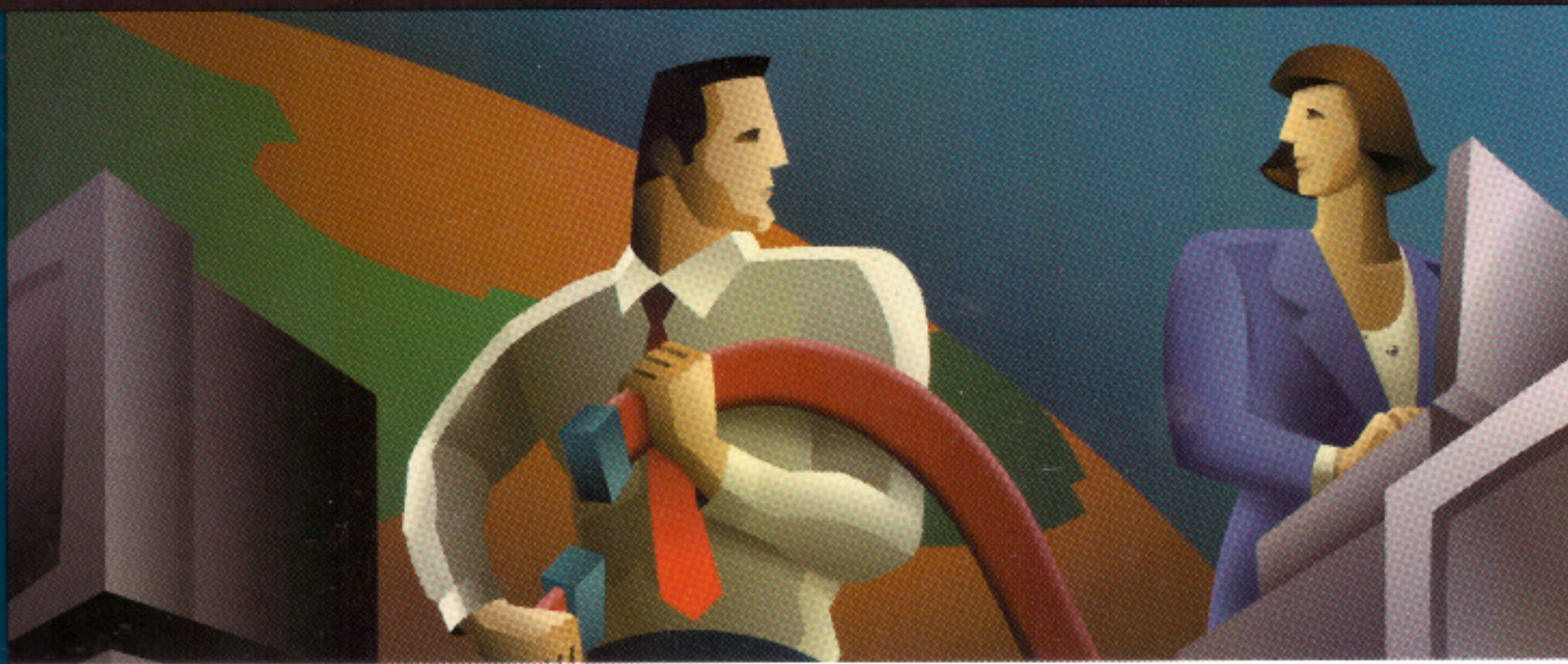




Internetworking Technologies Handbook

Third Edition

An essential reference for every network professional

ciscopress.com

Internetworking Technologies Handbook

Third Edition

Cisco Systems, et. al.

Copyright© 2001 Cisco Systems, Inc.

Published by:

Cisco Press

201 West 103rd Street

Indianapolis, IN 46290 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America 5 6 7 8 9 0

Fifth Printing December 2001

Library of Congress Cataloging-in-Publication Number: 00-105-169

ISBN: 1-58705-001-3

Warning and Disclaimer

This book is designed to provide information about **Internetworking Technologies**. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The author, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Publ
Exec
Man
Cisco

Acq
Pro
Cop
Tech

Boo
Cov
Com
Inde

Corporate
Cisco Sys
170 West
San Jose,
USA
<http://www>
Tel: 408
800
Fax: 408

Cisco Sys

Argentina
Brazil • C
Hong •
Mexico •
Romania
• Switzer
• Zimbab

Copyright © 2001
Cisco Press, Inc.
All rights reserved.
No part of this book
may be reproduced
without written
permission from
Cisco Press, Inc.

CHAPTER 18

Virtual Private Networks

Background

Virtual private networks (VPNs) are a fairly quixotic subject; there is no single defining product, nor even much of a consensus among VPN vendors as to what comprises a VPN. Consequently, everyone knows what a VPN is, but establishing a single definition can be remarkably difficult. Some definitions are sufficiently broad as to enable one to claim that Frame Relay qualifies as a VPN when, in fact, it is an overlay network. Although an overlay network secures transmissions through a public network, it does so passively via logical separation of the data streams.

VPNs provide a more active form of security by either encrypting or encapsulating data for transmission through an unsecured network. These two types of security—encryption and encapsulation—form the foundation of virtual private networking. However, both *encryption* and *encapsulation* are generic terms that describe a function that can be performed by a myriad of specific technologies. To add to the confusion, these two sets of technologies can be combined in different implementation topologies. Thus, VPNs can vary widely from vendor to vendor.

This chapter provides an overview of building VPNs using the Layer 2 Tunneling Protocol (L2TP), and it explores the possible implementation topologies.

Layer 2 Tunneling Protocol

The Internet Engineering Task Force (IETF) was faced with competing proposals from Microsoft and Cisco Systems for a protocol specification that would secure the transmission of IP datagrams through uncontrolled and untrusted network domains. Microsoft's proposal was an attempt to standardize the Point-to-Point Tunneling Protocol (PPTP), which it had championed. Cisco, too, had a protocol designed to perform a similar function. The IETF combined the best elements of each proposal and specified the open standard L2TP.

The simplest description of L2TP's functionality is that it carries the *Point-to-Point Protocol (PPP)* through networks that aren't point-to-point. PPP has become the most popular communications protocol for remote access using circuit-switched transmission

facilities such as POTS lines or ISDN to create a temporary point-to-point connection between the calling device and its destination.

L2TP simulates a point-to-point connection by encapsulating PPP datagrams for transportation through routed networks or internetworks. Upon arrival at their intended destination, the encapsulation is removed, and the PPP datagrams are restored to their original format. Thus, a point-to-point communications session can be supported through disparate networks. This technique is known as *tunneling*.

Operational Mechanics

In a traditional remote access scenario, a remote user (or client) accesses a network by directly connecting a *network access server (NAS)*. Generally, the NAS provides several distinct functions: It terminates the point-to-point communications session of the remote user, validates the identity of that user, and then serves that user with access to the network. Although most remote access technologies bundle these functions into a single device, L2TP separates them into two physically separate devices: the *L2TP Access Server (LAS)* and the *L2TP Network Server (LNS)*.

As its names imply, the L2TP Access Server supports authentication, and ingress. Upon successful authentication, the remote user's session is forwarded to the LNS, which lets that user into the network. Their separation enables greater flexibility for implementation than other remote access technologies.

Implementation Topologies

L2TP can be implemented in two distinct topologies:

- Client-aware tunneling
- Client-transparent tunneling

The distinction between these two topologies is whether the client machine that is using L2TP to access a remote network is aware that its connection is being tunneled.

Client-Aware Tunneling

The first implementation topology is known as client-aware tunneling. This name is derived from the remote client initiating (hence, being "aware" of) the tunnel. In this scenario, the client establishes a logical connection within a physical connection to the LAS. The client remains aware of the tunneled connection all the way through to the LNS, and it can even determine which of its traffic goes through the tunnel.

Client-Transparent Tunneling

Client-transparent tunneling features L2TP access concentrators distributed geographically close to the remote users. Such geographic dispersion is intended to reduce the long-distance telephone charges that would otherwise be incurred by remote users dialing into a centrally located LAC.

The remote users need not support L2TP directly; they merely establish a point-to-point communication session with the LAC using PPP. Ostensibly, the user will be encapsulating IP datagrams in PPP frames. The LAC exchanges PPP messages with the remote user and establishes an L2TP tunnel with the LNS through which the remote user's PPP messages are passed.

The LNS is the remote user's gateway to its home network. It is the terminus of the tunnel; it strips off all L2TP encapsulation and serves up network access for the remote user.

Adding More Security

As useful as L2TP is, it is important to recognize that it is not a panacea. It enables flexibility in delivering remote access, but it does not afford a high degree of security for data in transit. This is due in large part to the relatively nonsecure nature of PPP. In fairness, PPP was designed explicitly for point-to-point communications, so securing the connection should not have been a high priority.

An additional cause for concern stems from the fact that L2TP's tunnels are not cryptographic. Their data payloads are transmitted in the clear, wrapped only by L2TP and PPP framing. However, additional security may be afforded by implementing the IPSec protocols in conjunction with L2TP. The IPSec protocols support strong authentication technologies as well as encryption.

Summary

VPNs offer a compelling vision of connectivity through foreign networks at greatly reduced operating costs. However, the reduced costs are accompanied by increased risk. L2TP offers an open standard approach for supporting a remote access VPN. When augmented by IPSec protocols, L2TP enables the realization of the promise of a VPN: an open standard technology for securing remote access in a virtually private network.

Review Questions

Q—*What is a VPN?*

A—A VPN is a generic term that describes any combination of technologies that can be used to secure a connection through an otherwise unsecured or untrusted network.

Q—*Explain the difference between L2TP's LAC and LSN.*

A—The LAC provides authentication and access concentration for remote users. After a remote user is authenticated, that user's communications session is then forwarded to the LSN, which provides access to that user's home network.

Q—*What additional functionality does IPSec offer an L2TP implementation?*

A—L2TP's native security mechanisms build on the assumption that the nature of a point-to-point connection satisfies most of a remote user's security requirements. IPSec complements L2TP by offering a more robust set of technologies for authenticating remote users and for securing data in transit through foreign networks by encrypting data.

Q—*What is a tunnel?*

A—A tunnel is a logical structure that encapsulates the frame and data of one protocol inside the Payload or Data field of another protocol. Thus, the encapsulated data frame may transit through networks that it would otherwise not be capable of traversing.

For More Information

For more information about L2TP and virtual private networking, refer to the following sources of information:

- Black, Ulysses. *PPP and L2TP: Remote Access Communications*. Prentice Hall: New York, 1999.
- Shea, Richard. *L2TP Implementation and Operation*. Addison Wesley Longman: Boston, 1999.
- RFC 2401, "Security Architecture for the Internet Protocol"
- RFCs 2402 through 2410 (various IPSec specifications)
- RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP"
- RFC 2408, "Internet Security Association and Key Management Protocol (ISAKMP)"
- <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120tl/12tpt.htm>
- <http://www.cisco.com/warp/public/707/24.html>