WHITEPAPER

Lucent Technologies
Bell Labs Innovations

Virtual Private Networking:

Layer Two Tunneling Protocol (L2TP) on Lucent Technologies PortMaster products

Layer Two Tunneling Protocol (L2TP) allows Point-to-Point Protocol (PPP) frames to be encapsulated in an Internet Protocol (IP) packet and tunneled over any IP-based network, including the Internet and Frame Relay or ATM networks. There are two devices used for an L2TP tunnel: the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS).

An L2TP access concentrator is attached to a switched network fabric, such as the Public Switched Telephone Network (PSTN), or co-located with a PPP end-point capable of handling L2TP sessions. It handles calls from remote sites and encapsulates PPP frames within L2TP packets, including any protocol carried within PPP. It then passes tunneled traffic to one or more L2TP network servers over an IP-based transport (the Internet, Frame Relay, ATM) chosen by the service provider.

Optimizing Voice and Data Networks

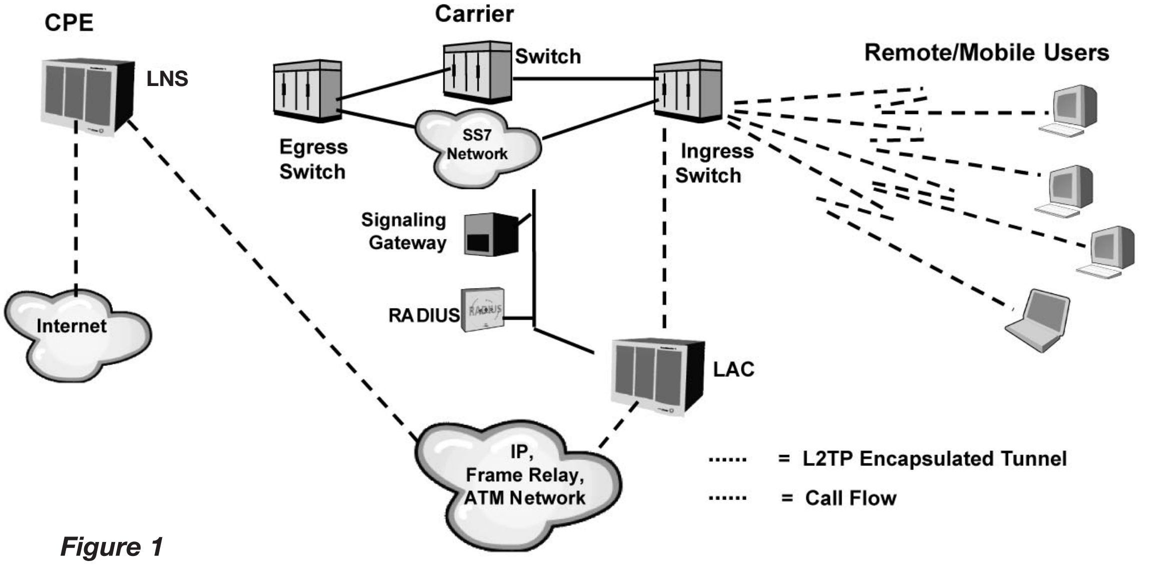


Figure 1

- ***30% of traditional switch traffic is data (Source: BellCore)***
- ***Higher call completion rate with IP/SS7 Network Integration***

The L2TP network server handles the server side of L2TP tunnels; hence, scalability and performance are critical. As the L2TP tunnels arrive over a single transport, the LNS may have only a single LAN or WAN interface, while still terminating calls that arrive at the LAC on any of its interfaces (async, ISDN, ATM, Frame Relay). The LNS de-encapsulates the L2TP packets, processes PPP frames and routes them onto the local area network.

L2TP Applications

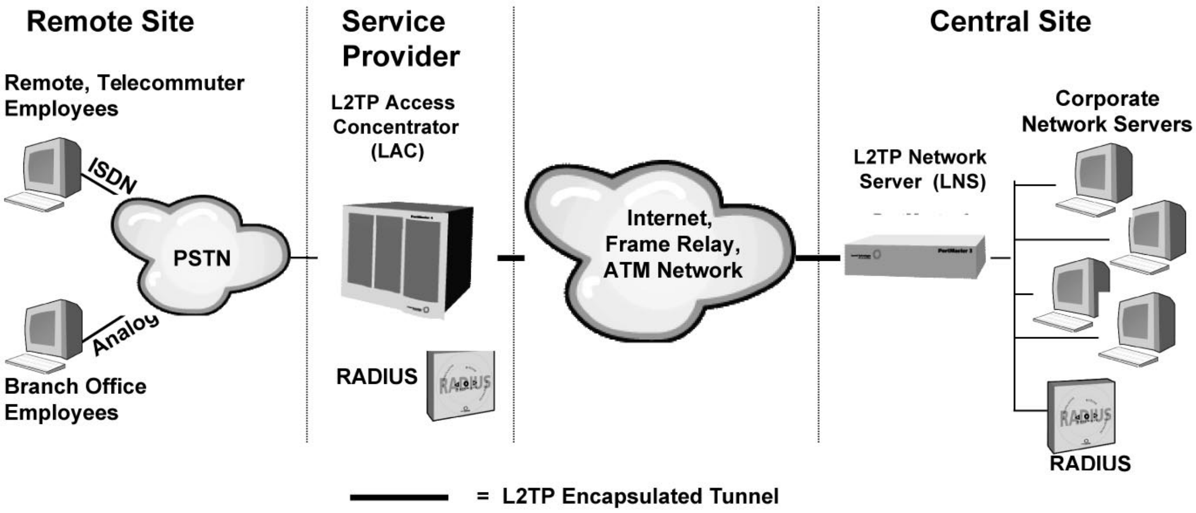
Remote Access Outsourcing. This application uses the existing network infrastructure of a larger service provider to offer remote access termination services to customers, with data traveling between the larger provider and the customer through an L2TP tunnel. The customer thus requires less equipment, saves associated costs, and can focus more on service creation.

Optimization of Network Infrastructures. L2TP-based Virtual Private Networks facilitate strategies that move data traffic off the voice switched network, maintaining performance of the voice network and network infrastructure utilization overall.

Feature Services. L2TP enables the delivery of value-added services such as IP multicasting and low-latency IP service classes, supporting applications like video conferencing, Internet call waiting and other managed voice/data applications.

Business to Business Services. Content hosting for intranets and extranets, along with integrated intranet and extranet applications is also facilitated by L2TP. Once the Public Key Infrastructure (PKI) is in place, non-repudiation and directory services will support electronic commerce over the Internet.

L2TP with PortMaster


Remote Site
Remote, Telecommuter Employees
ISDN
PSTN
Analog
Branch Office Employees
Service Provider
L2TP Access Concentrator (LAC)
RADIUS
Internet, Frame Relay, ATM Network
Central Site
Corporate Network Servers
L2TP Network Server (LNS)
RADIUS
= L2TP Encapsulated Tunnel

PortMaster 4 as L2TP Access Concentrator (LAC)

IETF-compliant LAC functionality on Lucent Technologies PortMaster 4 remote access concentrators is enabled in software, beginning with ComOS® 4.1. In this application, the PortMaster 4 can support up to 864 simultaneous L2TP tunnels.

The PortMaster 4's next-generation, distributed processing architecture makes it ideally suited for LAC applications. It delivers any service, any port, any time flexibility – terminating analog, ISDN, leased line and Frame Relay connections – combined with linearly scalable high-performance and carrier-class reliability.

Lucent's robust ComOS® routing engine allows routes to be configured statically or learned through support for a variety of dynamic routing protocols. For example, Open Shortest Path First (OSPF) support ensures efficient allocation of scarce IP addresses, while Border Gateway Protocol version 4 (BGP4) support permits multi-homing to maintain connections to multiple Internet service providers.

PortMaster 4 as L2TP Network Server (LNS)

Because terminating L2TP tunnels is highly CPU intensive, Lucent developed a purpose-built LNS card for the PortMaster 4. Every card added to the PortMaster 4's ten slot chassis adds processing power, therefore linear scalability and high performance are maintained. As with all Lucent PortMaster hardware, the LNS Card is configured and managed using Lucent Technologies PMVision™ management software.

Each LNS card supports 500 L2TP session terminations. A PortMaster 4 can be configured with eight LNS cards, one System Manager module and one WAN interface card, to support 4,000 session terminations per chassis. As five PortMaster 4 chassis can be stacked in a standard 7' rack, up to 28,000 L2TP sessions can be terminated in a limited amount of floor space.

PortMaster 3 VPN Support

Lucent Technologies PortMaster 3 supports IETF Draft 13 compliant L2TP tunneling in software, with ComOS® 3.9 and above. Acting as an LNS, the PortMaster 3 can terminate up to 64 simultaneous session per chassis. Additional LNS termination capabilities can be attained with software upgrades.

Because software-only secure VPN (IPSec) solutions do not scale well nor meet the performance requirements of typical network implementations, Lucent also offers an optional IPSec encryption daughter card to deliver near wire-speed 56-bit Data Encryption Standard (DES) and/or 168-Bit Triple DES encryption with MD-5 Authentication in Encapsulated Security Payload (ESP) mode.

PortMaster 4 LNS Card Specifications

- 500 L2TP Network Server (LNS) session/tunnel terminations per card
- Support for IETF L2TP RFC Internet Draft draft-ietf-pppext-12rp-13; IPIP tunneling (IETF RFC 2003), and IP Encapsulation within IP (IPIP)
- Stac LZS & MS Stac hardware compression
- 32MB non parity 72 pin SIMM
- 30 watts power consumption

PortMaster 3 VPN Specifications

Optional IPSec Encryption Acceleration daughter card; 100 MIPS processor, 1.1 Mbps ESP Mode at small packet sizes, 1.5 Mbps ESP Mode at large packet sizes

IETF L2TP RFC Internet draft-ietf-pppext-12rp-13;

IETF IPSec RFC drafts including:

- RFC 2104 – HMAC: Keyed Hashing for Message Authentication
- RFC 2401 – Security Architecture for the Internet protocol
- RFC 2402 – IP Authentication header
- RFC 2403 – Use of HMAC-MD5-96 within ESP and AH
- RFC 2404 – Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405 – ESP DES-CBC Cipher Algorithm with Explicit IV
- RFC 2406 – IP Encapsulating Security Payload(ESP)
- RFC 2451 – ESP CBC-Mode Cipher Algorithms
- RFC 2003 – IPIP Tunneling IP Encapsulation within IP (IPIP)

PMVision is a trademark and ComOS and PortMaster are registered trademarks of Lucent Technologies. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to these products and services.

Lucent Technologies
Remote Access Business Unit
4464 Willow Road
Pleasanton, California 94588-8519
Tel: (888) 303-9919 or (925) 730-2500 Fax: (925) 730-2510
www.lucent.com/dns

Printed in the USA 04/99

Lucent Technologies
Bell Labs Innovations