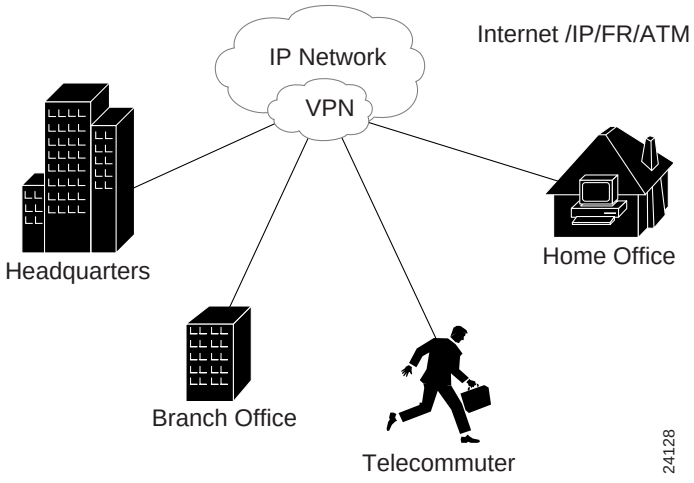
Virtual Private Networks (VPNs)

Virtual private network is defined as customer connectivity deployed on a shared infrastructure with the same policies as a private network. The shared infrastructure can leverage a service provider IP, Frame Relay, or ATM backbone, or the Internet. There are three types of VPNs, which align with how businesses and organizations use VPNs

- *Access VPN*—Provides remote access to a corporate intranet or extranet over a shared infrastructure with the same policies as a private network. Access VPNs enable users to access corporate resources whenever, wherever, and however they require. Access VPNs encompass analog, dial, ISDN, Digital Subscriber Line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, or branch offices.
- *Intranet VPN*—Links corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network, including security, quality of service (QoS), manageability, and reliability.
- *Extranet VPN*—Links customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network, including security, QoS, manageability, and reliability.

Figure 19-1 This figure provides a logical topology view of a VPN.



Cisco Systems VPNs

Currently there are no standards outlining the software and hardware components of a VPN. Every vendor that provides a VPN service performs it in a method that is best supported by its own hardware platforms and software applications. The following sections of this chapter discuss the Cisco Systems implementation of VPN services.

The Cisco Systems VPN Design

Cisco's end-to-end hardware and Cisco IOS software networking products provide sophisticated security for sensitive private transmissions over the public infrastructure, QoS through traffic differentiation, reliability for mission-critical applications, scalability for supporting large bandwidth of data, and comprehensive network management to enable a complete access VPN solution.

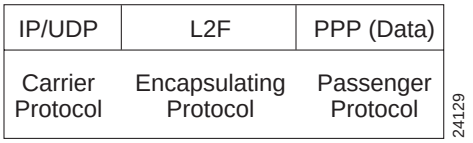
The following sections discuss how Cisco network access servers (NASs) and routers with Cisco IOS software provide new functionality with virtual dialup services. This functionality is based on the L2F protocol Internet Engineering Task Force (IETF) draft request for comments (RFC). The L2F protocol focuses on providing a standards-based tunneling mechanism for transporting link-layer frames—for example, High-Level Data Link Control (HDLC), async Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or PPP Integrated Services Digital Network (ISDN)—of higher-layer protocols. Using such tunnels, it is possible to divorce the location of the initial dialup server from the location at which the dialup protocol connection is terminated and the location at which access to the network is provided (usually a corporate gateway).

Tunneling Defined

A key component of the virtual dialup service is tunneling, a vehicle for encapsulating packets inside a protocol that is understood at the entry and exit points of a given network. These entry and exit points are defined as tunnel interfaces. The tunnel interface itself is similar to a hardware interface, but is configured in software.

Figure 19-2 shows the format in which a packet would traverse the network within a tunnel.

Figure 19-2 This is an overview of a tunneling packet format.



Tunneling involves three types of protocols.

- The *passenger protocol* is the protocol being encapsulated; in a dialup scenario, this protocol could be PPP, SLIP, or text dialog.
- The *encapsulating protocol* is used to create, maintain, and tear down the tunnel. Cisco supports several encapsulating protocols, including the L2F protocol, which is used for virtual dialup services.
- The c*arrier protocol* is used to carry the encapsulated protocol; IP is the first carrier protocol used by the L2F protocol because of its robust routing capabilities, ubiquitous support across different media, and deployment within the Internet.

No dependency exists between the L2F protocol and IP. In subsequent releases of the L2F functionality, Frame Relay, X.25 virtual circuits (VCs), and Asynchronous Transfer Mode (ATM) switched virtual circuits (SVCs) could be used as a direct Layer 2 carrier protocol for the tunnel.

Tunneling has evolved to become one of the key components in defining and using VPNs. Cisco Systems provides virtual dialup service through a telecommuting form of a VPN.

Cisco's Virtual Dialup Services

The following terms are defined to fully describe the virtual dialup service that Cisco provides in its Cisco IOS software:

- *Remote user*—The client who is dialing ISDN/Public Switched Telephone Network (PSTN) from either home or a remote location.
- *NAS*—The telecommuting device that terminates the dialup calls either over analog (basic telephone service) or digital (ISDN) circuits.
- *Internet service provider (ISP)*—The ISP, which supplies the dialup services, can provide for services itself through the NAS or can deliver the dialup remote user to a designated corporate gateway.
- *Corporate gateway*—The destination router that provides access to the services the remote user is requesting. The services could be a corporation or even another ISP.

Remote users (using either asynchronous PPP or ISDN) access the corporate LAN as if they were dialed directly into the corporate gateway, although their physical dialup is through the ISP NAS. Figure 19-2 gives a topological view of how these conventions would be deployed within a virtual dialup service.

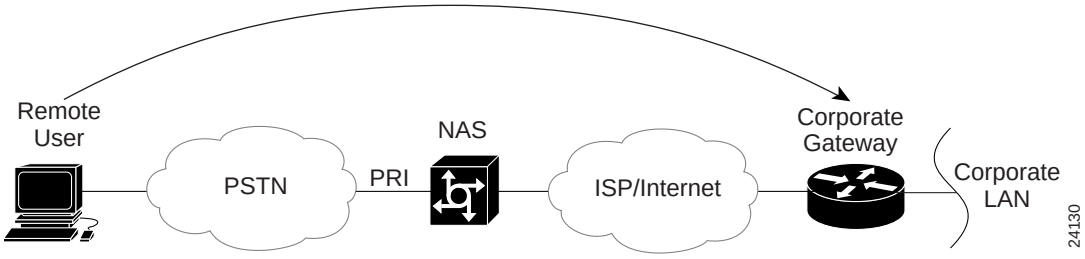
Cisco's L2F Implementation

The key management requirements of service that are provided by Cisco's L2F implementation are as follows:

- Neither the remote end system nor its corporate hosts should require any special software to use this service in a secure manner.
- Authentication as provided by dialup PPP, Challenge Handshake Authentication Protocol (CHAP), or Password Authentication Protocol (PAP), including Terminal Access Controller Access Control System Plus (TACACS+) and Remote Authentication Dial-In User Service (RADIUS) solutions, as well as support for smart cards and one-time passwords; the authentication will be manageable by the user independently of the ISP.
- Addressing will be as manageable as dedicated dialup solutions; the address will be assigned by the remote user's respective corporation, and not by the ISP.
- Authorization will be managed by the corporation's remote users, as it would be in a direct dialup solution.
- Accounting will be performed by both the ISP (for billing purposes) and by the user (for chargeback and auditing).

These requirements are primarily achieved based on the functionality provided by tunneling the remote user directly to the corporate location using the L2F protocol. In the case of PPP, all Link Control Protocol (LCP) and Network Control Protocol (NCP) negotiations take place at the remote user's corporate location. PPP is allowed to flow from the remote user and terminate at the corporate gateway. Figure 19-3 illustrates this process.

Figure 19-3 The remote client establishes a PPP connection with the corporate network to complete the virtual dialup topology.

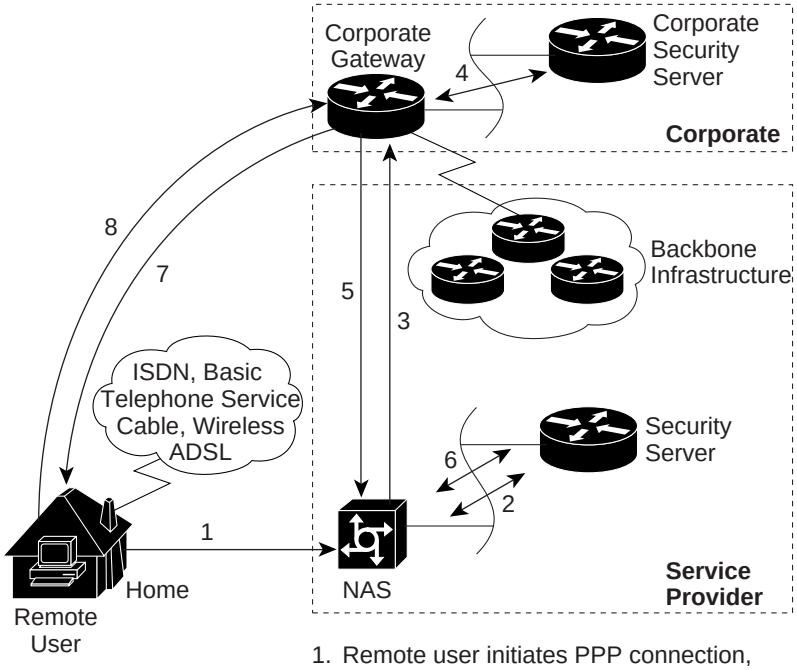


End-to-End Virtual Dialup Process

To illustrate how the virtual dialup service works, the following example describes what might happen when a remote user initiates access. Figure 19-4 gives a step-by-step flow of this end-to-end process.

The remote user initiates a PPP connection to an ISP over the PSTN or natively over ISDN. The NAS accepts the connection, and the PPP link is established. (See Figure 19-4, step 1.)

Figure 19-4 Eight steps are required for communications between a remote VPN client and a corporate LAN.



1. Remote user initiates PPP connection, NAS accepts call.
2. NAS identifies remote user.
3. NAS initiates L2F tunnel to desired corporate gateway.
4. Corporate gateway authenticates remote user and accepts or declines tunnel.
5. Corporate gateway confirms acceptance of call and L2F tunnel.
6. NAS logs acceptance/traffic optional.
7. Corporate gateway exchanges PPP negotiations with remote user. IP address can be assigned by corporate gateway at this point.
8. End-to-end data tunneled from remote user and corporate gateway.

24131

The ISP authenticates the end system/user using CHAP or PAP. Only the username field is interpreted to determine whether the user requires a virtual dialup service. It is expected that usernames will be structured (for example, *smith@cisco.com*) or that the ISP will maintain a database mapping users to services. In the case of virtual dialup, the mapping will name a specific endpoint, the corporate gateway. At the time of the first release, this endpoint is the IP address of the corporate gateway known to the public ISP network. (See Figure 19-4, step 2.)

Note that if permitted by the organization's security policy, the authorization of the dial-in user at the NAS can be performed only on a domain name within the username field and not on every individual username. This setup can substantially reduce the size of the authorization database.

If a virtual dialup service is not required, traditional access to the Internet may be provided by the NAS. All address assignment and authentication would be performed locally by the ISP in this situation.

If no tunnel connection currently exists to the desired corporate gateway, one is initiated. The details of such tunnel creation are outside the scope of this specification; L2F requires only that the tunnel media provide point-to-point connectivity. Obvious examples of such media are the User Datagram

Protocol (UDP), Frame Relay, ATM, and X.25 VCs. Cisco supports UDP in its first release of the virtual dialup service. Based on UDP using a carrier protocol of IP, any media supporting IP will support the virtual dialup functionality. (See Figure 19-4, step 3.)

When the tunnel connection is established, the NAS allocates an unused multiplex ID (MID) and sends a connect indication to notify the corporate gateway of this new dialup session. The MID identifies a particular connection within the tunnel. Each new connection is assigned a MID that is currently unused within the tunnel. The corporate gateway either accepts the connection or rejects it. Rejection may include a reason indication, which may be displayed to the dialup user, after which the call should be disconnected.

The initial setup notification may include the authentication information required to allow the corporate gateway to authenticate the user and decide to accept or decline the connection. In the case of CHAP, the setup packet includes the challenge, username, and raw password; for PAP, it includes username and clear text password. The corporate gateway can be configured to use this information to complete its authentication, avoiding an additional cycle of authentication. Note that the authentication takes place at the corporate customer, allowing the corporation to impose its own security and corporate policy on the remote users accessing its network. In this way, the organization does not have to fully trust the authentication that was performed by the ISP. (See Figure 19-4, step 4.)

If the corporate gateway accepts the connection, it creates a virtual interface for PPP in a manner analogous to what it would use for a direct-dialed connection. With this virtual interface in place, link-layer frames can pass over this tunnel in both directions. (See Figure 19-4, step 5.) Frames from the remote user are received at the NAS, stripped of any link framing or transparency bytes, encapsulated in L2F, and forwarded over the appropriate tunnel. In the first release, the carrier protocol used by the L2F protocol within the tunnel is IP, requiring the frames to also be encapsulated within IP.

The corporate gateway accepts these frames, strips L2F, and processes the frames as normal incoming frames for the appropriate interface and protocol. The virtual interface behaves very much like a hardware interface, except that the hardware in this case is physically located at the ISP NAS. The reverse traffic direction behaves analogously, with the corporate gateway encapsulating the packet in L2F, and the NAS stripping L2F encapsulation before transmitting it out the physical interface to the remote user.

In addition, the NAS can optionally log the acceptance of the call and any relevant information with respect to the type of services provided to the remote user, such as duration of call, packets/bytes transferred, and protocol ports accessed. (See Figure 19-4, step 6.)

At this point, the connectivity is a point-to-point PPP connection whose endpoints are the remote user's networking application on one end and the termination of this connectivity into the corporate gateway's PPP support on the other. Because the remote user has become simply another dialup client of the corporate gateway access server, client connectivity can now be managed using traditional mechanisms with respect to further authorization, address negotiation, protocol access, accounting, and filtering. (See Figure 19-4, steps 7 and 8.)

Because L2F connection notifications for PPP clients contain sufficient information for a corporate gateway to authenticate and initialize its LCP state machine, the remote user is not required to be queried for CHAP authentication a second time, nor is the client required to undergo multiple rounds of LCP negotiation and convergence. These techniques are intended to optimize connection setup and are not intended to circumvent any functions required by the PPP specification.

Highlights of Virtual Dialup Service

The following sections discuss some of the significant differences between the standard Internet access service and the virtual dialup service with respect to authentication, address allocation, authorization, and accounting. It should be noted that the functionality provided by Cisco's network access servers are intended to provide for both the virtual dialup and traditional dialup services.

Authentication/Security

In a traditional dialup scenario, the ISP using a NAS in conjunction with a security server follows an authentication process by challenging the remote user for both the username and password. If the remote user passes this phase, the authorization phase can begin.

For the virtual dialup service, the ISP pursues authentication to the extent required to discover the user's apparent identity (and by implication, the user's desired corporate gateway). No password interaction is performed at this point. As soon as the corporate gateway is determined, a connection is initiated with the authentication information gathered by the ISP. The corporate gateway completes the authentication by either accepting or rejecting the connection. (For example, the connection is rejected in a PAP request in which the username or password is found to be incorrect.) When the connection is accepted, the corporate gateway can pursue another phase of authentication at the PPP layer. These additional authentication activities are outside the scope of the specification, but might include proprietary PPP extensions or textual challenges carried within a TCP/IP Telnet session.

For each L2F tunnel established, L2F tunnel security generates a unique random key to resist spoofing attacks. Within the L2F tunnel, each multiplexed session maintains a sequence number to prevent the duplication of packets.

Cisco provides the flexibility of allowing users to implement compression at the client end. In addition, encryption on the tunnel can be done using IP security (IPsec).

Authorization

When providing a traditional dialup service, the ISP is required to maintain per-user profiles defining the authorization. Thus a security server could interact with the NAS to provide policy-based usage to connecting users, based on their authentication. These policy statements can range from simple source/destination filters for a handful of sites to complex algorithms that determine specific applications, time of day access, and a long list of permitted or denied destinations. This process can become burdensome to the ISP, especially if providing access to remote users on behalf of corporations that require constant change to this policy.

In a virtual dialup service, the burden of providing detailed authorization based on policy statements is given directly to the remote user's corporation. By allowing end-to-end connectivity between remote users and their corporate gateway, all authorization can be performed as if the remote users are dialed into the corporate location directly. This setup frees the ISP from having to maintain a large database of individual user profiles based on many different corporations. More importantly, the virtual dialup service becomes more secure for the corporations using it because it allows the corporations to quickly react to changes in their remote user community.

Address Allocation

For a traditional Internet service, the user accepts that the IP address may be allocated dynamically from a pool of service provider addresses. This model often means that remote users have little or no access to their corporate network's resources because firewalls and security policies deny access to the corporate network from external IP addresses.

For the virtual dialup service, the corporate gateway can exist behind the corporate firewall and allocate addresses that are internal (and, in fact, can be RFC 1597 addresses, or non-IP addresses). Because L2F tunnels operate exclusively at the frame layer, the actual policies of such address management are irrelevant to correct virtual dialup service; for all purposes of PPP protocol handling, the dial-in user appears to have connected at the corporate gateway.

Accounting

The requirement that both the NAS and the corporate gateway provide accounting data can mean that they may count packets, octets, and connection start and stop times.

Because virtual dialup is an access service, accounting of connection attempts (in particular, failed connection attempts) is of significant interest. The corporate gateway can reject new connections based on the authentication information gathered by the ISP, with corresponding logging. For cases in which the corporate gateway accepts the connection and then continues with further authentication, the corporate gateway might subsequently disconnect the client. For such scenarios, the disconnection indication back to the ISP can also include a reason.

Because the corporate gateway can decline a connection based on the authentication information collected by the ISP, accounting can easily draw a distinction between a series of failed connection attempts and a series of brief successful connections. Without this facility, the corporate gateway must always accept connection requests, and would need to exchange numerous PPP packets with the remote system.