP 14, len 8, flag 0x0x8000 (M)
20:50:30: As7 9/1 L2TP: Assigned Call ID 1
```

```
20:50:30: As7 9/1 L2TP: No missing AVPs in ICRP
20:50:30: Tnl 9 L2TP: Clean Queue packet 2
20:50:30: As7 9/1 L2TP: I ICRP, flg TLF, ver 2, len 28, tnl 9, cl 1, ns 1, nr 3
 contiguous pak, size 28
         C8 02 00 1C 00 09 00 01 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 01
20:50:30: As7 9/1 L2TP: O ICCN to stella 8/1
20:50:30: As7 9/1 L2TP: O ICCN, flg TLF, ver 2, len 203, tnl 8, cl 1, ns 3, nr 2
20:50:30: contiguous buffer, size 203
         C8 02 00 CB 00 08 00 01 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 00 00 DA C0 80 0A
         00 00 00 13 00 00 00 02 00 28 00 00 00 1B 02 ...
20:50:30: Tnl 9 L2TP: Clean Queue packet 3
20:50:30: As7 9/1 L2TP: I ZLB ctrl ack, flg TLF, ver 2, len 12, tnl 9, cl 1, ns 2, nr 4
 contiguous pak, size 12
         C8 02 00 0C 00 09 00 01 00 02 00 04
20:50:30: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async7, changed state to up
```