L2TP Large-Scale Dial-Out

Feature History

Release	Modification
12.2(4)T	This feature was introduced.
12.2(11)T	This feature was implemented on Cisco access server platforms.

This document describes the L2TP Large-Scale Dial-Out feature. It includes the following sections:

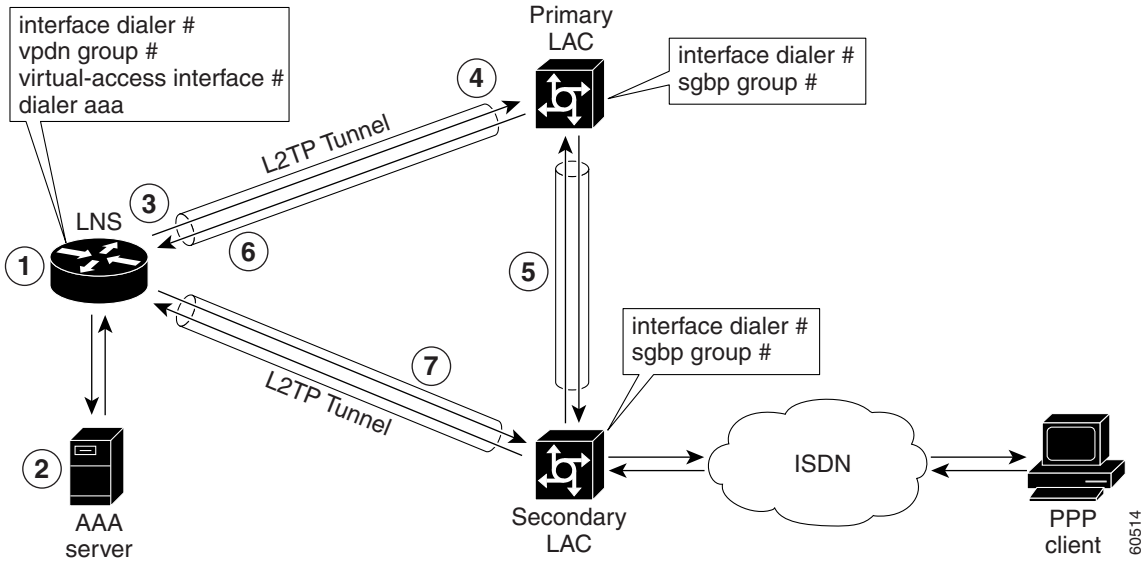
Feature Overview

The Asynchronous Line Monitoring feature feature enables the router to dial multiple Layer 2 Tunnel Protocol (L2TP) access concentrators (LACs) from a single L2TP network server (LNS). The LACs are signaled through the LNS and use L2TP to establish the dial sessions. User-defined profiles can be configured on an authentication, authorization, and accounting (AAA) server and retrieved by the LNS when dial-out occurs.The Asynchronous Line Monitoring feature feature also supports multiple LACs bound into one stack group, call traffic load balancing, and outbound call congestion management.

Figure 1 provides an example of L2TP large-scale dial-out session startup. Each part of the process is numbered and described in text following the figure.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Figure 1 Sample Scenario L2TP Large-Scale Dial-Out Session



1. The IP packets arrive at the LNS and are forwarded to the dialer interface by the routing protocol. (A virtual access interface has not been created yet.)
2. A dialer session is created and placed in a pending state while the dialer interface sends a Dial Out Request message to the AAA server requesting the user profile. The AAA server sends the user profile, and the LNS builds a dynamic map based on the reply.
3. The dialer interface looks for its dial resources and finds the virtual private dialup network (VPDN) group. The dialer interface then issues a dial call request to the VPDN group, which creates a virtual access interface. The virtual access interface becomes a member of a rotary group.
4. If there is no existing L2TP tunnel between the LNS and the primary LAC, the LNS would establish one; otherwise, it uses the existing tunnel. The LNS sends an Outgoing Call ReQuest (OCRQ) message, inside of which is the dynamic dialer map, to the primary LAC.
5. Upon receiving the OCRQ message, the primary LAC determines whether it is congested. If the primary LAC is congested, it sends a Stack Group Bidding Protocol (SGBP) Discover message through a new tunnel to the secondary LAC in the scenario depicted in Figure 1, but it could send the message to any other LAC configured in the SGBP stack group.

   After the secondary LAC receives the SGBP Discover message from the LNS, it responds with an SGBP Offer message describing available resources.
6. If neither LAC has resources to dial out, the primary LAC would send a Call Disconnect Notification (CDN) message to the LNS. The LNS would then tear down the tunnel.

   If the secondary LAC has more resources, the primary LAC can choose to dial through the secondary LAC. The primary LAC sends a CDN message to the LNS with error code 7, which means “Try another” as defined in RFC 2661. Inside this message, the LNS learns that its dial-out request should be redirected to the secondary LAC, and the LNS clears the session to the primary LAC.
7. The LNS creates a new tunnel to the secondary LAC if one does not exist. The dial-out LAC creates a VPDN session and sets it in a pending state. It then places a call to the PPP client. Once the call is connected, the LAC determines to which pending VPDN session the connected interface belongs and binds the connected interface with the session. The secondary LAC sends an Outgoing Call

Connected (OCCN) message to the LNS. The LNS determines for which pending virtual access interface and VPDN session this OCCN is meant, and then the LNS brings up the virtual access interface.

Benefits

Large-Scale Dial-Out Integrated with L2TP

Before Cisco IOS Release 12.2(4)T, L2TP required that requests for tunneled dial-out calls be from a single LNS to a single LAC, and that configurations be available on the local server. The Asynchronous Line Monitoring feature feature introduced in Cisco IOS Release 12.2(4)T allows dialing multiple LACs from a single LNS. The LACs are signaled through the LNS using L2TP to establish the dial sessions. User-defined profiles can also be configured on a AAA server and retrieved by the LNS when dial-out occurs.

Enhanced Dial Management

The Asynchronous Line Monitoring feature feature also provides the following benefits:

- Multiple LACs bound into one stack group
- Call traffic load balancing
- Outbound call congestion management

Related Features and Technologies

L2TP, VPDNs, and large-scale dial-out are described in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2. Refer to the chapter "Configuring Virtual Private Networks" in the part "Virtual Templates, Profiles, and Networks," and the chapter "Configuring Large-Scale Dial-Out" in the part "Dial Access Specialized Features."

Supported Platforms

See the next section for information about Feature Navigator and how to use this tool to determine the platforms and software images in which this feature is available.

Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. As of May 2001, Feature Navigator supports M, T, E, S, and ST releases. You can access Feature Navigator at the following URL:

http://www.cisco.com/go/fn

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

- RFC 2661, *Layer Two Tunneling Protocol (L2TP)*

Configuration Tasks

See the following sections for configuration tasks for the Asynchronous Line Monitoring feature feature. Each task in the list is identified as either required or optional:

- Configuring the LNS to Request Dial-Out (required)
- Configuring a LAC to Accept Dial-Out (required)

Configuring the LNS to Request Dial-Out

Virtual profiles depend on PPP authentication; therefore the LNS must authenticate the connection to use virtual profiles.

You must configure AAA network security services on the LNS. For more information about AAA, refer to the chapter “AAA Overview” in the *Cisco IOS Security Configuration Guide*, Release 12.2. The *Cisco IOS Security Command Reference*, Release 12.2, describes the commands to configure AAA.

You also need to configure your LNS to communicate with the applicable security server, either a TACACS+ or RADIUS daemon.

If you are using RADIUS and Ascend attributes, use the **radius-server host non-standard** global configuration command to enable your Cisco router, acting as a network access server, to recognize that the RADIUS security server is using a vendor-proprietary version of RADIUS. Use the **radius-server key** global configuration command to specify the shared secret text string used between your Cisco router and the RADIUS server. For more information, refer to the chapter “Configuring RADIUS” in the *Cisco IOS Security Configuration Guide*, Release 12.2.

If you are using TACACS+, use the **tacacs-server host** global configuration command to specify the IP address of one or more TACACS+ daemons. Use the **tacacs-server key** global configuration command to specify the shared secret text string used between your Cisco router and the TACACS+ daemon. For more information, see the *Cisco IOS Security Configuration Guide*, Release 12.2.

To configure the LNS to request dial-out tunneled PPP connections from a LAC, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Device(config)# vpdn enable`	Enables VPDN and directs the router to look for tunnel definitions on a remote authorization server.
Step 2	`Device(config)# vpdn group 1`	Creates VPDN group 1 and enters VPDN group configuration mode.
Step 3	`Device(config-vpdn)# request-dialout`	Enters VPDN request-dialout group configuration mode and enables the tunnel server to send L2TP dial-out requests.
Step 4	`Device(config-vpdn-req-ou)# protocol l2tp`	Specifies L2TP as the tunneling protocol. **Note** L2TP is the only protocol that supports dial-out.
Step 5	`Device(config-vpdn-req-ou)# rotary-group` *group-number*	Specifies the dialer rotary group that will be used to dial out. **Note** You can configure only one dialer rotary group. Attempting to configure a second dialer resource will remove the first from the configuration.
Step 6	`Device(config-vpdn-req-ou)# virtual-template` *template-number*	Specifies the number of the virtual template that will be used to clone the virtual access interface.
Step 7	`Device(config-vpdn-req-ou)# exit`	Returns to VPDN group configuration mode.
Step 8	`Device(config-vpdn)# initiate-to ip` *ip-address*	Specifies the IP address that will be dialed out. This is the IP address of the LAC. **Note** The **limit** and **priority** keywords are not available for VPDN dial-out.
Step 9	`Device(config-vpdn)# local name` *hostname*	Specifies that the L2TP tunnel will identify itself with this host name.
Step 10	`Device(config-vpdn)# exit`	Returns to global configuration mode.
Step 11	`Device(config)# virtual-template` *template-number*	Specifies the number of the virtual template that will be used to clone the virtual access interface. Enters interface configuration mode so that you can set the configuration parameters that you want applied to virtual access interfaces.
Step 12	`Device(config-if)# interface virtual-template` *number*	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

	Command	Purpose
Step 13	`Device(config-if)# no ip directed-broadcast`	Disables the translation of a directed broadcast to physical broadcasts.
Step 14	`Device(config-if)# encapsulation ppp`	Sets the PPP encapsulation method on the interface.
Step 15	`Device(config-if)# ppp multilink`	Enables Multilink PPP (MLP) on an interface.
Step 16	`Device(config-if)# exit`	Returns to global configuration mode.
Step 17	`Device(config)# aaa new-model`	Enables AAA access control .
Step 18	`Device(config)# aaa authentication` *arguments*	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP. Refer to the Cisco IOS security guides for specific authentication arguments for your network security configuration.
Step 19	`Device(config)# aaa authorization` *arguments*	Sets parameters that restrict user access to a network. Refer to the Cisco IOS security guides for specific authentication arguments for your network security configuration.
Step 20	`Device(config)# interface dialer 1`	Enters interface configuration mode for dialer interface 1.
Step 21	`Device(config-if)# dialer in-band`	Specifies that DDR is to be supported.
Step 22	`Device(config-if)# dialer vpdn`	Enables a dialer profile to use L2TP dial-out.
Step 23	`Device(config-if)# dialer aaa` [**suffix** *suffix* **password** *password*]	Allows a dialer to access the AAA server for dialing information or, optionally, specifies a suffix and nondefault password for authentication.
Step 24	`Device(config-if)# no ip directed-broadcast`	Disables the translation of a directed broadcast to physical broadcasts.
Step 25	`Device(config-if)# dialer-group` *group-number*	Controls access by configuring an interface to belong to a specific dialing group.
Step 26	`Device(config-if)# dialer-list` *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}	Defines a DDR dialer list to control dialing by protocol or by a combination of a protocol and a previously defined access list.
Step 27	`Device(config-if)# encapsulation ppp`	Sets the PPP encapsulation method on the dialer interface.
Step 28	`Device(config-if)# ppp multilink`	Enables MLP on an interface.

The MLP feature provides load-balancing functionality over multiple WAN links and offers load calculation on both inbound and outbound traffic. Refer to the part “PPP Configuration” and the chapter “Configuring Media-Independent PPP and Multilink PPP” in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2, for more information.

See the configuration examples later in this document for additional commands that may be configured on the LAC.

Configuring a LAC to Accept Dial-Out

You must configure SGBP to allow a primary LAC that is congested or otherwise unable to dial out to select an alternate LAC to dial out. Configure SGBP using the **sgbp group** and **sgbp member** global configuration commands before enabling the stack group to bid for dial-out connection. Configuring SGBP is described in the chapter "Configuring Multichassis Multilink PPP" in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2. The *Cisco IOS Dial Technologies Command Reference*, Release 12.2, describes the commands to configure a stack group.

Additionally, the information about configuring network security in the section "Configuring the LNS to Request Dial-Out" of this document also applies to configuring the LAC.

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

	Command	Purpose
Step 1	`Device(config)# vpdn enable`	Enables VPDN and directs the router to look for tunnel definitions on a remote authorization server.
Step 2	`Device(config)# vpdn group 1`	Creates VPDN group 1 and enters VPDN group configuration mode.
Step 3	`Device(config-vpdn)# accept-dialout`	Enters VPDN accept-dialout group configuration mode and enables the NAS to accept L2TP dial-out requests.
Step 4	`Device(config-vpdn-acc-ou)# protocol l2tp`	Specifies L2TP as the tunneling protocol. **Note** L2TP is the only protocol that supports dial-out.
Step 5	`Device(config-vpdn-acc-ou)# dialer` *dialer-interface*	Specifies the dialer that is used to dial out to the client.
Step 6	`Device(config-vpdn-acc-ou)# exit`	Returns to VPDN group configuration mode.
Step 7	`Device(config-vpdn)# initiate-to ip` *ip-address* `[limit` *limit-number*`] [priority` *priority-number*`]`	Specifies the IP address that will be tunneled to.
Step 8	`Device(config-vpdn)# local name` *hostname*	Specifies that the L2TP tunnel will identify itself with this host name.
Step 9	`Device(config-vpdn)# exit`	Returns to global configuration mode.
Step 10	`Device(config)# aaa new-model`	Enables the AAA access control model.
Step 11	`Device(config)# aaa authentication` *arguments*	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP. Refer to the Cisco IOS security guides for specific authentication arguments for your network security configuration.
Step 12	`Device(config)# aaa authorization` *arguments*	Sets parameters that restrict user access to a network. Refer to the Cisco IOS security guides for specific authorization arguments for your network security configuration.
Step 13	`Device(config)# username` *name* `password` *password*	Creates authentication credentials for the stack group.
Step 14	`Device(config)# sgbp group` *name*	Creates the stack group and assigns this router to it.

	Command	Purpose
Step 15	`Device(config)# sgbp member peer-name [peer-ip-address]`	Specifies a peer member of the stack group.
Step 16	`Device(config)# interface dialer 1`	Enters interface configuration mode for dialer interface 1.
Step 17	`Device(config-if)# dialer aaa`	Allows a dialer to access the AAA server for dialing information.
Step 18	`Device(config-if)# dialer in-band`	Specifies that DDR is to be supported.
Step 19	`Device(config-if)# no ip directed-broadcast`	Disables the translation of a directed broadcast to physical broadcasts.
Step 20	`Device(config-if)# encapsulation ppp`	Sets the PPP encapsulation method on the dialer interface.
Step 21	`Device(config-if)# ppp multilink`	Enables MLP on an interface.

See the configuration examples later in this document for additional commands that may be configured on the LAC.

Verifying L2TP Large-Scale Dial-Out

To verify that L2TP large-scale dial-out is configured correctly, perform the following steps:

Note Effective with Cisco Release 12.4(11)T, the **L2F protocol** was removed in Cisco IOS software.

Step 1 From the LNS, display tunnel statistics by entering the **show vpdn** and the **show vpdn tunnel all** EXEC commands:

```
Device# show vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions
55788 55043 rdt5300-15    est    10.23.1.1        1701  1
LocID RemID TunID Intf          Username              State  Last Chg
Fastswitch
83    50    55788 Vi1           rdt7204-1             est    00:01:08
enabled

%No active L2F tunnels

%No active PPTP tunnels

%No active PPPoE tunnels


Device# show vpdn tunnel all

L2TP Tunnel Information Total tunnels 1 sessions 1

Tunnel id 8873 is up, remote id is 41736, 1 active sessions
  Tunnel state is established, time since change 00:00:05
  Remote tunnel name is rdt5300-15
    Internet Address 10.23.1.1, port 1701
  Local tunnel name is rdt7206vxr-8
    Internet Address 10.23.1.100, port 1701
```

```
  11 packets sent, 12 received
  653 bytes sent, 666 received
  Control Ns 3, Nr 3
  Local RWS 10000 (default), Remote RWS 800
  Tunnel PMTU checking disabled
  Retransmission time 1, max 1 seconds
  Unsent queuesize 0, max 0
  Resend queuesize 0, max 2
  Total resends 0, ZLB ACKs sent 2
  Current nosession queue check 0 of 5
  Retransmit time distribution: 0 2 0 0 0 0 0 0 0 0
  Sessions disconnected due to lack of resources 0

%No active L2F tunnels

%No active PPTP tunnels

%No active PPPoE tunnels
```

Step 2 From the LNS, enter the **show interfaces virtual-access** EXEC command to verify that the interface is up and that no errors are reported:

```
Device# show interfaces virtual-access  1

Virtual-Access1 is up, line protocol is up
  Hardware is Virtual Access interface
  MTU 1500 bytes, BW 64 Kbit, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 5 seconds on reset
  Time to interface disconnect:  idle 00:01:16
  Interface is bound to Di1 (Encapsulation PPP)
  LCP Open, multilink Open
  Open: IPCP, CDPCP
  Last input 00:00:07, output never, output hang never
  Last clearing of "show interface" counters 00:01:33
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/16 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 48 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     9 packets input, 767 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
     10 packets output, 849 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Step 3 From the LNS, display information for MLP bundles by entering the **show ppp multilink** EXEC command:

```
Device# show ppp multilink

Virtual-Access3, bundle name is rdt7204-1
  Bundle up for 00:01:19
  Using relaxed lost fragment detection algorithm.
  Dialer interface is Dialer1
  0 lost fragments, 0 reordered, 0 unassigned
  0 discarded, 0 lost received, 1/255 load
  0x8 received sequence, 0x8 sent sequence
```

```
  Member links: 4 (max not set, min not set)
    rdt5300-15:Virtual-Access1  (10.23.1.1), since 00:01:19, last rcvd seq
000006, unsequenced
    rdt5300-15:Virtual-Access5  (10.23.1.1), since 00:01:18, last rcvd seq
000007, unsequenced
    rdt5300-15:Virtual-Access4  (10.23.1.1), since 00:00:48, no frags rcvd,
unsequenced
    rdt5300-15:Virtual-Access6  (10.23.1.1), since 00:00:18, no frags rcvd,
unsequenced
```

Step 4 From the LAC, display active tunnel statistics by entering the **show vpdn** and **show vpdn tunnel all** EXEC commands:

```
Device# show vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID RemID Remote Name   State  Remote Address  Port  Sessions
51111 46115 rdt7206vxr-8  est    10.23.1.100      1701  1

LocID RemID TunID Intf          Username               State  Last Chg
Fastswitch
2     86    51111 Se0:22        rdt7204-1              est    00:00:05
enabled

%No active L2F tunnels

%No active PPTP tunnels

%No active PPPoE tunnels


Device# show vpdn tunnel all

L2TP Tunnel Information Total tunnels 1 sessions 1

Tunnel id 51111 is up, remote id is 46115, 1 active sessions
  Tunnel state is established, time since change 00:00:18
  Remote tunnel name is rdt7206vxr-8
    Internet Address 10.23.1.100, port 1701
  Local tunnel name is rdt5300-15
    Internet Address 10.23.1.1, port 1701
  13 packets sent, 12 received
  1156 bytes sent, 677 received
  Control Ns 3, Nr 3
  Local RWS 800 (default), Remote RWS 800 (max)
  Tunnel PMTU checking disabled
  Retransmission time 1, max 1 seconds
  Unsent queuesize 0, max 0
  Resend queuesize 0, max 1
  Total resends 1, ZLB ACKs sent 2
  Current nosession queue check 0 of 5
  Retransmit time distribution: 0 3 1 0 0 0 0 0 0
  Sessions disconnected due to lack of resources 0

%No active L2F tunnels

%No active PPTP tunnels

%No active PPPoE tunnels
```

Step 5 From the LAC, confirm active SGBP group members by entering the **show sgbp** EXEC command:

```
Device# show sgbp
```

```
Group Name: bri_pri Ref: 0x7B920584
Seed bid: default, 50, default seed bid setting

  Member Name: rdt3640-17 State: active Id: 2
  Ref: 0x73069C41
  Address: 10.23.1.2
```

Step 6 From the LAC, display connection status by entering the **show isdn status** EXEC command or the **show user** EXEC command:

```
Device# show isdn status

Global ISDN Switchtype = primary-5ess
ISDN Serial0:23 interface
        dsl 0, interface ISDN Switchtype = primary-5ess
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        2 Active Layer 3 Call(s)
        CCB:callid=8008, sapi=0, ces=0, B-chan=23, calltype=DATA
        CCB:callid=8009, sapi=0, ces=0, B-chan=22, calltype=DATA
    Active dsl 0 CCBs = 2
    The Free Channel Mask:  0x801FFFFF
    Number of L2 Discards = 0, L2 Session ID = 0
    Total Allocated ISDN CCBs = 2


Device# show user

    Line       User       Host(s)              Idle       Location
*  0 con 0                idle                 00:00:00

  Interface      User        Mode                    Idle     Peer
Address
  Se0:20                 Sync PPP                  -
  Se0:21                 Sync PPP                  -
  Se0:22                 Sync PPP                  -
```

Monitoring and Maintaining L2TP Large-Scale Dial-Out

To monitor and maintain L2TP large-scale dial-out, use the following EXEC commands:

Command	Purpose
`Device> clear dialer sessions`	Removes all dialer sessions and disconnects links.
`Device# clear vpdn tunnel l2tp` *network-access-server gateway-name*	Shuts down a specific tunnel and all the sessions within the tunnel.
`Device> show dialer sessions`	Displays all dialer sessions.

Command	Purpose
`Device# show interfaces virtual access number`	Displays information about the virtual access interface, LCP, protocol states, and interface statistics. The status of the virtual access interface should be: `Virtual-Accessn is up, line protocol is up`
`Device> show ip route [static [download]]`	Displays all static IP routes or those installed using the AAA route download function.
`Device> show ppp multilink`	Displays MLP and Multichassis Multilink PPP (MMP) bundle information.
`Device# show vpdn`	Displays a summary of all active VPDN tunnels.
`Device# show vpdn group [name | name domain | name endpoint]`	Displays a summary of the relationships among VPDN groups and customer or VPDN profiles. **Note** When you include the name of the VPDN group, the output displays information on domain or DNIS, tunnel endpoint, session limits, group priority, active sessions, group status, and reserved sessions.
`Device# show vpdn history failure`	Displays information about VPDN user failures.
`Device# show vpdn multilink`	Displays VPDN multilink information.
`Device# show vpdn session [all | packets | sequence | state | timers | window] [interface | tunnel | username]`	Displays VPDN session information including interface, tunnel, username, packets, status, and window statistics.
`Device# show vpdn tunnel [all | packets | state | summary | transport] [id | local-name | remote-name]`	Displays VPDN tunnel information including tunnel protocol, ID, local and remote tunnel names, packets sent and received, tunnel, and transport status.

Configuration Examples

This section provides the following configuration examples:

- LNS Configured to Request Dial-Out Example
- LAC Configured to Accept Dial-Out Example

LNS Configured to Request Dial-Out Example

In the following example, the LNS VPDN group is configured to make a dial-out request using L2TP:

```
vpdn enable
!
vpdn group 2
 request-dialout
  protocol l2tp
  rotary-group 1
 local name group1
 initiate-to ip 10.3.2.1 limit 5 priority 2
!
interface virtual-template 1
 no ip directed-broadcast
 encapsulation ppp
 ppp multilink
```

```
!
interface Dialer 1
 no ip directed-broadcast
 dialer in-band
 dialer vpdn
 dialer aaa
 dialer-group 1
 access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
 dialer-list 1 protocol ip list 101
 encapsulation ppp
 ppp multilink
 no fair-queue
 ppp authentication chap
```

LAC Configured to Accept Dial-Out Example

In the following example, the VPDN group of a LAC is configured to accept dial-outs using L2TP as the tunneling protocol and dialer interface 2:

```
vpdn enable
!
vpdn group 1
 accept-dialout
  protocol l2tp
  dialer 2
 local name group2
 terminate-from hostname host2
!
aaa new-model
aaa authentication ppp default radius local
aaa authorization network default radius none
aaa authorization configuration default radius
aaa route download 720
enable password 7 1236173C1B0F
!
username LAC1 password 7 030752180500
!
sgbp group dialbid
sgbp seed-bid offload
sgbp member LAC2 172.21.17.17
sgbp dial-bids
isdn switch-type basic-5ess
!
interface dialer 2
 ip address 172.19.2.3 255.255.128
 encapsulation ppp
 dialer remote-name group1
 dialer string 5551234
 dialer aaa

 dialer pool 1
 dialer-group 1
 ppp authentication chap
.
.
.
end
```

Command Reference

This feature uses no new or modified commands. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List*.

- **xremote**
