

L2TP Questions and Answers

Terminology

Q. What is L2TP?

A. L2TP, which stands for Layer 2 Tunneling Protocol, is an IETF standard emerging that combines Layer 2 Forwarding protocol (L2F) and Point-to-Point Tunneling protocol (PPTP). As of July 1998, it was nearing final-draft status on the way to becoming a standard. We expect L2TP to have a standard RFC soon.

L2TP is a Cisco IOS Software feature that is a key building block of the Access virtual private (VPN). Access VPNs enable mobile workforces to connect to their corporate intranets or extranets wherever and whenever they require, improving productivity and flexibility while reducing costs.

Q. What are LAC and LNS?

A. *L2TP Access Concentrator (LAC)*—LAC is a device attached to a switched network fabric (such as, PSTN or ISDN) or colocated with a PPP end system capable of handling the L2TP protocol. A LAC device implements the media, over which L2TP passes traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. LAC is the initiator of incoming calls and the receiver of outgoing calls. LAC is also known as NAS in Layer 2 Forwarding (L2F) terminology.

L2TP Network Server (LNS)—LNS operates on any platform capable of PPP termination. It handles the server side of the L2TP protocol. Since L2TP relies on the single media over which L2TP tunnels arrive, an LNS may have only a single LAN or WAN interface, yet still be able to terminate calls arriving at any of the LACs' full range of PPP interfaces (async ISDN). LNS is the initiator of outgoing calls and the receiver of incoming calls.

Network Access Server (NAS)—NAS is a device providing temporary, on-demand network access to users. This access is point-to-point, typically using PSTN or ISDN lines. In the Cisco implementation a NAS serves as a LAC.

Q. What is a client-initiated tunnel?

A. Client-initiated tunnel is a tunnel initiated by client software on the PC. If a client initiated tunnel is used, PC is the LAC.

Q. What is a NAS or SP initiated tunnel?

A. NAS or SP initiated tunnel is a tunnel initiated from a NAS or a device from a SP location. For a NAS initiated tunnel, NAS is the LAC

General

Q. Why would I want L2TP?

A. L2TP is a standard way to build Access VPN. Access VPNs simulate private networks using a shared infrastructure such as the Internet. They offer access for mobile users, telecommuters, and small offices through dial, ISDN, xDSL, and cable.

Q. How does L2TP fit in a VPN solution?

A. L2TP can be used wherever PPTP or L2F is being used today. L2TP can either be operated as a client- initiated tunnel such as PPTP or as a NAS initiated tunnel such as L2F. That means L2TP can be used by service providers to offer a value-added Corporate VPN solution for corporate enterprise networks. L2TP can be also used as part of a wholesale access solution in which telcos or service providers deliver VPNs to ISPs and other service providers. L2TP, along with Cisco SS7 support can be used in a voice congestion offload solution in which telcos and carriers can offload data from the congested voice network using L2TP. L2TP can also be operated as a client-initiated VPN solution in which enterprise customers use the client-initiated L2TP from Windows NT 5.0 client software (or other third party) to a tunnel termination at a Windows NT 5.0 server or a Cisco router.

L2TP is one way to build VPN, voice offload, or wholesale dial solutions. Many other methods allow you to build those solutions with other technologies. Cisco provides a full set of technologies and solutions to customers with different needs and environments.

Q. What are the advantages of the Cisco L2TP offering?

A. Cisco is supporting the latest full IETF standard draft. In addition, all value-added features available with L2F, such as load sharing and backup, and extensive MIB support will be available in Cisco L2TP products. The full feature list is shown in the technical detail section. Cisco is also providing a seamless migration path from L2F to L2TP. The L2F and L2TP tunnels will be able to coexist in the same Cisco network platforms.

Q. Will L2TP be only for service providers?

A. No. L2TP can be implemented at the SP or client to initiate a tunnel. As a result, both SPs and enterprises will be able to deploy L2TP. This provides the maximum flexibility for our customers.

Q. Will L2TP support user roaming (such as, multiple ISP scenario)?

A. Yes, Cisco has added support for L2F to support user roaming. This feature is using Global Roaming Server (GRS) based on CiscoSecure. L2TP will have the same support.

L2F, L2TP, PPTP, and IPSec

Q. What are the differences between L2F and L2TP?

A. L2F is a Layer 2 tunneling solution developed by Cisco Systems. L2F is also supported by other vendors such as Shiva and Nortel. L2TP is an IETF and industry-standard Layer 2 tunneling solution. If interoperability among different vendor equipment is desired, L2TP is the correct choice. If an end-to-end L2F solution is sufficient today, customers need not migrate to L2TP. Cisco will continue to provide L2F in the Cisco IOS software. Currently, L2F is available as an informational RFC (RFC 2341).

Q. If I have L2F already, why would I use L2TP?

A. In addition to L2TP being a standard track protocol, a few new functions available with L2TP that are not available in L2F. L2TP will support flow control and outbound calls to the remote users. Microsoft will also support L2TP in Windows NT 5.0 client software, so if you want a client-initiated tunnel, L2TP is the correct choice. Other client vendors such as Routerware also plan to support L2TP in Windows 95 and Windows NT 4.0 client software (see WinVPN Client by Routerware, Inc. at <http://www.routerware.com>)

Q. What are the differences between L2F, PPTP, and L2TP?

A. The differences from a user's perspective are general availability more than technical details of the protocols. All three protocols tunnel PPP, thus they are similar. They are all Layer 2 tunneling protocols that support Access VPN solutions. L2TP represents the best of both L2F and PPTP combined.

Q. Will L2TP be backwardly compatible with L2F?

A. Yes. To facilitate migration of customers from L2F to L2TP, Cisco will support concurrent operation of L2F sessions and L2TP sessions on a single network access server and a single home gateway. The NAS will set up the tunnel using either L2F or L2TP based upon the domain attributes in the AAA server, and the home gateway will then set up the appropriate de-encapsulation scheme.

This approach will allow L2TP-capable home gateways to work with existing installed L2F NASs (without changes) and concurrently support new or newly upgraded NASs running L2TP. The home gateways are not required to be reconfigured every time an individual NAS is upgraded from L2F to L2TP.

Q. Do I need L2TP if I already have IPSec?

A. L2TP is a standard for Layer 2 tunneling. IPSec is a standard for encryption and security. They are independent, yet complementary standard efforts, and Cisco will provide the combination to take advantage of the strengths in both technologies. Strengths in L2TP include per-user authentication, dynamic address allocation from an address pool or by using DHCP server, and RADIUS and AAA support. Some of the strengths in IPSec are secure encryption and data confidentiality.

Q. If I have end-to-end encrypted tunnel, do I need to use L2TP?

A. The two solutions are complementary. NAS-initiated L2TP tunnels can provide quality of service benefits, per-user authentication, dynamic address allocation, and RADIUS support. Client initiated L2TP tunnels can provide per-user authentication, dynamic address allocation, and RADIUS support. In some IPSec implementations, these features are proprietary. IPSec provides encryption and additional security for L2TP.

Layer 2 and Layer 3 Tunneling Protocols

Q. Is it true that Layer 2 tunneling is not scalable?

A. Scalability for Layer 2 tunneling is implementation dependent. Cisco L2TP implementation supports unlimited sessions on each LAC and support more than 2000 sessions per each LNS on a Cisco router platform.

Q. What is Layer 3 tunneling?

A. Layer 3 tunneling is not a new technology. Generic Routing Encapsulation (GRE) with RFC 1701 has existed for a long time. Cisco has offered this tunneling technology since Cisco IOS software version 9.21. IPSec is the new IETF standard for encryption and encrypted tunnel. Cisco is providing IPSec in Cisco IOS software version 11.3(3)T and later. Cisco is providing Mobile IP in Cisco IOS version 12.0(1)T.

Q. What is the difference between Layer 2 and Layer 3 tunneling?

A. Layer 2 leverages existing PPP technologies such as NCP and access-authentication protocols. Layer 3 loses much of this by recreating the NCP as Layer 3 tunnel endpoints within the customer network. Layer 2 does not require additional special IP software for end users, corporation, and ISP. The Layer 3 solutions require an IP substrate shared between the Corporation and the ISP. In terms of security, user authentication and tunnel authentication features in Layer two tunneling provide better resistance against hackers. In some Layer 3 solutions, authentication is done only at the SP. This solution may pose a security risk for the corporation. The emerging standard for Layer 2 tunneling protocol is L2TP.

Q. Why is Cisco pushing for Layer 2 tunneling instead of Layer 3 tunneling?

A. Cisco is providing both Layer 2 and Layer 3 tunneling solutions. Cisco does not favor one type over the other. Layer 2 tunneling is primarily an Access VPN solution while Layer 3 tunneling provides support for intranet and extranet VPNs between branch offices and a corporate headquarters. Layer 3 tunneling may also make sense in some of the Access VPN implementations such as client-initiated tunnel mode and Internet wholesale access solutions.

Standard and Interoperability with Other Vendors

Q. Is L2TP an industry-standard protocol?

A. Yes. It is the emerging (IETF) standard. The PPP extension working group has attempted to make L2TP an industry standard. L2TP is well accepted and endorsed by the industry at large. See the industry vendors' support on this technology in the following press announcements—"CompuServe Network Services Hosts Industry Leaders at Interoperability Workshop Aimed at Establishing Tunneling Standard to Enable Secure Virtual Private Networks (VPNs) via the Internet" (<http://149.174.215.151/news/1997/10-21-97.html>).

Q. When will L2TP be a standard?

A. L2TP is in the final stage of standard process. The draft has been finalized and approved by the PPP extensions working group. It is currently being approved by the IETF and expects L2TP to have a standard RFC in the near future.

Q. What is the current status of the L2TP draft? When is it expected to be finalized?

A. As of June 12, 1998, the latest L2TP draft is version 11.

Q. Will L2TP have independent vendor interoperability tests?

A. Three vendor independent interoperability tests are sponsored by the California ISDN Users Group (CIUG). Cisco participated in all of the CIUG tests. Cisco also tested L2TP and IPSec at the Automobile Network Exchange (ANX) interoperability test in April 1998.

Q. What is the relationship between Microsoft and Cisco?

A. Microsoft and Cisco are partners in many areas, and L2TP is one example. The companies are also working together in IPSec and directory initiatives.

Microsoft and Cisco have been leading the L2TP effort in the IETF since 1996. See: "Cisco and Microsoft Demonstrate Interoperability of Next-Generation Tunneling Protocol Implementations; Interoperability Marks Milestone of Future Standard for Virtual Private Networks". This release indicated the first interoperability between Cisco and Microsoft L2TP implementations.

Security

Q. How secure is L2TP?

A. L2TP has all the security benefits of PPP, including multiple per user authentication options (CHAP, PAP, and MS-CHAP). It also can authenticate the tunnel end points, which prevents potential intruders from building a tunnel and accessing precious corporate data. L2TP can be used in conjunction with secure ID cards on the client side, and it works with firewalls on the corporate server side. To ensure further data confidentiality, Cisco recommends adding IPSec to any L2TP implementation. Depending on the corporation's specific network security requirements, L2TP can be used in conjunction with tunnel encryption, end-to-end data encryption, or end-to-end application encryption.

Q. Can you use context-based access control (CBAC) with L2TP?

A. Yes. CBAC support is provided in the Cisco IOS Firewall feature set which was introduced in Version 11.3(3)T. Starting with 11.3(3)T, the Cisco IOS Firewall is available in 1600, and 2500 routers. In Version 12.0(1)T, CBAC and L2TP can be used together on the Cisco 1600, 2500, 2600, and 3600 routers.

Q. What encryption services will be supported for L2F/L2TP tunnels, clients, and so on? What is the status of IPSEC on the router and client?

A. Cisco IOS software Version 11.2 currently supports DES 40 bits and 56 bits. IPsec support is available in the Cisco IOS software Version 11.3(3)T. Cisco is working together with Microsoft to have IPsec available in Windows NT 5.0 software. For Windows 95 and Windows NT 4.0 support, Cisco is partnering with RedCreek.

Q. How can customers protect against denial of service attacks targeted against L2TP tunnels (at both ends)?

A. Both tunnel authentication and the preauthentication option at the LAC to provide security within L2TP. At the LNS, tunnel authentication and username authentication are nonoptional features. Therefore, an attacker would not be able to authenticate and would not be able to mount an attack.

Deliverables

Q. When will L2TP be available?

A. L2TP is scheduled to be available in Cisco IOS software Version 11.3(5)AA. This version is expected to be deployable in August 1998.

Q. Which platforms will support L2TP?

A. Cisco IOS Version 11.3(5)AA will be available on Cisco AS5200, AS5300, AS5800, and the 7200 router series. Support on the Cisco 1600, 2500, 2600, 3600, 4000, 4500, 7500, and UAC 6400 is targeted for Version 12.0(1)T of Cisco IOS software.

Q. Which images will support L2TP?

A. The Cisco IOS images IP Plus on the AS5800; IP Plus, Desktop Plus, Enterprise, Enterprise Plus, IP Plus 40, IP Plus IPS 56, Enterprise Plus 40, and Enterprise Plus IPsec 56 on the AS5200 and AS5300; Enterprise image on the 7200 router series support the L2TP feature.

Technical Details

Q. Will Cisco support the full implementation of L2TP?

A. Cisco will implement the latest IETF draft. The current IETF draft version is available on the web at <http://www.masinter.net/~l2tp/ftp/draft-ietf-pppext-l2tp-11.txt> .

Q. What are the technical differences between L2F and L2TP?

A. The functional differences between L2F and L2TP are minimal. The L2TP is made up of structured Attribute Value (AV) pairs. These AV pairs are designed to maximize extensibility while permitting interoperability for a uniform method of encoding messages throughout the L2TP protocol. This protocol allows for future protocol extension without sacrificing the interoperability among multiple vendors.

L2TP has the following functions as optional:

- Dial-out function—traffic initiating from the LNS-initiated traffic that causes the call to occur will be considered a dial-out function.
- User authentication at the LAC as well as LNS

Q. Will Cisco support L2TP over Frame Relay or ATM?

A. Currently, no standard protocol is being defined for L2TP using native Frame Relay or ATM. Cisco supports emerging standard-based L2TP that uses UDP encapsulation over any WAN protocol—whether Frame Relay, ATM, or X25.

Q. What switching paths will support L2TP?

A. L2TP will be available with Cisco Express Forwarding (CEF), fast-switching, and process-switching.

Q. Which encapsulation is supported with L2TP?

A. L2TP uses UDP encapsulation. L2TP tunnel is initiated by Point to Point (PPP), UDP, L2TP, PPP and Payload.

Q. Which interfaces does Cisco L2TP support?

A. L2TP is supported on any PPP-capable interfaces. Therefore, on the LAC, L2TP supports async and ISDN. Since PPP over ATM and PPP over FR are available, support for xDSL and Cable is also possible. For the WAN backbone support, all WAN technologies (ATM OC3, ATM OC12, FR, SONET, T1, E1, T3, and E3) are supported. For LAN backbone, LAN media such as Ethernet, Fast Ethernet, Token Ring, and FDDI are supported.

Q. What kind of access support is available with L2TP?

A. Async, ISDN, and xDSL

Q. What L2F/L2TP result codes will Cisco support (as defined in the L2F/L2TP RFCs)?

A. Also plans to support all result codes.

Q. What extensions beyond the L2TP RFC will Cisco implement?

A. The following L2F features will also be available in L2TP:

- Home gateway load sharing
- Home gateway stacking
- Home gateway primary and secondary backup
- DNS name support
- Domain name flexibility
- Idle and absolute time-out
- Multilink PPP (MP) support
- Multichassis Multilink PPP (MMP) support
- Multihop support
- MIB and Syslog support
- Roaming user authentication support

Implementation Questions

Q. How would I use IPSec with L2TP?

A. Cisco recommends use of IPSec with L2TP if further security is needed. Both modes of IPSec—transport and tunnel mode—can be used with L2TP. The entire tunnel will be encrypted, along with all subsequent sessions.

Transport mode: UDP, L2TP, PPP, and payload signed and optionally encrypted

Tunnel mode: IP, UDP, L2TP, PPP, and payload signed and optionally encrypted

Q. What are the performance implications of using L2TP?

A. The number should be nearly the same as (if not better than) with L2F (with flow control turned off).

Q. Is L2TP for dial only? How about xDSL?

A. In a dial environment, an L2TP tunnel can be initiated from (1) a network access server (NAS) as a NAS-initiated tunnel or (2) client software as a client-initiated tunnel to a router that acts as a tunnel termination point.

In a xDSL environment, user ATM PVCs extend from the CPE to a centrally located NAS function, which then originates L2TP tunnels to the LNSes. This NAS (such as the Cisco 6400 UAC) may be operated by either the ILEC/PTT offering the ADSL service or by a CLEC or ISP at edge of the ILEC.

Client-Initiated Tunnels

Q. Will the Cisco implementation of L2TP work with RedCreek Ravlin Soft Client?

A. Redcreek Ravlin Soft Client currently supports IPSec only. End-to-end encryption will work in conjunction with the Cisco L2TP implementation.

Q. Can I create client-initiated tunnels over ethernet?

A. Yes. You can on a Cisco router, as long as the tunnel termination device can support IP frame.



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
<http://www-europe.cisco.com>
Tel: 33 1 6918 61 00
Fax: 33 1 6928 83 26

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters

Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Connection Online Web site at <http://www.cisco.com>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China (PRC) • Colombia • Costa Rica • Czech Republic • Denmark
England • France • Germany • Greece • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Russia • Saudi Arabia • Scotland • Singapore