

Layer 2 Tunneling Protocol

A Feature in Cisco IOS Software

A Key Building Block for an Access Virtual Private Network

Overview

Cisco is a leader in delivering technologies that transform Access Virtual Private Networks (VPNs) from a promising idea into a practical reality. With the availability of Layer 2 Tunneling Protocol (L2TP) to Cisco IOS[®] software, Cisco offers a standard way to provide Access VPN connectivity. Cisco's end-to-end hardware and Cisco IOS software networking products provide sophisticated security for sensitive private transmissions over the public infrastructure; quality of service through traffic differentiation; reliability for mission-critical applications; scalability for supporting large bandwidth of data; and comprehensive network management to enable a complete Access VPN solution.

VPNs enable today's increasingly mobile workforce to connect to their corporate intranets or extranets whenever, wherever, or however they require, improving productivity and flexibility while reducing access costs.

To provide a low-cost, easily accessible pathway to a corporate intranet or extranet, Access VPNs simulate a private network—but over a shared infrastructure, such as the Internet. They offer access for mobile users, telecommuters, and small offices through a range of technologies, including dial, ISDN, xDSL, mobile IP, and cable.

A key building block for Access VPNs is L2TP (Layer 2 Tunneling Protocol), an extension to the Point-to-point (PPP) protocol and a fundamental building block for VPNs. L2TP merges the best features of two other tunneling protocols: Layer 2 Forwarding (L2F) from Cisco Systems and Point-to-Point Tunneling (PPTP) from Microsoft. L2TP is an Internet Engineering Task Force (IETF) emerging standard, currently under codevelopment and endorsed by Cisco Systems, Microsoft, Ascend, 3Com, and other networking industry leaders.

Key L2TP Terms

L2TP Access Concentrator (LAC). A LAC device is attached to the switched network fabric, such as public switched telephone network (PSTN) or ISDN or colocated with a PPP end system capable of handling the L2TP protocol. A LAC only needs to implement the media, over which L2TP operates in order to pass traffic to one or more LNSs. It may tunnel any protocol carried within PPP. LAC is the initiator of incoming calls and the receiver of outgoing calls. It is also known as the network access server in Layer 2 Forwarding (L2F).

L2TP Network Server (LNS). An LNS operates on any platform capable of PPP termination. LNS handles the server side of the L2TP protocol. Since L2TP relies only on the single media over which L2TP tunnels arrive, LNS may only have a single LAN or WAN interface, yet still be able to terminate calls arriving at any LACs full range of PPP interfaces (async, ISDN, PPP over ATM, PPP over Frame Relay). It is the initiator of outgoing calls and the receiver of incoming calls. LNS is also known as Home Gateway (HGW) in L2F terminology.

Network Access Server. This device provides 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.

Cisco Access VPN Features at a Glance

Cisco provides customers with a broad range of technologies to simplify deployment of a complete Access VPN solution:

Layer 2 Tunneling Protocol (L2TP). The Cisco implementation of L2TP support is based on the latest draft of the L2TP standard. Cisco provides full support of standard L2TP features and most of the optional functions. The Cisco implementation of L2TP offers:

- Support for Multiprotocol Environments—L2TP can transport any routed protocols, including IP, IPX, and Appletalk.
- Media Independent—In Cisco implementation of L2TP it operates on any network capable of delivering IP frames. It supports any WAN backbone technology, including Frame Relay, ATM, X.25, or SONET. It also supports LAN media such as Ethernet, Fast Ethernet, Token Ring, and FDDI.

Security. L2TP is a tunneling protocol that supports tunnel and user authentication. For additional Access VPN security protection, Cisco offers:

- *Authentication, Authorization, and Accounting (AAA)*, including:
 - Support for username/password or Dialed Number Identification Service (DNIS) to determine authorization of the Access VPN services.
 - User authentication support includes PAP, CHAP, MS-CHAP (MD4-CHAP), and One-Time Password.
 - Per-user configuration support, including per-user provisioning of IP address assignment, static routes, and access filters.
 - Accounting that can be performed on the LAC and the LNS includes connection, start/stop, and full logging information of failed connection attempts.
 - RADIUS and TACACS+ support.
 - AAA support and CiscoSecure global roaming server (GRS), providing proxy and translation of Access-VPN roaming user authentication.
- *IPSec*—IPSec provides data confidentiality, integrity, and authenticity among participating peers in a network. Cisco provides full encapsulating security payload (ESP) and authentication header (AH) support. IPSec is available from Cisco on network access servers such as the AS5300 and AS5800; router platforms such as the 1600 through 7500; and the PIX—firewall. IPSec is also available on Windows 95 and Windows NT 4.0 with the RavlinSoft IPSec software.
- *IKE*—The Internet Security Association Key Management Protocol formally known as ISAKMP/Oakley provides security association management. IKE authenticates each peer in an IPSec transaction, negotiates security policy, and handles the session keys exchange. Cisco has been leading the IKE standardization effort.
- *Cisco Encryption Technologie (CET)*—CET is the original network-based encryption solution.
- *Certificate Management*—Cisco fully supports the use of X.509-V3 certificates for device authentication as required by IKE.
- *Cisco IOS Firewall Feature Set*—Cisco IOS Firewall feature is a value-added option of Cisco IOS software that builds on the strength of existing Cisco IOS security capabilities. The Cisco IOS Firewall feature set includes context based-access control (CBAC), which secures traffic flow by tracking the state and context of network connections. It also includes Java blocking, which controls downloading of potentially malicious applets; denial-of-service detection and prevention; real-time alerts; and UDP transaction logs that track user access by source/destination address and port pair.
- *Quality of Service*—Cisco IOS software supports IP precedence, priority queuing, custom queuing, WFQ, WRR, GTS, CAR, fragmentation & interleaving, ABR, WRED, IP precedence, and BGP4 precedence propagation. Leveraging IP precedence, with multiple tunnels to a given LNS, service providers can offer enterprise users differentiated tunnels with varying bandwidth levels.

- *Address Allocation and Management*—L2TP provides full support of dynamic IP address allocation from an IP address pool maintained by the enterprise, including full support of the private addresses defined in RFC 1918. L2TP also supports dynamic address allocation from the DHCP server. Cisco IOS software supports network address translation (NAT) while preventing internal “inside addresses” from being published to the outside world.
- *Reliability*—The Cisco L2TP implementation provides a backup capability, allowing multiple LNS peers to be configured with backup LNSs. If the connection to the primary LNS is unreachable, the NAS (LAC) will establish a connection with a backup LNS.
- *Scalability*—The Cisco L2TP implementation supports unlimited sessions on each LAC and can support more than 2000 sessions per each LNS on a Cisco router platform. More than 8000 sessions support on the Cisco 6400 Universal Access Concentrator (UAC) provides massive scalability for large ISPs, Internet wholesalers, and corporations.
When using the Cisco L2TP implementation load sharing and stackable LNS features, multiple LNSs can perform load-sharing across multiple tunnel connections between one LAC and the LNSs. The statistical load sharing capability across multiple LNSs provides added reliability and scalability. The stackable LNS feature has additional support for multilink PPP sessions. One of the LNSs will take responsibility for assembling segmented packets for each session across the multiple tunnels.
- *Management*—For enhanced fault management, the Cisco L2TP implementation includes support for the L2TP SNMP MIB prior to the availability of the IETF standard MIB. MIB support provides full failure code and reports reasons for disconnect. L2TP also includes a full suite of messages that can be sent to a syslog server. This set of capabilities provides a full end-to-end troubleshooting solution for Access VPNs built on L2TP.

L2TP Access VPN Architecture

- In a dial environment, an L2TP tunnel can be initiated from a Network Access Server (NAS) as a NAS-initiated tunnel or from 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 LNSs. 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.

Benefits

Because L2TP is a standard protocol, all customers—service providers and corporate network managers alike—can enjoy a wide range of service offerings available from multiple vendors. Interoperability among the vendors will help ensure rapid international deployment of a standard Access VPN service.

The Cisco L2TP implementation is a solution that provides a long list of benefits to enterprise users. These benefits include:

- Security and guaranteed priority for their most mission-critical applications
- Improved connectivity, reduced costs, and freedom to refocus resources on core competencies
- Flexible, scalable remote network access environment without compromising corporate security or endangering mission-critical applications

Service providers gain the following benefits from Access VPNs built on a foundation of Cisco IOS software that incorporates L2TP:

- The ability to provision, bill, and manage Access VPNs that provide a competitive advantage, minimize customer turnover, and increase profitability.
- The flexibility to offer a wide range of VPN services across many different architectures, using the Cisco IOS software implementation of L2TP.
- The capability to provide differentiated services for secure, enterprise-wide remote access using Access VPNs over the public Internet or service provider backbones.

Cisco Access VPN Feature and Benefit Summary

Feature	Benefit
Layer 2 Tunneling protocol (L2TP) L2TP simplifies deployment of Access virtual private networks (VPNs).	Industry-standard Layer 2 tunneling protocol ensures interoperability among vendors, increasing customer flexibility and service availability.
AAA Support Cisco AAA support uses Cisco IOS software and Cisco Secure (RADIUS, TACACS+, and translation services), plus Cisco Global Roaming servers for roaming user authentication.	Provides VPN user authentication, flexible authorization policies and robust accounting through Cisco's leading standard, centralized server packages.
Encryption For protecting sensitive data, Cisco offers a range of encryption technologies, such as IPSec and DES encryption (40 and 56 bits are supported today, with plans for 168-bit support).	Gives enterprises a level of data security that's on par with their private network—even when they're operating Access VPNs using Cisco L2TP and IPSec over the Internet or their service provider's backbone.
Quality of Service Leveraging IP precedence, with multiple tunnels to a given LNS, service provider s can offer enterprise users differentiated tunnels with varying bandwidth levels.	Allows service providers to offer the quality of service guarantees that enterprise users need for mission-critical and latency-sensitive applications.
Reliability With backup LNSs, multiple tunnel peers can be configured. If a connection to a primary LNS is unreachable, the NAS (LAC) will reestablish the connection with the backup LNSs.	Enhances Access VPN reliability and fault tolerance for corporations, while service providers can be sure of meeting their SLA agreements.
Scalability on a Single LNS Cisco L2TP supports unlimited sessions on the LACs and can support more than 2000 sessions on a single LNS on a given Cisco router platform.	Enhances VPN scalability; allows networks to meet large-scale user demand.
Scalability on a Single Site Load sharing across the multiple L2TP tunnels between one LAC and multiple LNSs; the stackable home LNS feature also supports multilink sessions.	Enhanced scalability and performance with minimal intervention from either the enterprise user or the service provider as traffic loads grow.
Address Management Dynamic address allocation and management, including support for DHCP proxy client to the DHCP server and private address usage (RFC 1918).	Eliminates concern about shortage of public IP addresses; use of private address enhances security.
Network Management L2TP SNMP MIB and SYSLOG support (in advance of the availability of the IETF standard MIB).	Simplifies end-to-end troubleshooting from any standard management console.

L2TP Case Studies

These three scenarios explain how enterprise users and service providers can leverage the power and promise of Access VPNs by building with Cisco IOS software using L2TP.


Scenario 1: Cost-Effective Remote Access for an Enterprise Corporation

The rise of telecommuting, the need to conduct business globally, and the value and necessity of creating stronger strategic links with suppliers, customers, and dealers create an enormous demand for remote network access at a large multinational corporation. However, building a dedicated, private remote access infrastructure is expensive. As a result, the company searched for cost-effective alternatives for serving its remote users and partners.

The company turned to its service provider to create an Access VPN to outsource its remote access links. Cisco IOS software with the L2TP feature provides a standards-based platform for the Access VPN by providing the security, reliability, and scalability the company needs to move sensitive internal traffic over the service provider's public infrastructure. The company's service provider used L2TP to differentiate traffic streams between employees and external users of the extranet. L2TP also ensures quality of service for the company's desktop video and mission-critical customer service applications, which needed high priority to ensure reliable performance.

Scenario 2: Competitive Edge for an Internet Service Provider

The need to offer faster Internet services due to the Internet explosion is both a challenge and an opportunity for internet service providers. To accelerate their growth rates and create stronger presences in the highly competitive Internet market, a medium-sized service provider unveils a strategy to add Points of Presence (PoPs) in several new locations to give customers local access from any business location.



The goal of the Internet Service Providers (ISPs) is to build and maintain affordable networks of geographically dispersed PoPs. By outsourcing dial and xDSL access from Internet wholesalers, telcos, Regional Bell Operating companies (RBOC), carriers, or other Service Providers who already have the dispersed PoPs, the medium-sized ISP can build revenue while overcoming resource constraints. These outsourcing services—known as “wholesale Internet” or “wholesale access” —can use L2TP technology to offload Internet dialup network traffic from the service provider’s traditional voice network, creating new revenue streams over existing, underutilized links and offering added flexibility to growing ISPs.

Scenario 3: A Telco Alleviates the Strain of Internet Usage on a Voice Infrastructure

Soaring Internet usage is creating a tremendous burden on the traditional voice network for a large regional telco. The voice network was built for traditional phone conversations typically lasting 3 minutes. Most Internet usage averages more than 30 minutes.

As more corporations seek to deploy VPNs over the Internet, connection duration threatens to increase exponentially, as casual e-mail or Web surfing turns into continuous usage for business applications.

L2TP offers a solid solution for RBOC and telecommunication carriers by enabling them to separate data applications from voice switches and offload data to purpose-built data networks.

Availability and Products Supported for Cisco IOS Software with L2TP

Cisco IOS Version 11.3(5)AA

- L2TP feature is in Cisco IOS software version 11.3(5)AA
- Availability: (shipping August 1998)
- Supported products: Cisco AS5200, AS5300, AS5800, and the 7200 series

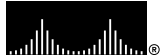
Cisco IOS Version 12.0(1)T

- Availability: (shipping TBD)
- Supported products: Cisco 1600, 2500, 2600, 3600, 4000, 4500, 7500, and UAC 6400

Cisco IOS Images

- 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 supports the L2TP feature.

CISCO SYSTEMS



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

Copyright © 1998 Cisco Systems, Inc. All rights reserved. Printed in USA. AccessPath, AtmDirector, the CCIE logo, CD-PAC, Centri, the Cisco Capital logo, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, the Cisco Press logo, ClickStart, ControlStream, DAGAZ, Fast Step, FireRunner, IGX, JumpStart, Kernel Proxy, LoopRunner, MGX, Natural Network Viewer, NetRanger, NetSonar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RouteStream, Secure Script, SMARTnet, SpeedRunner, Stratin, StreamView, *The Cell*, TrafficDirector, TransPath, VirtualStream, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn and Empowering the Internet Generation are service marks; and BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, Enterprise/Solver, EtherChannel, FastHub, FastPacket, ForeSight, FragmentFree, IPX, LightStream, MICA, Phase/IP, StrataSphere, StrataView Plus, and SwitchProbe are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. 8/98 SP