

L2TP

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol

Secure dial-in corporate solutions have traditionally required long-distance telephone calls and investments in infrastructure such as Network Access Servers. Interpeak L2TP introduces a new amount of flexibility by allowing the public Internet to be used for secure dial-in VPN.

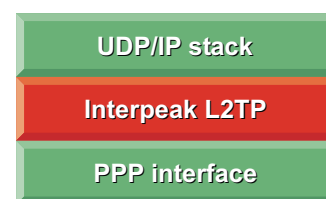
Many companies today are looking for a dial-in solution where the employees can access the corporate network from a remote location. Since security is a major concern in such networks, the only available setup has involved long-distance telephone calls to corporate Network Access Servers (NAS). This has introduced a number of important drawbacks:

- Increasing the call capacity requires that additional telephone lines and NAS's are used.
- Evolving broadband technologies require updates of the NAS's.
- Long-distance telephone calls often have to be used.

The L2TP Solution

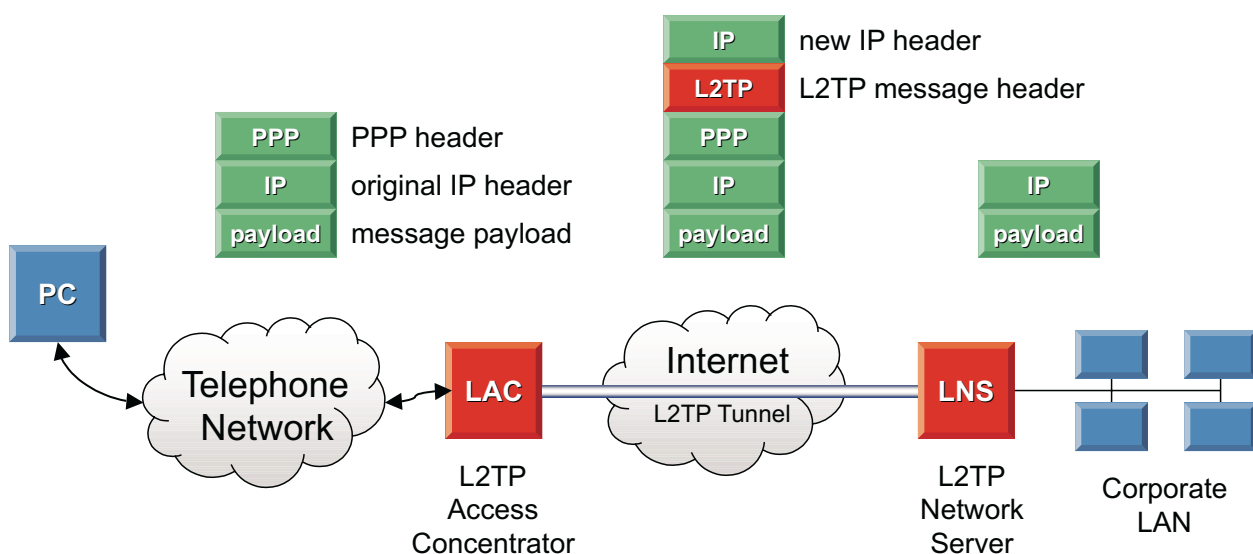
The L2TP protocol provides a powerful solution to this, where traditional NAS work is split in two parts which can be physically separated from each other. The first part of the NAS work is managed by an L2TP Access Concentrator (LAC) and contains the physical interface to the dial-in user. The second part of the NAS work is performed by an L2TP Network Server (LNS), which is connected to the corporate LAN.

The LAC and LNS communicate through the public Internet, using the User Datagram Protocol (UDP). This enables the use of local distance dial-in connections to the LAC, which may be



Interpeak L2TP inserted in a TCP/IP stack to perform tunneling of PPP frames.

located near the dial-in client. It also means that the corporate infrastructure (i.e. number and characteristics of incoming lines) remains unmodified if call capacity has to be increased.



In the compulsory tunneling mode, PPP frames from the remote client are tunneled transparently to the corporate LAN. This means that the remote client has no control of the tunnel, and it will appear as it is connected directly to the corporate

network through a PPP connection. The L2TP software will add an L2TP header to each PPP frame that is to be tunneled. This header is used in the other end of the tunnel, where the L2TP packets are demultiplexed.

Interpeak L2TP Features

L2TP operates by tunneling Point-to-Point Protocol (PPP) frames over non-point-to-point networks. PPP is the most commonly used protocol to provide remote access over dial-up lines.

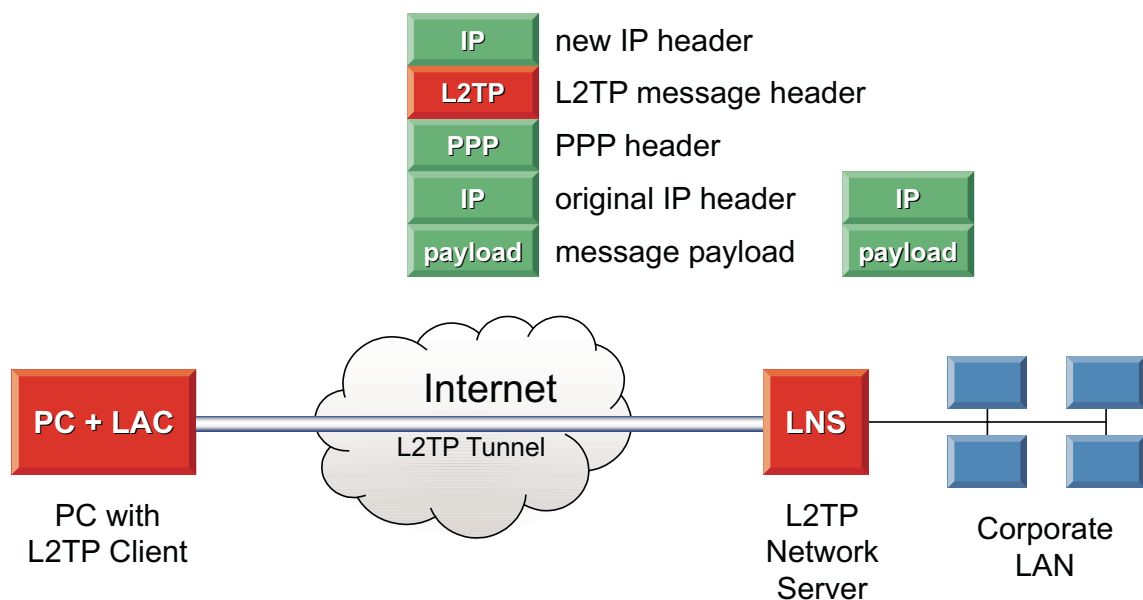
Since the remote client is communicating by means of the PPP protocol, no extra client software is required. The same setup is used as when connecting to a normal ISP.

Widely Used Protocol

The L2TP protocol is specified in RFC 2661, and is created by merging the Cisco L2F and the Microsoft PPTP protocols. L2TP has now replaced its two predecessors, and is widely used in new VPN designs. Windows 2000 from Microsoft contains for example an L2TP client.

- Supports LAC operation compliant to RFC-2661.
- SNMP/MIB support:
L2TP MIB [draft-ietf-l2tpext-l2tp-mib-00.txt]
Interfaces MIB [RFC-2233]
IP Tunnel MIB [RFC-2667]
- Configurable host name or challenge authentication.
- Supports proxy authentication and LCP.
- Uses slow start and congestion avoidance algorithm.
- Explicit or implicit tunnel control.
- Supports both incoming and outgoing tunnels and sessions.
- Delivered in ANSI compliant "C" source code.
- Complete ready-to-run RTOS integration with examples, makefiles etc.
- Configured by powerful shell commands.

Interpeak L2TP features.



The voluntary tunneling mode is characterized by the remote client having LAC functionality built-in and thereby being able to control the tunnel. Since the L2TP protocol operates exactly

the same way as when using compulsory tunneling, the LNS will see no difference between the two modes.

Interpeak Network Security

Interpeak AB, located in Stockholm, Sweden, specializes in network security software and new Internet communication protocols for embedded systems. Interpeak products include IPSec, IKE, SSH, SSL, Web Server Security and NAT. Internet protocols such as LDAP, L2TP, RADIUS, and PPPoE, as well as a dual-mode IPv4/IPv6 TCP/IP stack is also available. For additional information, please visit our homepage: www.interpeak.se, or send a mail to info@interpeak.se.

All Interpeak products are trademarks or registered trademarks of Interpeak AB. Other brand and product names are trademarks or registered trademarks of their respective holders. The information in this document has been carefully reviewed, and is believed to be accurate and reliable. However, Interpeak AB assumes no liabilities for inaccuracies in this document. Furthermore, Interpeak AB reserves the right to change specifications embodied in this document without prior notice.

Version 1.10. Copyright © 2001, Interpeak AB. All rights reserved.