

VPN Connection Types

A *virtual private network* (VPN) connection simulates a secure private link over a shared public infrastructure such as the Internet by encapsulating and encrypting all traffic from the remote access client to the VPN server. VPN offers affordable, secure access for home and small offices over any networking technology that transports IP packets. A Windows XP Professional remote access VPN connection makes use of one of two tunneling protocols to encapsulate all traffic.

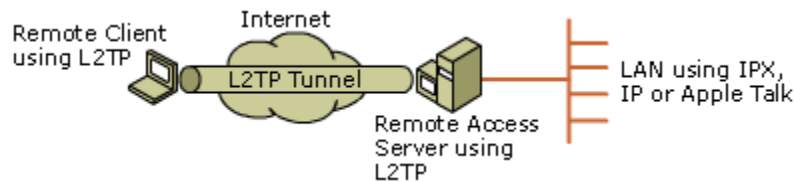
PPTP

Point-to-Point Tunneling Protocol (PPTP), while developed by Microsoft and others, is an open industry standard that supports the tunneling of PPP frames. PPP frames can include IP and other networking protocols. Although L2TP used in conjunction with the IP security (IPSec) protocol provides greater security, PPTP is considerably easier to set up. PPTP uses Point-to-Point Protocol (PPP) authentication, compression, and encryption and can provide good security when used with Microsoft Challenge-Handshake Authentication Protocol version 2 (MS-CHAPv2) and a strong password. Companies can use PPTP to outsource their remote dial-up needs to an Internet service provider (ISP) or other carrier to reduce cost and complexity.

L2TP

Layer 2 Tunneling Protocol (L2TP) is an industry-standard Internet tunneling protocol with roughly the same functionality as PPTP. In Windows XP Professional, L2TP is designed to run natively over IP networks. Like PPTP, L2TP encapsulates PPP frames, which in turn encapsulate the frames of other protocols, thereby allowing users to run applications remotely that are dependent upon specific network protocols. Figure 21.2 demonstrates how an L2TP tunnel can connect a remote computer to a private network. That tunnel can be configured to run over the Internet or an intermediary private network.

Figure 21.2 L2TP tunneling



The use of L2TP, in tandem with IPSec, provides data authentication, data integrity, and data encryption that greatly improves security when sending data over non-secure networks. For more information about IPSec, see "[IPSec](#)" later in this chapter.

Note

- UDP Ports 500 and 1701 need to be open when using L2TP with IPSec for encryption.

For more information about VPNs, see Windows 2000 Server Help or Windows XP Professional Help and Support Center.