Comparing, Designing, and Deploying VPNs
By Mark Lewis, - CCIE No. 6280
.....
Publisher: **Cisco Press**
Pub Date: **April 12, 2006**
Print ISBN-10: **1-58705-179-6**
Print ISBN-13: **978-1-58705-179-1**
Pages: **1080**

Table of Contents | Index

Overview

A practical guide for comparing, designing, and deploying IPsec, MPLS Layer 3, L2TPv3, L2TPv2, AToM, and SSL virtual private networks

- Explore the major VPN technologies and their applications, design, and configurations on the Cisco IOS® Router, Cisco® ASA 5500 Series, and the Cisco VPN 3000 Series Concentrator platforms
- Compare the various VPN protocols and technologies, learn their advantages and disadvantages, and understand their real-world applications and methods of integration
- Find out how to design and implement Secure Socket Layer (SSL) VPNs, including consideration of clientless operation, the Cisco SSL VPN Client, the Cisco Secure Desktop, file and web server access, e-mail proxies, and port forwarding
- Learn how to deploy scalable and secure IPsec and L2TP remote access VPN designs, including consideration of authentication, encryption, split-tunneling, high availability, load-balancing, and NAT transparency
- Master scalable IPsec site-to-site VPN design and implementation including configuration of security protocols and policies, multiprotocol/ multicast traffic transport, NAT/PAT traversal, quality of service (QoS), Dynamic Multipoint VPNs (DMVPNs), and public key infrastructure (PKI)

Virtual private networks (VPNs) enable organizations to connect offices or other sites over the Internet or a service provider network and allow mobile or home-based users to enjoy the same level of productivity as those who are in the same physical location as the central network. However, with so many flavors of VPNs available, companies and providers are often hard pressed to identify, design, and deploy the VPN solutions that are most appropriate for their particular network architecture and service needs.

Comparing, Designing, and Deploying VPNs brings together the most popular VPN technologies for convenient reference. The book examines the real-world operation, application, design, and configuration of the following site-to-site VPNs: Layer 2 Tunneling Protocol version 3 (L2TPv3)-based Layer 2 VPNs (L2VPN); Any Transport over MPLS (AToM)-based L2VPN; MPLS Layer 3-based VPNs; and IP Security (IPsec)-based VPNs. The book covers the same details for the following remote access VPNs: Layer 2 Tunneling Protocol version 2 (L2TPv2) VPNs; L2TPv3 VPNs; IPsec-based VPNs; and Secure Socket Layer (SSL) VPNs. Through the operation, application, and configuration details offered in each chapter, you'll learn how to compare and contrast the numerous types of VPN technologies, enabling you to consider all relevant VPN deployment options and select the VPN technologies that are most appropriate for your network.

Comparing, Designing, and Deploying VPNs begins with an introduction of the types of VPNs available. Subsequent chapters begin with an overview of the technology, followed by an examination of deployment

pros and cons that you can use to determine if the particular VPN technology is appropriate for your network. Detailed discussion of design, deployment, and configuration make up the heart of each chapter. Appendix A offers insight into two multipoint emulated LAN services that can be deployed over a MAN or WAN: Virtual Private LAN Service (VPLS) and IP-only Private LAN Service (IPLS).

If you are a network architect, network engineer, network administrator, an IT manager, or CIO involved in selecting, designing, deploying, and supporting VPNs, you'll find Comparing, Designing, and Deploying VPNs to be an indispensable reference.

This book is part of the Cisco Press® Networking Technology Series, which offers networking professionals valuable information for constructing efficient networks, understanding new technologies, and building successful careers.

Comparing, Designing, and Deploying VPNs
By Mark Lewis, - CCIE No. 6280
.....
Publisher: **Cisco Press**
Pub Date: **April 12, 2006**
Print ISBN-10: **1-58705-179-6**
Print ISBN-13: **978-1-58705-179-1**
Pages: **1080**

Table of Contents | Index

Copyright
About the Author
Acknowledgments
Icons Used in This Book
Command Syntax
Conventions
Introduction
Part I: Understanding
VPN Technology
Chapter 1. What Is a
Virtual Private
Network?
VPN Devices
Deploying
Site-to-Site and
Remote Access
VPNs: A
Comparison
Summary
Review Questions
Part II: Site-to-Site VPNs

Copyright

Comparing, Designing, and Deploying VPNs

Mark Lewis

Published by:

Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing April 2006

Library of Congress Cataloging-in-Publication Number: 2003114910

Trademark Acknowledgments

Corporate and Government Sales

Warning and Disclaimer

Feedback Information

improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher	John Wait
Editor-in-Chief	John Kane
Cisco Representative	Anthony Wolfenden
Cisco Press Program Manager	Jeff Brady
Production Manager	Patrick Kanouse
Senior Development Editor	Christopher Cleveland
Copy Editor and Indexer	Keith Cline
Technical Editors	Henry Benjamin, Lei Chen, Mark Newcomb, Ajay Simha
Book and Cover Designer	Louisa Adair
Composition	Interactive Composition Corporation

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

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

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

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

About the Author

Mark Lewis, CCIE No. 6280, is technical director of MJL Network Solutions (www.mjlnet.com), a leading provider of internetworking solutions that focuses on helping enterprise and service provider customers to implement leading-edge technologies. Mark specializes in next-generation network technologies and has extensive experience designing, deploying, and migrating large-scale IP/MPLS networks. He is an active participant in the IETF, a member of the IEEE, and a certified Cisco Systems instructor. Mark is also the author of Troubleshooting Virtual Private Networks, published by Cisco Press.

Mark can be contacted at mark@mjlnet.com.

About the Technical Reviewers

Henry Benjamin, CCIE No. 4695, holds three CCIE certifications (Routing and Switching, ISP Dial, and Communications and Services). He has more than 10 years experience with Cisco networks and recently worked for Cisco in the internal IT department helping to design and implement networks throughout Australia and Asia. Henry was a key member of the CCIE global team, where he was responsible for writing new laboratory examinations and questions for the CCIE exams. Henry is an independent consultant with a large security firm in Australia. Henry is the author of CCIE Security Exam Certification Guide and CCNP Practical Studies: Routing, both published by Cisco Press.

Lei Chen, CCIE No. 6399, received a master of science degree in computer science from DePaul University in 2000. He joined the Cisco NSITE system testing group in 2000, and then went on to support Cisco high-tier customers as part of the Cisco TAC VPN team in 2002. He has first-hand experience in troubleshooting, designing, and deploying IPsec VPNs.

Mark Newcomb, CCNP, CCDP, is a retired network security engineer. Mark has more than 20 years experience in the networking industry, focusing on the financial and medical industries. Mark is a frequent contributor and reviewer for Cisco Press books.

Ajay Simha, CCIE No. 2970, joined the Cisco TAC in 1996. He then went on to support tier 1 and 2 ISPs as part of the Cisco ISP Expert team. He worked as an MPLS deployment engineer from October 1999 to November 2003. Currently, he is a senior network consulting engineer in Advanced Services at Cisco working on Metro Ethernet and MPLS design and deployment. Ajay is the coauthor of the Cisco Press title Traffic Engineering with MPLS.

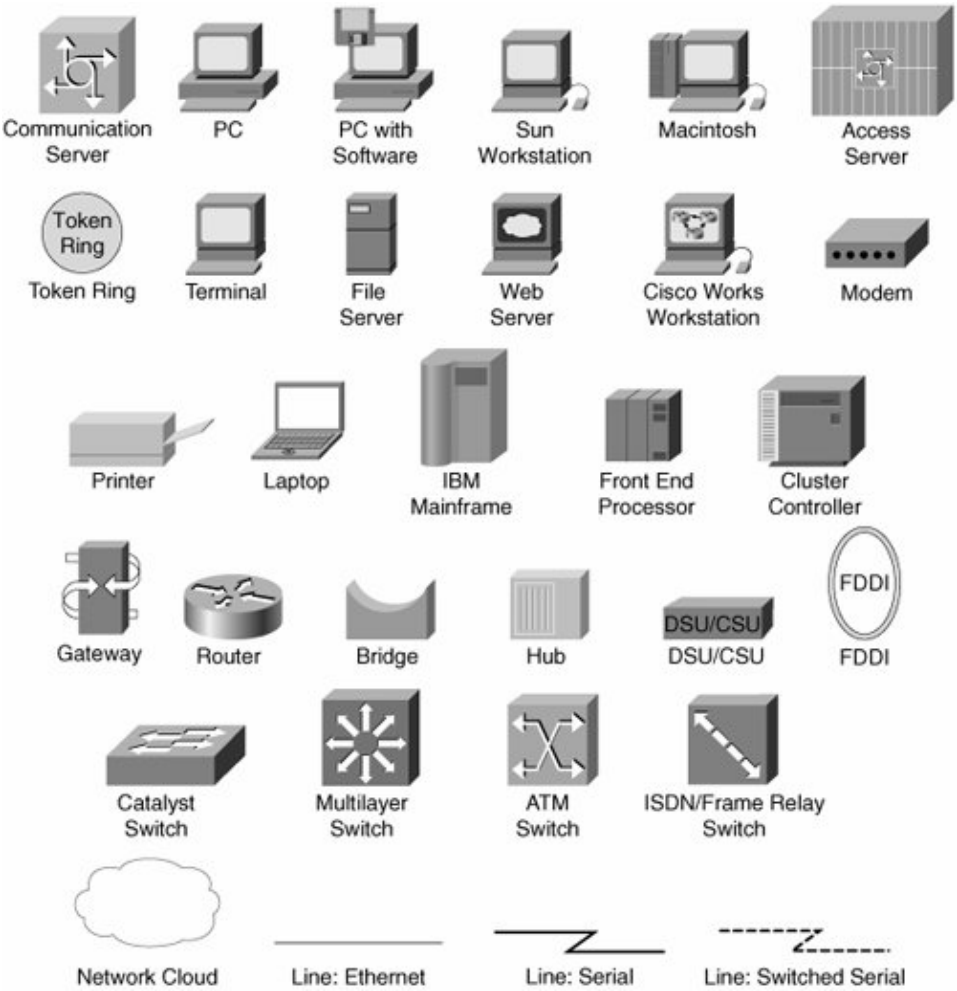
Acknowledgments

I'd like to thank a number of people who helped me to complete this book. I'd like to thank Michelle, Chris, John, and Patrick at Cisco Press, who helped to get this project started in the first place and then provided indispensable help and encouragement along the way.

And I'd also like to thank the technical reviewersMark Newcomb, Henry Benjamin, Ajay Simha, and Lei Chenwho all provided useful comments and suggestions.

Icons Used in This Book

[View full size image]



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the Cisco IOS Command Reference. The Command Reference describes these conventions as follows:

- Boldface indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a show command).
- Italics indicate arguments for which you supply actual values.
- Vertical bars | separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Introduction

As the number and sophistication of virtual private network (VPN) technologies has grown, the complexity of choice, design, and deployment has also increased.

It is now possible to implement site-to-site VPNs, remote access VPNs, LAN-to-LAN VPNs, trusted VPNs, secure VPNs, L1VPNs, L2VPNs, L3VPNs, VPWS VPNs, VPLS VPNs, IPLS VPNs, network-based VPNs, C(P)E-based VPNs, multiservice VPNs, provider-provisioned VPNs, customer-provisioned VPNs, Internet VPNs, intranet VPNs, extranet VPNs, point-to-point VPNs, multipoint-to-multipoint VPNs, overlay VPNs, peer (-to-peer) VPNs, connection-oriented VPNs, connectionless VPNs, and clientless VPNs.

And then there are L2TPv3-based VPNs, AToM-based VPNs, MPLS Layer 3 VPNs, L2F VPNs, L2TPv2 VPNs, PPTP VPNs, and SSL VPNs.

No wonder VPNs can be confusing!

This book shows you how to navigate the spaghetti soup of VPN terminology and acronyms and how to differentiate and select the appropriate VPN type.

But, the ability to differentiate and select the appropriate VPN type is not enough! After you have decided which VPN type is appropriate, the next steps are its design and deployment.

Thankfully, this book also steers you through the design and deployment phases and shows you how each individual VPN technology works in detail, what its capabilities are, how it can be configured, and what the advanced design and implementation considerations are.

Motivation for the Book

Although existing material describes the various VPN technologies, it became obvious to me that a requirement exists for a single book that not only clarifies the differences between the various VPN types and technologies but also describes those various VPN technologies in detail. Hopefully, this book fulfills that requirement and clears up a lot of the confusion that has hitherto existed with regard to VPNs.

Who Should Read This Book?

In this book, you will find in-depth coverage of site-to-site VPN technologies such as L2TPv3, AToM, MPLS Layer 3 (RFC2547bis) VPNs, IPsec, VPLS, and IPLS. You will also find detailed examinations of remote access VPN technologies, including L2TPv2/3, IPsec, and SSL. In addition, you will find information about how to integrate remote access VPN technologies with site-to-site VPNs.

So, who will find this breadth and depth of VPN technology coverage useful? It will be very useful to network architects, network implementation engineers, network support staff, and IT manager/CIOs involved with selecting, designing, deploying, and supporting VPNs. It will also be helpful to people preparing for networking tests such as the Security and Service Provider CCIE exams.

How This Book Is Organized

This book is organized such that it can either be dipped into for information on a specific VPN type or it can be read from cover to cover.

If you are in the process of comparing and evaluating different VPN types with a view to their deployment in your network, or are preparing for a networking exam that includes coverage of VPN technologies, you may want to read Chapter 1 (which gives a high-level comparison), followed by one or more of the following chapters that deal with specific VPN technologies.

If, on the other hand, you are looking to improve and deepen your knowledge of VPN technologies in general, you might want to read the book cover to cover.

The book is arranged as follows:

- Chapter 1, "What Is a VPN?" Chapter 1 poses (and answers) the deceptively simple question "What is a VPN?" In this chapter, you will find a high-level discussion and comparison of the various VPN types and technologies, which will clarify what the various VPN terms mean and how the technologies work. By the end of this chapter, the previously confused will be a lot more clear about what a VPN really is.
- Chapter 2, "Designing and Deploying L2TPv3-Based Layer 2 VPNs (L2VPN)" L2TP has evolved from a tunneling protocol for PPP to become, in its latest incarnation (L2TPv3), a universal transport mechanism for a host of protocols such as Ethernet, Frame Relay, ATM (cell-relay and AAL5), HDLC, and PPP. This chapter discusses in-depth L2TPv3's advantages and disadvantages, how it operates, and how L2TPv3-based Layer 2 VPNs can be designed and deployed.
- Chapter 3, "Designing and Implementing AToM-Based Layer 2 VPNs (L2VPN)" Any Transport over MPLS (AToM) provides a similar transport mechanism to L2TPv3, but over MPLS rather than IP. It, too, can transport protocols including Ethernet, Frame Relay, and ATM, and as such can be used to consolidate service provider networks and build Layer 2 VPNs. AToM's underlying technology, configuration, verification, and advanced design considerations are examined in this chapter.
- Chapter 4, "Designing MPLS Layer 3 Site-to-Site VPNs" MPLS Layer 3 VPNs provide a highly scalable VPN architecture that provides any-to-any connectivity and can support real-time applications such as voice and video. This chapter provides a detailed discussion of the principles of its operation, its configuration, the provision of complex topologies, and Internet access.
- Chapter 5, "Advanced MPLS Layer 3 VPN Deployment Considerations" Building on the foundation of Chapter 4, this chapter describes how MPLS Layer 3 VPNs can be extended to support carrier customers, interprovider and inter-autonomous system VPNs, QoS, and customer IPv6 VPNs.
- Chapter 6, "Deploying Site-to-Site IPsec VPNs" IPsec remains a popular choice for implementing site-to-site VPNs. In this chapter, you can find a description of the algorithms and mechanisms that underlie IPsec, together with an in-depth discussion of the fundamentals of IPsec site-to-site VPN configuration using preshared key, encrypted nonce, and digital certificate authentication. Also included is detailed information about issues with IPsec and NAT (and how to get around them).
- Chapter 7, "Scaling and Optimizing IPsec VPNs" This chapter builds on the discussion of the fundamentals of site-to-site IPsec VPNs in Chapter 6 by describing their scaling and optimization. Specific topics covered include Tunnel Endpoint Discovery (TED), Dynamic Multipoint VPN (DMVPN), scaling IPsec VPNs using digital signature authentication, quality of service (QoS), and avoiding the performance degradation caused by IPsec packet fragmentation.
- Chapter 8, "Designing and Implementing L2TPv2 and L2TPv3 Remote Access VPNs" L2TP can be used to implement industry-standard remote access VPNs. This chapter provides comprehensive information about designing and deploying L2TP voluntary tunnel mode/client-initiated and compulsory tunnel mode/NAS-initiated remote access VPNs. Methods of securing L2TP remote access VPNs using IPsec as well as the integration of L2TP remote access VPNs with MPLS Layer 3 VPNs are also discussed.
- Chapter 9, "Designing and Deploying IPsec Remote Access and Teleworker VPNs" IPsec can not only be used to provision site-to-site VPNs, but can also be used to implement remote access VPNs. A thorough description of their design and deployment is included in this chapter. The chapter describes configuration as well as special considerations, including the integration of IPsec remote access VPNs with MPLS Layer 3 VPNs, provisioning high availability, and allowing or disallowing split tunneling.
- Chapter 10, "Designing and Building SSL Remote Access VPNs (WebVPN)" Although SSL is a relative newcomer as a VPN technology, it can provide significant advantages, especially if remote access users need to access the corporate network from insecure locations such as Internet cafés and airport kiosks.

In this chapter, you will find detailed information on designing and deploying both clientless remote access SSL VPNs, and SSL remote access VPNs using the Cisco SSL VPN Client. Also included is an examination of the Cisco Secure Desktop, which enables users to greatly improve the security of SSL VPN connections from insecure locations.

- Appendix A, "VPLS and IPLS Layer 2 VPNs" This appendix describes two VPN technologies that provide multipoint Ethernet connectivity for customer sites. VPLS provides multipoint, multiprotocol connectivity, but does involve a relatively high degree of complexity; whereas IPLS provides multipoint, IP-only connectivity with a lower degree of complexity.
- Appendix B, "Answers to Review Questions" You will find the answers to the review questions at the end of each chapter here.

Part I: Understanding VPN Technology

Chapter 1. What Is a Virtual Private Network?

A virtual private network (VPN) allows the provisioning of private network services for an organization or organizations over a public or shared infrastructure such as the Internet or service provider backbone network. The shared service provider backbone network is known as the VPN backbone and is used to transport traffic for multiple VPNs, as well as possibly non-VPN traffic.

VPNs provisioned using technologies such as Frame Relay and Asynchronous Transfer Mode (ATM) virtual circuits (VC) have been available for a long time, but over the past few years IP and IP/Multiprotocol Label Switching (MPLS)-based VPNs have become more and more popular.

This book focuses on describing the deployment of IP- and IP/MPLS-based VPNs.

The large number of terms used to categorize and describe the functionality of VPNs has led to a great deal of confusion about what exactly VPNs are and what they can do. The sections that follow cover VPN devices, protocols, technologies, as well as VPN categories and models.

VPN Devices

Before describing the various VPN technologies and models, it is useful to first describe the various customer and provider network devices that are relevant to the discussion.

Devices in the customer network fall into one of two categories:

- Customer (C) devices C devices are simply devices such as routers and switches located within the customer network. These devices do not have direct connectivity to the service provider network. C devices are not aware of the VPN.
- Customer Edge (CE) devices CE devices, as the name suggests, are located at the edge of the customer network and connect to the provider network (via Provider Edge [PE] devices).

  In CE-based VPNs, CE devices are aware of the VPN. In PE-based VPNs, CE devices are unaware of the VPN.

  CE devices are either categorized as Customer Edge routers (CE-r), or Customer Edge switches (CE-s).

In a site-to-site VPN, devices in the service provider network also fall into one of two categories:

- Service Provider (P) devices P devices are devices such as routers and switches within the provider network that do not directly connect to customer networks. P devices are unaware of customer VPNs.
- Service Provider Edge (PE) devices PE devices connect directly to customer networks via CE devices. PE devices are aware of the VPN in PE-based VPNs, but are unaware of the VPN in CE-based VPNs.

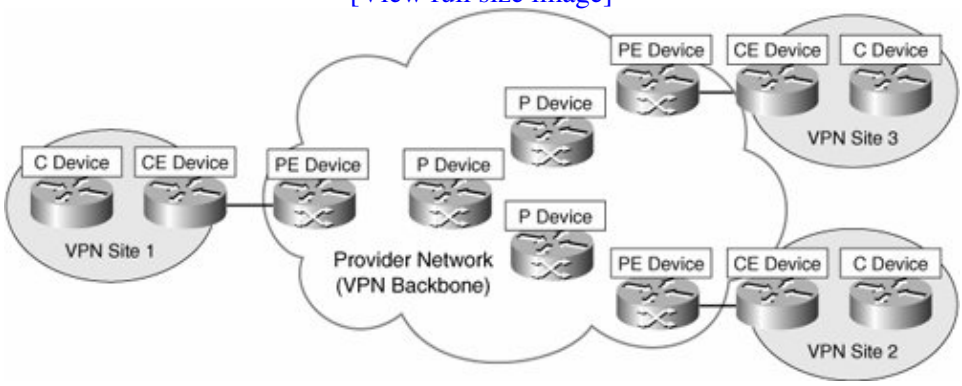
  There are three types of PE device:

  - Provider Edge routers (PE-r)
  - Provider Edge switches (PE-s)
  - Provider Edge devices that are capable of both routing and switching (PE-rs)

Figure 1-1 illustrates customer and provider network devices.

Figure 1-1. Customer and Provider Network Devices

[View full size image]

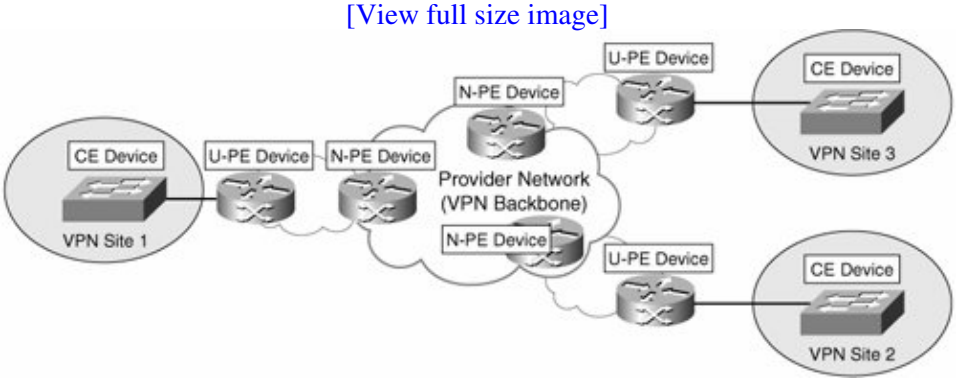


In Layer 2 VPNs, such as a Virtual Private LAN Service (VPLS), an additional level of hierarchy can be introduced into the network to improve scalability (VPLS then becomes Hierarchical VPLS [H-VPLS]). In this case, the functionality of the PE device is divided between a User-facing PE (U-PE) devices and Network-facing PE (N-PE) devices.

Note that alternative (and dated) equivalent terms for the U-PE and N-PE are PE-CLE and PE-POP, respectively. In addition, where a Layer 2 PE-U device is installed in a multitenant building, this may be referred to as an MTU-s. Figure 1-2 illustrates U-PE and N-PE devices.

Figure 1-2. User-Facing and Network-Facing PE Devices

[View full size image]



Other device types used in VPNs include Network Access Servers (NAS) and VPN gateways/concentrators. A NAS is a device that interfaces between an access network (such as a Public Switched Telephone Network [PSTN]) and a packet-switched network (such as an IP backbone). In a remote access VPN, a NAS can serve as a tunnel endpoint.

Note that depending upon the remote access VPN protocol in use, the NAS may variously be called a Layer Two Forwarding (L2F) Protocol NAS, a Layer Two Tunneling Protocol (L2TP) Access Concentrator (LAC), or a Point-to-Point Tunneling Protocol (PPTP) Access Concentrator (PAC).

See Figure 1-5 for an illustration of the role performed by a NAS.

A VPN gateway/concentrator acts as the endpoint of a VPN tunnel, especially in a remote access VPN or CE-based site-to-site VPN. See Figure 1-5 later in the chapter for an illustration of the role performed by a VPN gateway/concentrator.

Depending on the remote access VPN protocol in use, the VPN gateway/concentrator may, for example, be called an L2F Home Gateway, an L2TP Network Server (LNS), or a PPTP Network Server (PNS).

VPN Technologies and Protocols

A number of technologies and protocols are used to enable site-to-site and remote access VPNs. These protocols and technologies are described in the sections that follow.

Technologies and Protocols Used to Enable Site-to-Site VPNs

In site-to-site VPNs (discussed later in this chapter), customer user data traffic is either tunneled between CE devices or between PE devices.

Note

Site-to-site VPNs are also occasionally referred to as LAN-to-LAN VPNs.

Protocols and technologies used to enable site-to-site VPNs include IP Security (IPsec), Generic Routing Encapsulation (GRE), the Layer Two Tunneling Protocol version 3 (L2TPv3), Draft Martini pseudowires

(emulated circuits), IEEE 802.1Q tunneling (Q-in-Q), and MPLS Label Switched Paths (LSP). These protocols and technologies are described as follows:

- IPsec IPsec consists of a suite of protocols designed to protect IP traffic between security gateways or hosts as it transits an intervening network. IPsec tunnels are often used to build a site-to-site between CE devices (CE-based VPNs).
- GRE GRE can be used to construct tunnels and transport multiprotocol traffic between CE devices in a VPN. GRE has little or no inherent security, but GRE tunnels can be protected using IPsec.
- Draft Martini (Any Transport over MPLS [AToM]) Draft Martini transport allows point-to-point transport of protocols such as Frame Relay, ATM, Ethernet, Ethernet VLAN (802.1Q), High-Level Data Link Control (HDLC), and PPP traffic over MPLS.
- L2TPv3 L2TPv3 allows the point-to-point transport of protocols such as Frame Relay, ATM, Ethernet, Ethernet VLAN, HDLC, and PPP traffic over an IP or other backbone.
- IEEE 802.1Q tunneling (Q-in-Q) 802.1Q tunneling allows a service provider to tunnel tagged Ethernet (802.1Q) customer traffic over a shared backbone. Customer 802.1Q traffic is tunneled over the shared provider backbone by prepending another 802.1Q tag.
- MPLS LSPs An LSP is a path via Label Switch Routers (LSR) in an MPLS network. Packets are switched based on labels prepended to the packet. LSPs may be signaled using the Tag Distribution Protocol (TDP), the Label Distribution Protocol (LDP), or the Resource Reservation Protocol (RSVP).

Technologies and Protocols Used to Enable Remote Access VPNs

Protocols used to enable remote access VPNs (discussed later in this chapter) include the following:

- The Layer Two Forwarding (L2F) Protocol L2F is a Cisco proprietary protocol that is designed to allow the tunneling of PPP (or Serial Line Interface Protocol [SLIP]) frames between a NAS and a VPN gateway device located at a central site. Remote access users connect to the NAS, and the PPP frames from the remote access user are then tunneled over the intervening network to the VPN (home) gateway.
- The Point-to-Point Tunneling Protocol (PPTP) PPTP is a protocol that was developed by a consortium of vendors, including Microsoft, 3Com, and Ascend Communications. Like L2F, PPTP allows the tunneling of remote access client PPP frames between a NAS and a VPN gateway/concentrator. PPTP also allows a tunnel to be set up directly from a remote access client to a VPN gateway/concentrator.

  PPP encapsulated packets carried over PPTP tunnels are often protected using Microsoft Point-to-Point Encryption (MPPE).
- The Layer 2 Tunneling Protocol versions 2 and 3 (L2TPv2/L2TPv3) L2TP is an Internet Engineering Task Force (IETF) standard and combines the best features of L2F and PPTP. In a remote access environment, L2TP allows either tunneling of remote access client PPP frames via a NAS to a VPN gateway/concentrator or tunneling of PPP frames directly from the remote access client to the VPN gateway/concentrator.

  L2TP has limited intrinsic security, and so L2TP tunnels are often protected using IPsec.
- IPsec As well as enabling site-to-site VPNs, IPsec can also be used to securely tunnel data traffic between remote access or mobile users and a VPN gateway/concentrator.
- The Secure Sockets Layer (SSL) SSL is a security protocol that was originally developed by Netscape Communications (SSL versions 1, 2, and 3), and it provides secure remote access for mobile users or home users. Functionality may be limited (when compared with L2F, PPTP, L2TPv2, or IPsec) if clientless SSL remote access VPNs are deployed.

  Note that Transport Layer Security (TLS), an IETF standard, is similar to SSLv3.

In spite of the limited functionality provided by clientless SSL VPNs, one advantage of this type of remote access VPN is that no special client software is required because SSL is included in pretty much every web browser. Therefore, if a remote user has a web browser, the user has SSL client software.

Because no special client software is required other than a web browser, SSL VPNs are sometimes referred to as web VPNs or clientless VPNs.

More functionality may be added to SSL VPNs by installing specific SSL VPN client software on remote access client devices.

Modeling and Characterizing VPNs

A plethora of methods are used to model and characterize VPNs. The purpose of this section is to introduce and explain each of these models and characterizations.

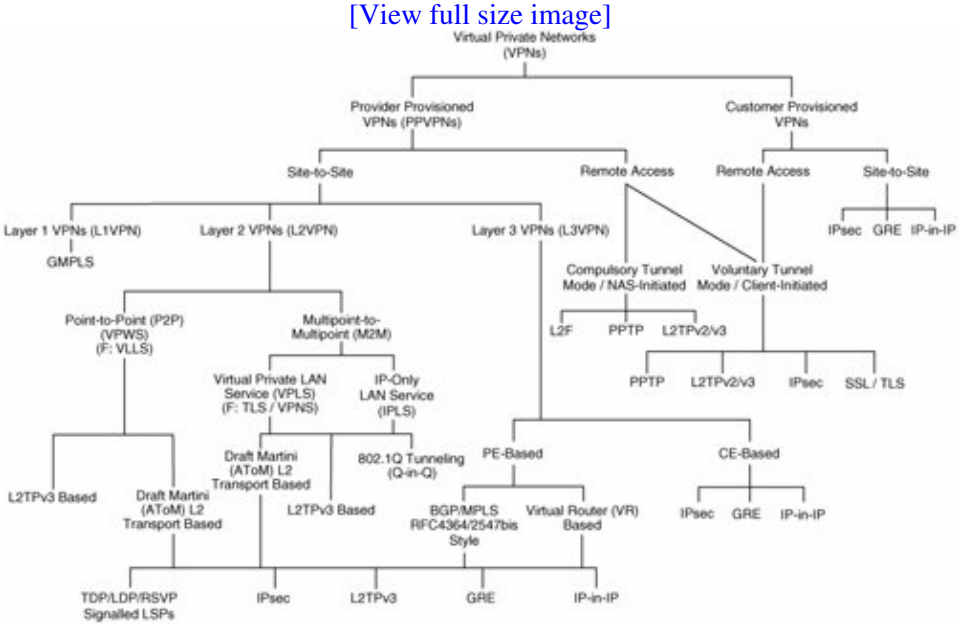
As you read this section, you may ask yourself how it is that we have ended up with so many terms to describe VPNs. The answer is a desire to accurately describe the characteristics of a VPN protocol or technology but also a simple lack of coordination among protocol designers and engineers (this is getting much better), and on top of that a certain amount of "help" from our marketing colleagues ("How can I differentiate our products?").

As you read this section, be sure to refer to Figure 1-3. Figure 1-3 clarifies the relationship of the VPN models to each other; it also describes the VPN (tunneling) protocols and technologies associated with the various models.

Figure 1-3. Virtual Private Networks

Note that in Figure 1-3, F: denotes a former name for a particular technology.

[View full size image]



The bottom level of the hierarchy in Figure 1-3 describes protocols or mechanisms used to tunnel VPN traffic between CE or PE devices.

Service Provider and Customer Provisioned VPNs

VPNs can be either one of the following:

- Service provider provisioned VPNs that are configured and managed by a service provider or providers
- Customer provisioned VPNs that are configured and managed by the (service provider) customer itself

Note that the customer of the service provider may be either an enterprise or another service provider, in which case, the service provider that offers the VPN service is known as a carrier of carriers, and the service offered to the customer service provider is known as a carrier's carrier VPN service.

Additionally, a VPN service might be offered over the backbone networks of multiple cooperating autonomous systems and/or service providers. In this case, the VPN service is known as an inter-AS or interprovider VPN service.

Examples of provider provisioned VPNs are as follows:

- Virtual Private Wire Service (VPWS) VPNs
- Virtual Private LAN Service (VPLS) VPNs
- IP-Only Private LAN Service (IPLS) VPNs
- BGP/MPLS (RFC4364/2547bis) VPNs (BGP/MPLS VPNs are also known as MPLS Layer 3 VPNs.)
- Virtual Router (VR)-based VPNs
- IPsec VPNs

Examples of customer provisioned VPNs are as follows:

- GRE VPNs
- IPsec VPNs

Site-to-Site and Remote Access VPNs

VPNs, whether provider or customer provisioned, fall into one of two broad categories:

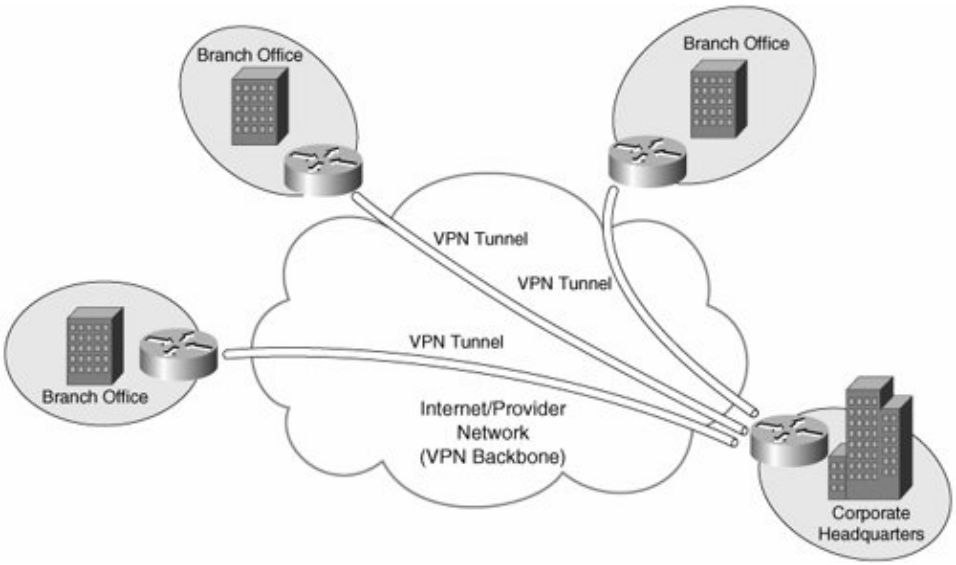
- Site to site
- Remote access

Site-to-site VPNs allow connectivity between an organization's (or organizations') geographically dispersed sites (such as a head office and branch offices).

Figure 1-4 illustrates a typical site-to-site VPN.

Figure 1-4. Typical Site-to-Site VPN

[View full size image]



There are two types of site-to-site VPN:

- Intranet VPNs Allow connectivity between sites of a single organization
- Extranet VPNs Allow connectivity between organizations such as business partners or a business and its customers

Remote access VPNs (also called access VPNs) allow mobile or home-based users to access an organization's resources remotely.

Figure 1-5 illustrates typical remote access VPNs.

Figure 1-5. Remote Access VPNs

[View full size image]