Glossary

attribute-value pair (AV pair)—A generic pair of values passed from a AAA server to a AAA client. For example, in the AV pair user = bill, “user” is the attribute and “bill” is the value.

calling line identification (CLID)—A unique number that informs the called party of the phone number of the calling party.

challenge handshake authentication protocol (CHAP)—A PPP cryptographic challenge/response authentication protocol in which the cleartext password is not passed over the line. CHAP allows the secure exchange of a shared secret between the two endpoints of a connection.

client—The hardware and software that the user uses to establish the PPP session. Because all clients discussed in these case studies are remote clients, the term “client” refers to any “remote client.”

cloning—Creating and configuring a virtual access interface by applying a specific virtual template interface. The template is the source of the generic user and router-dependent information. The result of cloning is a virtual access interface configured with all the commands in the template.

control messages—Exchange messages between the NAS and home gateway pairs, operating in-band within the tunnel protocol. Control messages govern the aspects of the tunnel and sessions within the tunnel.

Dialed Number identification Service (DNIS)—The called party number used by call centers or a central office where different numbers are assigned to a specific service.

home gateway—The device, maintained by the enterprise customer, where a tunnel terminates. A home gateway is analogous to the L2TP network server.

Integrated Services Digital Network (ISDN)—Communication protocols offered by telephone companies that permit telephone networks to carry date, voice, and other source traffic.

Layer 2 Forwarding (L2F)—A Layer 2 tunneling protocol that establishes a secure tunnel across a public infrastructure (such as the Internet) that connects an ISP POP to a enterprise home gateway. This tunnel creates a virtual point-to-point connection between the user and the enterprise customer’s network. L2F is the most established and stable Layer 2 tunneling protocol.

Layer 2 Tunnel Protocol (L2TP)—A Layer 2 tunneling protocol that is an extension of the PPP protocol used for virtual private networks (VPNs). L2TP merges the best features of two existing tunneling protocols: Microsoft’s PPTP and Cisco’s L2F. L2TP is the emerging IETF standard, currently being drafted by participants from Ascend, Cisco Systems, Copper Mountain Networks, IBM, Microsoft, and 3Com.

Link Control Protocol (**LCP)**—A protocol that establishes, configures, and tests data link connections used by the PPP.

L2TP access concentrator (LAC)—In L2TP technology, a device that the client directly connects to and through which PPP frames are tunneled to the L2TP network server (LNS). The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F network access server (NAS).

L2TP network server (LNS)—In L2TP technology, a termination point for L2TP tunnels, and an access point where PPP frames are processed and passed to higher layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single media over which L2TP tunnels arrive. The LNS may have a single LAN or WAN interface—yet it can terminate calls arriving at any of the LAC's full range of PPP interfaces (asynchronous, synchronous, ISDN, V.120, etc.). The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.

Message Digest 5 (MD5)—An algorithm used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

Multiplex Identifier (MID)—The number associated with a specific user's L2TP/L2F session.

Multilink PPP Protocol (MLP)—A protocol that splits and recombines packets to a single end system across a logical pipe (also called a bundle) formed by multiple links. Multilink PPP provides bandwidth on demand and reduces transmission latency across WAN links.

Network Access Server (NAS)—A device providing temporary, on-demand network access to users. The access is typically point-to-point using PSTN or ISDN lines. In Cisco's implementation for L2TP, the NAS serves as a LAC for incoming calls and serves as a LNS for outgoing calls. A NAS is analogous to an L2TP access server (LAC).

Network Control protocol (NCP)—A PPP protocol for negotiating OSI Layer 3 (the network layer) parameters.

Password Authentication Protocol (PAP)—A simple PPP authentication mechanism where a cleartext username and password are transmitted to prove identity. PAP is not as secure as CHAP because the password is passed in cleartext.

point-of-presence (POP)—The access point to a service provider's network. The device that the user dials in to.

Point-to-Point Protocol (PPP)—A protocol that encapsulates network layer protocol information over point-to-point links. The RFC for PPP is RFC 1661.

Point-to-Point Tunneling Protocol (PPTP)—A Microsoft proprietary tunneling protocol that was combined with L2F to create L2TP.

public switched telephone network (PSTN)—Telephone networks and services in place worldwide.

remote client—See client.

remote user—See user.

session—A single tunneled PPP call.

tunnel—A virtual pipe between the ISP and home gateway that can carry multiple PPP sessions.

tunnel ID—A two-octet value that denotes a tunnel between an ISP and a home gateway.

user—Instigator of a PPP session. Because all users discussed in these case studies are remote users, the term "user" refers to any "remote user."

virtual access interface—A unique virtual interface that is created dynamically and exists temporarily. Virtual access interfaces can be created and configured differently by different applications, such as virtual profiles and virtual private dialup networks. Virtual access interfaces are cloned from virtual template interfaces. In access VPNs, the home gateway clones a virtual access interface for VPN users.

virtual template—A template that is used to create a logical interface configured with generic configuration information for a specific purpose or common configuration. The template takes the form of a list of Cisco IOS interface commands that are applied to virtual access interfaces, as needed. In access VPNs, the virtual template is configured on the home gateway and used to clone virtual access interfaces for VPN users.

virtual private dialup networking (VPDN)—See virtual private network.

virtual private network (VPN)—A system that permits networks to extend beyond a physical home networks while giving the appearance and functonality of being directly connected to a home network. VPNs use L2TP and L2F to extend the Layer 2 and higher parts of the network connection from the ISP to the home gateway. The specific term “VPDN” is being replaced by the more general term “VPN.”