

Configuring Virtual Private Dialup Networks

Virtual private dialup networks allow separate and autonomous protocol domains to share common access infrastructure including modems, access servers, and ISDN routers. VPDN uses the Layer 2 Forwarding protocol (L2F) which permits the tunneling of link level frames.

Using L2F tunneling, an Internet Service Provider (ISP) or other access service can create a virtual tunnel to link a customer's remote sites or remote users with corporate home networks. In particular, a network access server at the ISP's point of presence (POP) exchanges PPP messages with the remote users, and communicates by L2F requests and responses with the customer's home gateway to set up tunnels.

L2F passes protocol-level packets through the virtual tunnel between endpoints of a point-to-point connection.

Frames from the remote users are accepted by the ISP's POP, stripped of any linked framing or transparency bytes, encapsulated in L2F, and forwarded over the appropriate tunnel. The customer's home gateway accepts these L2F frames, strips the L2F encapsulation, and processes the incoming frames for the appropriate interface.

Note This implementation of VPDN supports PPP dialup only.

Cisco routers fast switch Layer 2 Forwarding traffic. In stack group environments in which some L2F traffic is offloaded to a powerful router, fast switching provides improved scalability.

For a complete description of the commands mentioned in this chapter, refer to the *Dial Solutions Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

How VPDN Works

Virtual private dialup networking enables users to configure secure networks that take advantage of Internet Service Providers that tunnel the company's remote access traffic through the ISP cloud.

Remote offices or mobile users can connect to their home network using local dialup services of third parties. The dialup service provider agrees to forward the company's traffic from the ISP POP to a company-run home gateway. Network configuration and security remains in the control of the client. The dialup service provider provides a virtual pipe between the company's sites.

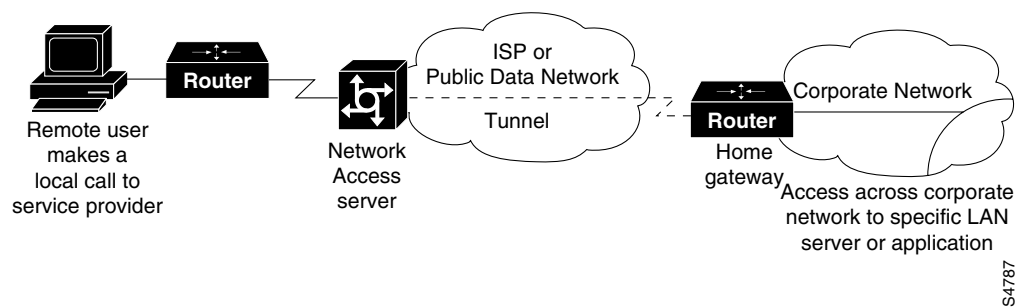
Note The MMP feature uses L2F to connect multiple PPP sessions for which individual dial-in calls have arrived on different stack group members. L2F provides speed and reliability for the setup and shutdown of Multilink PPP.

A VPDN connection between a remote user and the home LAN is accomplished in the following steps:

- 1 The remote user initiates a PPP connection to the ISP using the analog telephone system or ISDN.
- 2 The ISP network access server accepts the connection.
- 3 The ISP network access server authenticates the end user with CHAP or PAP. The username is used to determine whether the user is a VPDN client. If the user is not a VPDN client, the client accesses the Internet or other contacted service.
- 4 The tunnel endpoints—the network access server and the home gateway—authenticate *each other* before any sessions are attempted within a tunnel.
- 5 If no L2F tunnel exists between the network access server and the remote users' home gateway, a tunnel is created. Once the tunnel exists, an unused slot within the tunnel is allocated.
- 6 The home gateway accepts or rejects the connection. Initial setup can include authentication information required to allow the home gateway to authenticate the user.
- 7 The home gateway sets up a virtual interface. Link-level frames can now pass through this virtual interface through the L2F tunnel.

Figure 314 illustrates a VPDN connection from a remote user, who makes a local call, to the corporate network, through an end-to-end L2F tunnel (shown by the dotted line). The user can even be sent directly to a restricted part or a restricted set of servers on the corporate based on the user's authentication. In Figure 314, the restriction placed on this user is suggested by the arc isolating a part of the corporate network cloud.

Figure 314 Virtual Private Dialup Network



Configure VPDN on the Home Gateway Router

To configure virtual private dialup networks on the home gateway router, complete the tasks in the following sections:

- Configure a Virtual Template and Create a Virtual Template Interface
- Configure Incoming VPDN Connections

For more information, see the draft RFC *Level Two Forwarding (Protocol) "L2F,"* which describes the proposed implementation of L2F.

Configure a Virtual Template and Create a Virtual Template Interface

To configure a virtual template for interfaces on a home gateway access server, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	interface virtual-template <i>number</i>	Create a virtual template interface, and enter interface configuration mode.
2	ip unnumbered ethernet 0	Identify the virtual template interface type and number on the LAN.
3	encapsulation ppp	Enable PPP encapsulation on the virtual template interface.
4	ppp authentication chap	Enable PPP authentication on the virtual template interface.

Configure Incoming VPDN Connections

To configure virtual private dialup networking on a home gateway router or access server, use the following commands in global configuration mode:

Command	Purpose
vpdn enable	Enable virtual private networking.
vpdn incoming <i>remote-name local-name virtual-template number</i>	Specify the remote host (the network access server), the local name (the home gateway) to use for authenticating, and the virtual template to use.

Configure VPDN on the Network Access Server

You can configure the router to authenticate users and also to select the outgoing tunnel based on the home gateway's host name or based on the DNIS information in the incoming calls. In addition, you can configure the tunnel search order.

- Configure the Network Access Server to Authenticate Users
- Configure VPDN Tunnel Lookup Based on Domain Name
- or
- Configure VPDN Tunnel Lookup Based on Dialed Number Information
- Configure VPDN Tunnel Authorization Search Order

Configure the Network Access Server to Authenticate Users

You can configure the network access to authenticate users before forwarding each connection to the home gateway. This allows you to detect unauthorized users and possibly to lessen the amount of traffic sent over the tunnels. To enable the network access server to authenticate users, complete the following task in global configuration mode:

Command	Purpose
vpdn local-authentication	Enable the network access server to authenticate users.

Configure VPDN Tunnel Lookup Based on Domain Name

To configure a network access server to make outgoing L2F connections to a home gateway based on domain name, complete the following tasks in global configuration mode:

Command	Purpose
vpdn enable	Enable virtual private networking.
vpdn outgoing <i>domain-name local-name ip ip-address</i>	Specify the remote host that is to accept L2F connections.

Configure VPDN Tunnel Lookup Based on Dialed Number Information

The network service provider can select a specific VPDN tunnel for outgoing calls from a dial-in user by using the Dialed Number Information Service (DNIS) information provided on ISDN lines.

The ability to select a tunnel based on DNIS provides additional flexibility to network service providers who offer VPDN services and to the corporations that use the services. Instead of having to use only the domain name for tunnel selection, tunnel selection can be based on the dialed number.

With this feature, a corporation—which might have only one domain name—can provide multiple specific phone numbers for users to dial in to the network access server at the service provider’s point of presence. The service provider can select the tunnel to the appropriate services or portion of the corporate network based on the dialed number.

To configure a network access server to select outgoing L2F tunnel connections based on DNIS information for virtual private dialup networking, use the following commands in global configuration mode:

Command	Purpose
vpdn enable	Enable virtual private networking.
vpdn outgoing dnis <i>dialed-number</i>	Enable tunnel selection based on DNIS and specify the number to be dialed.

Configure VPDN Tunnel Authorization Search Order

When a service provider has multiple AAA servers configured, VPDN tunnel authorization searches based on domain name can be time consuming and might cause the client session to time out.

To provide more flexibility, service providers can now configure the network access server to perform tunnel authorization searches by domain name only, by DNIS only, or by both in a specified order.

To configure the network access server’s tunnel authorization searches, use one of the following commands in global configuration mode:

Command	Purpose
vpdn search-order dnis domain	Search first on the Dialed Number Information Service (DNIS) information provided on ISDN lines and then search on the domain name.
vpdn search-order domain dnis	Search first on the domain name and then search on the DNIS information.
vpdn search-order domain	Search on the domain name only.
vpdn search-order dnis	Search on the DNIS information only.

Monitor VPDN Virtual Interfaces

To monitor and maintain VPDN virtual interfaces, use the following commands in EXEC mode:

Command	Purpose
<code>show vpdn</code>	Display information about the active L2F tunnels and the L2F message identifiers.

VPDN MIB and Syslog Facility

The Virtual Private Dialup Network (VPDN) Management Information Base (MIB) feature is intended to support all the tables and objects defined in the Cisco VPDN Management MIB for VPDN user sessions. VPDN system wide information is available. This includes active VPDN tunnels, active user sessions in active VPDN tunnels, and failure history information, per username.

The VPDN Syslog facility provides generic logging output for VPDN information, such as Layer 2 Forwarding Protocol (L2F). The syslog messages are generated to inform authentication or authorization errors, resource issues, and time-out events.

VPDN MIB and Syslog Facility has the following benefits:

- The VPDN MIB feature offers a mechanism to track failures of user calls in a VPDN system allowing SNMP retrieval of user call failure information, on a per user basis.
- The VPDN Syslog Facility feature offers real-time access to VPDN fault information.

Configuration Tasks

Refer to the Cisco VPDN Management MIB for a list of supported objects for the VPDN MIB.

By default, VPDN failure history logging is enabled. In order to manually configure a router to capture information queries if this function was previously disabled, perform the following tasks. The first task is required. The last task is optional.

- Configure Event Logging
- Set the History Table Size

Configure Event Logging

The syslog mechanism provides generic and failure event logging. Generic logging is a mixture of type error, warning, notification, and information logging for VPDN. Logging can be done locally or at a remote tunnel destination. Both generic and failure event logging is enabled by default; therefore, if you wish to disable VPDN failure events you must specifically configure the router or access server to do so. In order to disable the router to log VPDN generic or history events, use the following commands in global configuration mode:

Command	Purpose
<code>no vpdn logging [local remote]</code>	Disable generic event logging, locally or at a remote endpoint.
<code>no vpdn history failure</code>	Disable the logging of failure events to the failure history table.

Set the History Table Size

You may set the failure history table to a specific number of entries based on the amount of data you wish to track. To set the failure history table, use the following commands in global configuration mode:

Command	Purpose
<code>vpdn history failure table-size <i>entries</i></code>	(Optional) Set the failure history table depth.

VPDN Configuration Examples

In the following example, the network access server is configured to select tunnels based on the dialed number of incoming calls:

```
vpdn enable
vpdn outgoing spartan dnis 4592367
```

In the following example, the network access server is configured to select tunnels based on the dialed number of incoming calls and to perform tunnel authorization searches on DNIS only:

```
vpdn enable
vpdn outgoing spartan dnis 4592367
vpdn search-order dnis
```

The following example enables VPDN history logging and sets the history failure table size to 30 entries:

```
vpdn history failure
vpdn history failure table-size 30
```