

L2TP Dialout

This document includes the following sections:

- Feature Overview on page 1
- Supported Platforms on page 5
- Supported Standards, MIBs, and RFCs on page 5
- Configuration Tasks on page 5
- Configuration Examples on page 11
- Command Reference on page 13
- Glossary on page 33

Feature Overview

The Layer 2 Tunneling Protocol (L2TP) Dialout feature enables L2TP Network Servers (LNSs) to tunnel dialout VPDN calls using L2TP as the tunneling protocol. This feature enables a centralized network to efficiently and inexpensively establish a virtual point-to-point connection with any number of remote offices.

Using the L2TP Dialout feature, Cisco routers can carry both dial-in and dialout calls in the same L2TP tunnels.

Previously, only dial-in VPDN calls were supported.

L2TP dialout involves two devices: an LNS and an L2TP Access Concentrator (LAC). When the LNS wants to perform L2TP dialout, it negotiates an L2TP tunnel with the LAC. The LAC then places a PPP call to the client(s) the LNS wants to dial out to.

Figure 1 shows a typical L2TP dialout scenario:

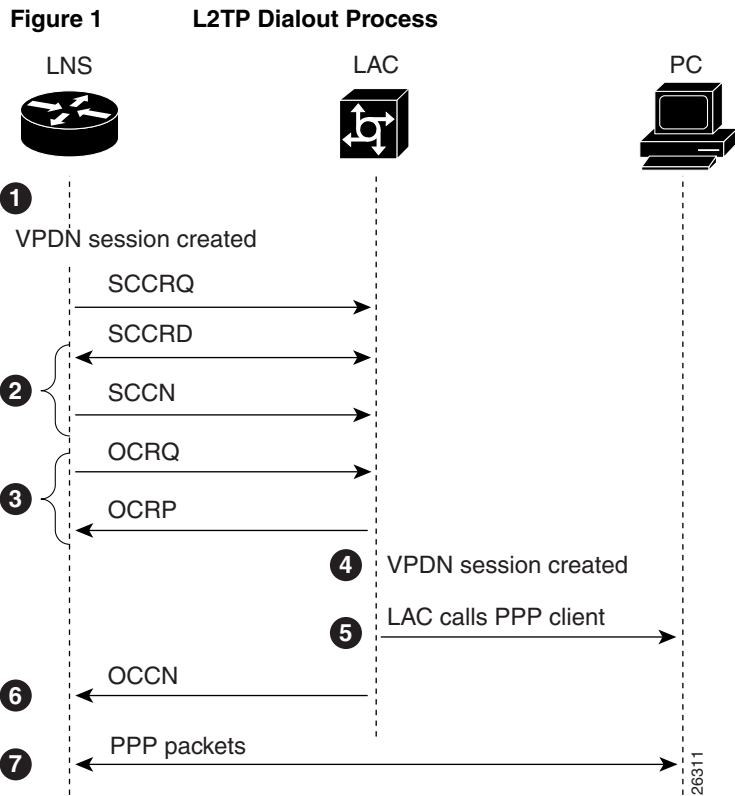


Table 1 explains the sequence of events described in Figure 1.

Table 1 L2TP Dialout Event Descriptions

Event	Description
1	The LNS receives Layer 3 packets, which are to be dialed out, and forwards them to its dialer interface. (either a dialer profile or DDR). The dialer issues a dial call request to the VPDN group, and the LNS creates a virtual-access interface. If the dialer is a dialer profile, this interface becomes a member of the dial pool. If the dialer is DDR, the interface becomes a member of the rotary group. The VPDN group creates a VPDN session for this connection and sets it in the pending state.
2	The LNS and LAC establish an L2TP tunnel (unless a tunnel is already open).
3	The LNS sends an Outgoing Call ReQuest (OCRQ) packet to the LAC, which checks if it has a dial resource available. If the resource is available, the LAC responds to the LNS with an Outgoing Call RePly (OCRP) packet. If the resource is not available, the LAC responds with a Call Disconnect Notification (CDN) packet, and the session is terminated.
4	If the LAC has an available resource, it creates a VPDN session and sets it in the pending state.
5	The LAC then initiates a call to the PPP client. When the LAC's call connects to the PPP client, the LAC binds the call's interface to the appropriate VPDN session.
6	The LAC sends an Outgoing Call CoNnected (OCCN) packet to the LNS. The LNS binds the call to the appropriate VPDN session and then brings the virtual-access interface up.
7	The dialer on the LNS and the PPP client can now exchange PPP packets. The LAC acts as a transparent packet forwarder. If the dialer interface is a DDR and a Virtual Profile is configured, the PPP endpoint is the LNS's virtual-access interface, not the dialer. All Layer 3 routes point to this interface instead of the dialer.

To facilitate L2TP Dialout, two new command modes are added to the Cisco IOS software: request-dialout mode and accept-dialout mode. These new command modes are accessed from VPDN group mode; therefore, they are generically referred to as VPDN subgroups. Table 2 shows the router prompts of these new command modes:

Table 2 New VPDN Group Command Modes

Command Mode	Router Prompt
request-dialout	router(config- <i>vpdn-req-out</i>) #
accept-dialout	router(config- <i>vpdn-acc-out</i>) #

Table 3 lists the new VPDN subgroup commands and which subgroups they apply to.

Table 3 VPDN Subgroup Commands

Command	VPDN Subgroups
protocol	all subgroups
default	all subgroups
dialer	accept-dialout
pool-member	request-dialout
rotary-group	request-dialout

The other existing VPDN group commands are now dependent on which VPDN subgroups exist on the VPDN group.

Table 4 lists the new VPDN group modes and which subgroups need to be enabled for them to be configurable.

Table 4 VPDN Group Commands

command	VPDN Subgroups
default	any subgroup
initiate-to	request-dialout
local name	any subgroup
source-ip	any subgroup
terminate-from	accept-dialout

For more information on the reorganization of the VPDN group, see the *VPDN Group Reorganization* feature module, which is located under *New Features in Release 12.0(5)T* on CCO.

Benefits

- Dial flexibility
- Centralized billing
- Callback support

Restrictions

- Large scale dialout is not supported.
- BAP and Dialer Watch are not supported.
- All configuration must be local on the router.

Related Documents

For more information about Cisco VPDN and dialout technologies, see the following documents:

- The *Layer 2 Tunnel Protocol* feature module, which is located under *New Features in Release 12.0(1)T* from CCO.
- The *Large Scale Dialout* feature module, which is located under *New Features in Release 12.0(3)T* from CCO.
- The *Resource Pool Management, VPDN Group Reorganization, VPDN Per-User Configuration and L2TP Tunnel Preservation of IP TOS* feature modules, which are located under *New Features in Release 12.0(5)T* from CCO.
- The “Virtual Private Dialup Network” chapter in the *Dial Solutions Configuration Guide*.
- The *Access VPN Solutions Using Tunneling Technology* solutions guide, which is located under the *Internetworking Solutions Guides* index on CCO’s documentation home page.

Supported Platforms

- Cisco 1600 series
- Cisco 1720 VPN Access Router
- Cisco 2500 series
- Cisco 2600
- Cisco 3600 series
- Cisco 4000-M series (Cisco 4000-M, 4500-M, 4700-M)
- Cisco 7000 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco AS5200
- Cisco AS5300
- Cisco AS5800

Supported Standards, MIBs, and RFCs

MIBs

- CISCO-VPDN-MGMT-MIB.my
- CISCO-VPDN-MGMT-MIB-V1SMI.my

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

L2TP RFC

Standards

None

Configuration Tasks

See the following sections for configuration tasks for the L2TP Dialout feature. Each task in the list indicates if the task is optional or required.

- Configuring an LNS to Request L2TP Dialout (Required)
- Configuring a LAC to Accept L2TP Dialout (Required)
- Configuring the Dialer on the LNS (Required)
- Configuring the Dialer on the LAC (Required)

Configuring an LNS to Request L2TP Dialout

To configure an LNS to request dialout tunneled PPP connections to a LAC, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	<code>dupree(config)# vpdn-group 1</code>	Creates VPDN group 1.
2	<code>dupree(config-vpdn)# request dialout</code>	Enables the LAC to send L2TP dialout requests.
3	<code>dupree(config-vpdn-req-out)# protocol l2tp</code>	Specifies L2TP as the tunneling protocol. Note L2TP is the only protocol that supports dialout.
4	<code>dupree(config-vpdn-req-out)# pool-member pool-number</code> or <code>dupree(config-vpdn-req-out)# rotary-group group-number</code>	Specifies the dialer profile pool that will be used to dial out. Specifies the dialer rotary group that will be used to dial out. You can only configure one dialer profile pool or dialer rotary group. Attempting to configure a second dialer resource will remove the first from the configuration.
5	<code>dupree(config-vpdn-req-out)# exit</code> <code>dupree(config-vpdn)# initiate-to ip ip-address</code>	Specifies the IP address that will be dialed out.
6	<code>dupree(config-vpdn)# local name hostname</code>	Specifies that the L2TP tunnel will identify itself with this hostname.

Configuring a LAC to Accept L2TP Dialout

To configure a LAC to accept tunneled dialout connections from an LNS, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	<code>sugaree(config)# vpdn-group 1</code>	Creates VPDN group 1.
2	<code>sugaree(config-vpdn)# accept dialout</code>	Enables the LAC to accept L2TP dialout requests.
3	<code>sugaree(config-vpdn-acc-out)# protocol l2tp</code>	Specifies L2TP as the tunneling protocol. Note L2TP is the only protocol that supports dialout.
4	<code>sugaree(config-vpdn-acc-out)# dialer dialer-interface</code>	Specifies the dialer that is used to dial out.
5	<code>sugaree(config-vpdn-acc-out)# exit</code> <code>sugaree(config-vpdn)# terminate-from hostname hostname</code>	Accepts L2TP tunnels that have this hostname configured as a local name.

Configuring the Dialer on the LNS

To enable an LNS to request L2TP dialout, use the following commands beginning in global configuration mode to configure the LNS's dialer:

Step	Command	Purpose
1	<code>sugaree(config)# interface dialer 1</code>	Defines a dialer rotary group.
2	<code>sugaree(config-if)# ip address 172.1.2.3 255.255.255.128</code>	Specifies an IP address for the group.
3	<code>sugaree(config-if)# encapsulation ppp</code>	Enables PPP encapsulation.
4	<code>sugaree(config-if)# dialer remote-name peer-name</code>	Specifies the name used to authenticate the remote router that is being dialed.
5	<code>sugaree(config-if)# dialer string dialer-number</code>	Specifies the number that is dialed.

Step	Command	Purpose
6	sugaree(config-if)# dialer vpdn	Enables L2TP dialout.
7	sugaree(config-if)# dialer pool <i>pool-number</i>	Specifies the dialer pool.
8	sugaree(config-if)# dialer-group <i>group-number</i>	Assigns the dialer to the specified dialer group.
9	sugaree(config-if)# ppp authentication chap	Specifies that CHAP authentication will be used.

Configuring the Dialer on the LAC

To enable a LAC to accept L2TP dialout, use the following commands beginning in global configuration mode to configure the LAC's dialer

Step	Command	Purpose
1	dupree(config)# interface dialer 1	Defines a dialer rotary group.
2	dupree(config-if)# ip unnumbered <i>interface-type number</i>	Configures the dialer to use the specified interface's IP address.
3	dupree(config-if)# encapsulation ppp	Enables PPP encapsulation
4	dupree(config-if)# dialer in-band	Enables DDR on the dialer.
5	dupree(config-if)# dialer aaa	Enables the dialer to use the AAA server to locate profiles for dialing information.
6	dupree(config-if)# dialer-group <i>group-number</i>	Assigns the dialer to the specified dialer group.
7	dupree(config-if)# ppp authentication chap	Specifies that CHAP authentication will be used.

Verifying L2TP Dialout

The following EXEC commands provide useful information for verifying VPDN sessions in general and L2TP dialout sessions in particular:

show interface virtual access <i>number</i>	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.

Dialout Show VPDN Example on a LAC

The following is an example of the **show vpdn** command for a successful dialout session on a LAC:

```
LAC# show vpdn

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

LocID RemID Remote Name   State Remote Address  Port  Sessions
1      1      lns_l2x0      est  10.40.1.150    1701  1

LocID RemID TunID Intf      Username      State  Last Chg Fastswitch
1      1      1      Se0:22                   est    00:00:02 enabled
```

Dialout Show VPDN Example on an LNS

The following is an example of the **show vpdn** command for a successful dialout session on an LNS:

```
LNS# show vpdn

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

LocID RemID Remote Name   State Remote Address  Port  Sessions
1      1      lac_l2x0      est  10.30.1.130    1701  1

LocID RemID TunID Intf      Username      State  Last Chg Fastswitch
1      1      1      Vi1              est    00:00:42 enabled

% No active L2F tunnels
```

Monitoring and Maintaining L2TP Dialout

The following EXEC commands will help you monitor and maintain VPDN sessions:

Command	Purpose
debug dialer events	Displays information about packets received on dialer interfaces.
debug ppp negotiation	Displays information about packets transmitted during PPP start-up and detailed PPP negotiation options.
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 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.

The following EXEC commands will provide more detailed information about VPDN sessions:

Command	Purpose
debug aaa authentication	Displays information on AAA authentication.

Command	Purpose
debug aaa authorization	Displays information on AAA authorization.
debug vpdn l2x-events	Displays L2F and L2TP events that are part of tunnel establishment or shutdown.
debug vpdn l2x-errors	Displays L2F and L2TP protocol errors that prevent tunnel establishment or normal operation.

Dialout Debug Example on a LAC

The following is an example of debug output from the **debug vpdn event**, **debug vpdn error**, and **debug dialer events** commands for a successful dialout session on a LAC:

```
LAC# show debugging
Dial on demand:
  Dial on demand events debugging is on
VPN:
  VPDN events debugging is on
  VPDN errors debugging is on
LAC#
*Mar 1 00:05:26.155:%SYS-5-CONFIG_I:Configured from console by console
*Mar 1 00:05:26.899:%SYS-5-CONFIG_I:Configured from console by console
*Mar 1 00:05:36.195:L2TP:I SCCRQ from lns_l2x0 tnl 1
*Mar 1 00:05:36.199:Tnl 1 L2TP:New tunnel created for remote lns_l2x0, address
10.40.1.150
*Mar 1 00:05:36.203:Tnl 1 L2TP:Got a challenge in SCCRQ, lns_l2x0
*Mar 1 00:05:36.207:Tnl 1 L2TP:O SCCRP to lns_l2x0 tnlid 1
*Mar 1 00:05:36.215:Tnl 1 L2TP:Tunnel state change from idle to wait-ctl-reply
*Mar 1 00:05:36.231:Tnl 1 L2TP:I SCCCN from lns_l2x0 tnl 1
*Mar 1 00:05:36.235:Tnl 1 L2TP:Got a Challenge Response in SCCCN from lns_l2x0
*Mar 1 00:05:36.239:Tnl 1 L2TP:Tunnel Authentication success
*Mar 1 00:05:36.239:Tnl 1 L2TP:Tunnel state change from wait-ctl-reply to established
*Mar 1 00:05:36.243:Tnl 1 L2TP:SM State established
*Mar 1 00:05:36.251:Tnl 1 L2TP:I OCRQ from lns_l2x0 tnl 1
*Mar 1 00:05:36.255:Tnl/Cl 1/1 L2TP:Session sequencing disabled
*Mar 1 00:05:36.259:Tnl/Cl 1/1 L2TP:Session FS enabled
*Mar 1 00:05:36.259:Tnl/Cl 1/1 L2TP:New session created
*Mar 1 00:05:36.263:12C:Same state, 0
*Mar 1 00:05:36.267:DSES 12C:Session create
*Mar 1 00:05:36.271:L2TP:Send OCRP
*Mar 1 00:05:36.275:Tnl/Cl 1/1 L2TP:Session state change from idle to wait-cs-answer
*Mar 1 00:05:36.279:DSES 0x12C:Building dialer map
*Mar 1 00:05:36.283:Dialout 0x12C:Next hop name is 71014
*Mar 1 00:05:36.287:Serial0:23 DDR:rotor dialout [priority]
*Mar 1 00:05:36.291:Serial0:23 DDR:Dialing cause dialer session 0x12C
*Mar 1 00:05:36.291:Serial0:23 DDR:Attempting to dial 71014
*Mar 1 00:05:36.479:%LINK-3-UPDOWN:Interface Serial0:22, changed state to up
*Mar 1 00:05:36.519:isdn_call_connect:Calling lineaction of Serial0:22
*Mar 1 00:05:36.519:Dialer0:Session free, 12C
*Mar 1 00:05:36.523::0 packets unqueued and discarded
*Mar 1 00:05:36.527:Se0:22 VPDN:Bind interface direction=1
*Mar 1 00:05:36.531:Se0:22 1/1 L2TP:Session state change from wait-cs-answer to
established
*Mar 1 00:05:36.531:L2TP:Send OCCN
*Mar 1 00:05:36.539:Se0:22 VPDN:bound to vpdn session
*Mar 1 00:05:36.555:Se0:22 1/1 L2TP:O FS failed
*Mar 1 00:05:36.555:Se0:22 1/1 L2TP:O FS failed
*Mar 1 00:05:42.515:%ISDN-6-CONNECT:Interface Serial0:22 is now connected to 71014
```

Dialout Debug Example on an LNS

The following is an example of debug output from the **debug vpdn event**, **debug vpdn error**, **debug ppp negotiation**, and **debug dialer events** commands for a successful dialout session on an LNS:

```
LNS# show debugging
Dial on demand:
  Dial on demand events debugging is on
PPP:
  PPP authentication debugging is on
  PPP protocol negotiation debugging is on
VPN:
  VPDN events debugging is on
  VPDN errors debugging is on
LNS#
*Apr 22 19:48:32.419:%SYS-5-CONFIG_I:Configured from console by console
*Apr 22 19:48:32.743:%SYS-5-CONFIG_I:Configured from console by console
*Apr 22 19:48:33.243:Di0 DDR:dialer_fsm_idle()
*Apr 22 19:48:33.271:Vi1 PPP:Phase is DOWN, Setup
*Apr 22 19:48:33.279:Vi1 PPP:Phase is DOWN, Setup
*Apr 22 19:48:33.279:Virtual-Access1 DDR:Dialing cause ip (s=10.60.1.160,
d=10.10.1.110)
*Apr 22 19:48:33.279:Virtual-Access1 DDR:Attempting to dial 71014
*Apr 22 19:48:33.279:Tnl/Cl 1/1 L2TP:Session sequencing disabled
*Apr 22 19:48:33.279:Tnl/Cl 1/1 L2TP:Session FS enabled
*Apr 22 19:48:33.283:Tnl/Cl 1/1 L2TP:Session state change from idle to wait-for-tunnel
*Apr 22 19:48:33.283:Tnl/Cl 1/1 L2TP:Create dialout session
*Apr 22 19:48:33.283:Tnl 1 L2TP:SM State idle
*Apr 22 19:48:33.283:Tnl 1 L2TP:O SCCRQ
*Apr 22 19:48:33.283:Tnl 1 L2TP:Tunnel state change from idle to wait-ctl-reply
*Apr 22 19:48:33.283:Tnl 1 L2TP:SM State wait-ctl-reply
*Apr 22 19:48:33.283:Vi1 VPDN:Bind interface direction=2
*Apr 22 19:48:33.307:Tnl 1 L2TP:I SCCRP from lac_l2x0
*Apr 22 19:48:33.307:Tnl 1 L2TP:Got a challenge from remote peer, lac_l2x0
*Apr 22 19:48:33.307:Tnl 1 L2TP:Got a response from remote peer, lac_l2x0
*Apr 22 19:48:33.311:Tnl 1 L2TP:Tunnel Authentication success
*Apr 22 19:48:33.311:Tnl 1 L2TP:Tunnel state change from wait-ctl-reply to established
*Apr 22 19:48:33.311:Tnl 1 L2TP:O SCCCN to lac_l2x0 tnlid 1
*Apr 22 19:48:33.311:Tnl 1 L2TP:SM State established
*Apr 22 19:48:33.311:L2TP:O OCRQ
*Apr 22 19:48:33.311:Vi1 1/1 L2TP:Session state change from wait-for-tunnel to
wait-reply
*Apr 22 19:48:33.367:Vi1 1/1 L2TP:I OCRP from lac_l2x0 tnl 1, cl 0
*Apr 22 19:48:33.367:Vi1 1/1 L2TP:Session state change from wait-reply to wait-connect
*Apr 22 19:48:33.631:Vi1 1/1 L2TP:I OCCN from lac_l2x0 tnl 1, cl 1
*Apr 22 19:48:33.631:Vi1 1/1 L2TP:Session state change from wait-connect to established
*Apr 22 19:48:33.631:Vi1 VPDN:Connection is up, start LCP negotiation now
*Apr 22 19:48:33.631:%LINK-3-UPDOWN:Interface Virtual-Access1, changed state to up
*Apr 22 19:48:33.631:Vi1 DDR:dialer_statechange(), state=4Dialer statechange to up
Virtual-Access1
*Apr 22 19:48:33.631:Vi1 DDR:dialer_out_call_connected()
*Apr 22 19:48:33.631:Vi1 DDR:dialer_bind_profile() to Di0
*Apr 22 19:48:33.631:%DIALER-6-BIND:Interface Virtual-Access1 bound to profile
Dialer0Dialer call has been placed Virtual-Access1
*Apr 22 19:48:33.635:Vi1 PPP:Treating connection as a callout
*Apr 22 19:48:33.635:Vi1 PPP:Phase is ESTABLISHING, Active Open
*Apr 22 19:48:33.635:Vi1 LCP:O CONFREQ [Closed] id 1 len 15
*Apr 22 19:48:33.635:Vi1 LCP:  AuthProto CHAP (0x0305C22305)
*Apr 22 19:48:33.635:Vi1 LCP:  MagicNumber 0x50E7EC2A (0x050650E7EC2A)
*Apr 22 19:48:33.663:Vi1 LCP:I CONFREQ [REQsent] id 1 len 15
*Apr 22 19:48:33.663:Vi1 LCP:  AuthProto CHAP (0x0305C22305)
*Apr 22 19:48:33.663:Vi1 LCP:  MagicNumber 0x10820474 (0x050610820474)
*Apr 22 19:48:33.663:Vi1 LCP:O CONFACK [REQsent] id 1 len 15
*Apr 22 19:48:33.663:Vi1 LCP:  AuthProto CHAP (0x0305C22305)
*Apr 22 19:48:33.663:Vi1 LCP:  MagicNumber 0x10820474 (0x050610820474)
```

```

*Apr 22 19:48:33.663:Vi1 LCP:I CONFACK [ACKsent] id 1 len 15
*Apr 22 19:48:33.663:Vi1 LCP: AuthProto CHAP (0x0305C22305)
*Apr 22 19:48:33.663:Vi1 LCP: MagicNumber 0x50E7EC2A (0x050650E7EC2A)
*Apr 22 19:48:33.663:Vi1 LCP:State is Open
*Apr 22 19:48:33.663:Vi1 PPP:Phase is AUTHENTICATING, by both
*Apr 22 19:48:33.663:Vi1 CHAP:Using alternate hostname lns0
*Apr 22 19:48:33.663:Vi1 CHAP:O CHALLENGE id 1 len 25 from "lns0"
*Apr 22 19:48:33.679:Vi1 CHAP:I CHALLENGE id 1 len 35 from "user0@foo.com0"
*Apr 22 19:48:33.679:Vi1 AUTH:Started process 0 pid 92
*Apr 22 19:48:33.679:Vi1 CHAP:Using alternate hostname lns0
*Apr 22 19:48:33.683:Vi1 CHAP:O RESPONSE id 1 len 25 from "lns0"
*Apr 22 19:48:33.695:Vi1 CHAP:I SUCCESS id 1 len 4
*Apr 22 19:48:33.699:Vi1 CHAP:I RESPONSE id 1 len 35 from "user0@foo.com0"
*Apr 22 19:48:33.699:Vi1 CHAP:O SUCCESS id 1 len 4
*Apr 22 19:48:33.699:Vi1 DDR:dialer_remote_name() for user0@foo.com0
*Apr 22 19:48:33.699:Vi1 PPP:Phase is UP
*Apr 22 19:48:33.703:Vi1 IPCP:O CONFREQ [Closed] id 1 len 10
*Apr 22 19:48:33.703:Vi1 IPCP: Address 10.20.1.150 (0x030614140196)
*Apr 22 19:48:33.703:Vi1 CCP:O CONFREQ [Closed] id 1 len 10
*Apr 22 19:48:33.703:Vi1 CCP: LZSDCP history 1 check mode SEQ process UNCOMPRESSED
(0x170600010201)
*Apr 22 19:48:33.711:Vi1 IPCP:I CONFREQ [REQsent] id 1 len 10
*Apr 22 19:48:33.715:Vi1 IPCP: Address 10.20.1.120 (0x030614140178)
*Apr 22 19:48:33.715:Vi1 IPCP:O CONFACK [REQsent] id 1 len 10
*Apr 22 19:48:33.715:Vi1 IPCP: Address 10.20.1.120 (0x030614140178)
*Apr 22 19:48:33.715:Vi1 CCP:I CONFREQ [REQsent] id 1 len 10
*Apr 22 19:48:33.715:Vi1 CCP: LZSDCP history 1 check mode SEQ process UNCOMPRESSED
(0x170600010201)
*Apr 22 19:48:33.715:Vi1 CCP:O CONFACK [REQsent] id 1 len 10
*Apr 22 19:48:33.715:Vi1 CCP: LZSDCP history 1 check mode SEQ process UNCOMPRESSED
(0x170600010201)
*Apr 22 19:48:33.719:Vi1 IPCP:I CONFACK [ACKsent] id 1 len 10
*Apr 22 19:48:33.719:Vi1 IPCP: Address 10.20.1.150 (0x030614140196)
*Apr 22 19:48:33.719:Vi1 IPCP:State is Open
*Apr 22 19:48:33.719:Vi1 DDR:Dialer protocol up
*Apr 22 19:48:33.719:Vi1 Dialer0:dialer_ckt_swt_client_connect:incoming circuit switched
call
*Apr 22 19:48:33.719:Di0 IPCP:Install route to 10.20.1.120
*Apr 22 19:48:33.719:Vi1 CCP:I CONFACK [ACKsent] id 1 len 10
*Apr 22 19:48:33.719:Vi1 CCP: LZSDCP history 1 check mode SEQ process UNCOMPRESSED
(0x170600010201)
*Apr 22 19:48:33.719:Vi1 CCP:State is Open
*Apr 22 19:48:34.699:Vi1 LINEPROTO-5-UPDOWN:Line protocol on Interface Virtual-Access1,
changed state to up

```

Configuration Examples

This section provides the following configuration examples:

- LNS Configured for Dialout
- LAC Configured for Dialout
- LNS Configured for Both Dial-In and Dialout
- LAC Configured for Both Dial-In and Dialout

LNS Configured for Dialout

In the following example, an LNS is configured to request L2TP dialout from IP address 10.3.2.1 using a dialer pool:

```
vpdn-group 1
  request dialout
  protocol l2tp
  pool-member 1
  initiate-to ip 10.3.2.1
  local name cerise
!
interface Dialer2
  ip address 172.1.2.3 255.255.128
  encapsulation ppp
  dialer remote-name reuben
  dialer string 5551234
  dialer vpdn
  dialer pool 1
  dialer-group 1
  ppp authentication chap
```

LAC Configured for Dialout

In the following example, a LAC is configured to accept L2TP dialout requests from a router using the hostname, cerise. It is configured to use DDR:

```
VPDN-group 1
  accept dialout
  protocol l2tp
  dialer 2
  terminate-from hostname cerise
!
interface Dialer2
  ip unnumbered Ethernet0
  encapsulation ppp
  dialer in-band
  dialer aaa
  dialer-group 1
  ppp authentication chap
```

LNS Configured for Both Dial-In and Dialout

You can also configure a device to perform both dial in and dial out. In the following example, a LNSs VPDN group is configured to dial in using virtual template 1 to clone the virtual-access interface and dial out using dialer pool 1:

```
vpdn-group 1
  accept dialin
  protocol l2tp
  virtual-template 1
  request dialout
  protocol l2tp
  pool-member 1
  local name reuben
  terminate-from hostname cerise
  initiate-to ip 10.3.2.1
```

LAC Configured for Both Dial-In and Dialout

You can also configure a device to dial in and dial out using different Layer 2 tunnels. In the following example, a LAC's VPDN group is configured to dial in using L2F and dial out using L2TP:

```
vpdn-group 1
 request dialin
  protocol l2f
  domain jgb.com
 accept dialout
  protocol l2tp
  dialer 2
 local name cerise
 terminate-from hostname reuben
 initiate-to ip 172.1.1.2.3
```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **accept dialout**
- **default**
- **dialer**
- **dialer aaa**
- **dialer vpdn**
- **initiate-to**
- **local name**
- **pool-member**
- **protocol**
- **request dialout**
- **rotary-group**
- **source-ip**
- **terminate-from**

accept dialout

To accept requests to tunnel L2TP dialout calls and create an accept-dialout VPDN subgroup, use the **accept dialout** VPDN group command. To remove the accept-dialout subgroup from the VPDN group, use the **no** form of this command.

- accept dialout**
- no accept dialout**

Syntax Description

This command has no keywords nor arguments.

Defaults

Disabled

Command Modes

VPDN group mode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Only L2TP can be used to dial out (not L2F).

For a VPDN group to accept dialout calls, you must also configure the following commands:

- **terminate-from** VPDN group command
- **protocol** VPDN subgroup command
- **dialer** accept-dialout command
- **dialer aaa** dialer interface command

Once an L2TP tunnel is established, both dial-in and dialout calls can use the same tunnel.

Examples

The following example configures a VPDN group to accept L2TP tunnels for dialout calls from the LNS cerise by using dialer 2 as its dialing resource:

```

vpdn-group 1
accept dialout
  protocol l2tp
  dialer 2
terminate-from hostname cerise
!
interface Dialer2
  ip unnumbered Ethernet0
  encapsulation ppp
  dialer in-band
  dialer aaa
  dialer-group 1
  ppp authentication chap

```

Related Commands

Command	Description
dialer	Specifies the dialer interface that an accept-dialout group will use to dial out calls.
dialer aaa	Enables the LAC's dialer to use the AAA server to locate profiles for dialing information.
dialer vpdn	Enables the dialer to place a call using VPDN.
protocol	Specifies the tunneling protocol that is used for the dialin connections.
request dialout	Enables an LNS to request L2TP tunnels for dialout calls.
terminate-from	Specifies the hostname the LNS uses when requesting a tunnel.

default

To reset a VPDN group command or a VPDN subgroup command to its default value, use the **default** command.

```
default { accept-dialin | accept-dialout | authen before-forward | dialer | dnis | domain |
force-local-chap | initiate-to | l2f | l2tp | lcp renegotiation | local | multilink | pool-member |
request-dialin | request-dialout | rotary-group | source-ip | terminate-from |
virtual-template }
```

Syntax Description

accept-dialin	Removes the accept-dialin group from the VPDN group.
accept-dialout	Removes the accept-dialout group from the VPDN group.
authen before-forward	Removes the authen before-forward command from the VPDN group.
dialer	Removes the dialer command from the accept-dialout group.
dnis	Removes all dnis commands from the request-dialin group.
domain	Removes all domain commands from the request-dialin group.
force-local-chap	Removes the force-local-chap command from the VPDN group.
initiate-to	Removes all initiate-to commands from the VPDN group.
l2f	Removes all l2f commands from the VPDN group.
l2tp	Removes all l2tp commands from the VPDN group.
lcp renegotiation	Removes the lcp renegotiation command from the VPDN group.
local	Removes the local command from the VPDN group.
multilink	Removes all multilink commands from the VPDN group.
pool-member	Removes the pool-member command from the request-dialout group.
request-dialin	Removes the request-dialin group from the VPDN group.
request-dialout	Removes the request-dialout group from the VPDN group.
rotary-group	Removes the rotary-group command from the request-dialout group.
source-ip	Removes the source-ip command from the VPDN group.
terminate-from	Removes the terminate-from command from the VPDN group.
virtual-template	Removes the virtual-template command from the accept-dialin group.

Defaults

Disabled

Command Modes

VPDN group mode

VPDN subgroup modes

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines



Caution Using the **default** command is similar to using the **no** form of a command.

Examples

The following example shows an LNS configured to accept L2F dial-in and L2TP dialout.

```

vpdn-group 1
  accept dialin
  protocol l2f
  virtual-template 1
  request dialout
  protocol l2tp
  pool-member 1
  local name reuben
  terminate-from hostname cerise
  initiate-to ip 10.3.2.1
  l2f ignore-mid-sequence
  l2tp ip udp checksum

```

If you then issue the **default protocol** command in request-dialout mode, the configuration will look like this:

```

vpdn-group 1
  accept dialin
  protocol l2f
  virtual-template 1
  request dialout
  local name reuben
  terminate-from hostname cerise
  initiate-to ip 10.3.2.1
  l2f ignore-mid-sequence

```

If you issue the **no accept dialin** command when the LNS is configured as in the first example, the configuration will change to this:

```

vpdn-group 1
  request dialout
  protocol l2tp
  pool-member 1
  local name reuben
  initiate-to ip 10.3.2.1
  l2tp ip udp checksum

```

dialer

To specify the dialer interface that an accept-dialout VPDN subgroup will use to dial out calls, use the **dialer** accept-dialout command. To remove the dialer interface from the accept-dialout VPDN subgroup, use the **no** form of this command.

dialer *dialer-interface*

no dialer

Syntax Description

dialer-interface Number of the dialer interface.

Defaults

Disabled

Command Modes

Accept-dialout mode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

You must first enable L2TP on the accept-dialout VPDN subgroup by using the **protocol l2tp** command before you can enable the **dialer** command. Removing the **protocol** command will remove the **dialer** command from the accept-dialout subgroup.

You can only specify one dialer per accept dialout group. Configuring a second **dialer** command will replace the first **dialer** command.

Examples

The following example creates an accept-dialout VPDN subgroup that uses dialer interface 2:

```

VPDN-group 1
  accept dialout
  protocol l2tp
  dialer 2
  terminate-from hostname cerise

```

Related Commands

Command	Description
accept dialout	Accepts requests to tunnel L2TP dialout calls.
protocol	Specifies the Layer 2 tunneling protocol that a VPDN subgroup uses.
terminate-from	Specifies the hostname the LNS uses when requesting a tunnel.

dialer aaa

To allow a dialer to access the AAA server for dialing information, use the **dialer aaa** command in interface configuration mode. To disable this function, use the **no** form of the command.

dialer aaa

no dialer aaa

Syntax Description

This command has no arguments or keywords.

Default

This feature is not enabled by default.

Command Mode

Interface configuration of a dialer rotary group leader.

Command History

Release	Modification
12.0(3)T	This command was introduced.

Usage Guidelines

This command is required for large scale dialout and L2TP dialout functionality.

Example

The following example shows how to configure the dialer interface and VPDN group on a LAC for L2TP dialout:

```
interface Dialer2
 ip unnumbered ethernet 0
 encapsulation ppp
 dialer in-band
 dialer aaa
 dialer-group 1
 ppp authentication chap

vpdn-group 1
 accept-dialout
 protocol l2tp
 dialer 2
 terminate-from hostname fishman
```

Related Commands

Command	Description
accept dialout	Accepts requests to tunnel L2TP dialout calls.
dialer vpdn	Enables a dialer profile or DDR dialer to use L2TP dialout.

dialer vpdn

To enable a Dialer Profile or DDR dialer to use L2TP dialout, use the **dialer vpdn** interface configuration command. To disable L2TP dialout on a Dialer Profile or DDR dialer, use the **no** form of this command.

dialer vpdn
no dialer vpdn

Defaults

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The **dialer vpdn** command must be configured on the LNS's dialer interface to enable L2TP dialout. This command enables the dialer to place a VPDN call.

Examples

The following example shows how to configure the dialer interface and VPDN group on an LNS for L2TP dialout:

```
interface Dialer2
 ip address 172.1.1.2.3 255.255.255.128
 encapsulation ppp
 dialer remote-name reuben
 dialer string 5551234
 dialer vpdn
 dialer pool 1
 dialer-group 1
 ppp authentication chap

vpdn-group 1
 request-dialout
 protocol l2tp
 pool-member 1
 initiate-to ip 172.21.9.4
```

Related Commands

Command	Description
dialer aaa	Allows a dialer to access the AAA server for dialing information.
request dialout	Enables a router to request L2TP tunnels for dialout calls.

initiate-to

To specify the IP address that will be tunneled to, use the **initiate-to** VPDN group command. To remove an IP address from the VPDN group, use the **no** form of this command.

initiate-to *ip ip-address*

no initiate-to [*ip ip-address*]

Syntax Description

ip *ip-address* The IP address of the router that will be tunneled to.

Defaults

Disabled

Command Modes

VPDN group mode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Before you can use this command, you must enable one of the two request VPDN subgroups by using either the **request dialin** or **request dialout** command.

A LAC configured to request dial-in can be configured with multiple **initiate-to** commands to tunnel to more than one IP address.

An LNS configured to request dialout can only be configured with a single **initiate-to** command. If you enter a second **initiate-to** command, it will replace the original **initiate-to** command.

Examples

The following example configures VPDN group 1 to request an L2TP tunnel to the peer at IP address 10.3.2.1 for tunneling dialout calls from dialer pool 1.

```
vpdn-group 1
 request dialout
  protocol l2tp
  pool-member 1
  initiate-to ip 10.3.2.1
```

Related Commands

Command	Description
request dialin	Enables a router to request either L2F or L2TP tunnels for dial-in.
request dialout	Enables a router to request L2TP tunnels for dialout calls.

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

Command History

Release	Modification
11.3(5)AA and 12.0(1)T	This command was introduced.

Usage Guidelines

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 host name is used (defined by the **hostname** command).

Examples

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

```
local name dustie
```

Related Commands

Command	Description
hostname	Specifies or modifies the host name of the router.
l2tp tunnel password	Sets the password that is used to authenticate the tunnel.
terminate-from	Specifies the host name the LNS uses when requesting a tunnel.

pool-member

To assign a request-dialout VPDN subgroup to a dialer pool, use the **pool-member** request-dialout command. To remove the request-dialout VPDN subgroup from a dialer pool, use the **no** form of this command

```
pool-member pool-number
no pool-member [pool-member]
```

Syntax Description

pool-member The dialer pool that this VPDN group belongs to.

Defaults

Disabled

Command Modes

Request-dialout mode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

You must first enable the **protocol l2tp** on the request-dialout VPDN subgroup before you can enable the **pool-member** command. Removing the **protocol l2tp** command will remove the **pool-member** command from the request-dialout subgroup.

You can only configure one dialer profile pool (using the **pool-member** command) or dialer rotary group (using the **rotary-group** command). If you attempt to configure a second dialer resource, you will replace the first dialer resource in the configuration.

Examples

The following example configures VPDN group 1 to request L2TP dialout to IP address 172.5.4.6 using dialer profile pool 1 and identifying itself using the local name harold.

```
vpdn-group 1
 request-dialout
  protocol l2tp
  pool-member 1
 initiate-to ip 172.5.4.6
 local name harold
```

Related Commands

Command	Description
initiate-to	Specifies the IP address that calls are tunneled to.
protocol	Specifies the tunneling protocol that is used for the dial-in connections.
request dialout	Enables a router to request L2TP tunnels for dialout calls.
rotary-group	Specifies the dialer rotary group that is used to dialout.

protocol

To specify the Layer 2 tunneling protocol that the VPDN subgroup will use, use the **protocol** VPDN subgroup command. To remove the protocol-specific configurations from a VPDN subgroup, use the **no** form of this command.

protocol {**l2f** | **l2tp** | **any**}

no protocol

Syntax Description

l2f	Enables the VPDN subgroup to establish L2F tunnels.
l2tp	Enables the VPDN subgroup to establish L2TP tunnels.
any	Enables the VPDN subgroup to establish either L2F or L2TP tunnels.

Defaults

Disabled

Command Modes

VPDN subgroup modes

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This command is required for all four of the VPDN subgroups.

L2TP is the only protocol that can be used for dialout.

Changing the protocol will remove all the commands from the VPDN subgroup and any protocol-specific commands from the VPDN group configuration.

Examples

The following example configures VPDN group 1 to accept dial-in calls using L2F and request dialout calls using L2TP:

```
vpdn-group 1
  accept dialin
  protocol l2f
  virtual-template 1
  request dialout
  protocol l2tp
  pool-member 1
  local name reuben
  terminate-from hostname cerise
  initiate-to ip 10.3.2.1
  l2f ignore-mid-sequence
  l2tp ip udp checksum
```

If you then use the **no protocol** command in request-dialout mode, the configuration will be changed to this:

```
vpdn-group 1
  accept dialin
  protocol l2f
  virtual-template 1
  request dialout
  local name reuben
  terminate-from hostname cerise
  l2f ignore-mid-sequence
```

Related Commands

Command	Description
accept dialin	Accepts requests to create either L2F or L2TP tunnels for dial-in.
accept dialout	Accepts requests to tunnel L2TP dialout calls.
request dialin	Enables a router to request either L2F or L2TP tunnels for dial-in.
request dialout	Enables a router to request L2TP tunnels for dialout calls.

request dialout

To enable an LNS to request VPDN dialout calls by using L2TP, use the **request dialout** VPDN group command. To disable L2TP dialout, use the **no** form of this command.

request dialout

no request dialout

Syntax Description

This command has no keywords nor arguments.

Defaults

Disabled

Command Modes

VPDN group mode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

If the dialer pool or dialer rotary group that the VPDN group is in contains physical interfaces, the physical interfaces will be used before the VPDN group.

For a VPDN group to request dialout calls, you must also configure the following commands:

- **initiate-to** VPDN group command
- Either the **pool-member** or **rotary-group** VPDN subgroup command
- **dialer vpdn** dialer interface command

Once an L2TP tunnel is established, both dial-in and dialout calls can use the same tunnel.

Examples

The following example configures VPDN group 1 to request an L2TP tunnel to the peer at IP address 10.3.2.1 for tunneling dialout calls from dialer pool 1.

```
vpdn-group 1
  request dialout
  protocol l2tp
  pool-member 1
  imitate-to ip 10.3.2.1
!
interface Dialer2
  ip address 172.1.2.3 255.255.128
  encapsulation ppp
  dialer remote-name reuben
  dialer string 5551234
  dialer vpdn
  dialer pool 1
  dialer-group 1
  ppp authentication chap
```

Related Commands

Command	Description
accept dialout	Accepts requests to tunnel L2TP dialout calls.
dialer vpdn	Enables the dialer to place a call using VPDN.
initiate-to	Specifies the IP address that calls are tunneled to.
protocol	Specifies the tunneling protocol that is used for the dialout connections.
pool-member	Specifies the dialer profile pool that is used to dial out.
rotary-group	Specifies the dialer rotary group that is used to dial out.

rotary-group

To assign a request-dialout VPDN subgroup to a dialer rotary group, use the **rotary-group** request-dialout command. To remove the request-dialout VPDN subgroup from the dialer rotary group, use the **no** form of this command.

```
rotary-group group-number
no rotary-group [group-number]
```

Syntax Description

group-number The dialer rotary group that this VPDN group belongs to.

Defaults

Disabled

Command Modes

Request-dialout mode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

If the dialer pool or dialer rotary group that the VPDN group is in contains physical interfaces, the physical interfaces will be used before the VPDN group.

You must first enable the **protocol l2tp** command on the request-dialout VPDN subgroup before you can enable the **rotary-group** command. Removing the **protocol l2tp** command will remove the **rotary-group** command from the request-dialout subgroup.

You can only configure one dialer profile pool (using the **pool-member** command) or dialer rotary group (using the **rotary-group** command). If you attempt to configure a second dialer resource, you will replace the first dialer resource in the configuration.

Examples

The following example configures VPDN group 1 to request L2TP dialout to IP address 172.5.4.6 using dialer profile pool 1 and identifying itself using the local name harold.

```
vpdn-group 1
  request-dialout
  protocol l2tp
  rotary-group 1
  initiate-to ip 172.5.4.6
  local name harold
```

Related Commands

Command	Description
initiate-to	Specifies the IP address that calls are tunneled to.
pool-member	Specifies the dialer profile pool that is used to dial out.
protocol	Specifies the tunneling protocol that is used for the dial in connections.
request dialout	Enables a router to request L2TP tunnels for dialout calls.

source-ip

To specify an alternate IP address for a VPDN tunnel that is different from the physical IP address used to open the tunnel, use the **source-ip** VPDN group command. To remove the alternate IP address, use the **no** form of this command.

source-ip *ip-address*

no source-ip

Syntax Description

<i>ip-address</i>	Alternate IP address (different from the physical IP address used to open the VPDN tunnel) that the router uses to identify the tunnel.
-------------------	---

Defaults

Disabled

Command Modes

VPDN group mode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Each VPDN group on a router can be configured with a unique **source-ip** command.

Examples

The following example configures a LAC to accept L2TP dialout calls using the alternate IP address 172.23.33.7, which is different from the physical IP address used to open the L2TP tunnel.

```

vpdn-group 3
  accept-dialout
  protocol l2tp
  dialer 2
  terminate-from hostname orpheus
  source-ip 172.23.33.7

```

Related Commands

Command	Description
accept dialin	Accepts requests to create either L2F or L2TP tunnels for dial-in.
accept dialout	Accepts requests to tunnel L2TP dialout calls.
request dialin	Enables a router to request either L2F or L2TP tunnels for dial-in.
request dialout	Enables a router to request L2TP tunnels for dialout calls.

terminate-from

To specify the host name of the remote LAC or LNS that will be required when accepting a VPDN tunnel, use the **terminate-from** VPDN group command. To remove the hostname from the VPDN group, use the **no** form of this command.

```
terminate-from hostname hostname
no terminate-from [hostname hostname]
```

Syntax Description

hostname *hostname* The host name that this VPDN group will accept connections from.

Defaults

Disabled

Command Modes

VPDN group mode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Before you can use this command, you must have already enabled one of the two accept VPDN subgroups by using either the **accept dialin** or **accept dialout** command.

Each VPDN group can only terminate from a single host name. If you enter a second **terminate-from** command on a VPDN group, it will replace the first **terminate-from** command.

Examples

The following example configures a VPDN group to accept L2TP tunnels for dialout calls from the LNS cerise by using dialer 2 as its dialing resource:

```
vpdn-group 1
  accept dialout
  protocol l2tp
  dialer 2
  terminate-from hostname cerise
```

Related Commands

Command	Description
accept dialin	Accepts requests to create either L2F or L2TP tunnels for dial-in.
accept dialout	Accepts requests to tunnel L2TP dialout calls.

Glossary

client—The hardware and software that the user uses to establish the PPP session.

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

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

L2TP access concentrator—See LAC.

L2TP network server—See LNS.

LAC—L2TP access concentrator. In L2TP technology, a device that the client directly connects to and through which PPP frames are tunneled to the L2TP network server (LNS). The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls.

Layer 2 Tunneling Protocol—See L2TP.

LNS—L2TP network server. In L2TP technology, a termination point for L2TP tunnels, and an access point where PPP frames are processed and passed to higher layer protocols. An LNS can operate on any platform that terminates PPP. 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 it can terminate calls arriving at any of the LAC's full range of PPP interfaces (asynchronous, synchronous, ISDN, V.120, etc.). The LNS initiates outgoing calls and receives incoming calls.

virtual-access interface—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. In access VPNs, the home gateway clones a virtual access interface for VPN users.

virtual private dialup network—See VPDN.

virtual template—A template that is used to create a logical interface configured with generic configuration information for a specific purpose or common configuration. The template takes the form of a list of Cisco IOS interface commands that are applied to virtual access interfaces, as needed. In access VPNs, the virtual template is configured on the home gateway and used to clone virtual-access interfaces for VPN users.

VPDN—virtual private dialup network. A system that permits networks to extend beyond a physical home networks while giving the appearance and functionality of being directly connected to a home network. VPDNs use L2TP and L2F to extend the Layer 2 and higher parts of the network connection from the ISP to the home gateway.

