Overview of Access VPNs and Tunneling Technologies

Introduction

A virtual private network (VPN) is a network that extends remote access to users over a shared infrastructure. VPNs maintain the same security and management policies as a private network. They are the most cost effective method of establishing a point-to-point connection between remote users and an enterprise customer's network.

There are three main types of VPNs: access VPNs, intranet VPNs, and extranet VPNs.

- **Access VPNs**—Provide remote access to an enterprise customer's intranet or extranet over a shared infrastructure. Access VPNs use analog, dial, ISDN, DSL, mobile IP, and cable technologies to securely connect mobile users, telecommuters, and branch offices.
- **Intranet VPNs**—Link enterprise customer headquarters, remote offices, and branch offices to an internal network over a shared infrastructure using dedicated connections. Intranet VPNs differ from extranet VPNs in that they only allow access to the enterprise customer's employees.
- **Extranet VPNs**—Link outside customers, suppliers, partners, or communities of interest to an enterprise customer's network over a shared infrastructure using dedicated connections. Extranet VPNs differ from intranet VPNS in that they allow access to users outside the enterprise.

This document focuses solely on access VPNs.

Access VPNs

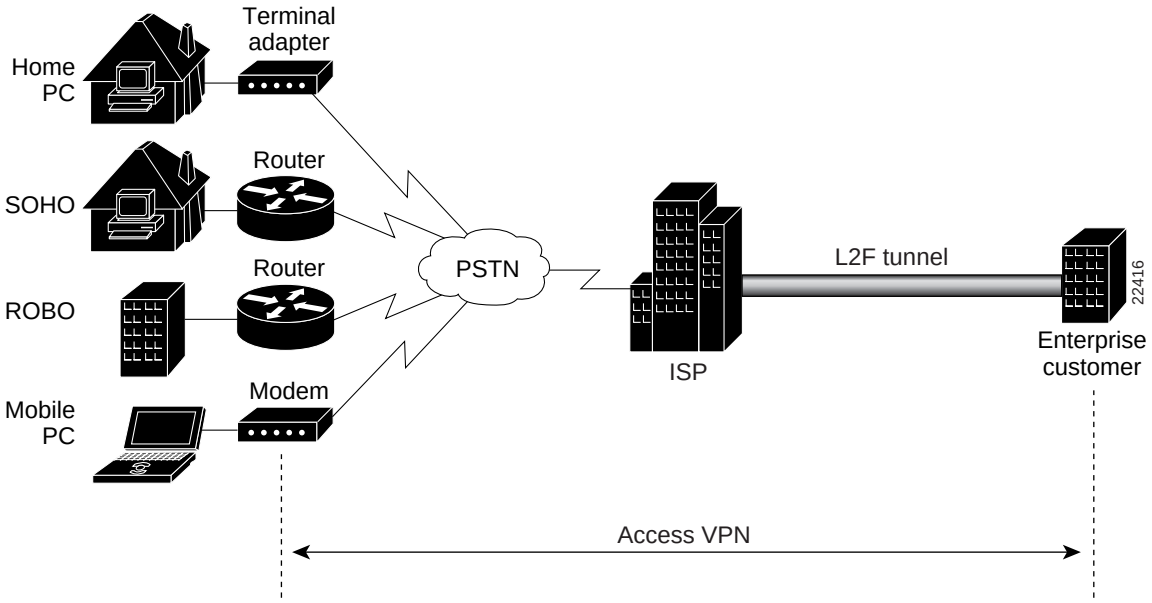
The main attraction of access VPNs is the way they delegate responsibilities for the network. The enterprise customer outsources the responsibility for the information technology (IT) infrastructure to an Internet service provider (ISP) that maintains the modems that the remote users dial into (called modem pools), access servers, and internetworking expertise. The enterprise customer is then only responsible for authenticating its users and maintaining its network.

Instead of connecting directly to the enterprise network by using the expensive public switched telephone network (PSTN), access VPN users only need to use the PSTN to connect to the ISP's local point of presence (POP). The ISP then uses the Internet to forward users from the POP to the enterprise customer network. Forwarding a user's call over the Internet provides dramatic cost saving for the enterprise customer. Access VPNs use layer 2 tunneling technologies to create a virtual point-to-point connection between users and the enterprise customer network. These tunneling technologies provide the same direct connectivity as the expensive PSTN by using the Internet. This means that users anywhere in the world have the same connectivity as they would at the enterprise customer's headquarters.

Access VPNs connect a variety of users: from a single, mobile employee to an entire branch office. Figure 1 illustrates the following methods of logging on to access VPNs:

- Home PC by using a terminal adapter
- Small office/home office (SOHO) by using a router
- Remote office/branch office (ROBO) by using a router
- Mobile PC by using a modem

Figure 1 Logging on to Access VPNs



The access VPN extends from the user to the enterprise customer. The Layer 2 Forwarding (L2F) tunnel is what makes access VPNs unique: Once the tunnel is established, the ISP is transparent to the user and the enterprise customer. The tunnel creates a secure connection between the user and the enterprise customer's network over the insecure Internet and is indistinguishable from a point-to-point connection.

This document describes three end-to-end access VPN case studies, which are primarily intended for ISPs who want to provide access VPN services to enterprise customers. The case studies are also useful to enterprise customers who want to establish access VPNs.

This document does not provide information on the entire spectrum of VPNs, nor does it cover all the details necessary to establish a network. Instead, this document focuses on a specific Layer 2 Forwarding (L2F) case study.

Access VPN Architectures

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

- **Client-initiated access VPNs**—Users establish an encrypted IP tunnel across the ISP's shared network to the enterprise customer's network. The enterprise customer manages the client software that initiates the tunnel. The main advantage of client-initiated VPNs is that they secure the connection between the client and the ISP. However, client-initiated VPNs are not as scalable and are more complex than NAS-initiated VPNs.
- **NAS-initiated access VPNs**—Users dial in to the ISP's NAS, which establishes an encrypted tunnel to the enterprise's private network. NAS-initiated VPNs are more robust than client-initiated VPNs, 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 VPNs do not encrypt the connection between the client and the ISP, but this is not a concern for most enterprise customers because the PSTN is much more secure than the Internet.

This document focuses solely on NAS-initiated access VPNs.

ISPs and Enterprise Customers

Access VPNs involve the cooperation of two partners: an internet service provider (ISP) and an enterprise customer.

- **ISP**—Responsible for maintaining the modem pool, access servers, and internetworking expertise. Often, the ISP will lease its IT infrastructure to smaller ISPs.
- **Enterprise Customer**—Responsible for maintaining its user database and private network. Often, the enterprise customer is a smaller ISP that does not want to take on the expense and commitment of establishing its own IT infrastructure.

In this document, ISP refers to the partner that is responsible for the IT infrastructure, and enterprise customer refers to the partner that leases the IT infrastructure.

Benefits

Access VPNs benefit both ISPs and enterprise customers as described in the following sections.

Benefits to the ISPs

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

Benefits to the 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

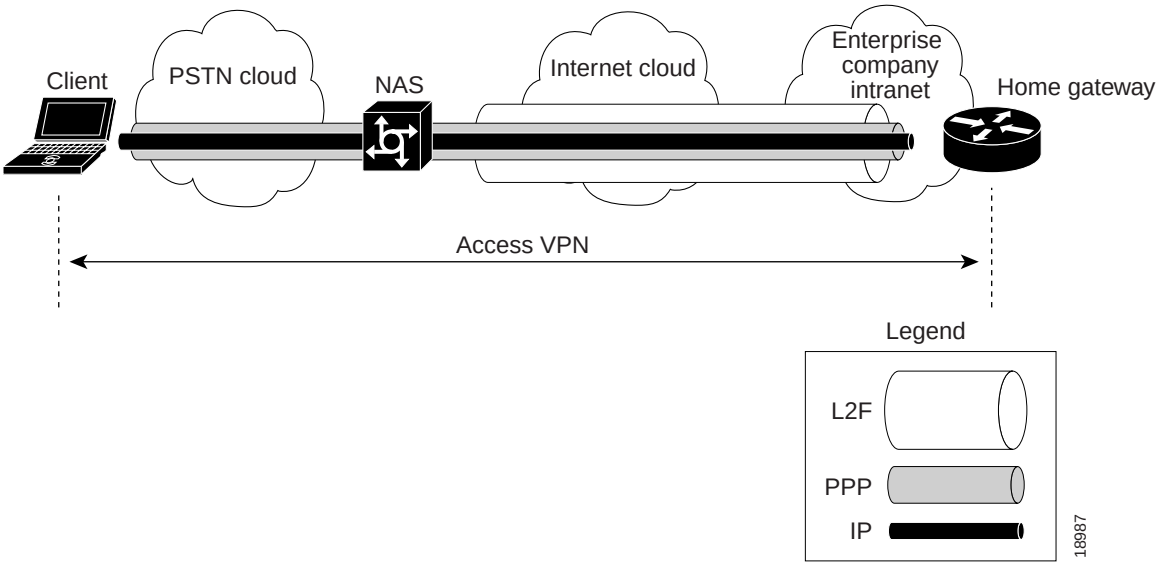
Access VPN Technologies

Access VPNs use L2F tunnels to tunnel the link layer of high-level protocols (for example, PPP frames or asynchronous High-Level Data Link Control). By using such tunnels, it is possible to detach the location of the ISP's NAS from the location of the enterprise customer's home gateway, where the dial-up protocol connection terminates and access to the enterprise customer's network is provided.

ISPs configure their NASs to receive calls from users and forward the calls to the enterprise customer's home gateway. The ISP only maintains information about the home gateway—the tunnel endpoint. The enterprise customer maintains the home gateway users' IP addresses, routing, and other user database functions. Administration between the ISP and home gateway is reduced to IP connectivity.

Figure 2 shows the PPP link running between a client (the user's hardware and software) and the home gateway. The NAS and home gateway establish an L2F tunnel that the NAS uses to forward the PPP link to the home gateway. The access VPN then extends from the client to the home gateway. The L2F tunnel creates a virtual point-to-point connection between the client and the home gateway.

Figure 2 End-to-End Access VPN Protocol Flow: L2F, PPP, and IP



The following sections give a functional description of the sequence of events that establish the access VPN:

- Protocol Negotiation Sequence
- L2F Tunnel Authentication Process
- Three-Way CHAP Authentication Process

The “Protocol Negotiation Sequence” section is an overview of the negotiation events that take place as the access VPN is established. The “L2F Tunnel Authentication Process” section gives a detailed description of how the NAS and home gateway establish the L2F tunnel. The “Three-Way CHAP Authentication Process” section gives a detailed description of how the NAS and home gateway authenticate a user.

Protocol Negotiation Sequence

When a user wants to connect to the enterprise customer's home gateway, he or she first establishes a PPP connection to the ISP's NAS. The NAS then establishes an L2F tunnel with the home gateway. Finally, the home gateway authenticates the client's username and password, and establishes the PPP connection with the client.

Figure 3 describes the sequence of protocol negotiation events between the ISP's NAS and the enterprise customer's home gateway.

Figure 3 Protocol Negotiation Events Between Access VPN Devices

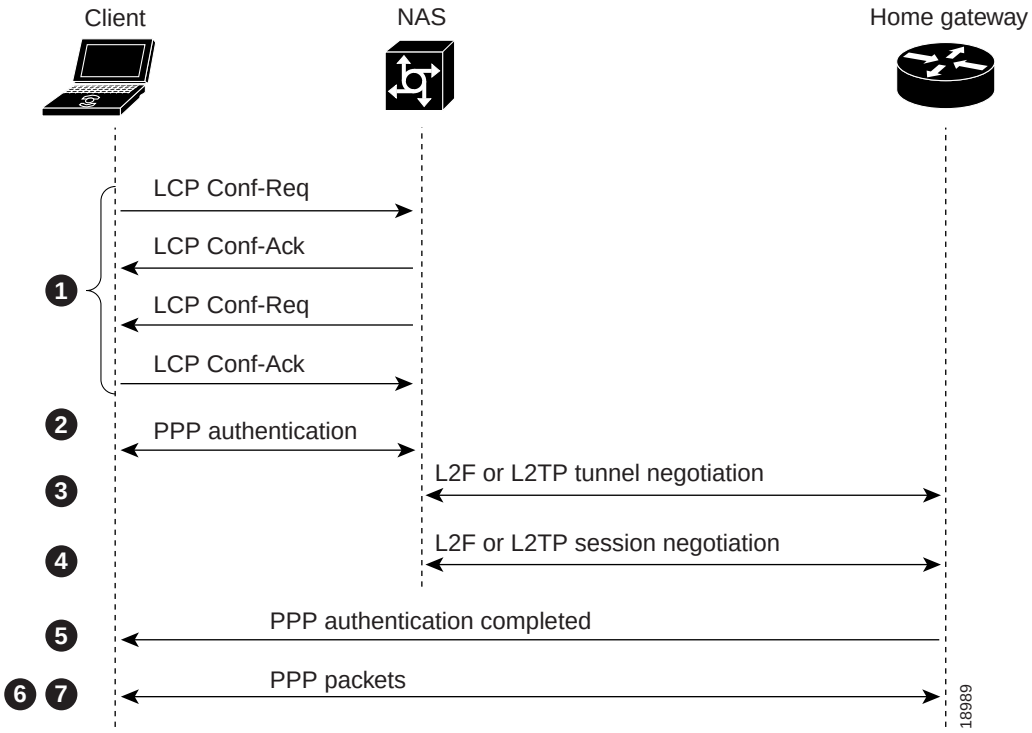


Table 1 explains the sequence of events shown in Figure 3.

Table 1 Protocol Negotiation Event Descriptions

Event	Description
1	The user's client and the NAS conduct a standard PPP link control protocol (LCP) negotiation.
2	The NAS begins PPP authentication by sending a Challenge Handshake Authentication Protocol (CHAP) challenge to the client.
3	The client replies with a CHAP response.
4	When the NAS receives the CHAP response, either the phone number the user dialed in from (when using DNIS-based authentication) or the user's domain name (when using domain name-based authentication) matches a configuration on either the NAS or its AAA server. This configuration instructs the NAS to create a VPN to forward the PPP session to the home gateway by using an L2F tunnel. Because this is the first L2F session with the home gateway, the NAS and the home gateway exchange L2F_CONF packets, which prepare them to create the tunnel. Then they exchange L2F_OPEN packets, which open the L2F tunnel.
5	Once the L2F tunnel is open, the NAS and home gateway exchange L2F session packets. The NAS sends an L2F_OPEN (Mid) packet to the home gateway that includes the client's information from the LCP negotiation, the CHAP challenge, and the CHAP response. The home gateway forces this information on to a virtual-access interface it has created for the client and responds to the NAS with an L2F_OPEN (Mid) packet.
6	The home gateway authenticates the CHAP challenge and response (using either local or remote AAA) and sends a CHAP Auth-OK packet to the client. This completes the three-way CHAP authentication.
7	When the client receives the CHAP Auth-OK packet, it can send PPP encapsulated packets to the home gateway.
8	The client and the home gateway can now exchange I/O PPP encapsulated packets. The NAS acts as a transparent PPP frame forwarder.
9	Subsequent PPP incoming sessions (designated for the same home gateway) do not repeat the L2F session negotiation because the L2F tunnel is already open.

L2F Tunnel Authentication Process

When the NAS receives a call from a client that instructs it to create an L2F tunnel with the home gateway, it first sends a challenge to the home gateway. The home gateway then sends a combined challenge and response to the NAS. Finally, the NAS responds to the home gateway's challenge, and the two devices open the L2F tunnel.

Before the NAS and home gateway can authenticate the tunnel, they must have a common "tunnel secret." A tunnel secret is a pair of usernames with the same password that is configured on both the NAS and the home gateway. By combining the tunnel secret with random value algorithms, which are used to encrypt to the tunnel secret, the NAS and home gateway authenticate each other and establish the L2F tunnel.

Figure 4 describes the tunnel authentication process.

Figure 4 L2F Tunnel Authentication Process

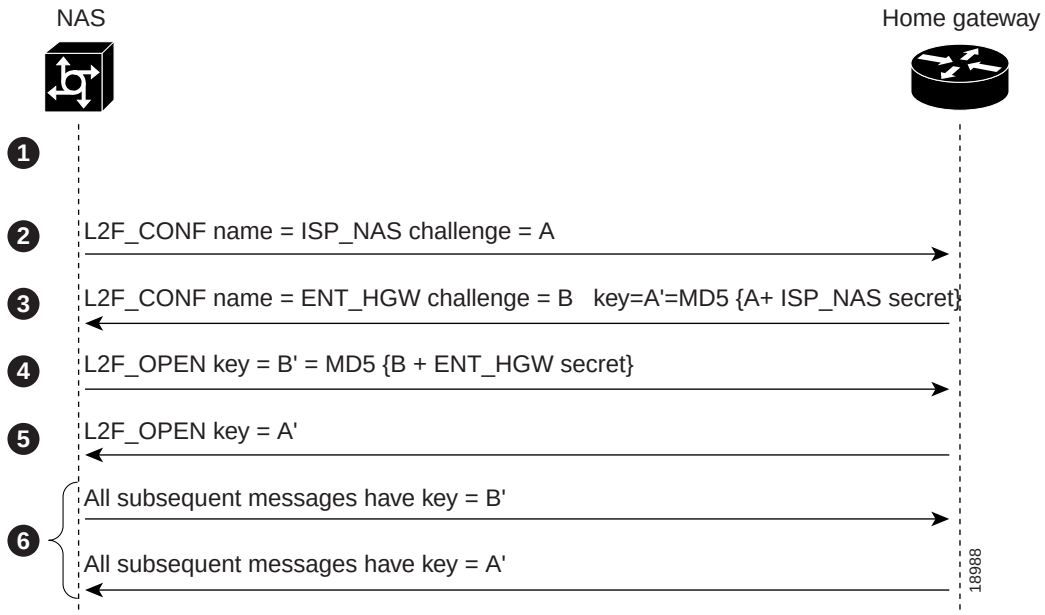


Table 2 explains the sequence of events shown in Figure 4.

Table 2 L2F Tunnel Authentication Event Descriptions

Event	Description
1	Before the NAS and home gateway open an L2F tunnel, both devices must have a common tunnel secret in their configurations.
2	The NAS sends an L2F_CONF packet that contains the NAS name and a random challenge value, A.
3	After the home gateway receives the L2F_CONF packet, it sends an L2F_CONF packet back to the NAS with the home gateway name and a random challenge value, B. This message also includes a key containing A' (the MD5 of the NAS secret and the value A).
4	When the NAS receives the L2F_CONF packet, it compares the key A' with the MD5 of the NAS secret and the value A. If the key and value match, the NAS sends an L2F_OPEN packet to the home gateway with a key containing B' (the MD5 of the home gateway secret and the value B).
5	When the home gateway receives the L2F_OPEN packet, it compares the key B' with the MD5 of the home gateway secret and the value B. If the key and value match, the home gateway sends an L2F_OPEN packet to the NAS with the key A'.
6	All subsequent messages from the NAS include key=B'; all subsequent messages from the home gateway include key=A'.

For more information on L2F, see RFC *Level Two Forwarding (Protocol) "L2F."*

Three-Way CHAP Authentication Process

When establishing an access VPN, the client, NAS, and home gateway use three-way CHAP authentication to authenticate the client's username and password. CHAP is a challenge/response authentication protocol in which the password is sent as a 64-bit signature instead of as plain text. This enables the secure exchange of the user's password between the user's client and the home gateway.

First, the NAS challenges the client, and the client responds. The NAS then forwards this CHAP information to the home gateway, which authenticates the client and sends a third CHAP message (either a success or failure message) to the client.

Figure 5 describes the three-way CHAP authentication process.

Figure 5 Three-Way CHAP Authentication Process

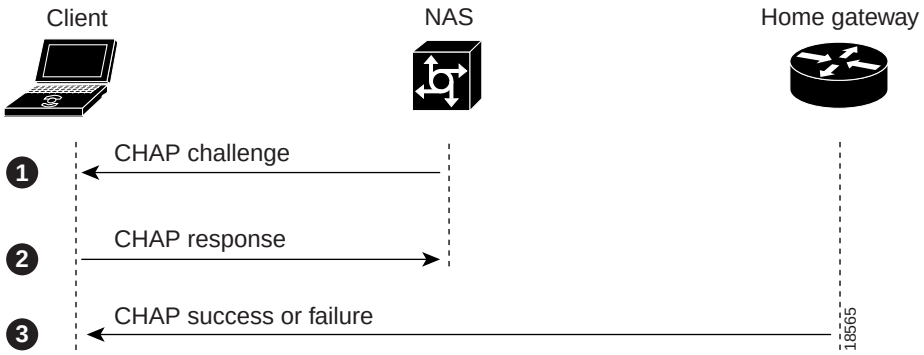


Table 3 explains the sequence of events shown in Figure 5.

Table 3 CHAP Event Descriptions

Event	Description
1	When the user initiates a PPP session with the NAS, the NAS sends a CHAP challenge to the client.
2	The client sends a CHAP response, which includes a plain text username, to the NAS. The NAS uses either the phone number the user dialed in from (when using DNIS-based authentication) or the user's domain name (when using domain name-based authentication) to determine the IP tunnel endpoint information. At this point, PPP negotiation is suspended, and the NAS asks its AAA server for IP tunnel information. The AAA server supplies the information needed to authenticate the tunnel between the NAS and the home gateway. Next, the NAS and the home gateway authenticate each other and establish an L2F tunnel. Then the NAS forwards the PPP negotiation to the home gateway.
3	The third CHAP event takes place between the home gateway and the client. The home gateway authenticates the client's CHAP response, which was forwarded by the NAS, and sends a CHAP success or failure to the client.

Once the home gateway authenticates the client, the access VPN is established. The L2F tunnel creates a virtual point-to-point connection between the client and the home gateway. The NAS acts as a transparent packet forwarder.

When subsequent clients dial in to the NAS to be forwarded to the home gateway, the NAS and home gateway do not need to repeat the L2F session negotiation because the L2F tunnel is already open.