

VPDN Group Reorganization

This document includes the following sections:

- Feature Overview on page 1
- Supported Platforms on page 4
- Supported Standards, MIBs, and RFCs on page 5
- Configuration Tasks on page 5
- Verifying VPDN Sessions on page 8
- Monitoring and Maintaining VPDN Sessions on page 11
- Configuration Examples on page 15
- Command Reference on page 18
- Glossary on page 55

Feature Overview

The VPDN Group Reorganization feature organizes the VPDN group commands into a new hierarchy. VPDN groups can now support:

- The following LNS VPDN services:
 - accept dialin
 - request dialout
- The following LAC VPDN services:
 - request dialin
 - accept dialout
- One of the four VPDN services

A VPDN group can act as either an LNS or a LAC, but not both. But individual routers can have both LNS VPDN groups and LAC VPDN groups.

To facilitate this reorganization, the VPDN group now contains the four corresponding command modes listed in Table 1. These new command modes are accessed from VPDN group mode; therefore, they are generically referred to as VPDN subgroups.

Table 1 New VPDN Group Command Modes

Command Mode	Router Prompt	Type of Service
accept-dialin	router (config-vpdn-acc-in) #	LNS
request-dialout	router (config-vpdn-req-out) #	LNS
request-dialin	router (config-vpdn-req-in) #	LAC
accept-dialout	router (config-vpdn-acc-out) #	LAC

The keywords and arguments for the existing **accept-dialin** and **request-dialin** commands are now independent accept-dialin mode and request-dialin mode commands.

The previous syntax is still supported, but when you display the configuration, the commands will be converted to appear in the new format.

For example, to configure a LAC to request dial-in, you could use the old command:

```
request dialin l2tp ip 10.1.2.3 domain jgb.com
```

When you view the configuration, the keywords and arguments are displayed in the new format as individual commands:

```
request dialin
protocol l2tp
domain jgb.com
initiate-to ip 10.1.2.3
```

Similarly, the new **accept-dialout** and **request-dialout** commands have subgroup commands that are used to specify such information as the tunneling protocol and dialer resource.

Table 2 lists the new VPDN subgroup commands and which command modes they apply to:

Table 2 VPDN Subgroup Commands

Command	VPDN Subgroups
protocol	all subgroups
default	all subgroups
dialer	accept-dialout
dnis	request-dialin
domain	request-dialin
pool-member	request-dialout
rotary-group	request-dialout
virtual-template	accept-dialin

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

Two new VPDN group commands are introduced: **initiate-to** and **terminate-from**. These commands are used to specify IP addresses to tunnel to, and hostnames to accept tunnels from.

Table 3 lists the VPDN group commands and which subgroups you need to enable for them to be configurable:

Table 3 VPDN Group Commands

Command	VPDN Subgroups
accept dialin	LNS VPDN group ¹
accept dialout	LAC VPDN group ²
authen before-forward	request-dialin
default	any subgroup
force-local-chap	accept-dialin
initiate-to	request-dialin or request-dialout
lcp renegotiation	accept-dialin
local name	any subgroup
multilink	request-dialin
request dialin	LAC VPDN Group
request dialout	LNS VPDN Group
source-ip	any subgroup
terminate-from	accept-dialin or accept-dialout

- 1 LNS VPDN groups can be configured for accept dialin and/or request dialout.
- 2 LAC VPDN groups can be configured for accept dialout and/or request dialin.

Benefits

The VPDN group reorganization makes VPDN groups easier to configure by breaking commands with a long list of keywords and arguments into separate commands.

This feature helps facilitate the following new features and protocol flexibility:

- Load sharing
- Dialout
- LAC and LNS services on a single tunnel

This feature enables individual VPDN groups to tunnel both dial-in and dialout calls using the same tunnel.

Restrictions

A VPDN group can act as either an LNS or a LAC, but not both. But individual routers can have both LNS VPDN groups and LAC VPDN groups.

Related Documents

For more information about Cisco VPDN, 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 *L2TP Dialout* and *Resource Pool Management* 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 VPDN Group Reorganization feature. Each task in the list indicates if the task is optional or required.

- Configuring a LAC to Request Dial-in (Optional)
- Configuring a LAC to Accept Dialout (Optional)
- Configuring an LNS to Accept Dial-in (Optional)
- Configuring an LNS to Request Dialout (Optional)
- Configuring the Dialer on a LAC for Dialout (Optional)
- Configuring the Dialer on an LNS for Dialout (Optional)

Configuring a LAC to Request Dial-in

To configure a LAC to accept PPP calls and tunnel them to an LNS, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	Router(config)# vpdn-group 1	Creates VPDN group 1.
2	Router(config- <i>vpdn</i>)# request dialin	Enables the LAC to request L2F or L2TP dial-in requests.
3	Router(config- <i>vpdn-req-in</i>)# protocol [l2f l2tp any]	Specifies which tunneling protocol is to be used.
4	Router(config- <i>vpdn-req-in</i>)# domain <i>domain-name</i> or Router(config- <i>vpdn-req-in</i>)# dnis <i>dnis-number</i>	Specifies the domain name of the users that are to be tunneled. Specifies the DNIS number of users that are to be tunneled.
5	Router(config- <i>vpdn-req-in</i>)# exit Router(config- <i>vpdn</i>)# initiate-to ip <i>ip-address</i> [limit <i>limit-number</i>] [priority <i>priority-number</i>]	Specifies the IP address that the LAC will establish the tunnel with. Optionally, you can configure a maximum number of connections that this VPDN group will support and the priority of this VPDN group.

Configuring a LAC to Accept 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 an LNS to Accept Dial-in

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

Step	Command	Purpose
1	<code>Router(config)# vpdn-group 1</code>	Creates VPDN group 1.
2	<code>Router(config-vpdn)# accept dialin</code>	Enables the LNS to accept dial-in requests.
3	<code>Router(config-vpdn-acc-in)# protocol [l2f l2tp any]</code>	Specifies which tunneling protocol is to be used.
4	<code>Router(config-vpdn-acc-in)# virtual-template</code> <code><i>template-number</i></code>	Specifies the number of the virtual template that will be used to clone the virtual-access interface.
5	<code>Router(config-vpdn-acc-in)# exit</code> <code>Router(config-vpdn)# terminate-from hostname hostname</code>	Accepts tunnels that have this hostname configured as a local name.

Configuring an LNS to Request 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 LNS 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 <i>pool-number</i></code> <code>or</code> <code>dupree(config-vpdn-req-out)# rotary-group <i>group-number</i></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.

Step	Command	Purpose
5	dupree(config-vpdn-req-out)# exit dupree(config-vpdn)# initiate-to ip <i>ip-address</i> [limit <i>limit-number</i>] [priority <i>priority-number</i>]	Specifies the IP address that will be dialed out. Optionally, you can configure a maximum number of connections that this VPDN group will support and the priority of this VPDN group.
6	dupree(config-vpdn)# local name <i>hostname</i>	Specifies that the L2TP tunnel will identify itself with this hostname.

Configuring the Dialer on a LAC for Dialout

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.

Configuring the Dialer on an LNS for Dialout

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

Verifying VPDN Sessions

The following EXEC commands provide useful information for verifying VPDN sessions:

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.

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 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
```

Dial-in Examples

The following is an example of the **show vpdn** command for a successful dialin 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
6      6      lns_l2x0    est   10.40.1.150    1701  1

LocID RemID TunID Intf    Username      State  Last Chg Fastswitch
38     38     6      Se0:0  user0@foo.com est    00:00:05 enabled

% No active L2F tunnels
```

The following is an example of the **show vpdn** command for a successful dialin 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
6      6      lac_l2x0    est   10.30.1.130    1701  1

LocID RemID TunID Intf    Username      State  Last Chg Fastswitch
38     38     6      Vi23   user0@foo.com est    00:03:51 enabled

% No active L2F tunnels
```

Dialout Examples

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 user0@foo.com est    00:00:02 enabled
```

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    user0@foo.com est    00:00:42 enabled

% No active L2F tunnels
```

Show VPDN Session Examples

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
```

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# show 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
```

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# show 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
```

Monitoring and Maintaining VPDN Sessions

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 chap	Displays CHAP packet exchanges.
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.
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.

Dial-in Debug Example on a LAC

The following is an example of debug output from the **debug vpdn event** commands for a successful dial-in session on a LAC:

```
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/C1 8/1 L2TP: Session FS enabled
20:47:35: Tnl/C1 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
```

Dial-in Debug Example on an LNS

The following is an example of debug output from the **debug vpdn event** command for a successful dial-in session on an LNS:

```
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/C1 7/1 L2TP: Session FS enabled
20:19:17: Tnl/C1 7/1 L2TP: Session state change from idle to wait-for-tunnel
20:19:17: Tnl/C1 7/1 L2TP: New session created
20:19:17: Tnl/C1 7/1 L2TP: O ICRP to DJ 8/1
20:19:17: Tnl/C1 7/1 L2TP: Session state change from wait-for-tunnel to wait-connect
20:19:17: Tnl/C1 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

```

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 chap**, **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: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:%LINEPROTO-5-UPDOWN:Line protocol on Interface Virtual-Access1,
changed state to up

```

Configuration Examples

This section provides the following configuration examples:

- LAC Comprehensive Dial-In Configuration
- LNS Comprehensive Dial-in Configuration
- LAC Configured for Both Dial-In and Dialout
- LNS Configured for Both Dial-In and Dialout

LAC Comprehensive Dial-In Configuration

The following example shows a LAC configured to tunnel PPP calls to an LNS using L2TP and local authentication and authorization:

```
aaa new-model
aaa authentication ppp default local
aaa authorization network default local
!
username ISP_NAS password 7 tunnelme
username ENT_HGW password 7 tunnelme
!
vpdn enable
!
vpdn search-order domain dnis
vpdn-group 1
  request dialin
  protocol l2TP
  domain hgw.com
  initiate-to ip 172.22.66.25
  local name ISP_NAS
!
controller T1 0
  framing esf
  clock source line primary
  linecode b8zs
  pri-group timeslots 1-24
!
interface Ethernet0
  ip address 172.22.66.23 255.255.255.192
```

LNS Comprehensive Dial-in Configuration

The following example show an LNS configured to accept L2TP tunnels from a LAC using local authentication and authorization:

```
aaa new-model
aaa authentication ppp default local
aaa authorization network default local
!
username ISP_NAS password 7 tunnelme
username ENT_HGW password 7 tunnelme
!
vpdn enable
!
vpdn-group 1
  accept dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname ISP_NAS
  local name ENT_HGW
!
interface FastEthernet0/0
  ip address 172.22.66.25 255.255.255.192
  no ip directed-broadcast
!
interface Virtual-Template1
  ip unnumbered FastEthernet0/0
  peer default ip address pool default
  ppp authentication chap
!
ip local pool default 172.30.2.1 172.30.2.96
```

LAC Configured for Both Dial-In and Dialout

You can configure a LAC to simultaneously initiate L2TP or L2F dial in tunnels to an LNS, and also accept L2TP dialout tunnels from an LNS.

In the following example, a LAC's VPDN group is configured to dial in using L2F and dial out using L2TP as the tunneling protocol and dialer interface 2. The example only shows the VPDN group and dialer configuration:

```

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
!
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 configure an LNS to simultaneously receive L2TP or L2F dial-in tunnels from a LAC and also initiate L2TP dialout tunnels to a LAC.

In the following example, a LNS's VPDN group is configured to dial in using virtual template 1 to clone the virtual-access interface and dial out using dialer pool 1. The example only shows the VPDN group and dialer configuration:

```

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
!
interface Dialer2
  ip address 172.1.1.2.3 255.255.128
  encapsulation ppp
  dialer remote-name reuben
  dialer string 5551234
  dialer vpdn
  dialer pool 1
  dialer-group 1
  ppp authentication chap

```

Command Reference

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

- **accept dialin**
- **accept dialout**
- **authen before-forward**
- **default**
- **dialer**
- **dialer aaa**
- **dialer vpdn**
- **dnis**
- **domain**
- **force-local-chap**
- **initiate-to**
- **lcp renegotiation**
- **local name**
- **multilink**
- **pool-member**
- **protocol**
- **request dialin**
- **request dialout**
- **rotary-group**
- **source-ip**
- **terminate-from**
- **virtual-template**

accept dialin

To configure an LNS to accept tunneled PPP connections from a LAC and create an accept-dialin VPDN subgroup, use the **accept dialin** VPDN group command. To remove the accept-dialin subgroup from a VPDN group, use the **no** form of this command.

accept dialin

no accept dialin

Syntax Description

This command has no keywords nor arguments.

Defaults

Disabled

Command Modes

VPDN group mode

Command History

Release	Modification
11.3(5)AA and 12.0(1)T	This command was introduced.
12.0(5)T	All keywords and arguments were removed and made into separate accept-dialin subgroup commands.

Usage Guidelines

For a VPDN group to accept dialin calls, you must also configure the:

- **terminate-from** VPDN group command
- **protocol** VPDN subgroup command
- **virtual-template** accept-dialin command

Once an L2F or L2TP tunnel is established, both dial-in and dial-out calls can use the same tunnel.

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.

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 enables the LNS to accept an L2TP tunnel from a LAC named mugsy. A virtual-access interface will be cloned from virtual-template 1:

```
vpdn-group 1
  accept dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname mugsy
```

If you do not use the **terminate-from** command, you automatically enable a default VPDN group, which allows all tunnels to share the same tunnel attributes:

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

Related Commands

Command	Description
force-local-chap	Forces the LNS to re-authenticate the client.
lcp renegotiation	Allows the LNS to re-negotiate the LCP on dialin calls.
protocol	Specifies the tunneling protocol that is used for the dialin connections.
request dialin	Enables a LAC to request either L2F or L2TP tunnels for dial-in.
terminate-from	Specifies the hostname the LAC uses when requesting a tunnel.
virtual-template	Specifies the virtual-template used to clone virtual-access interfaces.

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.

authen before-forward

To specify that VPDN send the entire structured username to the AAA server the first time the router contacts the AAA server, use the **authen before-forward** command in VPDN group configuration mode. Use the **no** form of this command to send just the domain name or DNIS.

authen before-forward

no authen before-forward

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

VPDN group configuration mode

Command History

Release	Modification
11.3(9) AA	This command was introduced.
12.0(5)T	This command was modified to only be available if the request-dialin VPDN subgroup is enabled.

Usage Guidelines

You must enable the **request-dialin** command on the VPDN group before you can use the **authen before-forward** command. Removing the **request-dialin** command will remove the **authen before-forward** command from the VPDN group.

Examples

The following example creates a VPDN group that send the entire username to the AAA server when a user dials in with a username that has the domain name philzone.com:

```

vpdn-group 1
 request dialin
  protocol l2f
  domain philzone.com
 initiate-to ip 10.0.0.1
 local name unbrokenchain
 authen before-forward

```

Related Commands

Command	Description
request dialin	Enables a router to request either L2F or L2TP tunnels for dial-in.
multilink	Limits sessions authorized for all multilink users.

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 LNSs 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.

dnis

To request that a LAC tunnel calls from a specific DNIS, use the **dnis** request-dialin command. To remove a DNIS from a request-dialin VPDN subgroup, use the **no** form of this command

dnis *dnis-number*

no dnis

Syntax Description

dnis-number Dialed number used for authorizing a specific tunnel that forwards traffic to the LNS.

Defaults

Disabled

Command Modes

Request-dialin mode

Command History

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

Usage Guidelines

You must first enable a tunneling protocol on the request-dialin VPDN subgroup (using the **protocol** command) before you can enable the **dnis** command. Removing the **protocol** command or configuring a different protocol removes all **dnis** commands from the request-dialin subgroup.

You can configure a request-dialin VPDN subgroup to tunnel calls from multiple DNIS numbers and domain names.

Examples

The following example configures VPDN group 1 to request dial-in to IP address 10.99.67.76 when it receives a PPP call from DNIS 8675309 and 8005556543.

```
vpdn-group 1
 request-dialin
  protocol l2tp
  dnis 8675309
  dnis 8005556543
 initiate-to ip 10.99.67.76
```

Related Commands

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

domain

To request that PPP calls from a specific domain name be tunneled, use the **domain** request-dialin command. To remove a domain from a request-dialin VPDN subgroup, use the **no** form of this command

domain *domain-name*

no domain

Syntax Description

domain-name Case-sensitive name of the domain that will be tunneled.

Defaults

Disabled

Command Modes

Request-dialin mode

Command History

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

Usage Guidelines

You must first enable a tunneling protocol on the request-dialin VPDN subgroup (using the **protocol** command) before you can enable the **domain** command. Removing the **protocol** command or configuring a different protocol removes the **domain** command from the request-dialin subgroup.

You can configure a request-dialin VPDN subgroup to tunnel calls from multiple DNIS numbers and domain names.

Examples

The following example configures VPDN group 1 to request dial-in to IP address 10.99.67.76 when it receives a PPP call from a username with the domain name jgb.com or ratdog.com.

```
vpdn-group 1
 request-dialin
 protocol l2tp
 domain jgb.com
 domain ratdog.com
 initiate-to ip 10.99.67.76
```

Related Commands

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

force-local-chap

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

force-local-chap

no force-local-chap

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

VPDN group mode

Command History

Release	Modification
11.3(5)AA and 12.0(1)T	This command was introduced.
12.0(5)T	This command was modified to only be available if the accept-dialin VPDN subgroup is enabled.

Usage Guidelines

You must enable the **accept-dialin** command on the VPDN group before you can use the **force-local-chap** command. Removing the **accept-dialin** command will remove the **force-local-chap** command from the VPDN group.

This command is only used if CHAP authentication is enabled for PPP (using the **ppp authentication chap** command). This command forces the LNS to re-authenticate 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 authentication** command is enabled.

Examples

The following example enables CHAP authentication at the LNS:

```
vpdn-group 1
  accept dialin
  protocol l2tp
  virtual-template 1
  terminate-from pat
  force-local-chap on-mismatch
```

Related Commands

Command	Description
accept dialin	Enables an LNS to accept either L2F or L2TP dial-in calls.
lcp renegotiation	Allows the LNS to renegotiate the LCP on dial-in 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* [**limit** *limit-number*] [**priority** *priority-number*]

no initiate-to ip *ip-address*

Syntax Description

ip <i>ip-address</i>	The IP address of the router that will be tunneled to.
limit <i>limit-number</i>	(Optional) The maximum number of connections that can be made to this IP address.
priority <i>priority-number</i>	(Optional) The priority for this IP address (1 is the highest).

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. This group can tunnel a maximum of five simultaneous users and it has the second highest priority for requesting dialout calls.

```
vpdn-group 1
 request dialout
  protocol l2tp
  pool-member 1
  imitate-to ip 10.3.2.1 limit 5 priority 2
```

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.

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 { **always** | **on-mismatch** }

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.

Defaults

LCP renegotiation is disabled on the LNS.

Command Modes

VPDN group mode

Command History

Release	Modification
11.3(5)AA and 12.0(1)T	This command was introduced.
12.0(5)T	This command was modified to only be available if the accept-dialin VPDN subgroup is enabled.

Usage Guidelines

You must enable the **accept-dialin** command on the VPDN group before you can use the **lcp renegotiation** command. Removing the **accept-dialin** command will remove the **lcp renegotiation** command from the VPDN group.

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.

Examples

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

```
vpdn-group 1
  accept dialin
  protocol l2tp
  virtual-template 1
  terminate-from pat
  lcp renegotiation on-mismatch
```

Related Commands

Command	Description
accept dialin	Enables an LNS to accept either L2F or L2TP dial-in calls.
force-local-chap	Forces the LNS to re-authenticate the client.

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.

multilink

To limit sessions authorized for all multilink users, enter the **multilink** VPDN group configuration command. To remove this function, use the **no** form of this command.

```
multilink {bundle number | link number}
no multilink {bundle number | link number}
```

Syntax Description

bundle number	Configures the number of bundles supported for a VPDN group. In general, each user requires one bundle. The limit has a range from 0 to 32,767.
link number	Configures the number of links or sessions supported for each bundle. The limit has a range from 0 to 32,767.

Defaults

No limit is set.

Command Modes

VPDN group configuration

Command History

Release	Modification
12.0(4)XI	This command was introduced.
12.0(5)T	This command was modified to only be available if the request-dialin VPDN subgroup is enabled.

Usage Guidelines

You must enable the **request-dialin** command on the VPDN group before you can use the **multilink** command. Removing the **request-dialin** command will remove the **multilink** command from the VPDN group.

Use the **multilink** VPDN group configuration command to limit sessions authorized for all multilink users. Each user requires one bundle—regardless if the user is a remote modem client or ISDN client.

One modem client using one B channel requires one link. One ISDN BRI node may require up to two links for one BRI line connection. The second B channel of a ISDN BRI node comes up when the maximum threshold is exceeded.

Examples

The following example creates one VPDN group called `joe_eastcoast`. One L2TP tunnel is set up to the home gateway router at IP address 10.2.2.2. Ten MLPPP bundles can be authorized for ten users. Each user dials into the domain called `bostonjoe.com`. Each bundle can be authorized to support a maximum of 5 links. This means that all 10 users can consume a maximum of 50 simultaneous sessions dialing into `bostonjoe.com`.

```
vpdn-group 1
  request dialin
  protocol l2tp
  domain bostonjoe.com
  initiate-to ip 10.2.2.2
  multilink bundle 10
  multilink link 5
```

Related Commands

Command	Description
<code>request dialin</code>	Enables a router to request either L2F or L2TP tunnels for dial-in.

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 dialin

To configure a LAC to request L2F or L2TP tunnels to an LNS and create a request-dialin VPDN subgroup, use the **request dialin** VPDN group command. To remove the request-dialin subgroup from a VPDN group, use the **no** form of this command.

request dialin
no request dialin

Syntax Description

This command has no keywords nor arguments.

Defaults

Disabled

Command Modes

VPDN group mode

Command History

Release	Modification
11.3(5)AA and 12.0(5)T	This command was introduced.
12.0(5)T	All keywords and arguments were removed and made into separate accept-dialin subgroup commands.

Usage Guidelines

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

- **initiate-to** VPDN group command
- **protocol** VPDN subgroup command
- At least one **dnis** or **domain** request-dialin command

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

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 dialin tunnel to a remote peer at IP address 172.17.33.125 for a user in the domain named partner.com:

```
vpdn-group 1
  request dialin
  protocol l2tp
  domain partner.com
  initiate-to ip 172.17.33.125
```

Related Commands

Command	Description
accept dialin	Accepts requests to create either L2F or L2TP tunnels for dial-in.
authen before-forward	Forces the LNS to re-authenticate the client.
dnis	Enables a request-dialin group to tunnel calls from a specific DNIS.
domain	Enables a request-dialin group to tunnel calls from a specific username.
initiate-to	Specifies the IP address that calls are tunneled to.
multilink	Limits sessions authorized for all multilink users.
protocol	Specifies the tunneling protocol that is used for the dial-in connections.

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

ip-address 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.

virtual-template

To specify which virtual template will be used to clone virtual-access interfaces, use the **virtual-template** accept-dialin command. To remove the virtual template from an accept-dialin VPDN subgroup, use the **no** form of this command.

virtual-template *template-number*

no virtual-template

Syntax Description

template-number Number of the virtual template that will be used to clone virtual-access interfaces.

Defaults

Disabled

Command Modes

Accept-dialin mode

Command History

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

Usage Guidelines

Each accept-dialin group can only clone virtual-access interfaces using one virtual template. If you enter a second **virtual-template** command on an accept-dialin subgroup, it will replace the first **virtual-template** command.

You must first enable a tunneling protocol on the accept-dialin VPDN subgroup (using the **protocol** command) before you can enable the **virtual-template** command. Removing or modifying the **protocol** command will remove **virtual-template** command from the request-dialin subgroup.

Examples

The following example enables the LNS to accept an L2TP tunnel from a LAC named mugsy. A virtual-access interface will be cloned from virtual template 1:

```
vpdn-group 1
  accept dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname mugsy
```

Related Commands

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

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.

