WIKIPEDIA

Layer 2 Tunneling Protocol

In computer networking, **Layer 2 Tunneling Protocol** (**L2TP**) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It uses encryption ('hiding') only for its own control messages (using an optional pre-shared secret), and does not provide any encryption or confidentiality of content by itself. Rather, it provides a tunnel for Layer 2 (which may be encrypted), and the tunnel itself may be passed over a Layer 3 encryption protocol such as IPsec.[1]

Contents

History

Published in 2000 as proposed standard RFC 2661, L2TP has its origins primarily in two older tunneling protocols for point-to-point communication: Cisco's Layer 2 Forwarding Protocol (L2F) and Microsoft's[2] Point-to-Point Tunneling Protocol (PPTP). A new version of this protocol, L2TPv3, appeared as proposed standard RFC 3931 in 2005. L2TPv3 provides additional security features, improved encapsulation, and the ability to carry data links other than simply Point-to-Point Protocol (PPP) over an IP network (for example: Frame Relay, Ethernet, ATM, etc.).

Description

The entire L2TP packet, including payload and L2TP header, is sent within a User Datagram Protocol (UDP) datagram. A virtue of transmission over UDP (rather than TCP) is that it avoids the "TCP meltdown problem".[3][4] It is common to carry PPP sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec (discussed below).

The two endpoints of an L2TP tunnel are called the L2TP access concentrator (LAC) and the L2TP network server (LNS). The LNS waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. To be useful for networking, higher-level protocols are then run through the L2TP tunnel. To facilitate this, an L2TP *session* is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS may initiate sessions. The traffic for each session is isolated by L2TP, so it is possible to set up multiple virtual networks across a single tunnel.

The packets exchanged within an L2TP tunnel are categorized as either *control packets* or *data packets*. L2TP provides reliability features for the control packets, but no reliability for data packets. Reliability, if desired, must be provided by the nested protocols running within each session of the L2TP tunnel.

L2TP allows the creation of a virtual private dialup network (VPDN)[5] to connect a remote client to its corporate network by using a shared infrastructure, which could be the Internet or a service provider's network.

Tunneling models

An L2TP tunnel can extend across an entire PPP session or only across one segment of a two-segment session. This can be represented by four different tunneling models, namely:

- voluntary tunnel
- compulsory tunnel — incoming call
- compulsory tunnel — remote dial
- L2TP multihop connection[6]

L2TP packet structure

An L2TP packet consists of :

Bits 0–15	Bits 16–31
Flags and Version Info	Length (opt)
Tunnel ID	Session ID
Ns (opt)	Nr (opt)
Offset Size (opt)	Offset Pad (opt)......
Payload data	

Field meanings:

Flags and version
control flags indicating data/control packet and presence of length, sequence, and offset fields.

Length (optional)
Total length of the message in bytes, present only when length flag is set.

Tunnel ID
Indicates the identifier for the control connection.

Session ID

Indicates the identifier for a session within a tunnel.

Ns (optional)

sequence number for this data or control message, beginning at zero and incrementing by one (modulo 2^{16}) for each message sent. Present only when sequence flag set.

Nr (optional)

sequence number for expected message to be received. Nr is set to the Ns of the last in-order message received plus one (modulo 2^{16}). In data messages, Nr is reserved and, if present (as indicated by the S bit), MUST be ignored upon receipt..

Offset Size (optional)

Specifies where payload data is located past the L2TP header. If the offset field is present, the L2TP header ends after the last byte of the offset padding. This field exists if the offset flag is set.

Offset Pad (optional)

Variable length, as specified by the offset size. Contents of this field are undefined.

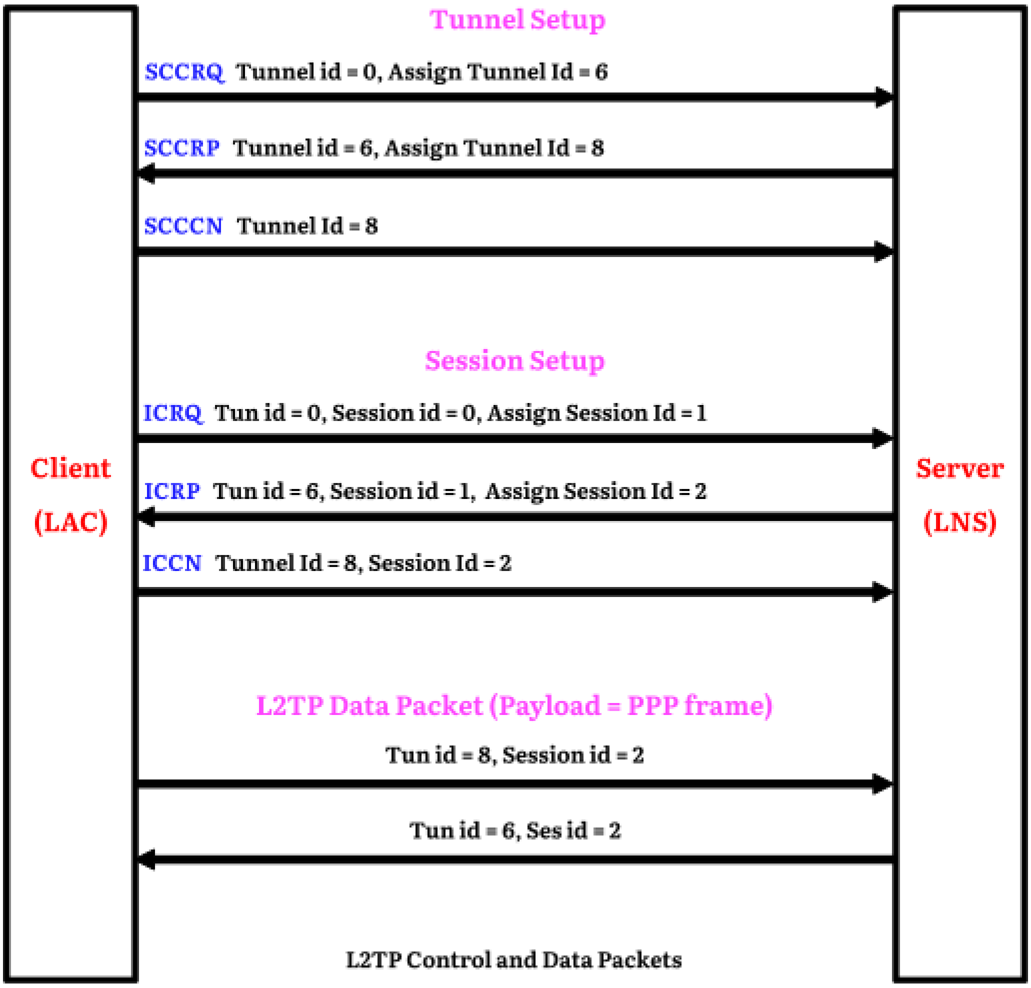
Payload data

Variable length (Max payload size = Max size of UDP packet − size of L2TP header)

L2TP packet exchange

At the time of setup of L2TP connection, many control packets are exchanged between server and client to establish tunnel and session for each direction. One peer requests the other peer to assign a specific tunnel and session id through these control packets. Then using this tunnel and session id, data packets are exchanged with the compressed PPP frames as payload.

The list of L2TP Control messages exchanged between LAC and LNS, for handshaking before establishing a tunnel and session in voluntary tunneling method are


Tunnel Setup
SCCRQ Tunnel id = 0, Assign Tunnel Id = 6
SCCRP Tunnel id = 6, Assign Tunnel Id = 8
SCCCN Tunnel Id = 8
Session Setup
ICRQ Tun id = 0, Session id = 0, Assign Session Id = 1
ICRP Tun id = 6, Session id = 1, Assign Session Id = 2
ICCN Tunnel Id = 8, Session Id = 2
L2TP Data Packet (Payload = PPP frame)
Tun id = 8, Session id = 2
Tun id = 6, Ses id = 2
Client
(LAC)
Server
(LNS)
L2TP Control and Data Packets

L2TP/IPsec

Because of the lack of confidentiality inherent in the L2TP protocol, it is often implemented along with IPsec. This is referred to as L2TP/IPsec, and is standardized in IETF RFC 3193. The process of setting up an L2TP/IPsec VPN is as follows:

1. Negotiation of IPsec security association (SA), typically through *Internet key exchange* (IKE). This is carried out over UDP port 500, and commonly uses either a shared password (so-called "pre-shared keys"), public keys, or X.509 certificates on both ends, although other keying methods exist.
2. Establishment of Encapsulating Security Payload (ESP) communication in transport mode. The IP protocol number for ESP is 50 (compare TCP's 6 and UDP's 17). At this point, a secure channel has been established, but no tunneling is taking place.
3. Negotiation and establishment of L2TP tunnel between the SA endpoints. The actual negotiation of parameters takes place over the SA's secure channel, within the IPsec encryption. L2TP uses UDP port 1701.

When the process is complete, L2TP packets between the endpoints are encapsulated by IPsec. Since the L2TP packet itself is wrapped and hidden within the IPsec packet, the original source and destination IP address is encrypted within the packet. Also, it is not necessary to open UDP port 1701 on firewalls between the endpoints, since the inner packets are not acted upon until after IPsec data has been decrypted and stripped, which only takes place at the endpoints.

A potential point of confusion in L2TP/IPsec is the use of the terms **tunnel** and **secure channel**. The term **tunnel-mode** refers to a channel which allows untouched packets of one network to be transported over another network. In the case of L2TP/PPP, it allows L2TP/PPP packets to be transported over IP. A **secure channel** refers to a connection within which the confidentiality of all data is guaranteed. In L2TP/IPsec, first IPsec provides a secure channel, then L2TP provides a tunnel. IPsec also specifies a tunnel protocol: this is not used when a L2TP tunnel is used.

Windows implementation

Windows has had native support (configurable in control panel) for L2TP since Windows 2000. Windows Vista added 2 alternative tools, an MMC snap-in called "Windows Firewall with Advanced Security" (WFwAS) and the "netsh advfirewall" command-line tool. One limitation with both of the WFwAS and netsh commands is that servers must be specified by IP address. Windows 10 added the "Add-VpnConnection (https://docs.microsoft.com/en-us/powershell/module/vpnclient/add-vpnconnection?view=win10-ps)" and "Set-VpnConnectionIPsecConfiguration (https://docs.microsoft.com/en-us/powershell/module/vpnclient/set-vpnconnectionipsecconfiguration?view=win10-ps)" PowerShell commands. A registry key must be created on the client and server if the server is behind a NAT-T device. [1] (https://support.microsoft.com/en-us/help/926179/how-to-configure-an-l2tp-ipsec-server-behind-a-nat-t-device-in-windows)

L2TP in ISPs' networks

L2TP is often used by ISPs when internet service over for example ADSL or cable is being *resold*. From the end user, packets travel over a wholesale network service provider's network to a server called a Broadband Remote Access Server (BRAS), a protocol converter and router combined. On legacy networks the path from end user customer premises' equipment to the BRAS may be over an ATM network. From there on, over an IP network, an L2TP tunnel runs from the BRAS (acting as LAC) to an LNS which is an edge router at the boundary of the ultimate destination ISP's IP network. See example of reseller ISPs using L2TP (http://www.kitz.co.uk/adsl/equip2.htm).

RFC references

- RFC 2341 (https://datatracker.ietf.org/doc/html/rfc2341) *Cisco Layer Two Forwarding (Protocol) "L2F"* (a predecessor to L2TP)
- RFC 2637 (https://datatracker.ietf.org/doc/html/rfc2637) *Point-to-Point Tunneling Protocol (PPTP)*
- RFC 2661 (https://datatracker.ietf.org/doc/html/rfc2661) *Layer Two Tunneling Protocol "L2TP"*
- RFC 2809 (https://datatracker.ietf.org/doc/html/rfc2809) *Implementation of L2TP Compulsory Tunneling via RADIUS*
- RFC 2888 (https://datatracker.ietf.org/doc/html/rfc2888) *Secure Remote Access with L2TP*
- RFC 3070 (https://datatracker.ietf.org/doc/html/rfc3070) *Layer Two Tunneling Protocol (L2TP) over Frame Relay*
- RFC 3145 (https://datatracker.ietf.org/doc/html/rfc3145) *L2TP Disconnect Cause Information*
- RFC 3193 (https://datatracker.ietf.org/doc/html/rfc3193) *Securing L2TP using IPsec*
- RFC 3301 (https://datatracker.ietf.org/doc/html/rfc3301) *Layer Two Tunneling Protocol (L2TP): ATM access network*
- RFC 3308 (https://datatracker.ietf.org/doc/html/rfc3308) *Layer Two Tunneling Protocol (L2TP) Differentiated Services*

- RFC 3355 (https://datatracker.ietf.org/doc/html/rfc3355) *Layer Two Tunneling Protocol (L2TP) Over ATM Adaptation Layer 5 (AAL5)*
- RFC 3371 (https://datatracker.ietf.org/doc/html/rfc3371) *Layer Two Tunneling Protocol "L2TP" Management Information Base*
- RFC 3437 (https://datatracker.ietf.org/doc/html/rfc3437) *Layer Two Tunneling Protocol Extensions for PPP Link Control Protocol Negotiation*
- RFC 3438 (https://datatracker.ietf.org/doc/html/rfc3438) *Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update*
- RFC 3573 (https://datatracker.ietf.org/doc/html/rfc3573) *Signaling of Modem-On-Hold status in Layer 2 Tunneling Protocol (L2TP)*
- RFC 3817 (https://datatracker.ietf.org/doc/html/rfc3817) *Layer 2 Tunneling Protocol (L2TP) Active Discovery Relay for PPP over Ethernet (PPPoE)*
- RFC 3931 (https://datatracker.ietf.org/doc/html/rfc3931) *Layer Two Tunneling Protocol - Version 3 (L2TPv3)*
- RFC 4045 (https://datatracker.ietf.org/doc/html/rfc4045) *Extensions to Support Efficient Carrying of Multicast Traffic in Layer-2 Tunneling Protocol (L2TP)*
- RFC 4951 (https://datatracker.ietf.org/doc/html/rfc4951) *Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*

See also

- IPsec
- Layer 2 Forwarding Protocol
- Point-to-Point Tunneling Protocol
- Point-to-Point Protocol
- Virtual Extensible LAN

References

1. IETF (1999), RFC 2661, Layer Two Tunneling Protocol "L2TP"
2. "Point-to-Point Tunneling Protocol (PPTP)" (http://www.thenetworkencyclopedia.com/entry/point-to-point-tunnelling-protocol-pptp/). TheNetworkEncyclopedia.com. 2013. Retrieved 2014-07-28. "Point-to-Point Tunneling Protocol (PPTP) [:] A data-link layer protocol for wide area networks (WANs) based on the Point-to-Point Protocol (PPP) and developed by Microsoft that enables network traffic to be encapsulated and routed over an unsecured public network such as the Internet."
3. Titz, Olaf (2001-04-23). "Why TCP Over TCP Is A Bad Idea" (http://sites.inka.de/bigred/devel/tcp-tcp.html). Retrieved 2015-10-17.
4. Honda, Osamu; Ohsaki, Hiroyuki; Imase, Makoto; Ishizuka, Mika; Murayama, Junichi (October 2005). "Understanding TCP over TCP: effects of TCP tunneling on end-to-end throughput and latency". In Atiquzzaman, Mohammed; Balandin, Sergey I (eds.). *Performance, Quality of Service, and Control of Next-Generation Communication and Sensor Networks III*. **6011**. Bibcode:2005SPIE.6011..138H (https://ui.adsabs.harvard.edu/abs/2005SPIE.6011..138H). CiteSeerX 10.1.1.78.5815 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.78.5815). doi:10.1117/12.630496 (https://doi.org/10.1117%2F12.630496). S2CID 8945952 (https://api.semanticscholar.org/CorpusID:8945952).
5. Cisco Support: Understanding VPDN – Updated Jan 29, 2008 (http://www.cisco.com/en/US/tech/tk801/tk703/technologies_tech_note09186a0080094586.shtml)

6. IBM Knowledge Center: L2TP multi-hop connection (http://publib.boulder.ibm.com/infocenter/iseries/v7r1m0/index.jsp?topic=%2Frzaiy%2Frzaiymultihop.htm)

External links

Implementations

- Cisco: Cisco L2TP documentation (https://web.archive.org/web/20090127060833/http://cisco.com/en/US/docs/ios/12_0t/12_0t1/feature/guide/l2tpT.html), also read Technology brief from Cisco (http://www.cisco.com/warp/public/cc/pd/iosw/tech/l2pro_tc.htm)
- Open source and Linux: xl2tpd (http://www.xelerance.com/software/xl2tpd/), Linux RP-L2TP (http://sourceforge.net/projects/rp-l2tp/), OpenL2TP (http://sourceforge.net/projects/openl2tp/), l2tpns (http://l2tpns.sourceforge.net/), l2tpd (http://sourceforge.net/projects/l2tpd/) (inactive), Linux L2TP/IPsec server (http://www.zeroshell.net/eng/vpndetails/), FreeBSD multi-link PPP daemon (http://mpd.sourceforge.net/), OpenBSD npppd(8) (http://bxr.su/OpenBSD/usr.sbin/npppd/), ACCEL-PPP - PPTP/L2TP/PPPoE server for Linux (http://accel-ppp.sourceforge.net/)
- Microsoft: built-in client included with Windows 2000 and higher; Microsoft L2TP/IPsec VPN Client (http://www.microsoft.com/technet/prodtechnol/windows2000serv/support/vpnclientag.mspx) for Windows 98/Windows Me/Windows NT 4.0
- Apple: built-in client included with Mac OS X 10.3 and higher.
- VPDN on Cisco.com (http://www.cisco.com/en/US/tech/tk801/tk703/tsd_technology_support_protocol_home.html)

Other

- IANA assigned numbers for L2TP (https://www.iana.org/assignments/l2tp-parameters)
- L2TP Extensions Working Group (l2tpext) (https://web.archive.org/web/20041207084942/http://www.ietf.org/html.charters/l2tpext-charter.html) - *(where future standardization work is being coordinated)*
- Using Linux as an L2TP/IPsec VPN client (http://www.jacco2.dds.nl/networking/linux-l2tp.html)
- L2TP/IPSec with OpenBSD and npppd (http://undeadly.org/cgi?action=article&sid=20120427125048&mode=expanded&count=3)
- Comparison of L2TP, PPTP and OpenVPN (https://www.ivpn.net/pptp-vs-l2tp-vs-openvpn)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Layer_2_Tunneling_Protocol&oldid=1054686445"

This page was last edited on 11 November 2021, at 14:58 (UTC).