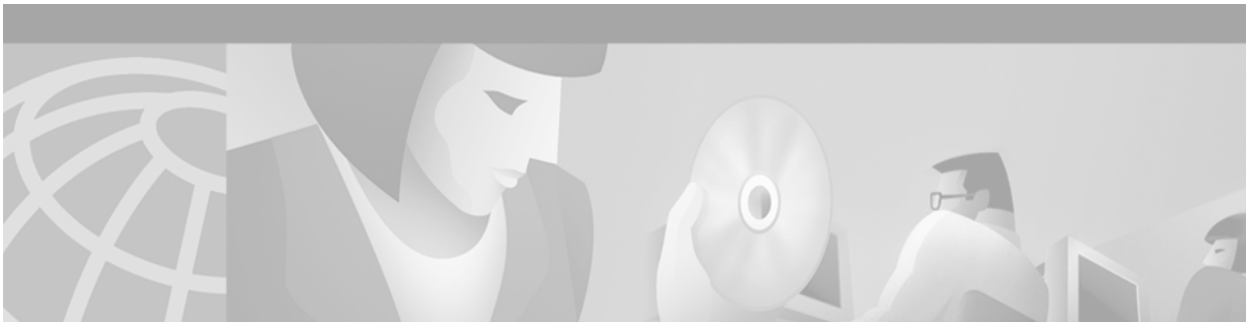


Synopsis of Access VPDN Dial-In Using L2TP

An access virtual private dial network (VPDN) is a network that extends dial access to users over a shared infrastructure. Access VPDNs maintain the same security and management policies as a private network. They are a cost-effective method of establishing long-distance point-to-point connections between remote users and a private network.

Note Access VPDNs should not be confused with dedicated virtual private networks (VPNs)—also called intranet VPNs or extranet VPNs. Dedicated VPNs connect remote offices to private networks using permanent, dedicated connections. Access VPDNs provide remote access to private networks using analog, ISDN, mobile IP, and cable technologies.

The main attraction of access VPDNs is the way they delegate responsibilities for the network. An Internet service provider (ISP) leases VPDN service to customers (typically enterprise customers or medium-sized service providers) that want to outsoure their information technology (IT) responsibilities or expand their geographical presence. The ISP is responsible for the modems, access servers, and internetworking expertise necessary to remotely access the network. The ISP customers are then responsible only for authenticating their users and maintaining their private network.

Instead of making connections directly to the network by using the expensive Public Switched Telephone Network (PSTN), access VPDN users only need to use the PSTN to connect to the ISP local point of presence (POP). The ISP then uses the Internet to forward users from the POP to the customer network. Forwarding calls over the Internet as opposed to making a long-distance PSTN call provides dramatic cost saving for the customer.

Access VPDNs use Layer 2 tunneling technologies to create virtual point-to-point connections between users and the customer network. These tunneling technologies provide the same direct connectivity as the expensive PSTN by using the inexpensive Internet. Users anywhere in the world then have the same connectivity as they would at the customer headquarters.

Access VPDN Architectures

VPDNs are designed based on one of two architectural options: client-initiated or network access server (NAS)-initiated VPDNs. A NAS is an access server, maintained by the ISP, that users dial in to and that forwards the call to the network:

- Client-initiated VPDNs—Users establish an encrypted IP tunnel across the ISP shared network to the customer network. The customer manages the client software that initiates the tunnel. The main advantage of client-initiated VPDNs is that they secure the connection between the client and the ISP. However, client-initiated VPDNs are not as scalable as NAS-initiated VPDNs.
- NAS-initiated VPDNs—Users dial in to the ISP NAS, which establishes an encrypted tunnel to the customer private network. NAS-initiated VPDNs are more robust than client-initiated VPDNs, allow users to connect to multiple networks by using multiple tunnels, and do not require the client to maintain the tunnel-creating software. NAS-initiated VPDNs do not encrypt the connection between the client and the ISP, which is not a concern for most customers because the PSTN is much more secure than the Internet.

This document focuses solely on NAS-initiated access VPDNs.

Layer 2 Tunneling Protocols

VPDNs can use any of the three following Layer 2 tunneling protocols:

- Layer 2 Forwarding—L2F is a Cisco proprietary tunneling protocol. Its main advantage is that it is a stable tunneling protocol supported by many vendors and client software applications. It is the most stable of the Layer 2 tunneling protocols.
- Point-to-Point Tunneling Protocol—PPTP is a Microsoft proprietary tunneling protocol that is only used for client-initiated VPDNs. It is bundled into many Windows operating systems, which makes it an easily deployable solution for many enterprises.
- Layer 2 Tunneling Protocol—L2TP is the Internet Engineering Task Force (IETF) standard Layer 2 tunneling protocol that was designed to merge the best features of L2F and PPTP.

L2TP offers the best scalability and most features of the three Layer 2 tunneling protocols.

This Integration Solutions Guide describes how a large ISP plans, designs, and implements an access VPDN using L2TP. The ISP works with two customers—a medium-sized service provider and an enterprise customer—to create two main types of VPDN service: wholesale dial and service for enterprise customers.

Wholesale Dial VPDN for Service Providers

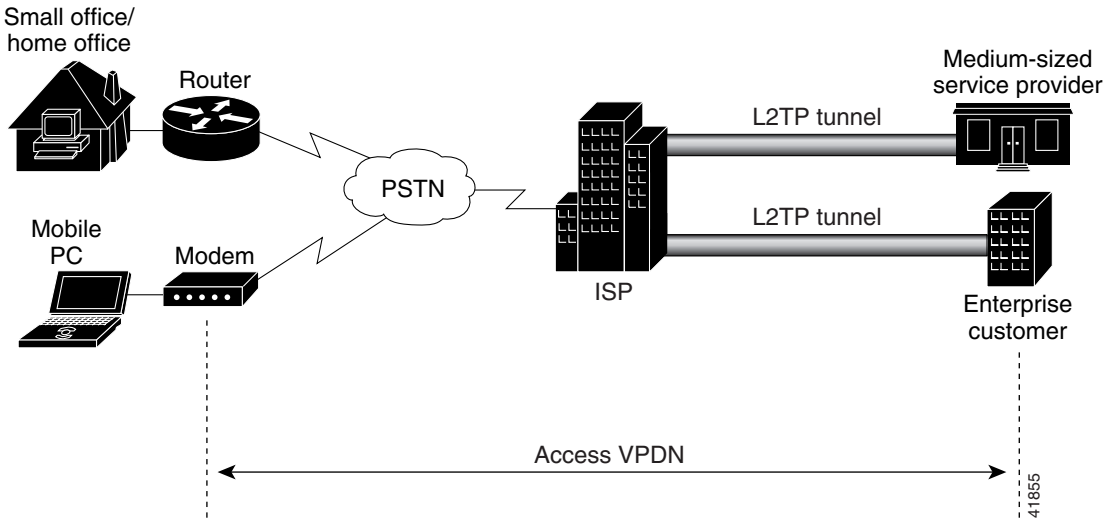
The L2TP network is primarily designed to provide wholesale dial service to medium-sized service providers. In a wholesale dial scenario, the large ISP maintains geographically dispersed POPs. The ISP then offers VPDN service to medium-sized service providers that do not have the resources to maintain multiple POPs, but want to offer geographically extended dial services (called roaming services) to their customers. The customers of the service providers dial in to the ISP local POP, and the ISP then creates a VPDN tunnel to the home networks of the service providers .

VPDN Service for Enterprise Customers

The ISP L2TP network is also designed to provide VPDN service to enterprise customers that want to outsource their IT responsibilities. Enterprise customers want to establish secure, comprehensive dial service for their employees and partners. Some enterprises also want dial-out service to upload information from their central network to remote sites.

This ISG describes how a large ISP partners with a wholesale dial customer and an enterprise customer to design and implement the VPDN network shown in Figure 1.

Figure 1 VPDN Business Scenario



Throughout the rest of this integration solutions guide, we will refer to the three companies—the ISP, service provider, and enterprise—as the partners. We will refer to the service provider and the enterprise as the customers of the ISP.

Benefits

Access VPDNs benefit ISPs, enterprise customers, and service providers as described in the following sections.

Benefits to ISPs and Service Providers

- Offers end-to-end custom solutions that help differentiate the ISP in a competitive market
- Eliminates responsibility of managing the enterprise customer user database
- Allows expansion to broadband technologies (such as cable and wireless) as they become available

Benefits to Enterprise Customers

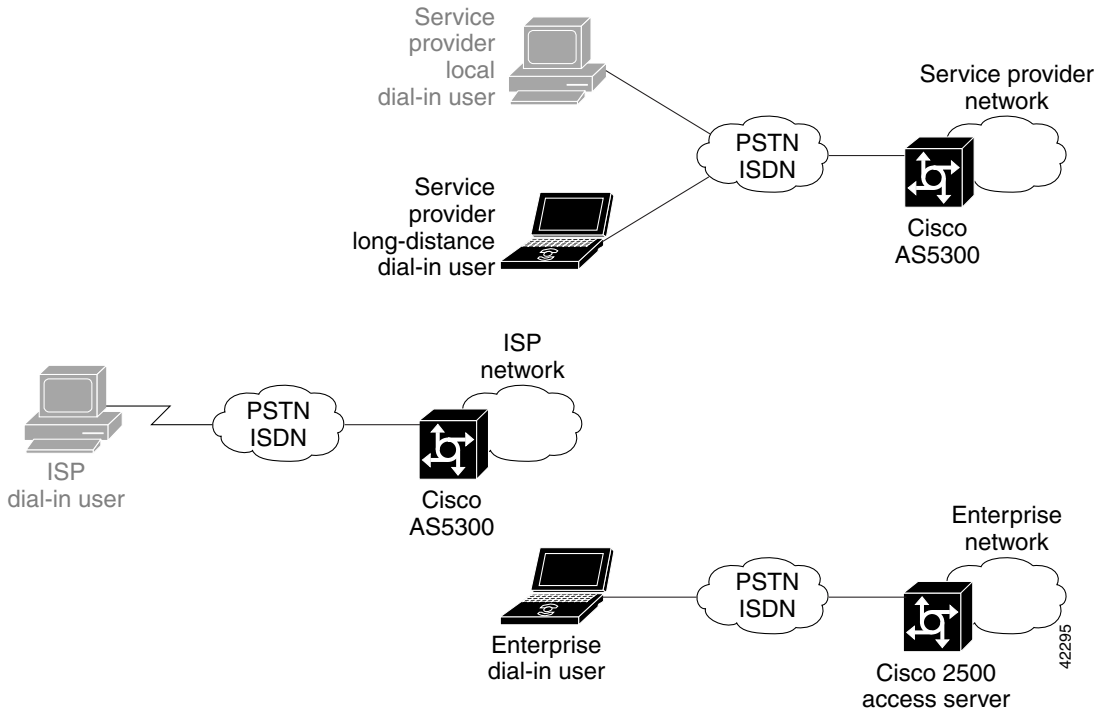
- Allows enterprise customers to focus on their core business responsibilities
- Minimizes equipment costs
- Simplifies complexity of upgrading technology
- Eliminates need of maintaining internetworking expertise
- Reduces long-distance and 800 number costs

- Increases flexibility and scalability of connecting and disconnecting branch offices, users, and external partners
- Prioritizes traffic to ensure bandwidth for critical applications

Preimplementation Environment

This section describes the service provider and enterprise networks before they implement the access VPDN network. Their networks are shown in Figure 2.

Figure 2 Preimplementation Network Topologies



Note The devices in the lighter shade of grey are not affected by the implementation of the access VPDN network.

The three networks function independently of each other. The ISP, service provider, and enterprise each maintains its own access server.

The ISP only has traffic from its own dial-in users.

In order to provide worldwide roaming dialup service, the service provider must maintain an 800 number that generates expensive long-distance phone calls. When customers need to access the network from overseas, they must deal with expensive and often problematic international phone service.

The enterprise customer must maintain its own access server in order to allow employees and partners to remotely access the enterprise network. The enterprise must maintain its own IT infrastructure and networking expertise, including leasing its own IP address subnet. These IT responsibilities distract from its core business responsibilities. When employees need to access the network from remote locations, the enterprise must pay for expensive long-distance phone calls.

Business Drivers

The service provider has the following motivations for establishing the access VPDN:

- To remain competitive, it must offer worldwide roaming dialup service.
- Leasing access VPDN service from a large ISP is more cost-effective than maintaining an 800 number for roaming service.
- It does not have the resources to maintain geographically dispersed POPs.

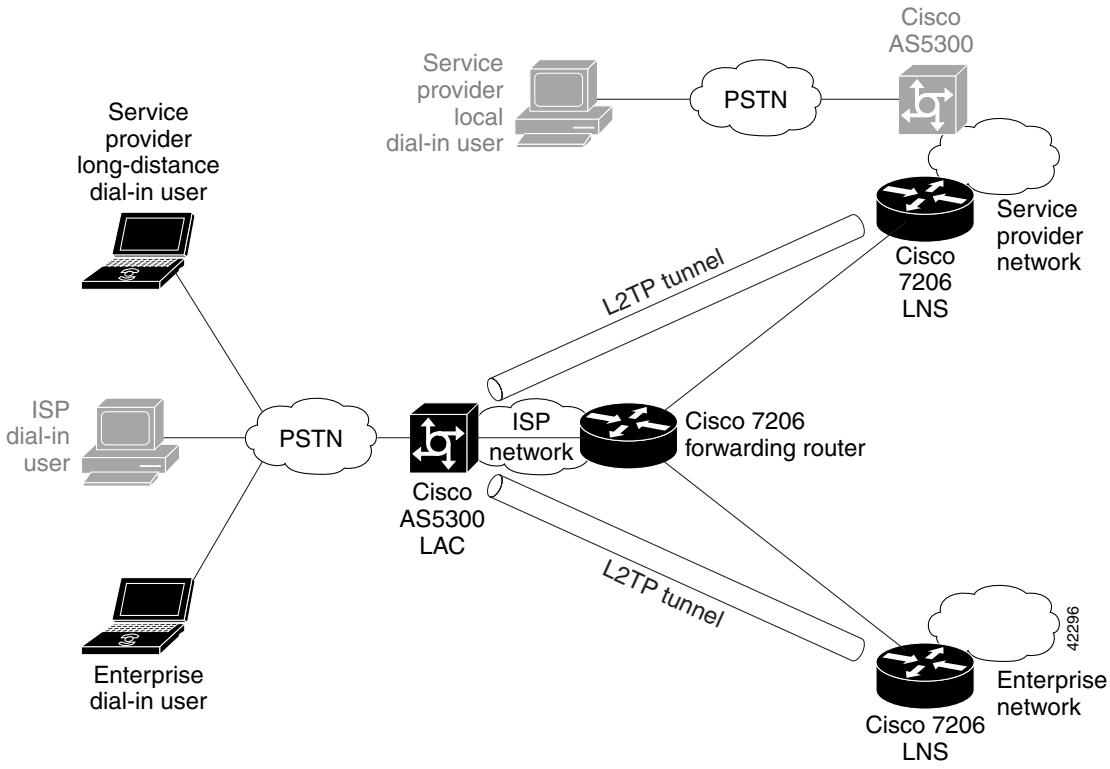
The enterprise customer has the following motivations for establishing the access VPDN:

- As the enterprise grows, it is forced to purchase more access servers and lease more phone lines to allow its employees remote access.
- As the IT infrastructure of the enterprise increases, the enterprise must hire more network administrators.
- The increasing complexity of the IT infrastructure of the enterprise causes increased network delays and failures.
- As the territory of the enterprise expands, costs of long-distance and 800 number phone bills from employees accessing the enterprise network increase.

Postimplementation Environment

Service provider customers and enterprise employees and partners that need to access the networks outside of the local calling area can dial in to the ISP access servers. The ISP then forwards the calls over the Internet to the proper network, which eliminates 800 number and long-distance charges. The ISP maintains the access servers, modems, phone lines, and internetworking expertise. The service provider and enterprise can then focus on their core business responsibilities. The VPDN network functions as shown in Figure 3.

Figure 3 PostImplementation Access VPDN Network Topology



Note The devices in the lighter shade of grey are not involved in the access VPDN network.

The access VPDN network operation is as follows:

1. The service provider and enterprise lease access VPDN dial-in service from the ISP.
2. The ISP works with the service provider and enterprise to determine the level of service they require. The service provider simply needs calls from its remote users forwarded to its home network.
3. The enterprise requires more extensive VPDN service: It leases IP address space from the ISP, it leases the L2TP Network Server (LNS) from the ISP, and it contracts with the ISP to configure and maintain this equipment.
4. The partners work together to configure the devices to establish L2TP tunnels from the L2TP Access Concentrator (LAC) to the customer LNSs.
5. Once the partners verify that the access VPDN network works, the service provider and enterprise configure the usernames and passwords of their users on their LNSs.

Network Implementation Strategy

The goal of the ISP is to design an access VPDN network that will meet the requirements of as many customers as possible. To design this network, the ISP meets with two different types of customers: a medium-sized service provider interested in wholesale dial VPDN service and an enterprise customer interested in access VPDN service. The ISP, service provider, and enterprise decide to partner to create the access VPDN network.

To ensure a smooth transition from their previous networks to the new networks, they begin with a basic VPDN network: a single LAC that creates VPDN tunnels with two LNSs. All tunnel endpoint information and usernames and passwords are stored locally on the devices.

Design Considerations

The ISP wants to make the VPDN network as flexible as possible. Although the initial implementation will be a basic VPDN network, it is designed to easily increase in scale and complexity. The service provider only wants the ISP to forward its user calls without relinquishing any further control of its network. The enterprise customer wants to outsource as much IT responsibility as possible. The enterprise will use the equipment, IP address space, and networking expertise of the ISP. Then, the enterprise is solely responsible for maintaining its usernames and passwords.

Implementation Process

To implement the access VPDN network, the partners perform the following tasks:

1. The partners determine the level of service the service provider and enterprise require.
2. The partners design the network topology and create a device characteristics table.
3. The ISP configures the LAC and forwarding router.
4. The service provider and enterprise configure their LNSs.
5. The partners verify that they can establish L2TP tunnels to both LNSs.
6. The service provider and enterprise configure the usernames and passwords of their users on the LNSs.

Postimplementation Ramifications

After the VPDN network is configured, the partners face the implications described in the following sections:

ISP Implications

- Scalability

  If the ISP needs to support more than 192 concurrent sessions, it will need to configure additional LACs to form a stack group bidding protocol (SGBP) stack group. All of the LACs can then answer incoming calls using the same PRI numbers, which makes the change transparent to VPDN users.

- Offload router

  When the ISP adds LACs, it can either allow all the LACs to answer calls and establish VPDN sessions, or it can dedicate offload routers to establish VPDN sessions that do not answer calls.

  Because the ISP is using the Cisco AS5300 access server, it need not designate offload routers. Cisco AS5300 access servers have enough CPU power to handle both answering calls and establish VPDN sessions without impacting performance.

  If the ISP were using the Cisco AS5200 access server, it would consider using offload routers.

- Remote authentication, authorization, and accounting (AAA)

  If the ISP wants to store VPDN tunnel information on a server separate from the LACs, it will need to configure a remote AAA server. AAA servers provide more advanced authorization and accounting functions than when AAA is performed locally on the router. The ISP will then need to decide which AAA protocol it will run—either RADIUS or TACACS.

- Multilink support

  If the ISP customers require the ability to establish Multilink PPP (MLP) connections using VPDN, the ISP will need to reconfigure the LACs for multilink VPDN.

- L2TP dial-out

  If the ISP customers require the ability to use VPDN to dial out from their networks to remote clients, the ISP will need to configure the dialers and VPDN groups on the LACs for L2TP dial-out.

- Encryption

  If the ISP customers require secure VPDN service, the ISP will need to configure the LACs to encrypt the VPDN tunnels using IPSec.

Service Provider Implications

- Scalability and backup

  If the service provider needs to support more than 1000 concurrent VPDN sessions, it will need to configure additional LNSs and have the ISP reconfigure the LACs to properly direct calls to the LNSs. The LNSs can balance the calls equally between them, or the LNSs can be designated as being primary or backup only.

- Remote AAA

  If the service provider wants to store its user information on a server separate from the LNSs, it will need to configure a remote AAA server. AAA servers provide more advanced authorization and accounting functions than when AAA is performed locally on the router. The service provider will then need to decide which AAA protocol it will run—either RADIUS or TACACS.

- Multilink support

  If the service provider customers require the ability to establish MLP connections using VPDN, the service provider will need to reconfigure the LNSs for multilink VPDN.

- Multihop VPDN

  If the service provider wants to provide multihop VPDN service, it will need to reconfigure its LNSs to function to establish VPDN tunnels to forward multihop calls to their proper destination.

Enterprise Implications

- Scalability and backup (see description in the “Service Provider Implications” section)
- Remote AAA (see description in the “Service Provider Implications” section)
- Multilink support (see description in the “Service Provider Implications” section)
- User segmentation

  If the enterprise wants to distinguish different levels of access, it will need to configure user segmentation. For example, the enterprise may want to give its employees access to the entire network, but only give limited access to its outside partners. The easiest way to configure user segmentation is through the remote AAA server.
- Encryption

  To provide added security to VPDN sessions, the enterprise can work with the ISP to configure IPSec encryption on its VPDN tunnels.