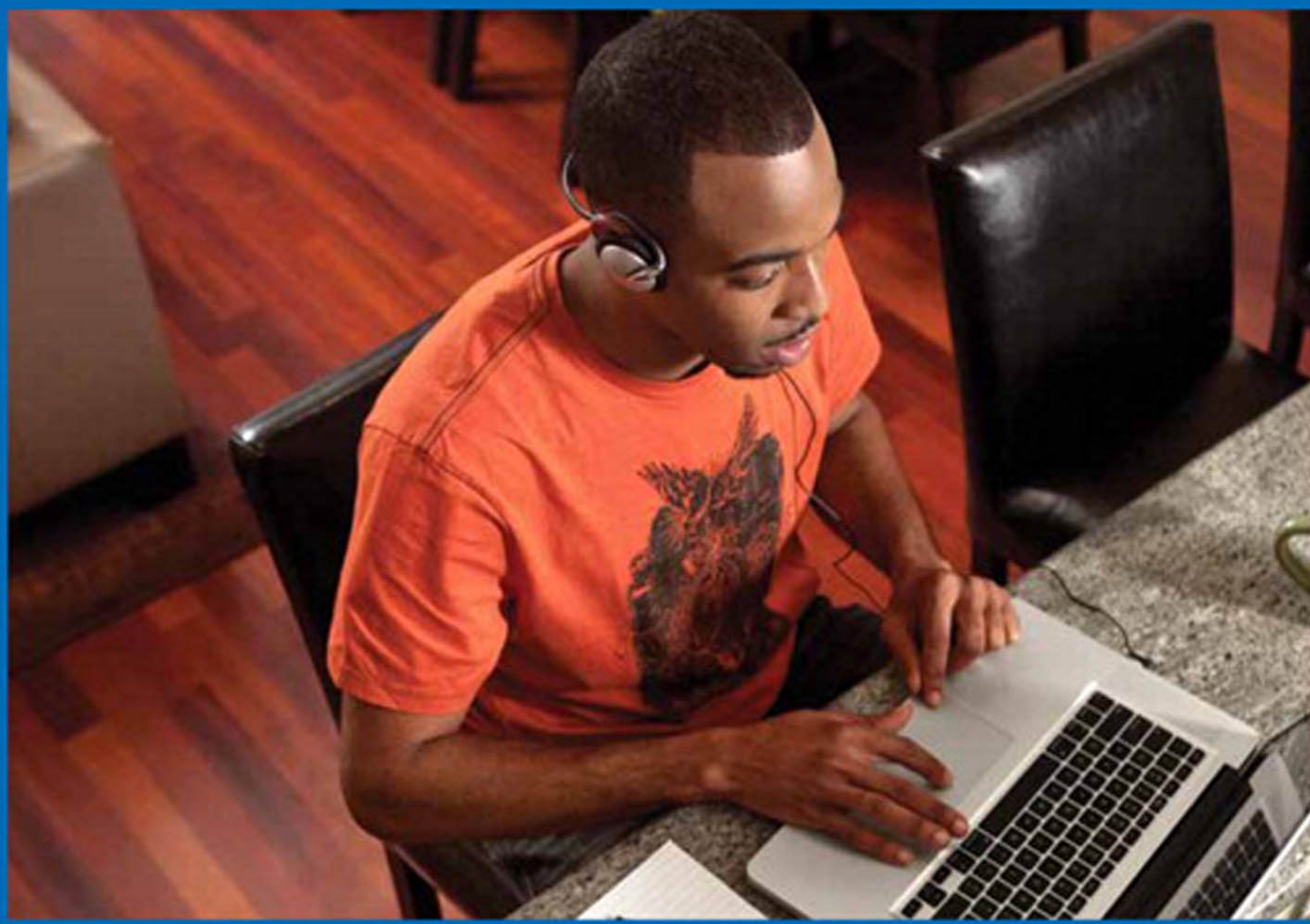
Connecting Networks

Companion Guide



Cisco | Networking Academy®
Mind Wide Open™

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Connecting Networks Companion Guide

Cisco Networking Academy

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

Connecting Networks Companion Guide

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

Printed in the United States of America

First Printing May 2014

Library of Congress Control Number: 2014933762

ISBN-13: 978-1-58713-332-9

ISBN-10: 1-58713-332-6

Warning and Disclaimer

This book is designed to provide information about the Connecting Networks course. 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 authors, 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.

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, Please visit www.cisco.com/edu.

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Business Operation Manager, Cisco Press
Jan Cornelssen

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Development Editor
Ellie C. Bru

Project Editor
Mandie Frank

Copy Editor
Keith Cline

Technical Editor
Kathleen Page

Editorial Assistant
Vanessa Evans

Designer
Mark Shirar

Composition
Trina Wurst

Indexer
Ken Johnson

Proofreader
Dan Knott

Trademark Acknowledgements

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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

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 email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Americas 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: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Contributing Authors

Rick Graziani teaches computer science and computer networking courses at Cabrillo College in Aptos, California. Prior to teaching, Rick worked in the information technology field for Santa Cruz Operation, Tandem Computers, and Lockheed Missiles and Space Corporation. He holds an M.A. in Computer Science and Systems Theory from California State University Monterey Bay. Rick is also a member of the Curriculum Development team for the Cisco Networking Academy since 1999.

Rick has authored multiple books for Cisco Press and multiple online courses for the Cisco Networking Academy. Rick is the author of the Cisco Press book *IPv6 Fundamentals* and has presented on IPv6 at several Cisco Academy conferences. He is the coauthor of the Cisco Press book *Routing Protocols Companion Guide*.

When Rick is not working, he is most likely surfing at one of his favorite Santa Cruz surf breaks.

Bob Vachon is a professor in the Computer Systems Technology program at Cambrian College in Sudbury, Ontario, Canada, where he teaches networking infrastructure courses. He has over 30 years of work and teaching experience in the computer networking and information technology field.

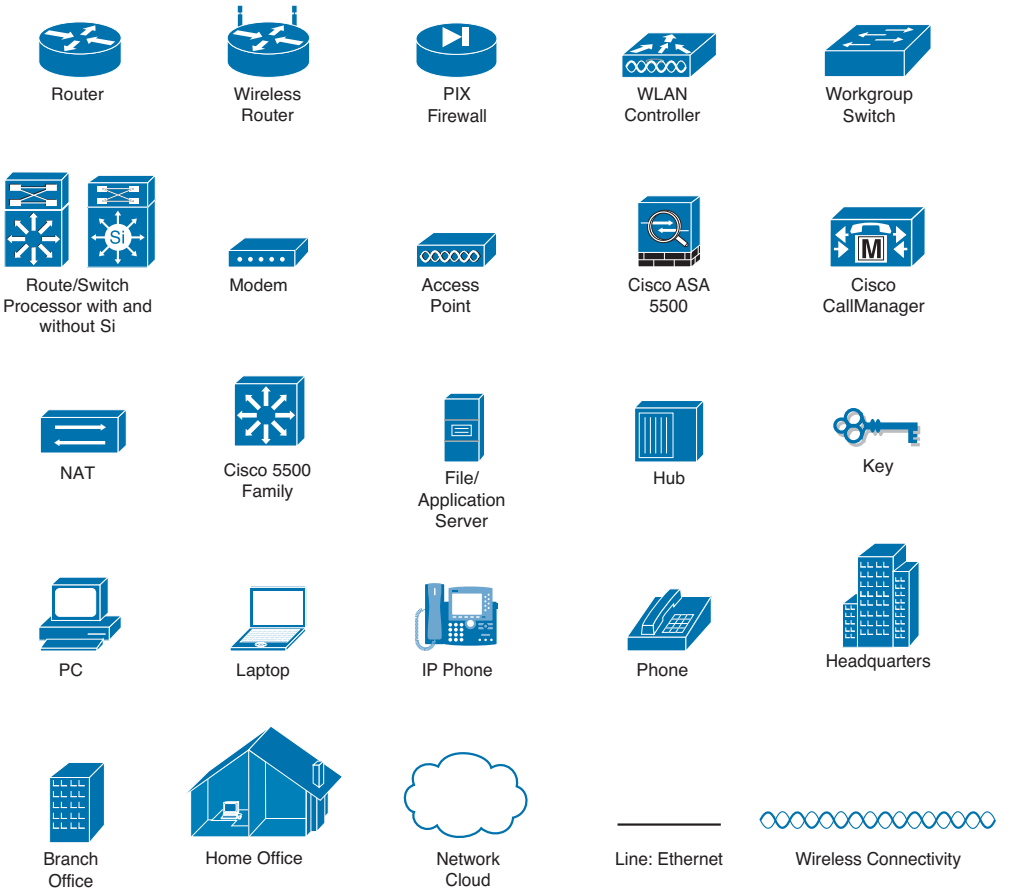
Since 2001, Bob has collaborated as team lead, lead author, and subject matter expert on various CCNA, CCNA-S, and CCNP projects for Cisco and the Cisco Networking Academy. He also authored the *CCNA Accessing the WAN Companion Guide* and the *CCNA Security (640-554) Portable Command Guide*. He is the coauthor of the Cisco Press book *Routing Protocols Companion Guide*.

In his downtime, Bob enjoys playing the guitar, shooting darts or pool, and either working in his gardens or white-water canoe tripping.

Contents At a Glance

Contents

Syntax Conventions



The conventions used to present command syntax in this book are the same conventions used in the 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).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Connecting Networks Companion Guide is the official supplemental textbook for the Cisco Network Academy Connecting Networks course. Cisco Networking Academy is a comprehensive program that delivers information technology skills to students around the world. The curriculum emphasizes real-world practical application while providing opportunities for you to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small- to medium-sized businesses, as well as enterprise and service provider environments.

As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. This book emphasizes key topics, terms, and activities and provides some alternate explanations and examples as compared with the course. You can use the online curriculum as directed by your instructor and then use this Companion Guide's study tools to help solidify your understanding of all the topics.

Who Should Read This Book

This book is intended for students enrolled in the Cisco Networking Academy Connecting Networks course. The book, as well as the course, is designed as an introduction to data network technology for those pursuing careers as network professionals as well as those who need only an introduction to network technology for professional growth. Topics are presented concisely, starting with the most fundamental concepts and progressing to a comprehensive understanding of network communication. The content of this text provides the foundation for additional Cisco Academy courses, and preparation for the CCENT and CCNA Routing and Switching certifications.

Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following features give you a thorough overview of the topics covered in each chapter so that you can make constructive use of your study time:

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in the Companion Guide encourages you to think about finding the answers as you read the chapter.

- **"How-to" feature:** When this book covers a set of steps that you need to perform for certain tasks, the text lists the steps as a how-to list. When you are studying, the icon helps you easily refer to this feature as you skim through the book.
- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries:** At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **Practice:** At the end of each chapter, there is a full list of all the labs, class activities, and Packet Tracer activities to refer back to for study time.

Readability

The following features have been updated to assist your understanding of the networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference from inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The glossary defines all the key terms.
- **Glossary:** This book contains an all-new glossary with 195 terms.

Practice

Practice makes perfect. This new Companion Guide offers you ample opportunities to put what you learn into practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **Check Your Understanding questions and answer key:** Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, "Answers to the 'Check Your Understanding' Questions," provides an answer key to all the questions and includes an explanation of each answer.

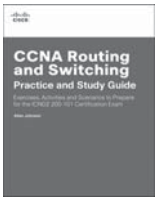
Packet Tracer Activity

Video

- **Labs and activities:** Throughout each chapter, you will be directed back to the online course to take advantage of the activities created to reinforce concepts. In addition, at the end of each chapter, there is a "Practice" section that collects a list of all the labs and activities to provide practice with the topics introduced in this chapter. The labs and class activities are available in the companion *Connecting Networks Lab Manual* (ISBN 978-1-58713-331-2). The Packet Tracer activity PKA files are found in the online course.
- **Page references to online course:** After headings, you will see, for example, (1.1.2.3). This number refers to the page number in the online course so that you can easily jump to that spot online to view a video, practice an activity, perform a lab, or review a topic.

Lab Manual

The supplementary book *Connecting Networks Lab Manual*, by Cisco Press (ISBN 978-1-58713-331-2), contains all the labs and class activities from the course.



Practice and Study Guide

Additional Study Guide exercises, activities, and scenarios are available in *CCNA Routing and Switching Practice and Study Guide* (978-158713-344-2) book by Allan Johnson. The Practice and Study Guide coordinates with the recommended curriculum sequence. The CCNA edition follows the course outlines for Scaling Networks and Connecting Networks.

About Packet Tracer Software and Activities

Interspersed throughout the chapters, you'll find many activities to work with the Cisco Packet Tracer tool. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in the course. Packet Tracer software is available only through the Cisco Networking Academy website. Ask your instructor for access to Packet Tracer.

How This Book Is Organized

This book corresponds closely to the Cisco Academy Connecting Networks course and is divided into nine chapters, one appendix, and a glossary of key terms:

- **Chapter 1, "Hierarchical Network Design"**: Structured engineering principles of network design are examined. The three layers of hierarchical design and the Cisco Enterprise Architecture model are discussed. Three business architectures are examined: Borderless Network Architecture, Collaboration Network Architecture, and Data Center/Virtualizing Network Architecture.
- **Chapter 2, "Connecting to the WAN"**: Basic WAN operations and services are examined. Private and public WAN technologies are discussed. Includes how to select the appropriate WAN protocol and service for a specific network requirement.
- **Chapter 3, "Point-to-Point Connections"**: Examines point-to-point serial communications using HDLC and PPP. Describes the features and benefits of PPP over HDLC. The PPP layered architecture is discussed as well as the functions of LCP and NCP. PPP authentication is included.
- **Chapter 4, "Frame Relay"**: Examines the benefits and operations of Frame Relay. Bandwidth control mechanisms and basic Frame Relay PVC configuration are discussed.
- **Chapter 5, "Network Address Translation for IPv4"**: Describes the characteristics, benefits and drawbacks of NAT. Configuration of static NAT, dynamic NAT, and PAT are discussed. Port forwarding and NAT64 are introduced.
- **Chapter 6, "Broadband Solutions"**: Introduces various broadband solutions including DSL and cable. Broadband wireless options are described. PPPoE operation and configuration are discussed.

- **Chapter 7, "Securing Site-to-Site Connectivity":** Describes the benefits of VPN technology. Site-to-site and remote-access VPNs are introduced. The purpose, benefits, and configuration of GRE tunnels are examined. IPsec characteristics and protocol framework are examined. How AnyConnect and clientless SSL remote-access VPM implementations support business requirements are discussed. The chapter also compares IPsec and SSL remote-access VPNs.
- **Chapter 8, "Monitoring the Network":** Focuses on monitoring the network including syslog, SNMP, and NetFlow operations. The operations, configuration, and monitoring capabilities of each technology are examined.
- **Chapter 9, "Troubleshooting the Network":** Examines how to develop network documentation that is used to troubleshoot network issues. Describes the general troubleshooting process, along with the systematic layer approach to troubleshooting. Troubleshooting tools are examined and how they are used to gather and analyze symptoms of network problems. Includes determining symptoms and causes of network problems using the layered model.
- **Appendix A, "Answers to the 'Check Your Understanding' Questions":** This appendix lists the answers to the "Check Your Understanding" review questions that are included at the end of each chapter.
- **Glossary:** The glossary provides you with definitions for all the key terms identified in each chapter.

This page intentionally left blank

CHAPTER 1

Hierarchical Network Design

Objectives

Upon completion of this chapter

- What are the structured engineering principles of network design?
- How do you apply the three hierarchical network layers in network design?
- What are the four basic modules in an enterprise campus network architecture that interconnect via the core?
- How do the modules of the Cisco Enterprise Architecture model differ?
- What are some trends that are challenging enterprise network architectures?
- How do the Borderless Network, Collaboration Network, and Data Center/Virtualization Network architectures address the network challenges?

Key Terms

This chapter uses the following key terms. You can find the definitions in the glossary.

small network *page 3*

medium-size network *page 3*

large network *page 3*

access layer *page 6*

distribution layer *page 7*

core layer *page 9*

three-tier hierarchical design *page 10*

two-tier hierarchical design *page 10*

collapsed core *page 10*

modular network design *page 11*

Cisco Enterprise Architecture model *page 14*

enterprise campus module *page 15*

enterprise edge module *page 17*

SP edge module *page 18*

enterprise branch module *page 21*

enterprise teleworker module *page 22*

enterprise data center module *page 22*

Cisco Borderless Network Architecture *page 24*

Cisco Collaboration Architecture *page 25*

Cisco Data Center/Virtualization Architecture *page 26*

Introduction (1.0.1.1)

Networks must meet the current needs of organizations and be able to support emerging technologies as new technologies are adopted. Network design principles and models can help a network engineer design and build a network that is flexible, resilient, and manageable.

This chapter introduces network design concepts, principles, models, and architectures. It covers the benefits that are obtained by using a systematic design approach. Emerging technology trends that will affect network evolution are also discussed.

Class Activity 1.0.1.2: Design Hierarchy

A network administrator is tasked with designing an expanded network for the company.

After speaking with network administrators in other branches of the company, it was decided to use the Cisco three-layer hierarchical network design model to influence the expansion. This model was chosen for its simple influence upon network planning.

The three layers of the expanded network design include

- Access
- Distribution
- Core

Hierarchical Network Design Overview (1.1)

The Cisco hierarchical (three-layer) internetworking model is an industry wide adopted model for designing a reliable, scalable, and cost-efficient internetwork. In this section, you will learn about the access, distribution, and core layers and their role in the hierarchical network model.

Enterprise Network Campus Design (1.1.1)

An understanding of network scale and knowledge of good structured engineering principles is recommended when discussing network campus design.

Network Requirements (1.1.1.1)

When discussing network design, it is useful to categorize networks based on the number of devices serviced:

- *Small network*: Provides services for up to 200 devices.
- *Medium-size network*: Provides services for 200 to 1,000 devices.
- *Large network*: Provides services for 1,000+ devices.

Network designs vary depending on the size and requirements of the organizations. For example, the networking infrastructure needs of a small organization with fewer devices will be less complex than the infrastructure of a large organization with a significant number of devices and connections.

There are many variables to consider when designing a network. For instance, consider the example in Figure 1-1. The sample high-level topology diagram is for a large enterprise network that consists of a main campus site connecting small, medium, and large sites.

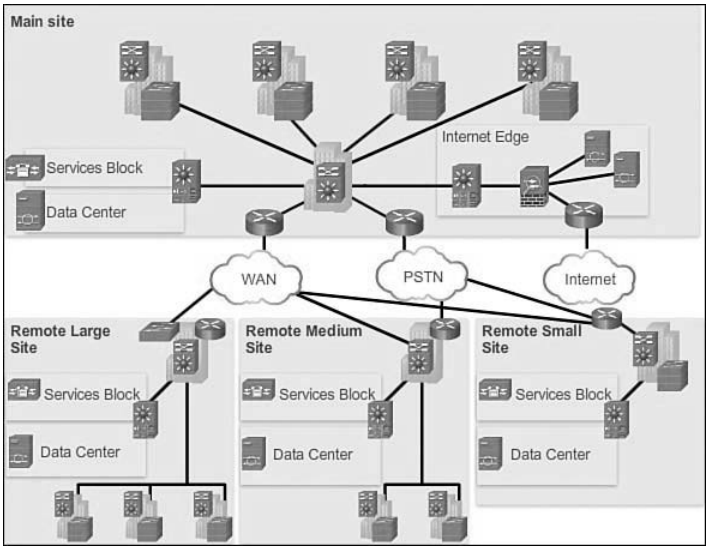


Figure 1-1 Large Enterprise Network Design

Network design is an expanding area and requires a great deal of knowledge and experience. The intent of this section is to introduce commonly accepted network design concepts.

Note

The Cisco Certified Design Associate (CCDA®) is an industry-recognized certification for network design engineers, technicians, and support engineers who demonstrate the skills required to design basic campus, data center, security, voice, and wireless networks.

Structured Engineering Principles (1.1.1.2)

Regardless of network size or requirements, a critical factor for the successful implementation of any network design is to follow good structured engineering principles. These principles include

- **Hierarchy**: A hierarchical network model is a useful high-level tool for designing a reliable network infrastructure. It breaks the complex problem of network design into smaller and more manageable areas.
- **Modularity**: By separating the various functions that exist on a network into modules, the network is easier to design. Cisco has identified several modules, including the enterprise campus, services block, data center, and Internet edge.
- **Resiliency**: The network must remain available for use under both normal and abnormal conditions. Normal conditions include normal or expected traffic flows and traffic patterns, as well as scheduled events such as maintenance windows. Abnormal conditions include hardware or software failures, extreme traffic loads, unusual traffic patterns, denial-of-service (DoS) events, whether intentional or unintentional, and other unplanned events.
- **Flexibility**: The ability to modify portions of the network, add new services, or increase capacity without going through a major forklift upgrade (i.e., replacing major hardware devices).

To meet these fundamental design goals, a network must be built on a hierarchical network architecture that allows for both flexibility and growth.

Hierarchical Network Design (1.1.2)

This topic discusses the three functional layers of the hierarchical network model: the access, distribution, and core layers.

Network Hierarchy (1.1.2.1)

Early networks were deployed in a flat topology as shown in Figure 1-2.

Hubs and switches were added as more devices needed to be connected. A flat network design provided little opportunity to control broadcasts or to filter undesirable traffic. As more devices and applications were added to a flat network, response times degraded, making the network unusable.

A better network design approach was needed. For this reason, organizations now use a hierarchical network design as shown in Figure 1-3.

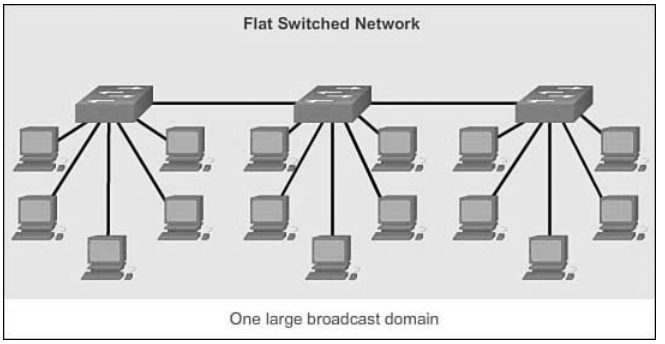


Figure 1-2 Flat Switched Network

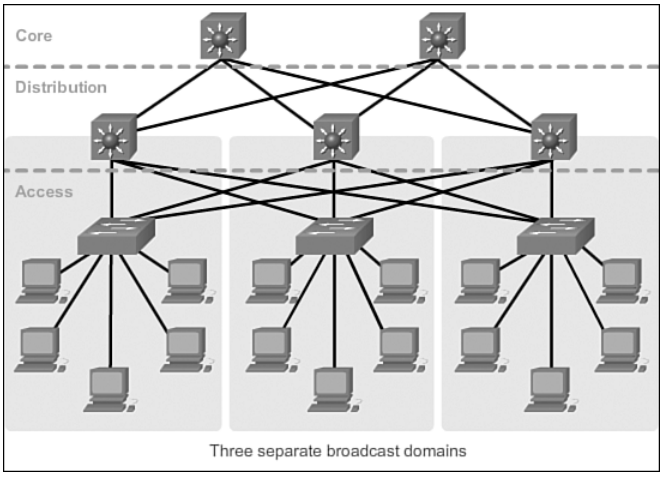


Figure 1-3 Hierarchical Network

A hierarchical network design involves dividing the network into discrete layers. Each layer, or tier, in the hierarchy provides specific functions that define its role within the overall network. This helps the network designer and architect to optimize and select the right network hardware, software, and features to perform specific roles for that network layer. Hierarchical models apply to both LAN and WAN design.

The benefit of dividing a flat network into smaller, more manageable blocks is that local traffic remains local. Only traffic that is destined for other networks is moved to a higher layer. For example, in Figure 1-3 the flat network has now been divided into three separate broadcast domains.

A typical enterprise hierarchical LAN campus network design includes the following three layers:

- **Access layer:** Provides workgroup/user access to the network
- **Distribution layer:** Provides policy-based connectivity and controls the boundary between the access and core layers
- **Core layer:** Provides fast transport between distribution switches within the enterprise campus

Another sample three-layer hierarchical network design is displayed in Figure 1-4. Notice that each building is using the same hierarchical network model that includes the access, distribution, and core layers.

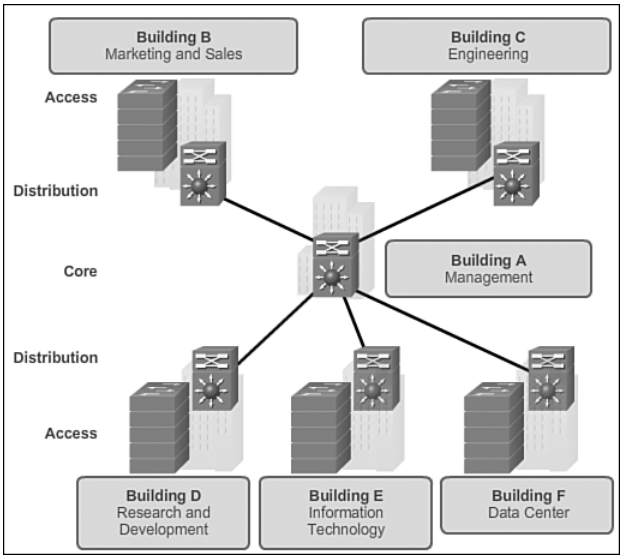


Figure 1-4 Multi Building Enterprise Network Design

Note

There are no absolute rules for the way a campus network is physically built. While it is true that many campus networks are constructed using three physical tiers of switches, this is not a strict requirement. In a smaller campus, the network might have two tiers of switches in which the core and distribution elements are combined in one physical switch. This is referred to as a collapsed core design.

The Access Layer (1.1.2.2)

In a LAN environment, the *access layer* highlighted grants end devices access to the network. In the WAN environment, it may provide teleworkers or remote sites access to the corporate network across WAN connections.

As shown in Figure 1-5, the access layer for a small business network generally incorporates Layer 2 switches and access points providing connectivity between workstations and servers.

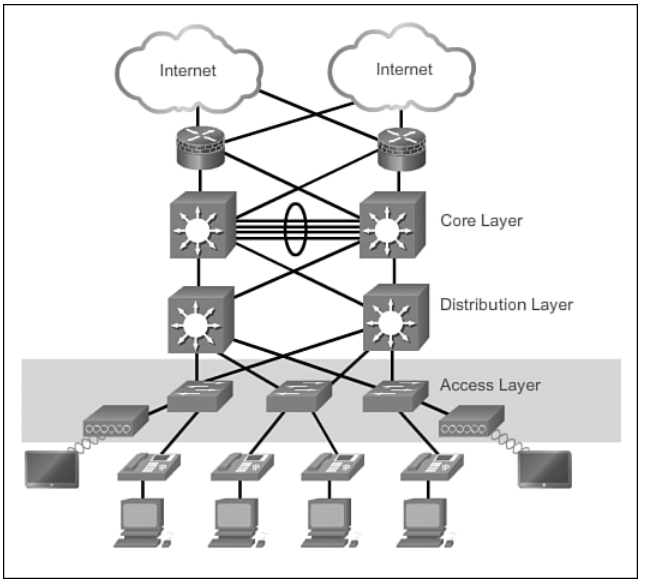


Figure 1-5 Access Layer

The access layer serves a number of functions, including

- Layer 2 switching
- High availability
- Port security
- QoS classification and marking and trust boundaries
- Address Resolution Protocol (ARP) inspection
- Virtual access control lists (VACLs)
- Spanning tree
- Power over Ethernet (PoE) and auxiliary VLANs for VoIP

The Distribution Layer (1.1.2.3)

The ***distribution layer*** aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. In Figure 1-6, the distribution layer is the boundary between the Layer 2 domains and the Layer 3 routed network.

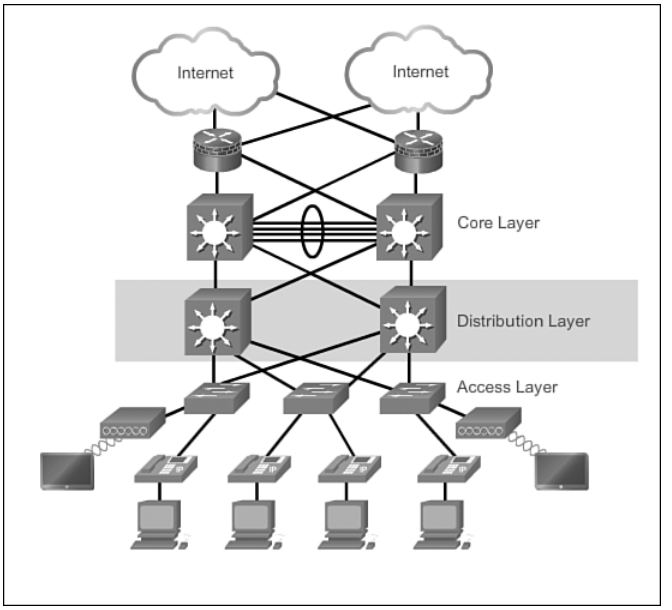


Figure 1-6 Distribution Layer

The distribution layer device is the focal point in the wiring closets. Either a router or a multilayer switch is used to segment workgroups and isolate network problems in a campus environment.

A distribution layer switch may provide upstream services for many access layer switches.

The distribution layer can provide

- Aggregation of LAN or WAN links.
- Policy-based security in the form of access control lists (ACLs) and filtering.
- Routing services between LANs and VLANs and between routing domains (e.g., EIGRP to OSPF).
- Redundancy and load balancing.
- A boundary for route aggregation and summarization configured on interfaces toward the core layer.
- Broadcast domain control, because routers or multilayer switches do not forward broadcasts. The device acts as the demarcation point between broadcast domains.

The Core Layer (1.1.2.4)

The *core layer* is also referred to as the network backbone. The core layer consists of high-speed network devices such as the Cisco Catalyst 6500 or 6800. These are designed to switch packets as fast as possible and interconnect multiple campus components, such as distribution modules, service modules, the data center, and the WAN edge.

As shown in Figure 1-7, the core layer is critical for interconnectivity between distribution layer devices (for example, interconnecting the distribution block to the WAN and Internet edge).

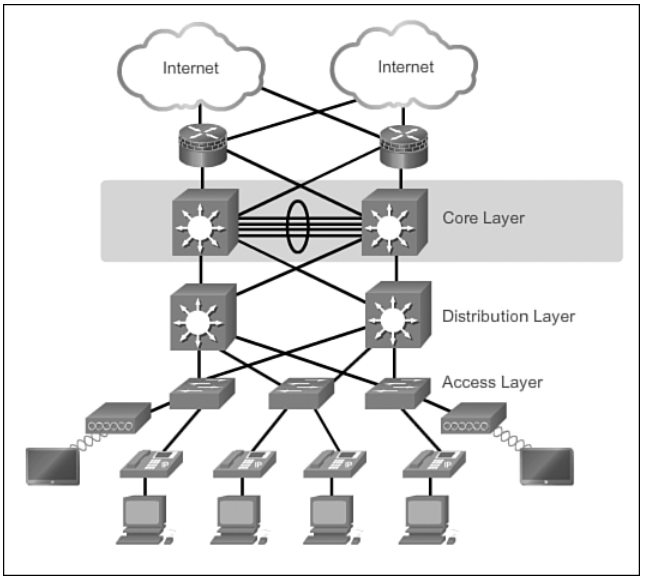


Figure 1-7 Core Layer

The core should be highly available and redundant. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly.

Considerations at the core layer include

- Providing high-speed switching (i.e., fast transport)
- Providing reliability and fault tolerance
- Scaling by using faster, and not more, equipment
- Avoiding CPU-intensive packet manipulation caused by security, inspection, quality of service (QoS) classification, or other processes

Two-Tier Collapsed Core Design (1.1.2.5)

The *three-tier hierarchical design* maximizes performance, network availability, and the ability to scale the network design.

However, many small enterprise networks do not grow significantly larger over time. Therefore, a *two-tier hierarchical design* where the core and distribution layers are collapsed into one layer is often more practical. A "*collapsed core*" is when the distribution layer and core layer functions are implemented by a single device. The primary motivation for the collapsed core design is reducing network cost, while maintaining most of the benefits of the three-tier hierarchical model.

The example in Figure 1-8 has collapsed the distribution layer and core layer functionality into multilayer switch devices.

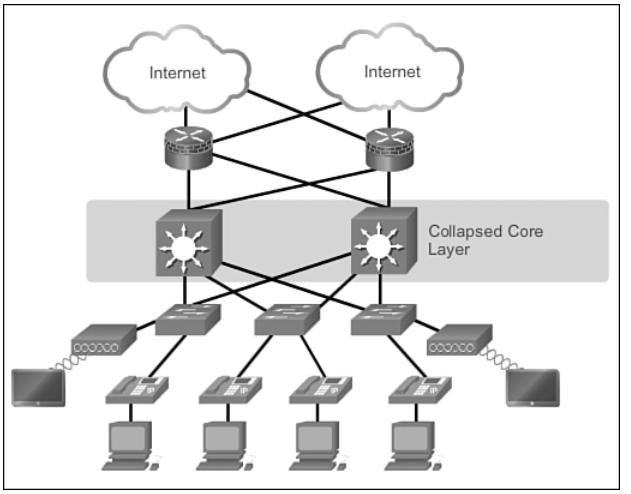


Figure 1-8 Two-Tier Hierarchical Design

The hierarchical network model provides a modular framework that allows flexibility in network design and facilitates ease of implementation and troubleshooting.

Interactive Graphic

Activity 1.1.2.6: Identify Hierarchical Network Characteristics

Go to the course online to perform this practice activity.

Cisco Enterprise Architecture (1.2)

The Cisco Enterprise Architecture is a modular approach to network design. This section identifies enterprise architecture modules that are commonly found in medium-to-large organizations.

Modular Design (1.2.1.1)

While the hierarchical network design works well within the campus infrastructure, networks have expanded beyond these borders. As shown in Figure 1-9, networks have become more sophisticated and complex. The central campus site now requires connections to branch sites and support for teleworking employees working from home offices or other remote locations. Large organizations may also require dedicated connections to offsite data centers.

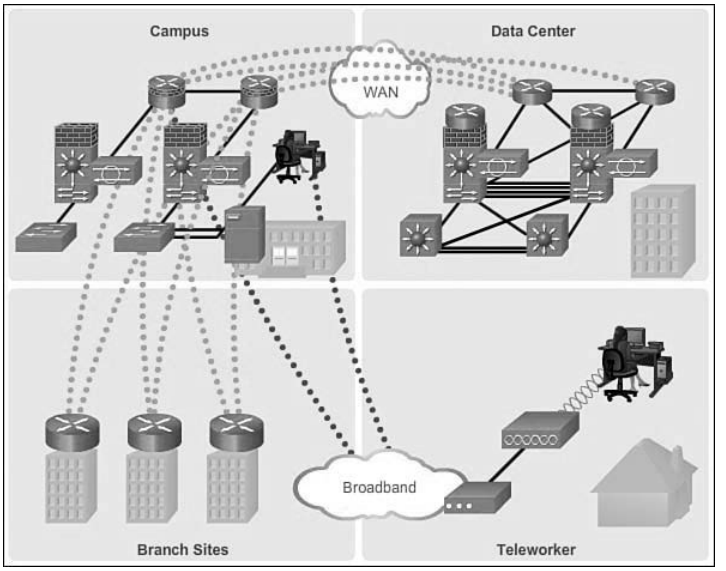


Figure 1-9 Expanding Beyond the Campus Infrastructure

As the complexity of the network increased to meet these demands, it became necessary to adjust the network design to one that uses a more modular approach.

A *modular network design* separates the network into various functional network modules, each targeting a specific place or purpose in the network. The modules represent areas that have different physical or logical connectivity. They designate where different functions occur in the network. Using a modular approach has several benefits, including

- Failures that occur within a module can be isolated from the remainder of the network, providing for simpler problem detection and higher overall system availability.
- Network changes, upgrades, or the introduction of new services can be made in a controlled and staged fashion, allowing greater flexibility in the maintenance and operation of the campus network.

- When a specific module no longer has sufficient capacity or is missing a new function or service, it can be updated or replaced by another module that has the same structural role in the overall hierarchical design.
- Security can be implemented on a modular basis allowing for more granular security control.

The use of modules in network design enables flexibility and facilitates implementation and troubleshooting.

Modules in the Enterprise Architecture (1.2.1.2)

A modular approach to network design further divides the three-layer hierarchical design by pulling out specific blocks or modular areas. These basic modules are connected together via the core of the network.

Basic network modules include

- **Access-distribution:** Also called the distribution block, this is the most familiar element and fundamental component of a campus design (see Figure 1-10).

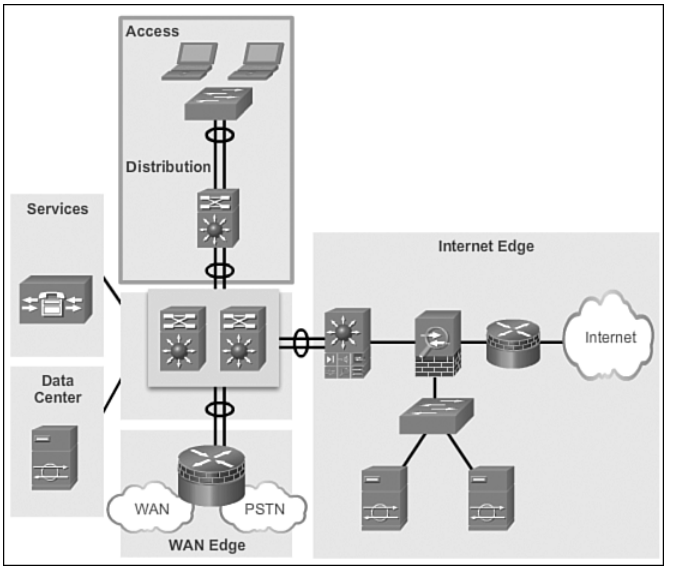


Figure 1-10 Access-Distribution Module

- **Services:** This is a generic block used to identify services such as centralized Lightweight Access Point Protocol (LWAPP) wireless controllers, unified communications services, policy gateways, and more (see Figure 1-11).

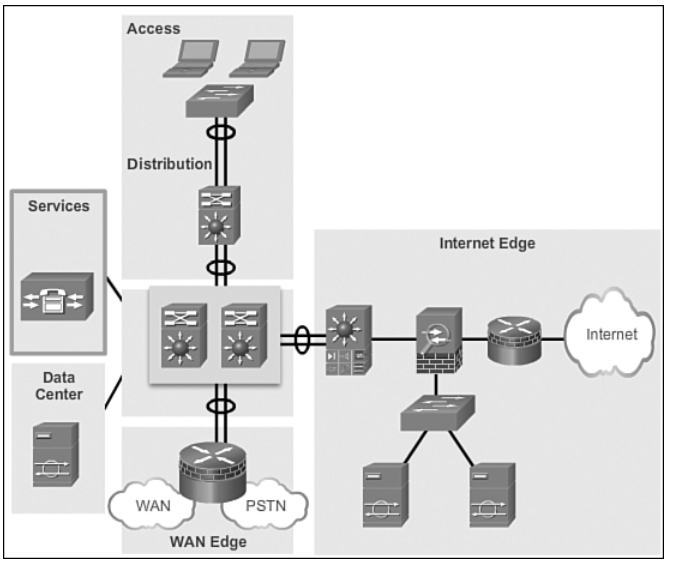


Figure 1-11 Services Module

- **Data center:** Originally called the server farm. This block is responsible for managing and maintaining many data systems that are vital to modern business operations. Employees, partners, and customers rely on data and resources in the data center to effectively create, collaborate, and interact (see Figure 1-12).

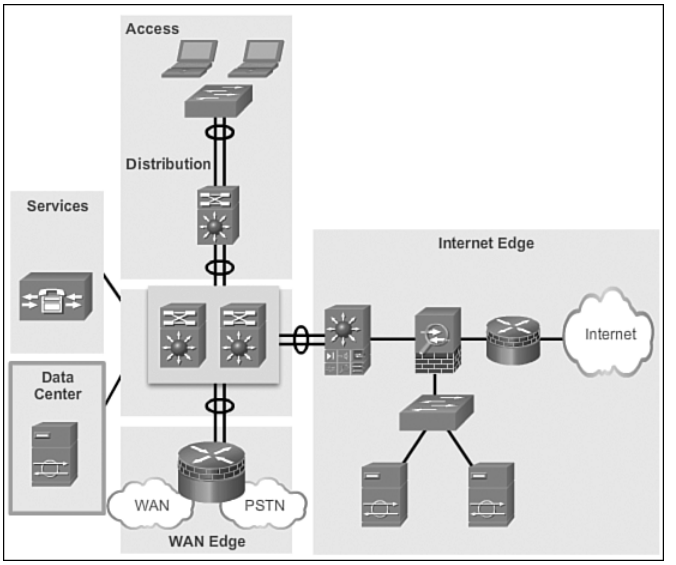


Figure 1-12 Data Center Module

- **Enterprise edge:** Consists of the Internet edge and the WAN edge. These blocks offer connectivity to voice, video, and data services outside the enterprise (see Figure 1-13).

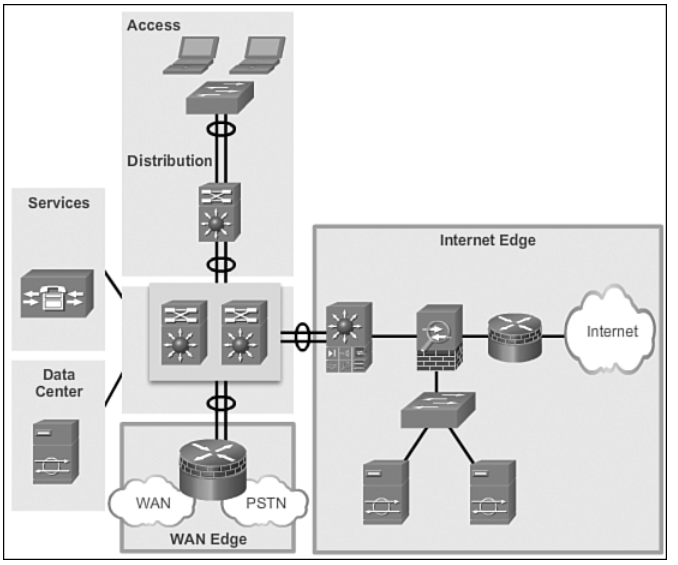


Figure 1-13 Enterprise Edge Module

Interactive Graphic

Activity 1.2.1.3: Identify Modules in a Network Design

Go to the course online to perform this practice activity.

Cisco Enterprise Architecture Model (1.2.2)

The Cisco Enterprise Architecture is a modular approach to network design. This topic discusses the enterprise campus module, enterprise edge module, and the service provider edge module.

Cisco Enterprise Architecture Model (1.2.2.1)

To accommodate the need for modularity in network design, Cisco developed the *Cisco Enterprise Architecture model*. This model provides all the benefits of the hierarchical network design on the campus infrastructure, and facilitates the design of larger, more scalable networks.

The Cisco Enterprise Architecture model separates the enterprise network into functional areas that are referred to as modules. The modularity that is built in to the architecture allows flexibility in network design and facilitates implementation and troubleshooting.

As shown in Figure 1-14, the following are the primary Cisco Enterprise Architecture modules:

- Enterprise campus
- Enterprise edge
- Service provider edge

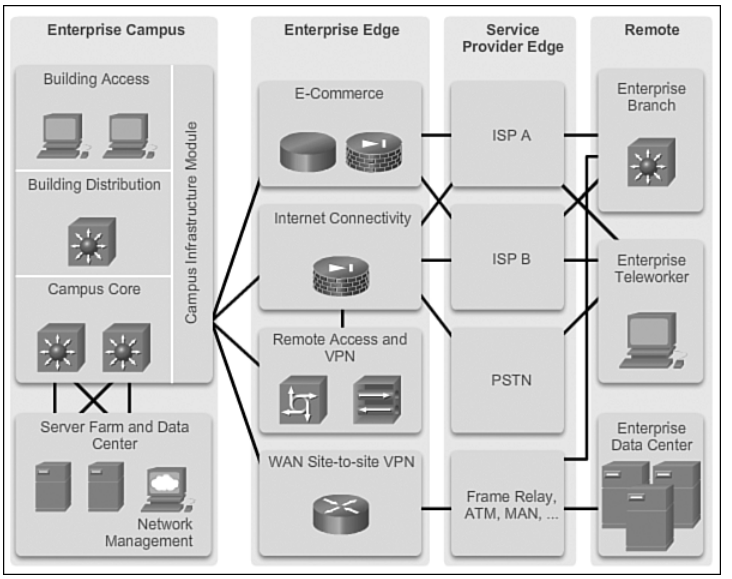


Figure 1-14 Cisco Enterprise Architecture Modules

Connected to the service provider edge are the remote modules, including

- Enterprise branch
- Enterprise teleworker
- Enterprise data center

Cisco Enterprise Campus (1.2.2.2)

A campus network is a building or group of buildings connected into one enterprise network that consists of many LANs. A campus is generally limited to a fixed geographic area, but it can span several neighboring buildings (for example, an industrial complex or business park environment). Regional offices, SOHOs, and mobile workers may need to connect to the central campus for data and information.

The *enterprise campus module* describes the recommended methods to create a scalable network while addressing the needs of campus-style business operations.

The architecture is modular and can easily expand to include additional campus buildings or floors as the enterprise grows.

As shown in Figure 1-15, the enterprise campus module consists of the following submodules:

- Building access
- Building distribution
- Campus core
- Data center

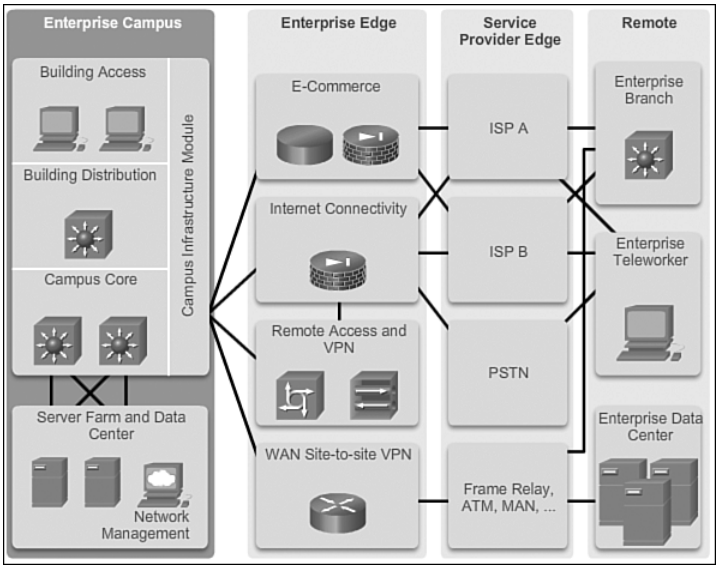


Figure 1-15 Enterprise Campus Module

Together these submodules

- Provide high availability through a resilient hierarchical network design
- Integrate IP communications, mobility, and advanced security
- Utilize multicast traffic and QoS to optimize network traffic
- Provide increased security and flexibility using access management, VLANs, and IPsec VPNs

The enterprise campus module architecture provides the enterprise with high availability through a resilient multilayer design, redundant hardware and software features, and automatic procedures for reconfiguring network paths when failures occur. Integrated security protects against and mitigates the impact of worms, viruses, and other attacks on the network, even at the switch port level.

A high-capacity, centralized data center module can provide internal server resources to users. The data center module typically also supports network management services for the enterprise, including monitoring, logging, troubleshooting, and other common management features from end to end. The data center submodule typically contains internal email and corporate servers that provide application, file, print, email, and Domain Name System (DNS) services to internal users.

Cisco Enterprise Edge (1.2.2.3)

The *enterprise edge module* provides connectivity for voice, video, and data services outside the enterprise. This module often functions as a liaison between the enterprise campus module and the other modules.

As shown in Figure 1-16, the enterprise edge module consists of submodules providing

- E-commerce services
- Internet connectivity
- Remote access and VPN access
- WAN site-to-site VPN access

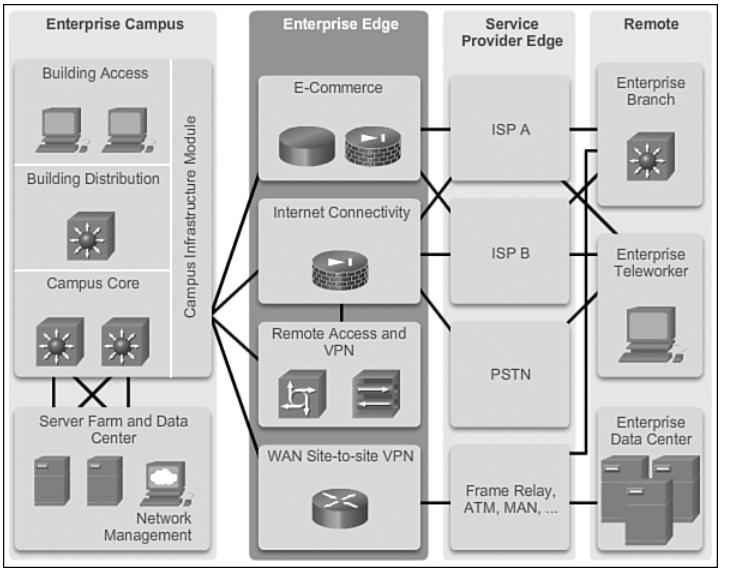


Figure 1-16 Enterprise Edge Submodules

Specifically, these submodules consist of:

- **E-commerce networks and servers**: The e-commerce submodule enables enterprises to support e-commerce applications through the Internet. It uses the high-availability designs of the data center module. Devices located in the e-commerce submodule include web, application, and database servers; firewall and firewall routers; and network intrusion prevention systems (IPS).
- **Internet connectivity and demilitarized zone (DMZ)** : The Internet submodule of the enterprise edge provides internal users with secure connectivity to Internet services such as public servers, email, and DNS. Connectivity to one or several Internet service providers (ISPs) is also provided. Components of this submodule include firewall and firewall routers, Internet edge routers, FTP and HTTP servers, SMTP relay servers, and DNS servers.
- **Remote access and VPN**: The VPN/remote access submodule of the enterprise edge provides remote-access termination services, including authentication for remote users and sites. Components of this submodule include firewalls, dial-in access concentrators, Cisco Adaptive Security Appliances (ASA), and network intrusion prevention system (IPS) appliances.
- **WAN**: The WAN submodule uses various WAN technologies for routing traffic between remote sites and the central site. Enterprise WAN links include technologies such as Multiprotocol Label Switching (MPLS), Metro Ethernet, leased lines, Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH), PPP, Frame Relay, ATM, cable, digital subscriber line (DSL), and wireless.

Service Provider Edge (1.2.2.4)

Enterprises use service providers (SPs) to link to other sites. As shown in Figure 1-17, the *SP edge module* can include

- Internet service providers (ISPs)
- WAN services such as Frame Relay, ATM, and MAN
- Public switched telephone network (PSTN) services

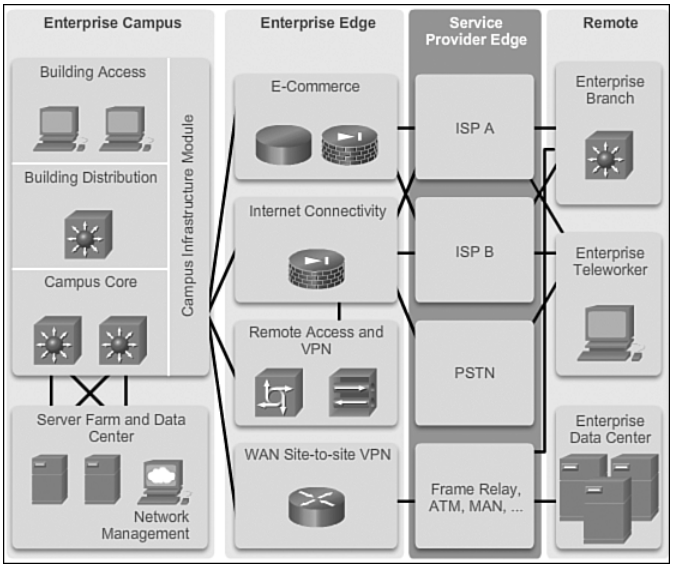


Figure 1-17 Service Provider Edge Module

The SP edge provides connectivity between the enterprise campus module to the remote enterprise data center, enterprise branch, and enterprise teleworker modules.

The SP edge module

- Spans across large geographic areas in a cost effective manner
- Converges voice, video, and data services over a single IP communications network
- Supports QoS and service level agreements
- Supports security using VPNs (IPsec / MPLS) over Layer 2 and Layer 3 WANs

When acquiring Internet services from an ISP, redundancy or failover should be considered. Redundant Internet connections vary depending if the enterprise is connecting to a single ISP or multiple ISPs.

As shown in Figure 1-18, redundant connections to a single ISP can include

- **Single-homed:** A single connection to an ISP
- **Dual-homed:** Two or more connections to a single ISP

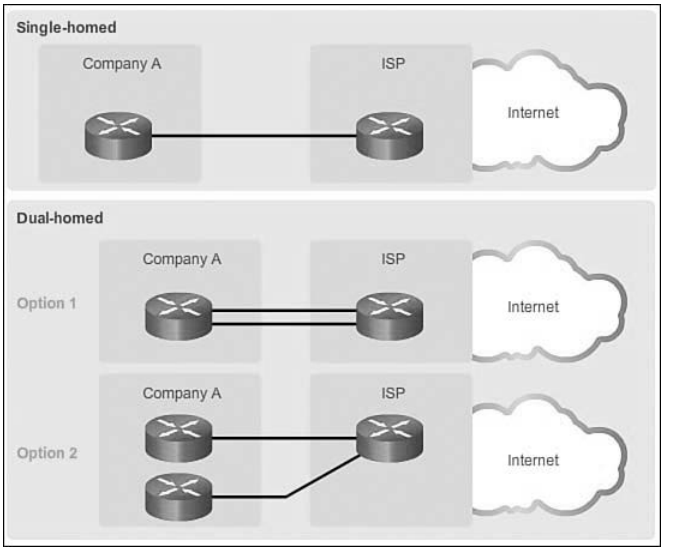


Figure 1-18 Connecting to a Single ISP

Alternatively, it is possible to set up redundancy using multiple ISPs, as shown in Figure 1-19. Options for connecting to multiple ISPs include

- **Multihomed:** Connections to two or more ISPs
- **Dual-multihomed:** Multiple connections to two or more ISPs

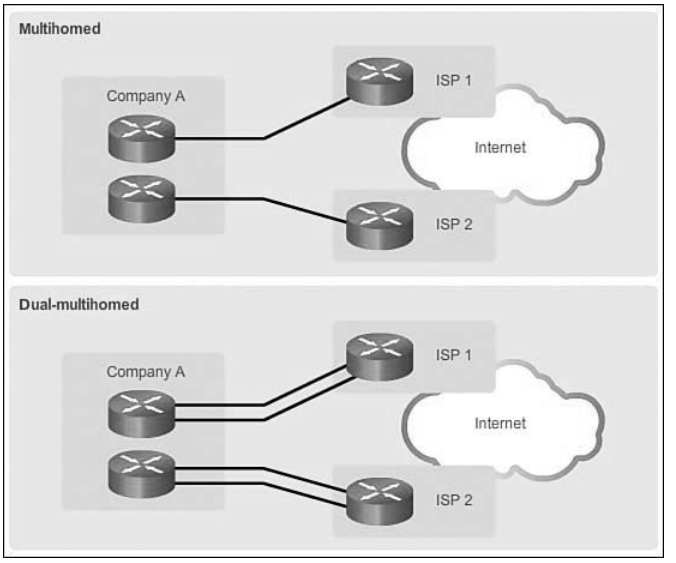


Figure 1-19 Connecting to Multiple ISPs

Remote Functional Area (1.2.2.5)

The remote functional area is responsible for remote connectivity options and includes the following modules, as shown in Figure 1-20.

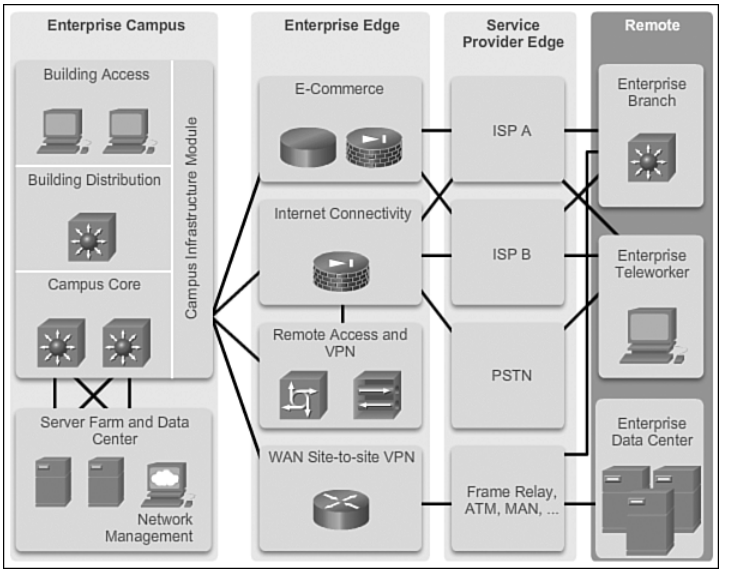


Figure 1-20 Remote Connectivity Areas

Enterprise Branch

The *enterprise branch module* includes remote branches that allow employees to work at noncampus locations. These locations are typically responsible for providing security, telephony, and mobility options to employees, as well as general connectivity into the campus network and the different components located inside the enterprise campus. The enterprise branch module allows enterprises to extend head-office applications and services, such as security, Cisco Unified Communications, and advanced application performance, to the remote branches. The edge device connecting the remote site to the central site varies depending on the needs and size of the site. Large remote sites may use high-end Cisco Catalyst switches, while smaller sites may use an ISR G2 router. These remote sites rely on the SP edge to provide services and applications from the main site. In Figure 1-20, the enterprise branch module connects to the enterprise campus site primarily using a WAN link. However, it also has an Internet link as a backup. The Internet link uses site-to-site IPsec VPN technology to encrypt corporate data.

Enterprise Teleworker

The *enterprise teleworker module* is responsible for providing connectivity for workers who operate out of different geographically dispersed locations, including home offices, hotels, or customer/client sites. The teleworker module recommends that mobile users connect to the Internet using the services of a local ISP, such as cable modem or DSL. VPN services can then be used to secure communications between the mobile worker and central campus. Integrated security- and identity-based networking services enable the enterprise to extend campus security policies to the teleworker. Staff can securely log in to the network over the VPN and gain access to authorized applications and services from a single cost-effective platform.

Enterprise Data Center

The *enterprise data center module* is a data center with all of the same functional options as a campus data center, but exists at a remote location. This provides an added layer of security as the offsite data center can provide disaster recovery and business continuance services for the enterprise. High-end switches such as the Cisco Nexus series switch use fast WAN services such as Metro Ethernet (MetroE) to connect the enterprise campus to the remote enterprise data center. Redundant data centers provide backup using synchronous and asynchronous data and application replication. Additionally, the network and devices offer server and application load balancing to maximize performance. This solution allows the enterprise to scale without major changes to the infrastructure.

Interactive Graphic

Activity 1.2.2.6: Identify Modules of the Cisco Enterprise Architecture

Go to the course online to perform this practice activity.

Evolving Network Architectures (1.3)

New technologies are constantly challenging network administrators. This section discusses new networking architecture trends.

IT Challenges (1.3.1.1)

As businesses have grown more dependent on networks for success, network architectures have evolved over the years. Traditionally, users, data, and applications were housed on premise. Users could only access network resources with company-owned computers. The network had distinct borders and access requirements. Maintaining

security, productivity, and services was simpler. Today, the network border has shifted, creating new challenges for IT departments. Networks are transforming from a data-only transportation system of connected LAN devices to a system that enables the connections of people, devices, and information in a media-rich, converged network environment.

As new technologies and end-user devices come to market, businesses and consumers must continue to adjust to this ever-changing environment. There are several new networking trends that continue to effect organizations and consumers. Some of the top trends include

- Bring your own device (BYOD)
- Online collaboration
- Video communication
- Cloud computing

These trends, while allowing for more advanced services than ever before, also introduce new security risks that IT must address.

Emerging Enterprise Architectures (1.3.1.2)

The speed of change in market and business environments is requiring IT to be more strategic than ever before. Evolving business models are creating complex technology challenges that IT must address.

To address these emerging network trends, new business network architectures are necessary. These architectures must account for the network design principles established in the Cisco Enterprise Architecture, as well as the overlaying policies and technologies that allow organizations to support emerging trends in a safe and manageable way.

To meet this need, Cisco has introduced the following three network architectures:

- Cisco Borderless Network Architecture
- Collaboration Architecture
- Data Center/Virtualization Architecture

Note

Network architectures continually evolve. The intent of this section is to provide an introduction and overview of emerging architecture trends.

Emerging Network Architectures (1.3.2)

Cisco has been at the forefront of network design for decades. They consistently adopt existing networks and develop new network architectures. This topic introduces the Cisco Borderless Network Architecture, the Collaboration Architecture, and the Data Center and Virtualization Architecture.

Cisco Borderless Networks (1.3.2.1)

The *Cisco Borderless Network Architecture* is a network solution that allows organizations and individuals to connect securely, reliably, and seamlessly to the corporate network in a BYOD environment. It is based on wired, wireless, routing, switching, security, and application optimization devices working in harmony to help IT balance demanding business challenges and changing business models.

It is not a static solution, but an evolving solution to help IT evolve its infrastructure to deliver secure, reliable, and seamless user experiences in a world with many new and shifting borders.

It enables an IT department to architect and deploy its systems and policies efficiently to all end user devices that require connection to the network. In doing this, it provides secure, reliable, and seamless access to resources from multiple locations, from multiple devices, and to applications that can be located anywhere.

Specifically, the Cisco Borderless Network Architecture delivers two primary sets of services:

- **Borderless end-point/user services:** As highlighted in Figure 1-21, borderless end-point/user services connect the various devices to provide access to network services. Devices that can connect to the borderless network can range from PCs to tablets and smartphones. It removes the location and device borders, providing unified access to wired and wireless devices. End-point/user services define the user experience and enable the attributes of secure, reliable, and seamless performance on a broad range of devices and environments, as shown in Figure 1-21. For example, most smartphones and tablets can download and use the Cisco AnyConnect software. It enables the device to establish a secure, persistent, policy-based connection for a seamless user experience.
- **Borderless network services:** As highlighted in Figure 1-22, borderless network services unify the approach to securely deliver applications to users in a highly distributed environment. It securely connects internal users and remote users and provides access to network resources. The crucial element to scaling secure access is a policy-based architecture that allows IT to implement centralized access controls.

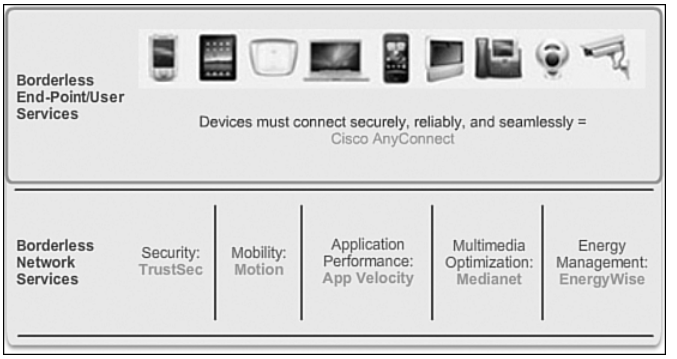


Figure 1-21 Borderless Network Architecture

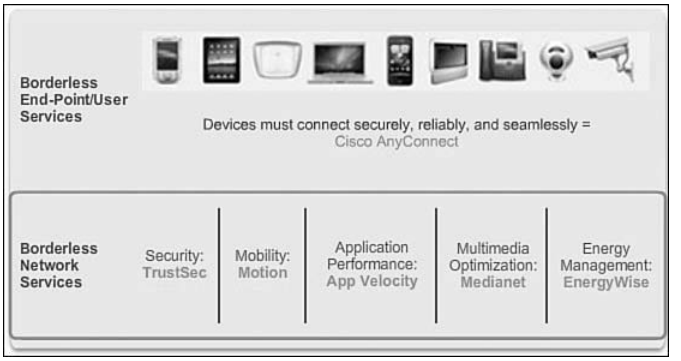


Figure 1-22 Services Supported in Borderless Networks

The borderless network architecture supports a highly secure, high-performing network that is accessible to a wide range of devices. It needs to be flexible enough to scale in its support for future growth in terms of business expansion, including BYOD, mobility and cloud computing and must be able to support the growing requirements for online voice and video.

Collaboration Architecture (1.3.2.2)

Working in a collaborative environment helps increase productivity. Collaboration and other types of groupware are used to bring people together for one reason or another: such as to socialize, to work together, to cooperate and contribute to the production of something, and to innovate.

The *Cisco Collaboration Architecture* comprises a portfolio of products, applications, software development kits (SDKs), and APIs. The individual components work together to provide a comprehensive solution.

As shown in Figure 1-23, Cisco's collaboration architecture is composed of three layers:

- **Application and Devices:** This layer contains unified communications and conference applications such as Cisco WebEx Meetings, WebEx Social, Cisco Jabber, and TelePresence. The applications within this layer help users stay connected and productive. These applications include voice, video, web conferencing, messaging, mobile applications, and enterprise social software.
- **Collaboration Services:** This layer supports collaboration applications including the following services: presence, location, session management, contact management, client frameworks, tagging, and policy and security management.
- **Network and Computer Infrastructure:** This layer is responsible for allowing collaboration anytime, from anywhere, on any device. It includes virtual machines, the network, and storage.

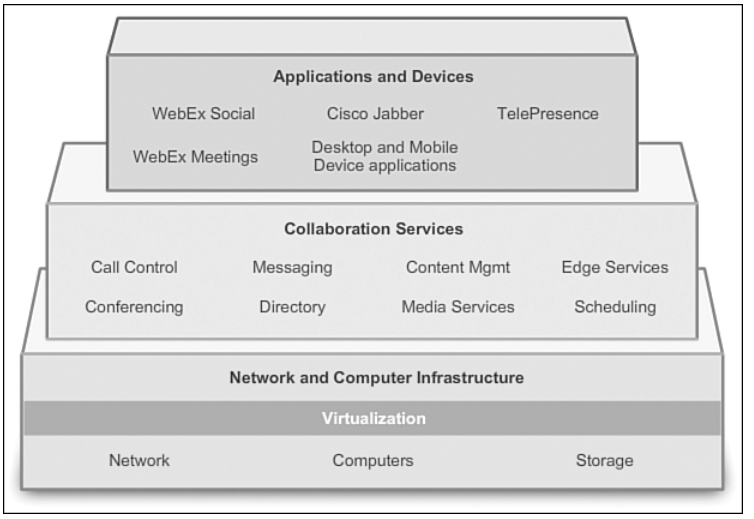


Figure 1-23 Cisco Collaboration Architecture

Data Center and Virtualization (1.3.2.3)

The *Cisco Data Center/Virtualization Architecture* is built upon Cisco Data Center 3.0. It comprises a comprehensive set of virtualization technologies and services that bring the network, computing, storage, and virtualization platforms together.

The Data Center Architecture consists of three components, as shown in Figure 1-24:

- **Cisco Unified Management Solutions:** Management solutions simplify and automate the process of deploying IT infrastructure and services with speed and enterprise reliability. Solutions operate transparently across physical and virtual resources in cloud environments.

- **Unified Fabric Solutions:** Flexible network solutions deliver network services to servers, storage, and applications, providing transparent convergence, scalability, and sophisticated intelligence. Solutions include Cisco Nexus switches, Catalyst switches, Cisco Fabric Manager, and Cisco NX-OS software.
- **Unified Computing Solutions:** Cisco's next-generation data center system unites computing, network, storage access, and virtualization into a cohesive system designed to reduce total cost of ownership (TCO) and increase business agility. The Cisco Unified Computing System (Cisco UCS) is built with blade servers, rack-mount servers, fabric interconnects, and virtual interface cards (VICs).

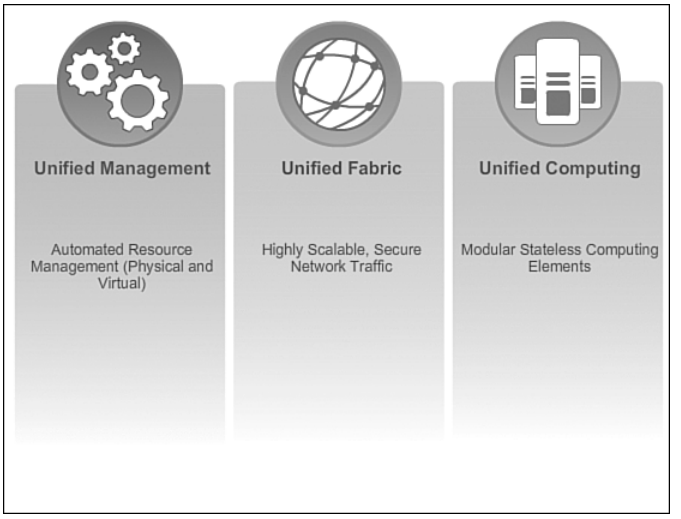


Figure 1-24 Components of the Data Center Architecture

Video

Video 1.3.2.3: Cisco Unified Fabric

Go to the course to see a short video on the Cisco Unified Fabric.

Expanding the Network (1.3.2.4)

These three architectures are built on an infrastructure of scalable and resilient hardware and software. Components of the architecture come together to build network systems that span an organization from network access to the cloud, and provide organizations with the services they need.

Building off the basic network infrastructure, organizations can use these network architectures to grow their network over time, adding features and functionality in an integrated solution.

One of the first steps in growing the network is expanding from the campus infrastructure to a network that connects remote sites through the Internet and through the WAN.

Interactive Graphic

Video 1.3.2.4: Evolution of a Corporate WAN

Go to the course to see a short video on the evolution of a network to a WAN infrastructure.

Interactive Graphic

Activity 1.3.2.5: Identify Evolving Network Architecture Terminology

Go to the course online to perform this practice activity.

Summary (1.4)

Class Activity 1.4.1.1: Borderless Innovations - Everywhere

You are the network administrator for your small- to medium-size business. Borderless network services interest you as you plan your network's future.

While planning for network policies and services, you realize that your wired and wireless networks need manageability and deployment design.

Therefore, this leads you to consider the following Cisco borderless services as possible options for your business:

- **Security:** TrustSec
- **Mobility:** Motion
- **Application performance:** App Velocity
- **Multimedia performance:** Medianet
- **Energy management:** EnergyWise

Packet Tracer Activity

Packet Tracer Activity 1.4.1.2: Skills Integration Challenge

This Packet Tracer Activity provides an opportunity to review skills from previous coursework.

Your business has just expanded into a different town and needs to expand its presence across the Internet. You are tasked with completing the upgrades to the enterprise network, which includes dual-stacked IPv4 and IPv6 as well as a variety of addressing and routing technologies.

Packet Tracer Activity

Packet Tracer Activity 1.4.1.3: Skills Integration Challenge - EIGRP

You are a network technician new to a company that has lost its last technician in the middle of a system upgrade. You are tasked with completing upgrades to the network infrastructure that has two locations. Half of the enterprise network uses IPv4 addressing, and the other half uses IPv6 addressing. The requirements also include a variety of routing and switching technologies.

The structured engineering principles of good network design include hierarchy, modularity, resiliency, and flexibility.

A typical enterprise hierarchical LAN campus network design includes the access layer, distribution layer, and the core layer. In smaller enterprise networks, a "collapsed core" hierarchy, where the distribution layer and core layer functions are implemented in a single device, can be more practical. The benefits of a hierarchical network include scalability, redundancy, performance, and maintainability.

A modular design that separates the functions of a network enables flexibility and facilitates implementation and management. The basic module blocks that are connected by the core include the access distribution block, the services block, the data center, and the enterprise edge. The Cisco Enterprise Architecture modules are used to facilitate the design of large, scalable networks. The primary modules include the enterprise campus, enterprise edge, service provider edge, enterprise data center, enterprise branch, and enterprise teleworker.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion Connecting Networks Lab Manual (978-1-58713-331-2). The Packet Tracer Activity PKA files are found in the online course.

Class Activities

Class Activity 1.0.1.2: Design Hierarchy

Class Activity 1.4.1.1: Borderless Innovations - Everywhere

Packet Tracer Activities

Packet Tracer Activity 1.4.1.2: Skills Integration Challenge - OSPF

Packet Tracer Activity 1.4.1.3: Skills Integration Challenge - EIGRP

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix, "Answers to the 'Check Your Understanding' Questions," lists the answers.

1. What are the four structured design principles?

   A. Availability, flexibility, modularity, and security
   B. Availability, hierarchy, modularity, quality of service (QoS)
   C. Flexibility, hierarchy, modularity, resiliency
   D. Flexibility, modularity, resiliency, and security
   E. Hierarchy, quality of service (QoS), resiliency, and security
   F. Hierarchy, modularity, resiliency, and security
   G. Modularity, quality of service (QoS), resiliency, and security

2. Which layer of the hierarchical network design model is often called the backbone?

   A. Access
   B. Core
   C. Distribution
   D. Network
   E. WAN
   F. Workgroup

3. Which network architecture combines individual components to provide a comprehensive solution allowing people to cooperate and contribute to the production of something?

   A. Cisco Collaboration Architecture
   B. Cisco Enterprise Campus Architecture
   C. Cisco Enterprise Branch Architecture
   D. Cisco Enterprise Data Center Architecture
   E. Cisco Borderless Network Architecture
   F. Cisco Enterprise Teleworker module

4. At which layer of the hierarchical network model do users connect to the network?

   A. Access
   B. Application
   C. Core
   D. Distribution
   E. Network

5. Which two statements regarding the Cisco AnyConnect software are true? (Choose two.)

   A. It is part of the borderless end-point/user services.
   B. It is part of the borderless network services.
   C. It is used to connect any device to the network.
   D. It is used to connect from anywhere.
   E. It is used to connect without an Internet connection.
   F. It is used to establish a secure, persistent, policy-based connection.

6. Which three devices are found in the access layer of the hierarchical network model? (Choose three.)

   A. Firewall appliance
   B. Layer 2 switch
   C. Layer 3 switch
   D. Modular multilayer switch
   E. VoIP phones
   F. Wireless access point

7. Which two statements correctly describe a collapsed core network design? (Choose two.)

   A. Also called a two-tier hierarchical network design
   B. Also called a three-tier hierarchical network design
   C. Consists of the access layer and distribution layer in one device
   D. Consists of the access layer and core layer in one device
   E. Consists of the distribution and core layer in one device

8. Which goal can be accomplished by implementing the Cisco enterprise teleworker module?

   A. It allows the enterprise to add large branch sites that span geographic areas.
   B. It allows the enterprise to deliver secure voice and data services to workers no matter where or when they work.
   C. To reduce remote security threats, it forces users who are located at main sites to log on to resources.
   D. It satisfies telephony requirements for users who are located at medium to large enterprise sites.

9. What should be considered first when starting the network design?

   A. Connectivity to the data center
   B. Connectivity to the branch site
   C. Protocols required
   D. Size of the network
   E. Type of security implemented
   F. Type of applications

10. Which network architecture functions through a combination of technologies that include wired, wireless, security, and more?

   A. Cisco Borderless Network
   B. Cisco Enterprise Branch
   C. Cisco Enterprise Campus
   D. Cisco Enterprise Edge
   E. Cisco Enterprise Teleworker

11. What does the application and device layer of the Cisco Collaboration Architecture do?

   A. It contains applications such as Cisco WebEx Meetings, Cisco Jabber, and TelePresence to help users stay connected and productive.
   B. It is responsible for allowing collaboration anytime, from anywhere, on any device.
   C. It supports collaboration applications with presence, location, session management, contact management, client frameworks, tagging, and policy and security management.

This page intentionally left blank

CHAPTER 2

Connecting to the WAN

Objectives

Upon completion of this chapter

- What is the purpose of a WAN?
- How does a circuit-switched network differ from a packet-switched network?
- How do service provider networks connect to enterprise networks?
- How do the link connection options available from private WAN infrastructures and public WAN infrastructures differ?
- What questions should you answer when choosing a WAN link connection?

Key Terms

This chapter uses the following key terms. You can find the definitions in the glossary.

service provider *page 38*

digital subscriber line (DSL) *page 40*

Point-to-Point Protocol (PPP) *page 45*

Frame Relay *page 45*

Asynchronous Transfer Mode (ATM) *page 45*

High-Level Data Link Control (HDLC) *page 45*

customer premises equipment (CPE) *page 46*

data communications equipment (DCE) *page 46*

data terminal equipment (DTE) *page 46*

demarcation point *page 46*

local loop *page 47*

central office (CO) *page 47*

toll network *page 47*

dialup modem *page 47*

access server *page 48*

broadband modem *page 48*

channel service unit / data service unit (CSU/DSU) *page 48*

circuit-switched network *page 48*

Integrated Services Digital Network (ISDN) *page 49*

packet-switched network (PSN) *page 50*

virtual circuit (VC) *page 50*

private WAN infrastructure *page 51*

public WAN infrastructure *page 51*

Synchronous Optical Networking (SONET) *page 52*

Synchronous Digital Hierarchy (SDH) *page 52*

light-emitting diodes (LEDs) *page 52*

dense wavelength-division multiplexing (DWDM) *page 53*

leased lines *page 54*

Basic Rate Interface (BRI) *page 57*

Introduction (2.0.1.1)

Businesses must connect local-area networks (LANs) together to provide communications between them, even when these LANs are far apart. Wide-area networks (WANs) are used to connect remote LANs together. A WAN may cover a city, country, or global region. A WAN is owned by a service provider, and a business pays a fee to use the provider's WAN network services.

Different technologies are used for WANs than for LANs. This chapter introduces WAN standards, technologies, and purposes. It covers selecting the appropriate WAN technologies, services, and devices to meet the changing business requirements of an evolving enterprise.

Class Activity 2.0.1.2: Branching Out

Your medium-size company is opening a new branch office to serve a wider, client-based network. This branch will focus on regular day-to-day network operations, but will also provide TelePresence, web conferencing, IP telephony, video on demand, and wireless services.

Although you know that an ISP can provide WAN routers and switches to accommodate the branch office connectivity for the network, you prefer to use your own customer premises equipment (CPE). To ensure interoperability, Cisco devices have been used in all other branch-office WANs.

As the branch-office network administrator, it is your responsibility to research possible network devices for purchase and use over the WAN.

WAN Technologies Overview (2.1)

As an organization expands, WAN connections are necessary. This section discusses the purpose of WANs, introduces WAN terminology, WAN devices, and circuit-switch / packet-switch networks.

Why a WAN? (2.1.1.1)

A WAN operates beyond the geographic scope of a LAN. As shown in Figure 2-1, WANs are used to interconnect the enterprise LAN to remote LANs in branch sites and telecommuter sites.

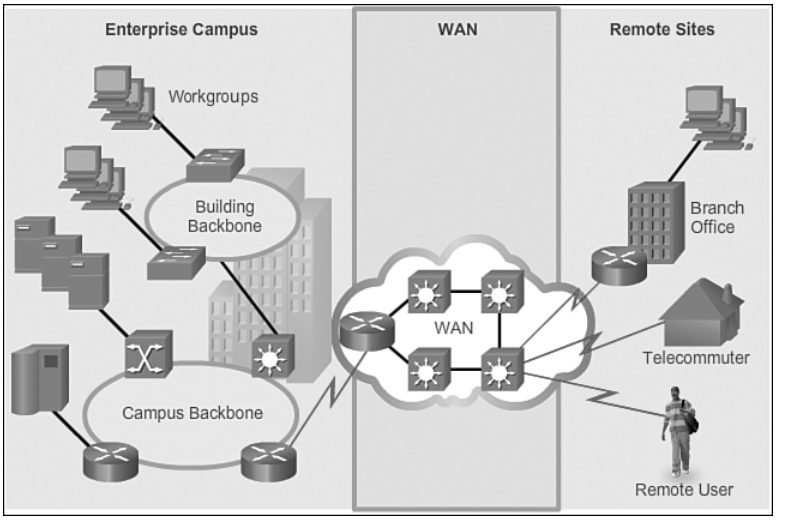


Figure 2-1 WANs Interconnect Users and LANs

A WAN is owned by a *service provider*. An organization must pay a fee to use the provider's network services to connect remote sites. WAN service providers include carriers, such as a telephone network, cable company, or satellite service. Service providers provide links to interconnect remote sites for the purpose of transporting data, voice, and video.

In contrast, LANs are typically owned by the organization and used to connect local computers, peripherals, and other devices within a single building or other small geographic area.

Are WANs Necessary? (2.1.1.2)

Without WANs, LANs would be a series of isolated networks. LANs provide both speed and cost-efficiency for transmitting data over relatively small geographic areas. However, as organizations expand, businesses require communication among geographically separated sites. The following are some examples:

- Regional or branch offices of an organization need to be able to communicate and share data with the central site.
- Organizations need to share information with other customer organizations. For example, software manufacturers routinely communicate product and promotional information to distributors that sell their products to end users.
- Employees who travel on company business frequently need to access information that resides on their corporate networks.

Home computer users also need to send and receive data across increasingly larger distances. Here are some examples:

- Consumers now commonly communicate over the Internet with banks, stores, and a variety of providers of goods and services.
- Students do research for classes by accessing library indexes and publications located in other parts of their country and in other parts of the world.

It is not feasible to connect computers across a country, or around the world, with physical cables. Therefore, different technologies have evolved to support this communication requirement. Increasingly, the Internet is being used as an inexpensive alternative to enterprise WANs. New technologies are available to businesses to provide security and privacy for their Internet communications and transactions. WANs used by themselves, or in concert with the Internet, allow organizations and individuals to meet their wide-area communication needs.

Evolving Networks (2.1.1.3)

Every business is unique, and how an organization grows depends on many factors. These factors include the type of products or service the business sells, the management philosophy of the owners, and the economic climate of the country in which the business operates.

In slow economic times, many businesses focus on increasing their profitability by improving the efficiency of their existing operations, increasing employee productivity, and lowering operating costs. Establishing and managing networks can represent significant installation and operating expenses. To justify such a large expense, companies expect their networks to perform optimally and to be able to deliver an ever increasing array of services and applications to support productivity and profitability.

The example used in this chapter is of a fictitious company called SPAN Engineering. The following topics provide an example of how the network requirements of SPAN Engineering change as the company grows from a small local business into a global enterprise.

Small Office (2.1.1.4)

SPAN Engineering is an environmental consulting firm that has developed a special process for converting household waste into electricity. SPAN Engineering is developing a small pilot project for a municipal government in its local area. The company, which has been in business for 4 years, has grown to include 15 employees: 6 engineers, 4 computer-aided drawing (CAD) designers, a receptionist, 2 senior partners, and 2 office assistants.

SPAN Engineering's management is working to win full-scale contracts after the pilot project successfully demonstrates the feasibility of their process. Until then, the company must manage its costs carefully.

For their small office, SPAN Engineering uses a single LAN to share information between computers, and to share peripherals, such as a printer, a large-scale plotter (to print engineering drawings), and fax equipment. They have recently upgraded their LAN to provide inexpensive Voice over IP (VoIP) service to save on the costs of separate phone lines for their employees.

The SPAN Engineering network consists of a small office as shown in Figure 2-2.

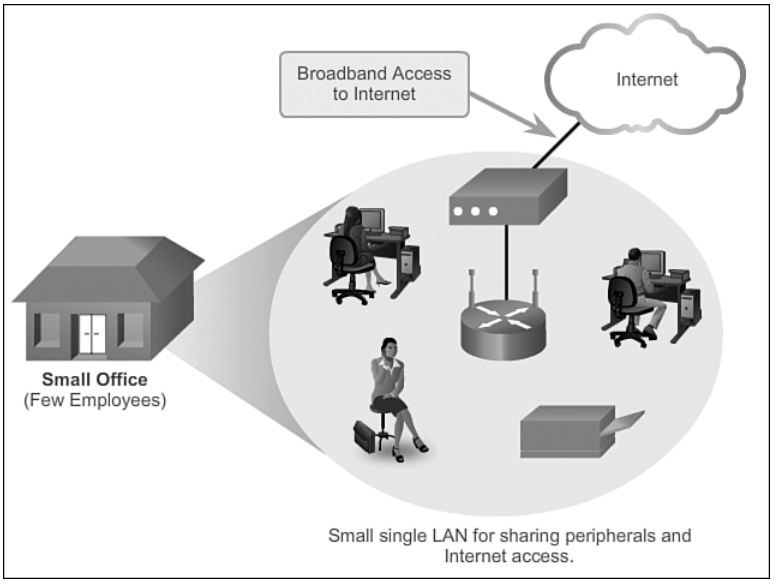


Figure 2-2 Connecting a Small Office

Connection to the Internet is through a common broadband service called *digital subscriber line (DSL)*, which is supplied by their local telephone service provider. With so few employees, bandwidth is not a significant problem.

The company cannot afford in-house IT support staff, and uses support services purchased from the DSL provider. The company also uses a hosting service rather than purchasing and operating its own FTP and email servers.

Campus Network (2.1.1.5)

Five years later, SPAN Engineering has grown rapidly. The company was contracted to design and implement a full-size waste-conversion facility soon after the successful implementation of their first pilot plant. Since then, SPAN has won other projects in neighboring municipalities, and in other parts of the country.

To handle the additional workload, the business has hired more staff and leased more office space. It is now a small- to medium-size business with several hundred employees. Many projects are being developed at the same time, and each requires a project manager and support staff. The company has organized itself into functional departments, with each department having its own organizational team. To meet its growing needs, the company has moved into several floors of a larger office building, as shown in Figure 2-3.

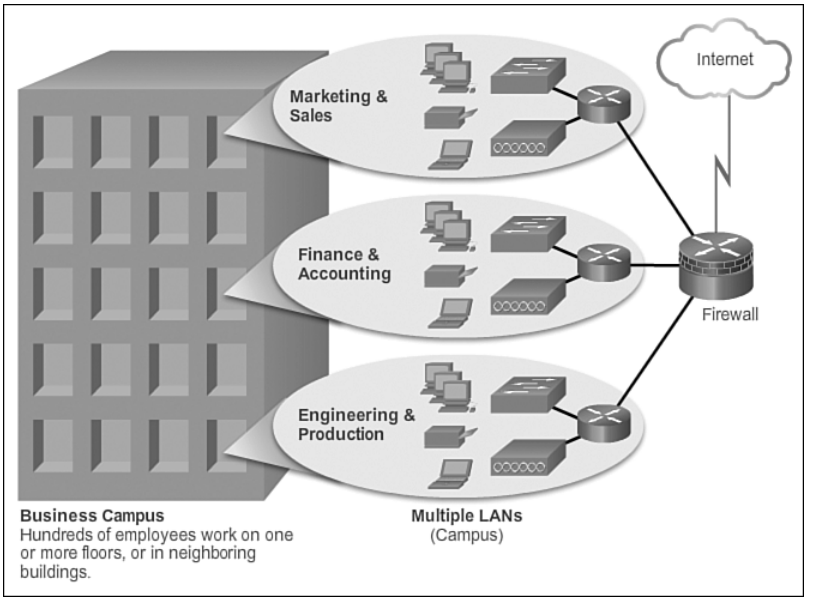


Figure 2-3 Connecting a Campus Network

As the business has expanded, the network has also grown. Instead of a single small LAN, the network now consists of several subnetworks, each devoted to a different department. For example, all the engineering staff is on one LAN, while the marketing staff is on another LAN.

These multiple LANs are joined to create a company-wide campus network which spans several floors of the building.

The business now has in-house IT staff to support and maintain the network. The network includes dedicated servers for email, data transfer, and file storage, and web-based productivity tools and applications. There is also a company intranet to provide in-house documents and information to employees. An extranet provides project information to designated customers.

Branch Networks (2.1.1.6)

Another 6 years later, SPAN Engineering has been so successful with its patented process that demand for its services has skyrocketed. New projects are underway in multiple cities. To manage those projects, the company has opened small branch offices closer to the project sites.

This situation presents new challenges to the IT team. To manage the delivery of information and services throughout the company, SPAN Engineering now has a data center, which houses the various databases and servers of the company. To ensure that all parts of the business are able to access the same services and applications regardless of where the offices are located, the company must now implement a WAN, as shown in Figure 2-4.

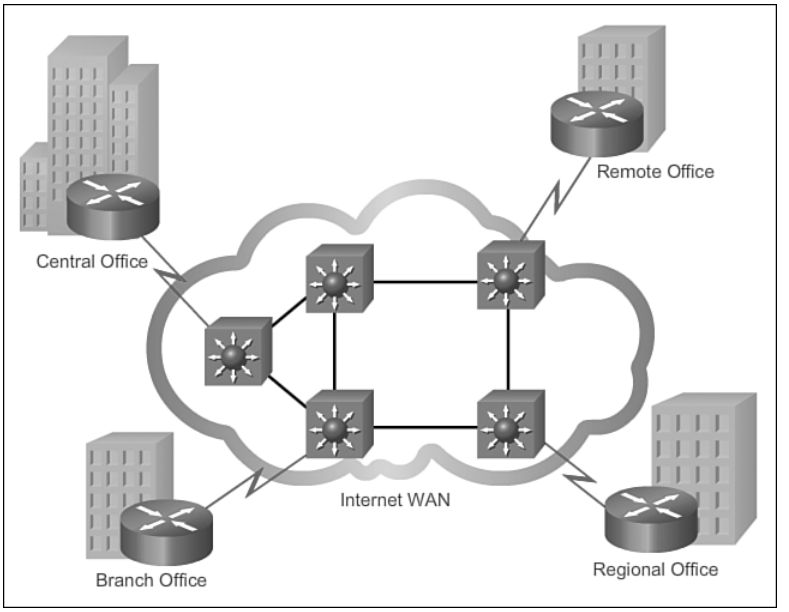


Figure 2-4 Connecting Branch Networks

Connecting to its branch sites may occur over dedicated private lines or by using the Internet. For its branch office that is in a nearby city, the company decides to use private dedicated lines through their local service provider. However, for its regional office and remote office located in another country, the Internet is an attractive WAN connection option. Although connecting offices through the Internet is economical, it introduces security and privacy issues that the IT team must address.

Distributed Network (2.1.1.7)

SPAN Engineering has now been in business for 20 years and has grown to thousands of employees distributed in offices worldwide. The cost of the network and its related services is a significant expense. The company is looking to provide its employees with the best network services at the lowest cost. Optimized network services would allow each employee to work at a high rate of efficiency.

To increase profitability, SPAN Engineering must reduce its operating expenses. It has relocated some of its office facilities to less-expensive areas. The company is also encouraging teleworking and virtual teams. Web-based applications, including web conferencing, e-learning, and online collaboration tools, are being used to increase productivity and reduce costs. Site-to-site and remote access virtual private networks (VPNs) enable the company to use the Internet to connect easily and securely with employees and facilities around the world. To meet these requirements, the network must provide the necessary converged services and secure Internet WAN connectivity to remote offices and individuals, as shown in Figure 2-5.

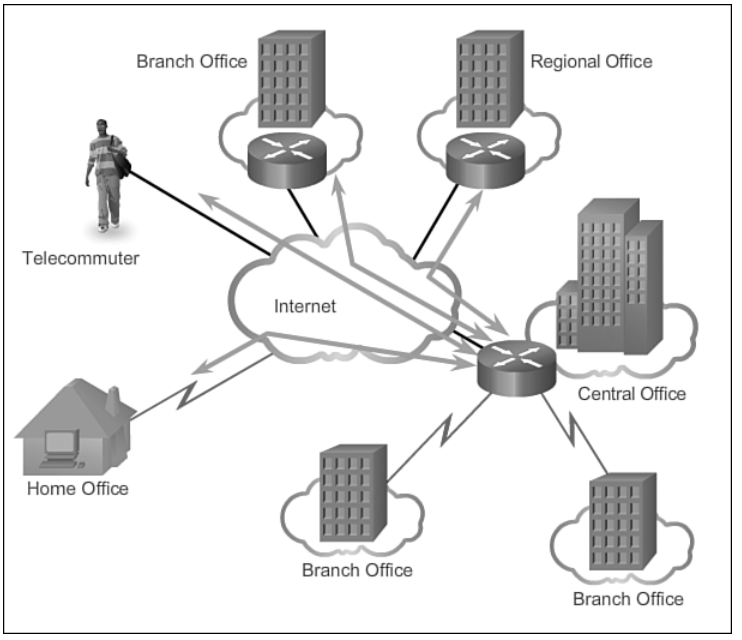


Figure 2-5 Connecting a Global Enterprise Network

As seen in this example, network requirements of a company can change dramatically as the company grows over time. Distributing employees saves costs in many ways, but it puts increased demands on the network. Not only must a network meet the day-to-day operational needs of the business, but it must also be able to adapt and grow as the company changes. Network designers and administrators meet

these challenges by carefully choosing network technologies, protocols, and service providers, and by optimizing their networks using many of the network design techniques and architectures described in this course.

Interactive Graphic

Activity 2.1.1.8: Identify WAN Topologies

Go to the course online to perform this practice activity.

WAN Operations (2.1.2)

This topic introduces common WAN terminology and devices and differentiates between circuit-switch and packet-switch networks.

WANs in the OSI Model (2.1.2.1)

As shown in Figure 2-6, WAN operations focus primarily on the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2).

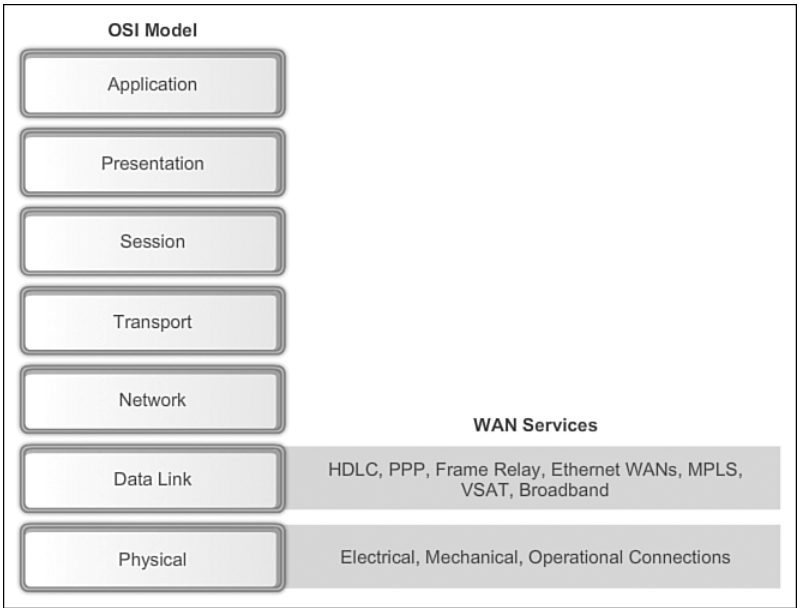


Figure 2-6 WANs Operate in Layer 1 and Layer 2

WAN access standards typically describe both physical layer delivery methods and data link layer requirements, including physical addressing, flow control, and encapsulation.

WAN access standards are defined and managed by a number of recognized authorities, including the

- Telecommunication Industry Association and the Electronic Industries Alliance (TIA/EIA)
- International Organization for Standardization (ISO)
- Institute of Electrical and Electronics Engineers (IEEE)

Layer 1 protocols describe how to provide electrical, mechanical, operational, and functional connections to the services of a communications service provider.

Layer 2 protocols define how data is encapsulated for transmission toward a remote location, and the mechanisms for transferring the resulting frames. A variety of different technologies are used, such as the ***Point-to-Point Protocol (PPP)***, ***Frame Relay***, and ***Asynchronous Transfer Mode (ATM)***. Some of these protocols use the same basic framing or a subset of the ***High-Level Data Link Control (HDLC)*** mechanism.

Most WAN links are point to point. For this reason, the address field in the Layer 2 frame is usually not used.

Common WAN Terminology (2.1.2.2)

One primary difference between a WAN and a LAN is that an organization must subscribe to an outside WAN service provider and use the WAN carrier network services to interconnect its sites and users. A WAN uses data links provided by carrier services to access the Internet and connect different locations of an organization to each other, to locations of other organizations, to external services, and to remote users.

The physical layer of a WAN describes the physical connections between the company network and the service provider network. As illustrated in Figure 2-7, common terminology is used to describe WAN components and reference points.

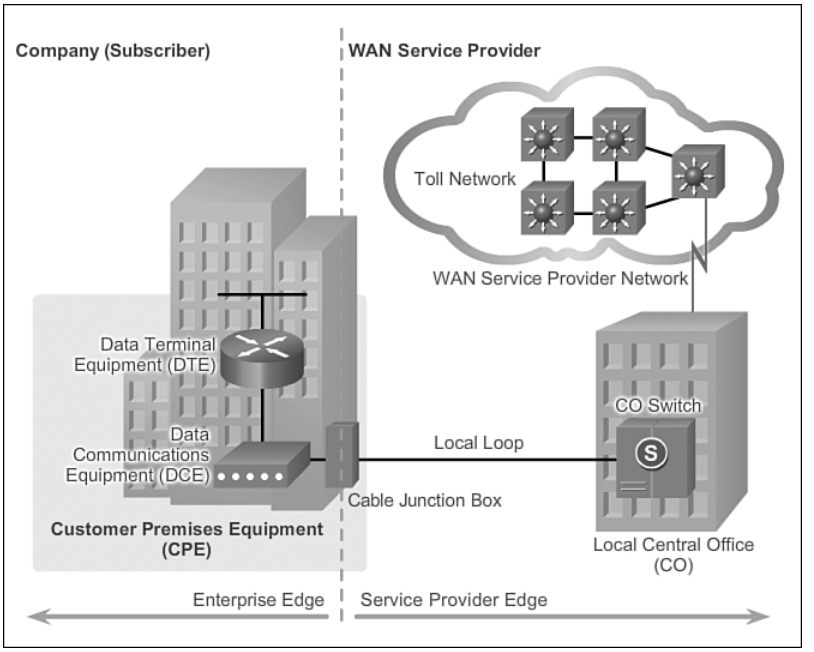


Figure 2-7 Common WAN Terminology

Specifically, these terms include

- *Customer premises equipment (CPE)*: The devices and inside wiring located on the enterprise edge connecting to a carrier link. The subscriber either owns the CPE or leases the CPE from the service provider. A subscriber, in this context, is a company that arranges for WAN services from a service provider.
- *Data communications equipment (DCE)*: Also called data circuit-terminating equipment, the DCE consists of devices that put data on the local loop. The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud.
- *Data terminal equipment (DTE)*: The customer devices that pass the data from a customer network or host computer for transmission over the WAN. The DTE connects to the local loop through the DCE.
- *Demarcation point*: A point established in a building or complex to separate customer equipment from service provider equipment. Physically, the demarcation point is the cabling junction box, located on the customer premises, that connects the CPE wiring to the local loop. It is usually placed for easy access by a technician. The demarcation point is the place where the responsibility for the connection changes from the user to the service provider. When problems arise, it is necessary to determine whether the user or the service provider is responsible for troubleshooting or repair.

- *Local loop*: The actual copper or fiber cable that connects the CPE to the CO of the service provider. The local loop is also sometimes called the "last mile."
- *Central office (CO)*: The CO is the local service provider facility or building that connects the CPE to the provider network.
- *Toll network*: This consists of the long-haul, all-digital, fiber-optic communications lines, switches, routers, and other equipment inside the WAN provider network.

WAN Devices (2.1.2.3)

As illustrated in Figure 2-8, there are various methods, and therefore devices, that are used to access the WAN connection. Service providers also have specific WAN devices within their network and devices that are required to interconnect to other WAN providers.

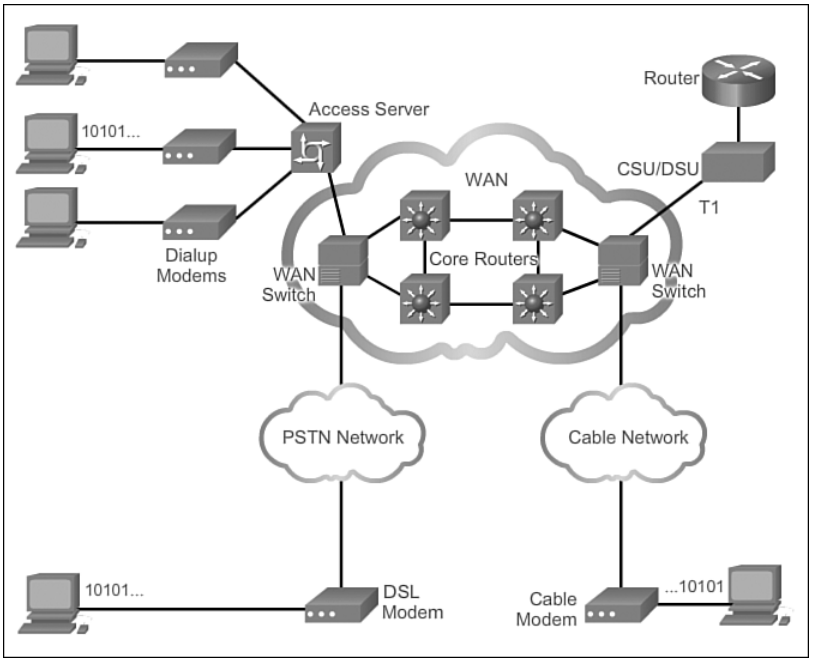


Figure 2-8 WAN Devices

The example in the figure identifies the following WAN devices:

- *Dialup modem*: Considered to be a legacy WAN technology, a voiceband modem converts (i.e., modulates) the digital signals produced by a computer into voice frequencies that can be transmitted over the analog lines of the public telephone network. On the other side of the connection, another modem converts the sounds back into a digital signal (i.e., demodulates) for input to a computer or network connection.

- *Access server*: Devices used to concentrate the dial-in and dial-out user communications of dialup modems. Considered to be a legacy technology, an access server may have a mixture of analog and digital interfaces and support hundreds of simultaneous users.
- *Broadband modem*: A type of digital modem used with high-speed DSL or cable Internet service. Both operate in a similar manner to the voiceband modem, but use higher broadband frequencies and transmission speeds.
- *Channel service unit / data service unit (CSU/DSU)*: Digital leased lines require a CSU and a DSU. A CSU/DSU can be a separate device like a modem or it can be an interface on a router. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the line frames into frames that the LAN can interpret and vice versa.
- **WAN switch:** A multiport internetworking device used in service provider networks. These devices typically switch traffic, such as Frame Relay or ATM and operate at Layer 2.
- **Router:** This is a CPE device that provides internetworking and WAN access interface ports used to connect to the service provider network. These interfaces may be serial connections, Ethernet, or other WAN interfaces. With some types of WAN interfaces, an external device, such as a DSU/CSU or modem (analog, cable, or DSL), is required to connect the router to the local service provider.
- **Core router/multilayer switch:** These are the routers and multilayer switches that reside within the service provider WAN backbone. To fulfill this role, the devices must be able to support routing protocols being used in the core and multiple high speed interfaces used in the WAN core backbone. They must also be able to forward IP packets at full speed on all of those interfaces. Key core routers interconnect to other provider core routers.

Note

The preceding list is not exhaustive, and other devices may be required depending on the WAN access technology chosen.

The type of devices used depends on the WAN technology implemented. These WAN technologies are implemented over either circuit-switched or packet-switched networks.

Circuit-Switched Networks (2.1.2.4)

A *circuit-switched network* is one that establishes a dedicated circuit (or channel) between nodes and terminals before the users may communicate. As illustrated in

Figure 2-9, circuit switching dynamically establishes a dedicated virtual connection for voice or data between a sender and a receiver. Before communication can start, it is necessary to establish the connection through the network of the service provider. It is important to note that the circuit must remain established and never change or communication will be terminated.

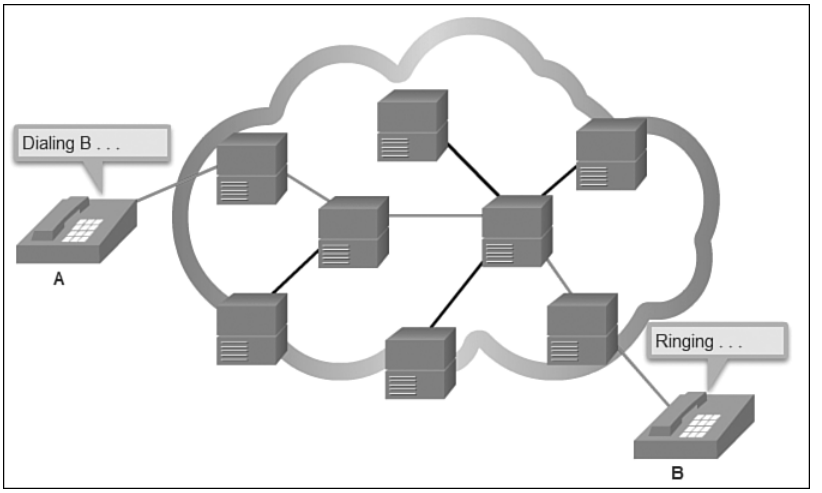


Figure 2-9 Circuit-Switched Connection

As an example, when a subscriber makes a telephone call, the dialed number is used to set switches in the exchanges along the route of the call so that there is a continuous circuit from the caller to the called party. Because of the switching operation used to establish the circuit, the telephone system is called a circuit-switched network. If the telephones are replaced with modems, then the switched circuit is able to carry computer data.

If the circuit carries computer data, the usage of this fixed capacity may not be efficient. For example, if the circuit is used to access the Internet, there is a burst of activity on the circuit while a web page is transferred. This could be followed by no activity while the user reads the page, and then another burst of activity while the next page is transferred. This variation in usage between none and maximum is typical of computer network traffic. Because the subscriber has sole use of the fixed capacity allocation, switched circuits are generally an expensive way of moving data.

The two most common types of circuit-switched WAN technologies are the public switched telephone network (PSTN) and the ***Integrated Services Digital Network (ISDN)***.

Video

Video 2.1.2.4: Circuit-Switched Network

Go to the course and play the animation to see how a circuit-switch network connects host A to host B.

Packet-Switched Networks (2.1.2.5)

In contrast to circuit switching, packet switching splits traffic data into packets that are routed over a shared network. Packet-switching networks do not require a circuit to be established, and they allow many pairs of nodes to communicate over the same channel.

The routers in a ***packet-switched network (PSN)*** determine the links that packets must be sent over based on the addressing information in each packet. The following are two approaches to this link determination:

- **Connectionless systems:** Full addressing information must be carried in each packet. Each router must evaluate the address to determine where to send the packet. An example of a connectionless system is the Internet.
- **Connection-oriented systems:** The network predetermines the route for a packet, and each packet only has to carry an identifier. The router determines the onward route by looking up the identifier in tables held in memory. The set of entries in the tables identifies a particular route or circuit through the system. When the circuit is established temporarily while a packet is traveling through it, and then breaks down again, it is called a ***virtual circuit (VC)***. An example of a connection-oriented system is Frame Relay. In the case of Frame Relay, the identifiers used are called data-link connection identifiers (DLCIs).

Because the internal links between the switches are shared between many users, the cost of packet switching is lower than that of circuit-switching. However, delays (latency) and variability of delay (jitter) are greater in packet-switched networks than in circuit-switched networks. This is because the links are shared and because packets must be entirely received at one switch before moving to the next. Despite the latency and jitter inherent in shared networks, modern technology allows satisfactory transport of voice and video communications on these networks.

Video

Video 2.1.2.5: Packet-Switched Network

Go to the course and play the animation to see how a packet-switch network connects host A to host B. In the animation, SRV1 is sending data to SRV2. As the packet traverses the provider network, it arrives at the second provider switch. The packet is added to the queue and forwarded after the other packets in the queue have been forwarded. Eventually, the packet reaches SRV2.

Interactive Graphic

Activity 2.1.2.6: Identify WAN Terminology

Go to the course online to perform this practice activity.

Selecting a WAN Technology (2.2)

Corporate networks can be interconnected using private WAN infrastructures and public WAN infrastructures. This section discusses both types of infrastructures.

WAN Link Connection Options (2.2.1.1)

There are several WAN access connection options that ISPs can use to connect the local loop to the enterprise edge. These WAN access options differ in technology, speed, and cost. Each has distinct advantages and disadvantages. Familiarity with these technologies is an important part of network design.

As summarized in Figure 2-10, an enterprise can get WAN access over a

- *Private WAN infrastructure*: Service providers may offer dedicated point-to-point leased lines, circuit-switched links, such as PSTN or ISDN, and packet-switched links, such as Ethernet WAN, ATM, or Frame Relay.
- *Public WAN infrastructure*: Service provider may offer broadband Internet access using digital subscriber line (DSL), cable, and satellite access. Broadband connection options are typically used to connect small offices and telecommuting employees to a corporate site over the Internet. Data traveling between corporate sites over the public WAN infrastructure should be protected using VPNs.

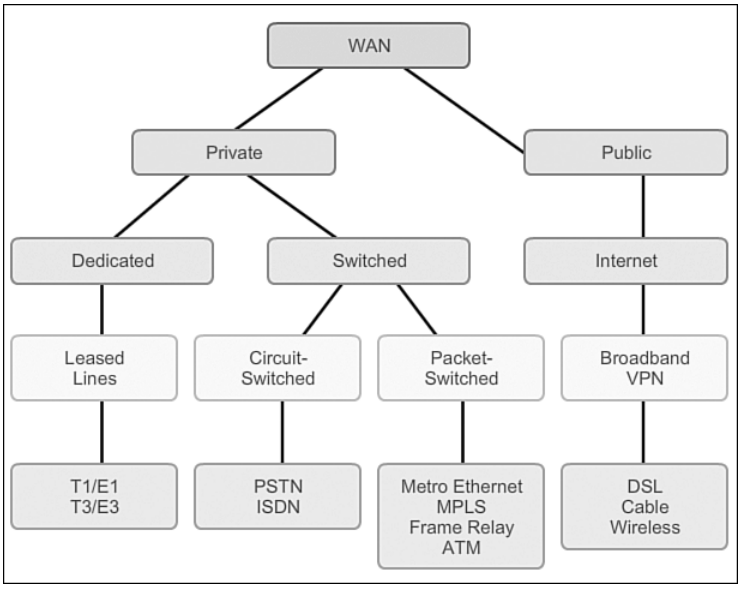


Figure 2-10 WAN Access Options

The topology in Figure 2-11 illustrates some of these WAN access technologies.

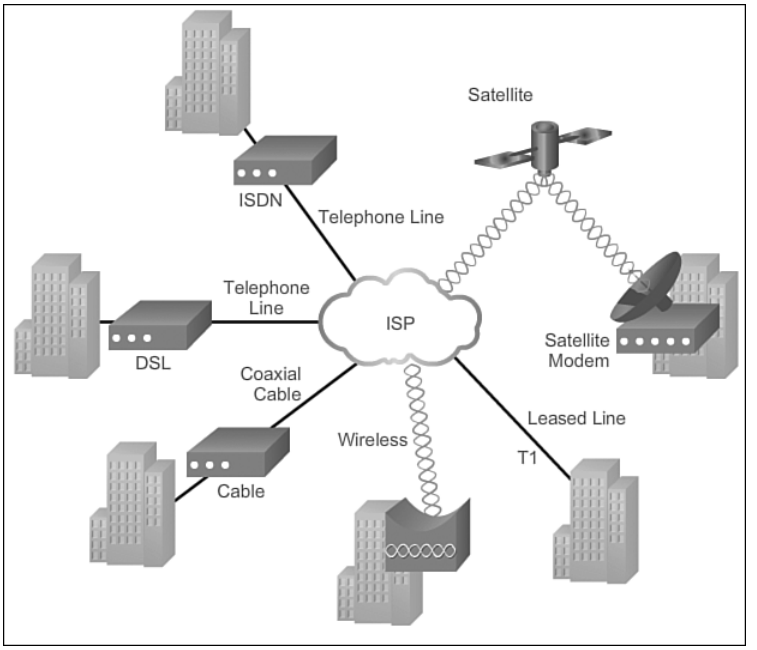


Figure 2-11 WAN Access Technologies

Service Provider Network Infrastructure (2.2.1.2)

When a WAN service provider receives data from a client at a site, it must forward the data to the remote site for final delivery to the recipient. In some cases, the remote site may be connected to the same service provider as the originating site. In other cases, the remote site may be connected to a different ISP, and the originating ISP must pass the data to the connecting ISP.

Long-range communications are usually those connections between ISPs or between branch offices in very large companies.

Service provider networks are complex. They consist mostly of high-bandwidth fiber-optic media, using either the ***Synchronous Optical Networking (SONET)*** or ***Synchronous Digital Hierarchy (SDH)*** standard. These standards define how to transfer multiple data, voice, and video traffic over optical fiber using lasers or ***light-emitting diodes (LEDs)*** over great distances.

Note

SONET is an American-based ANSI standard, while SDH is a European-based ETSI and ITU standard. Both are essentially the same and, therefore, often listed as SONET/SDH.

A newer fiber-optic media development for long-range communications is called *dense wavelength-division multiplexing (DWDM)*. DWDM multiplies the amount of bandwidth that a single strand of fiber can support. As illustrated in Figure 2-12, DWDM assigns incoming signals specific color wavelengths. These signals are transmitted over the fiber-optic cable to the end device, which then separates the traffic accordingly.

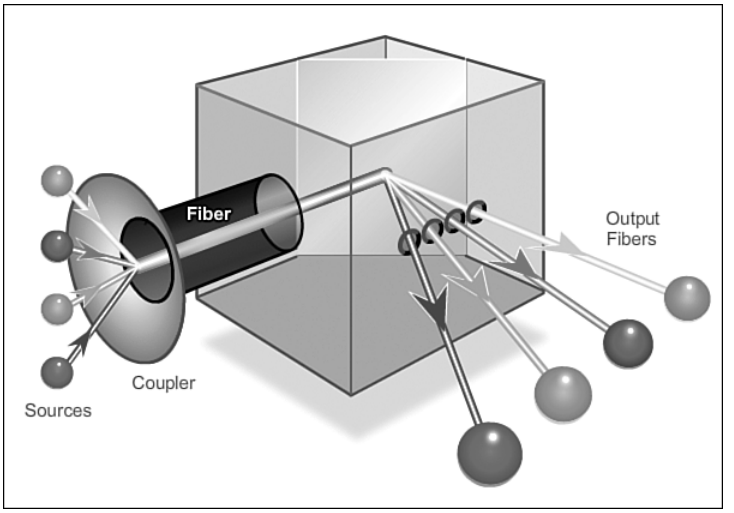


Figure 2-12 DWDM Concept

DWDM circuits are used in all modern submarine communications cable systems and other long-haul circuits.

Specifically, DWDM

- Enables bidirectional communications over one strand of fiber
- Assigns incoming optical signals to specific wavelengths of light (i.e., frequencies)
- Each channel is capable of carrying a 10-Gbps multiplexed signal
- Can multiplex more than 80 different channels of data (i.e., wavelengths) onto a single fiber
- Can amplify these wavelengths to boost the signal strength
- Supports SONET and SDH standards

Interactive Graphic

Activity 2.2.1.3: Classify WAN Access Options

Go to the course online to perform this practice activity.

Private WAN Infrastructures (2.2.2)

In this topic, private WAN infrastructures are discussed including leased lines, dialup access, ISDN, Frame Relay, ATM, MPLS, and Ethernet WANs, and VSAT.

Leased Lines (2.2.2.1)

When permanent dedicated connections are required, a point-to-point link is used to provide a pre-established WAN communications path from the customer premises to the provider network. Point-to-point lines are usually leased from a service provider and are called *leased lines*.

Leased lines have existed since the early 1950s, and for this reason are referred to by different names, such as leased circuits, serial link, serial line, point-to-point link, and T1/E1 or T3/E3 lines. The term leased line refers to the fact that the organization pays a monthly lease fee to a service provider to use the line. Leased lines are available in different capacities and are generally priced based on the bandwidth required and the distance between the two connected points.

In North America, service providers use the T-carrier system to define the digital transmission capability of a serial copper media link, while Europe uses the E-carrier system, as shown in Figure 2-13.

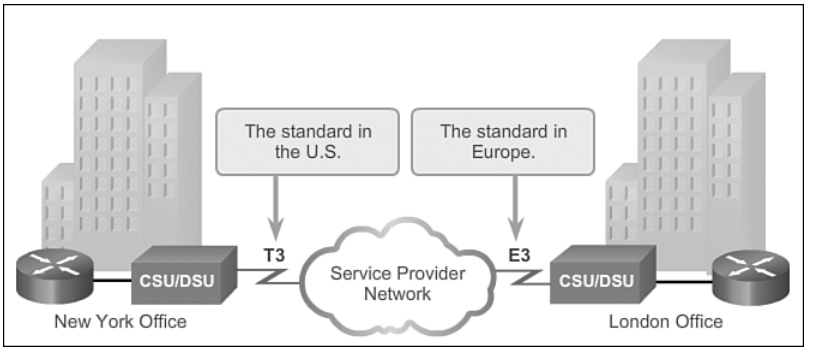


Figure 2-13 Sample Leased Line Topology

For instance, a T1 link supports 1.544 Mbps, an E1 supports 2.048 Mbps, a T3 supports 43.7 Mbps, and an E3 connection supports 34.368 Mbps. Optical Carrier (OC) transmission rates are used to define the digital transmitting capacity of a fiber-optic network.

The advantages of leased lines include

- **Simplicity:** Point-to-point communication links require minimal expertise to install and maintain.

- **Quality**: Point-to-point communication links usually offer high service quality, if they have adequate bandwidth. The dedicated capacity removes latency or jitter between the endpoints.
- **Availability**: Constant availability is essential for some applications, such as e-commerce. Point-to-point communication links provide permanent, dedicated capacity, which is required for VoIP or Video over IP.

The disadvantages of leased lines include

- **Cost**: Point-to-point links are generally the most expensive type of WAN access. The cost of leased line solutions can become significant when they are used to connect many sites over increasing distances. In addition, each endpoint requires an interface on the router, which increases equipment costs.
- **Limited flexibility**: WAN traffic is often variable, and leased lines have a fixed capacity, so that the bandwidth of the line seldom matches the need exactly. Any change to the leased line generally requires a site visit by ISP personnel to adjust capacity.

The Layer 2 protocol is usually HDLC or PPP.

Dialup (2.2.2.2)

Dialup WAN access may be required when no other WAN technology is available. For example, a remote location could use a modem and analog dialed telephone lines to provide low-capacity and dedicated switched connections. Dialup access is suitable when intermittent, low-volume data transfers are needed.

Traditional telephony uses a copper cable for the local loop to connect the telephone handset in the subscriber premises to the CO. The signal on the local loop during a call is a continuously varying electronic signal that is a translation of the subscriber voice into an analog signal.

Traditional local loops can transport binary computer data through the voice telephone network using a modem. The modem modulates the binary data into an analog signal at the source and demodulates the analog signal to binary data at the destination. The physical characteristics of the local loop and its connection to the PSTN limit the rate of the signal to less than 56 Kbps.

For small businesses, these relatively low-speed dialup connections are adequate for the exchange of sales figures, prices, routine reports, and email. Using automatic dialup at night or on weekends for large file transfers and data backup can take advantage of lower off-peak tariffs (toll charges). Tariffs are based on the distance between the endpoints, time of day, and the duration of the call.

The advantages of modem and analog lines are simplicity, availability, and low implementation cost. The disadvantages are the low data rates and a relatively long connection time. The dedicated circuit has little delay or jitter for point-to-point traffic, but voice or video traffic does not operate adequately at these low bit rates.

Figure 2-14 displays a sample topology of two remote sites interconnecting with dialup modems.

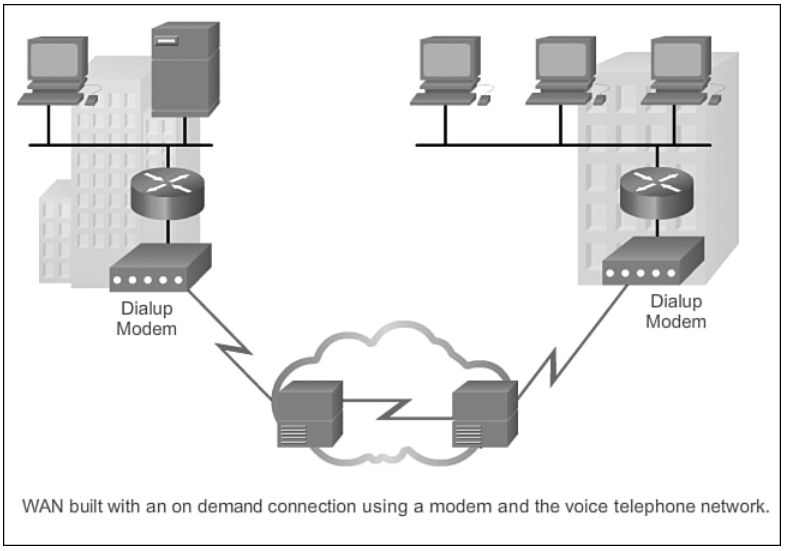


Figure 2-14 Sample Dialup Topology

Note

Although very few enterprises support dialup access, it is still a viable solution for remote areas with limited WAN access options.

ISDN (2.2.2.3)

Integrated Services Digital Network (ISDN) is a circuit-switching technology that enables the local loop of a PSTN to carry digital signals, resulting in higher-capacity switched connections.

ISDN changes the internal connections of the PSTN from carrying analog signals to time-division multiplexed (TDM) digital signals. TDM allows two or more signals, or bit streams, to be transferred as subchannels in one communication channel. The signals appear to transfer simultaneously; but physically, the signals are taking turns on the channel.

Figure 2-15 displays a sample ISDN topology. The ISDN connection may require a terminal adapter (TA), which is a device used to connect ISDN Basic Rate Interface (BRI) connections to a router.

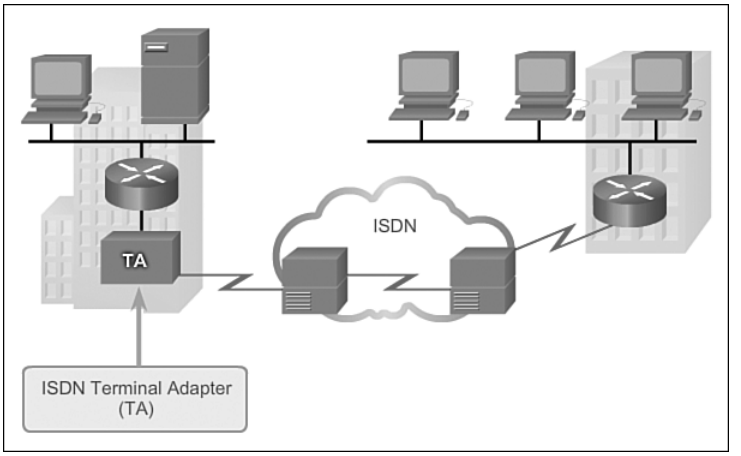


Figure 2-15 Sample ISDN Topology

ISDN turns the local loop into a TDM digital connection. This change enables the local loop to carry digital signals that result in higher-capacity switched connections. The connection uses 64-Kbps bearer channels (B) for carrying voice or data and a signaling delta channel (D) for call setup and other purposes.

There are two types of ISDN interfaces:

- *Basic Rate Interface (BRI)*: ISDN BRI is intended for the home and small enterprise and provides two 64-Kbps B channels and one 16-Kbps D channel. The BRI D channel is designed for control and often underused, because it has only two B channels to control (Figure 2-16).

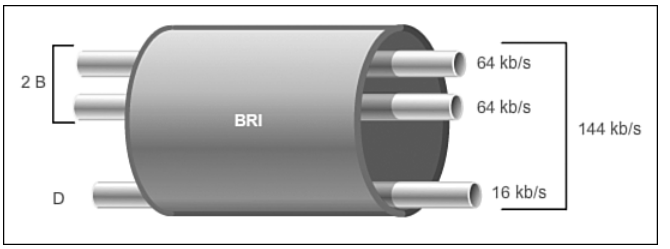


Figure 2-16 ISDN BRI

- *Primary Rate Interface (PRI)*: ISDN is also available for larger installations. In North America, PRI delivers 23 B channels with 64 Kbps and 1 D channel with 64 Kbps for a total bit rate of up to 1.544 Mbps. This includes some additional

overhead for synchronization. In Europe, Australia, and other parts of the world, ISDN PRI provides 30 B channels and 1 D channel, for a total bit rate of up to 2.048 Mbps, including synchronization overhead (see Figure 2-17).

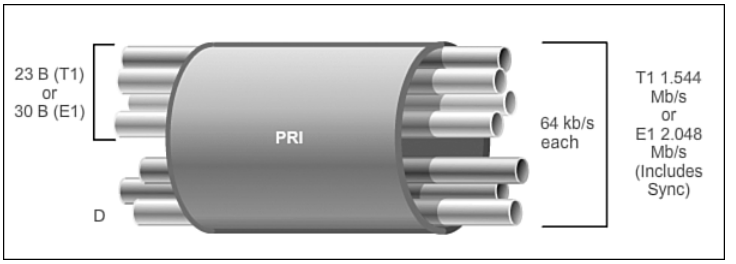


Figure 2-17 ISDN PRI

BRI has a call setup time that is less than a second, and the 64-Kbps B channel provides greater capacity than an analog modem link. If greater capacity is required, a second B channel can be activated to provide a total of 128 Kbps. Although inadequate for video, this permits several simultaneous voice conversations in addition to data traffic.

Another common application of ISDN is to provide additional capacity as needed on a leased line connection. The leased line is sized to carry average traffic loads while ISDN is added during peak demand periods. ISDN is also used as a backup if the leased line fails. ISDN tariffs are based on a per-B-channel basis and are similar to those of analog voice connections.

With PRI ISDN, multiple B channels can be connected between two endpoints. This allows for videoconferencing and high-bandwidth data connections with no latency or jitter. However, multiple connections can be very expensive over long distances.

Note

Although ISDN is still an important technology for telephone service provider networks, it is declining in popularity as an Internet connection option with the introduction of high-speed DSL and other broadband services.

Frame Relay (2.2.2.4)

Frame Relay is a simple Layer 2 nonbroadcast multiaccess (NBMA) WAN technology used to interconnect enterprise LANs. A single router interface can be used to connect to multiple sites using PVCs. PVCs are used to carry both voice and data traffic between a source and destination, and support data rates up to 4 Mbps, with some providers offering even higher rates.

An edge router only requires a single interface, even when multiple virtual circuits (VCs) are used. The short-leased line to the Frame Relay network edge allows cost-effective connections between widely scattered LANs.

Frame Relay creates PVCs, which are uniquely identified by a data-link connection identifier (DLCI). The PVCs and DLCIs ensure bidirectional communication from one DTE device to another.

For instance, in the example in Figure 2-18 R1 will use DLCI 102 to reach R2, while R2 will use DLCI 201 to reach R1.

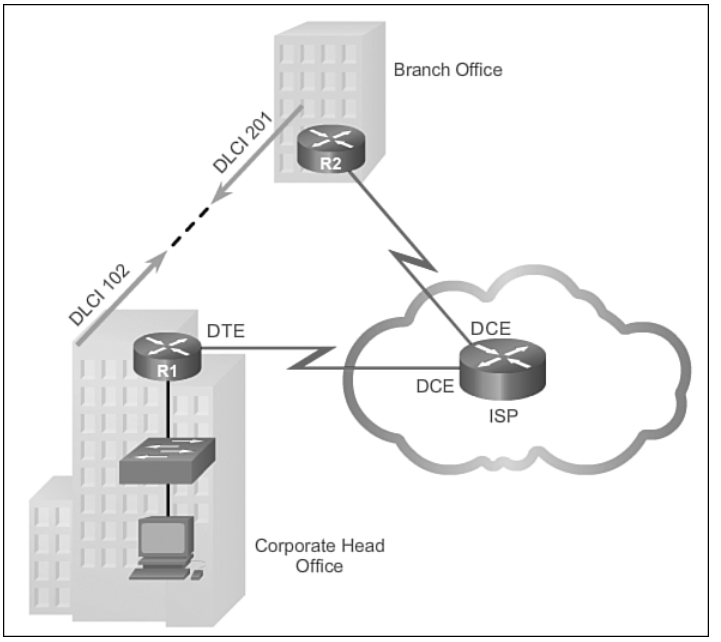


Figure 2-18 Sample Frame Relay Topology

ATM (2.2.2.5)

Asynchronous Transfer Mode (ATM) technology is capable of transferring voice, video, and data through private and public networks. It is built on a cell-based architecture rather than on a frame-based architecture. ATM cells are always a fixed length of 53 bytes. The ATM cell contains a 5-byte ATM header followed by 48 bytes of ATM payload. Small fixed-length cells are well-suited for carrying voice and video traffic because this traffic is intolerant of delay. Video and voice traffic do not have to wait for larger data packets to be transmitted.

The 53-byte ATM cell is less efficient than the bigger frames and packets of Frame Relay. Furthermore, the ATM cell has at least 5 bytes of overhead for each 48-byte payload. When the cell is carrying segmented network layer packets, the overhead is

higher because the ATM switch must be able to reassemble the packets at the destination. A typical ATM line needs almost 20 percent greater bandwidth than Frame Relay to carry the same volume of network layer data.

ATM was designed to be extremely scalable and to support link speeds of T1/E1 to OC-12 (622 Mbps) and faster.

ATM offers both PVCs and SVCs, although PVCs are more common with WANs. As with other shared technologies, ATM allows multiple VCs on a single leased-line connection to the network edge.

In the example in Figure 2-19, the ATM switch transmits four different traffic flows consisting of video, VoIP, web, and email.

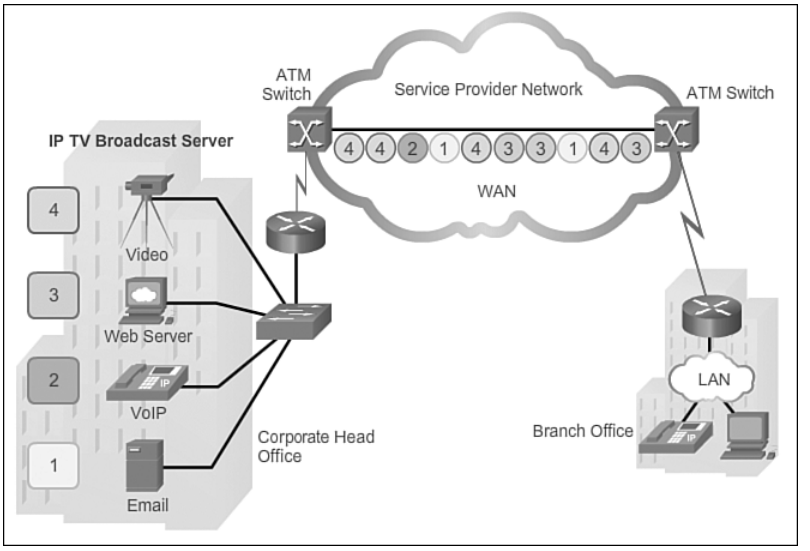


Figure 2-19 Sample ATM Topology

Ethernet WAN (2.2.2.6)

Ethernet was originally developed to be a LAN access technology. At that time however, it really was not suitable as a WAN access technology because the maximum cable length supported was only up to a kilometer. However, newer Ethernet standards using fiber-optic cables have made Ethernet a reasonable WAN access option. For instance, the IEEE 1000BASE-LX standard supports fiber-optic cable lengths of 5 km, while the IEEE 1000BASE-ZX standard supports up to 70 km cable lengths.

Service providers now offer Ethernet WAN service using fiber-optic cabling. The Ethernet WAN service can go by many names, including *Metropolitan Ethernet (MetroE)*, *Ethernet over MPLS (EoMPLS)*, and *Virtual Private LAN Service (VPLS)*.

Figure 2-20 displays a sample Ethernet WAN topology.

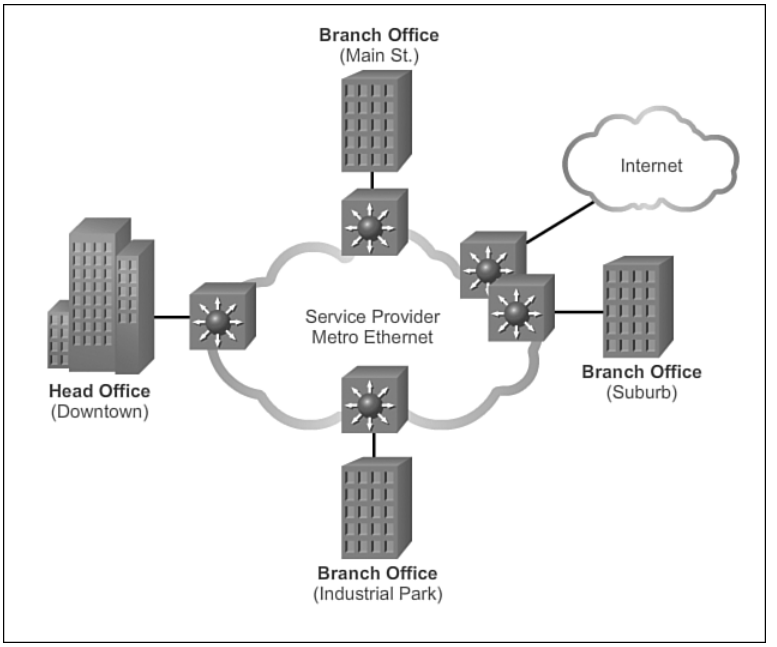


Figure 2-20 Sample Ethernet WAN Topology

Benefits of Ethernet WAN include

- **Reduced expenses and administration:** Ethernet WAN provides a switched, high-bandwidth Layer 2 network capable of managing data, voice, and video all on the same infrastructure. This characteristic increases bandwidth and eliminates expensive conversions to other WAN technologies. The technology enables businesses to inexpensively connect numerous sites, in a metropolitan area, to each other and to the Internet.
- **Easy integration with existing networks:** Ethernet WAN connects easily to existing Ethernet LANs, reducing installation costs and time.
- **Enhanced business productivity:** Ethernet WAN enables businesses to take advantage of productivity-enhancing IP applications that are difficult to implement on TDM or Frame Relay networks, such as hosted IP communications, VoIP, and streaming and broadcast video.

Note

Ethernet WANs have gained in popularity and are now commonly being used to replace the traditional Frame Relay and ATM WAN links.

MPLS (2.2.2.7)

Multiprotocol Label Switching (MPLS) is a multiprotocol high-performance WAN technology that directs data from one router to the next based on short path labels rather than IP network addresses.

MPLS has several defining characteristics. It is multiprotocol, meaning it has the ability to carry any payload including IPv4, IPv6, Ethernet, ATM, DSL, and Frame Relay traffic. It uses labels that tell a router what to do with a packet. The labels identify paths between distant routers rather than endpoints, and while MPLS actually routes IPv4 and IPv6 packets, everything else is switched.

MPLS is a service provider technology. Leased lines deliver bits between sites, and Frame Relay and Ethernet WAN deliver frames between sites. However, MPLS can deliver any type of packet between sites. MPLS can encapsulate packets of various network protocols. It supports a wide range of WAN technologies, including T-carrier / E-carrier links, Carrier Ethernet, ATM, Frame Relay, and DSL.

The sample topology in Figure 2-21 illustrates how MPLS is used.

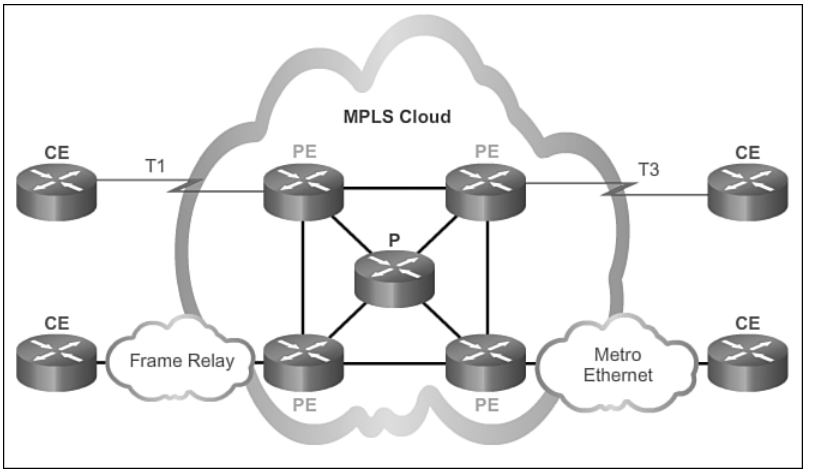


Figure 2-21 Sample MPLS Topology

Notice that the different sites can connect to the MPLS cloud using different access technologies. In the figure, CE refers to the customer edge, PE is the provider edge router, which adds and removes labels, while P is an internal provider router, which switches MPLS labeled packets.

Note

MPLS is primarily a service provider WAN technology.

VSAT (2.2.2.8)

All private WAN technologies discussed so far used either copper or fiber-optic media. What if an organization needs connectivity in a remote location where there are no service providers that offer WAN service?

Very small aperture terminal (VSAT) is a solution that creates a private WAN using satellite communications. A VSAT is a small satellite dish similar to those used for home Internet and TV. VSATs create a private WAN while providing connectivity to remote locations.

Specifically, a router connects to a satellite dish that is pointed to a service provider's satellite in a geosynchronous orbit in space. The signals must travel approximately 35,786 km (22,236 miles) to the satellite and back.

The example in Figure 2-22 displays a VSAT dish on the roofs of the buildings communicating with a satellite dish thousands of kilometers away in space.

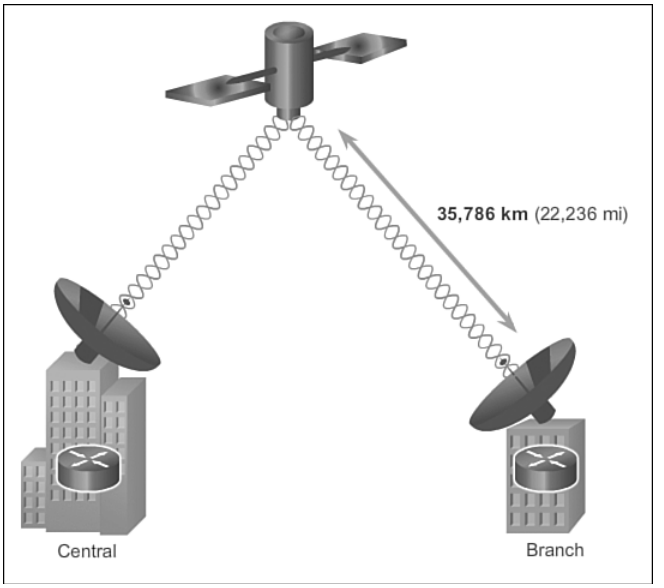


Figure 2-22 Sample VSAT Topology

Interactive Graphic

Activity 2.2.2.9: Identify Private WAN Infrastructure Terminology

Go to the course online to perform this practice activity.

Public WAN Infrastructure (2.2.3)

In this topic, public WAN infrastructures are discussed, including DSL, cable, wireless, 3G/4G cellular, as well as the need to secure data using site-to-site VPNs and remote-access VPNs.

DSL (2.2.3.1)

DSL technology is an always-on connection technology that uses existing twisted-pair telephone lines to transport high-bandwidth data, and provides IP services to subscribers. A *DSL modem* converts an Ethernet signal from the user device to a DSL signal, which is transmitted to the central office.

Multiple DSL subscriber lines are multiplexed into a single high-capacity link using a *DSL access multiplexer (DSLAM)* at the provider location. DSLAMs incorporate TDM technology to aggregate many subscriber lines into a single medium, generally a T3 (DS3) connection. Current DSL technologies use sophisticated coding and modulation techniques to achieve fast data rates.

There is a wide variety of DSL types, standards, and emerging standards. DSL is now a popular choice for enterprise IT departments to support home workers. Generally, a subscriber cannot choose to connect to an enterprise network directly, but must first connect to an ISP, and then an IP connection is made through the Internet to the enterprise. Security risks are incurred in this process, but can be mediated with security measures.

The topology in Figure 2-23 displays a sample DSL WAN connection.

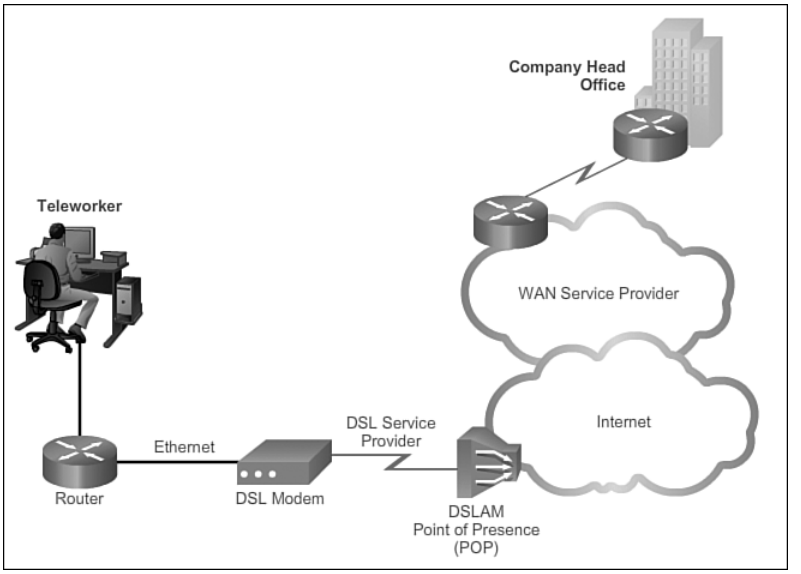


Figure 2-23 Sample DSL Topology

Cable (2.2.3.2)

Coaxial cable is widely used in urban areas to distribute television signals. Network access is available from many cable television providers. This allows for greater bandwidth than the conventional telephone local loop.

Cable modems provide an always-on connection and a simple installation. A subscriber connects a computer or LAN router to the cable modem, which translates the digital signals into the broadband frequencies used for transmitting on a cable television network. The local cable TV office, which is called the cable *headend*, contains the computer system and databases needed to provide Internet access. The most important component located at the headend is the *cable modem termination system (CMTS)*, which sends and receives digital cable modem signals on a cable network and is necessary for providing Internet services to cable subscribers.

Cable modem subscribers must use the ISP associated with the service provider. All the local subscribers share the same cable bandwidth. As more users join the service, available bandwidth may be below the expected rate.

The topology in Figure 2-24 displays a sample cable WAN connection.

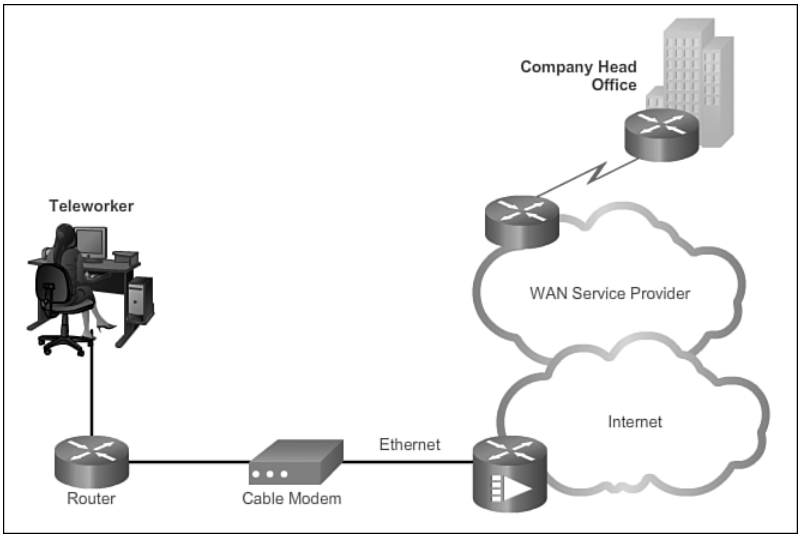


Figure 2-24 Sample Cable Topology

Wireless (2.2.3.3)

Wireless technology uses the unlicensed radio spectrum to send and receive data. The unlicensed spectrum is accessible to anyone who has a wireless router and wireless technology in the device they are using.

Until recently, one limitation of wireless access has been the need to be within the local transmission range (typically less than 100 feet) of a wireless router or a wireless modem that has a wired connection to the Internet. The following new developments in broadband wireless technology are changing this situation:

- *Municipal Wi-Fi*: Many cities have begun setting up municipal wireless networks. Some of these networks provide high-speed Internet access for free or for substantially less than the price of other broadband services. Others are for city use only, allowing police and fire departments and other city employees to do certain aspects of their jobs remotely. To connect to a municipal Wi-Fi, a subscriber typically needs a wireless modem, which provides a stronger radio and directional antenna than conventional wireless adapters. Most service providers provide the necessary equipment for free or for a fee, much like they do with DSL or cable modems.
- *WiMAX*: Worldwide Interoperability for Microwave Access (WiMAX) is a new technology that is just beginning to come into use. It is described in the IEEE standard 802.16. WiMAX provides high-speed broadband service with wireless access and provides broad coverage like a cell phone network rather than through small Wi-Fi hotspots. WiMAX operates in a similar way to Wi-Fi, but at higher speeds, over greater distances, and for a greater number of users. It uses a network of WiMAX towers that are similar to cell phone towers. To access a WiMAX network, subscribers must subscribe to an ISP with a WiMAX tower within 30 miles of their location. They also need some type of WiMAX receiver and a special encryption code to get access to the base station.
- *Satellite Internet*: Typically used by rural users where cable and DSL are not available. A VSAT provides two-way (upload and download) data communications. The upload speed is about one-tenth of the 500 Kbps download speed. Cable and DSL have higher download speeds, but satellite systems are about 10 times faster than an analog modem. To access satellite Internet services, subscribers need a satellite dish, two modems (uplink and downlink), and coaxial cables between the dish and the modem.

Figure 2-25 displays an example of a WiMAX network.

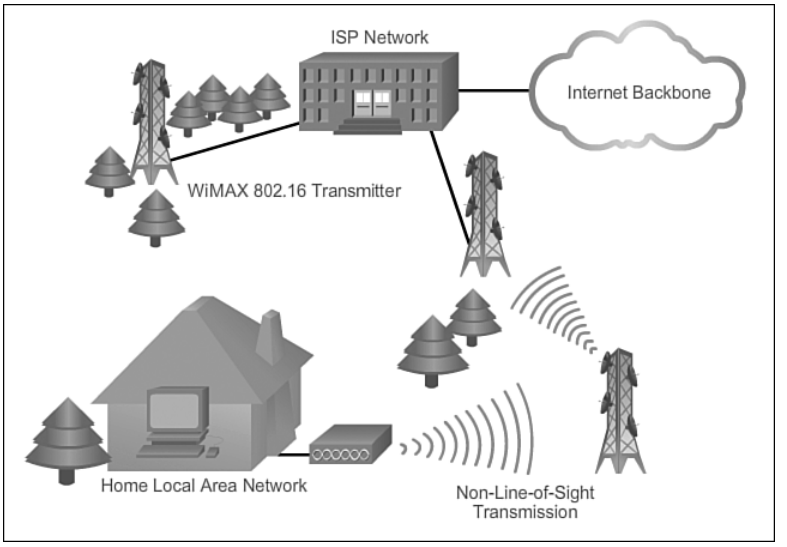


Figure 2-25 Sample Wireless Topology

3G/4G Cellular (2.2.3.4)

Increasingly, cellular service is another wireless WAN technology being used to connect users and remote locations where no other WAN access technology is available. Many users with smartphones and tablets can use cellular data to email, surf the Web, download apps, and watch videos.

Phones, tablet computers, laptops, and even some routers can communicate through to the Internet using cellular technology. As shown in Figure 2-26, these devices use radio waves to communicate through a nearby mobile phone tower.

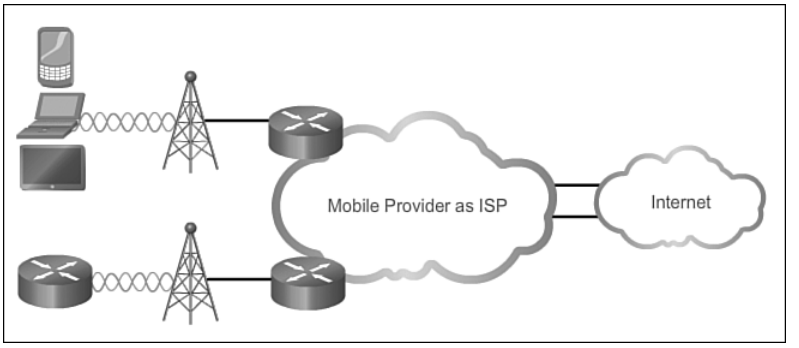


Figure 2-26 Sample Cellular Topology

The device has a small radio antenna, and the provider has a much larger antenna sitting at the top of a tower somewhere within miles of the phone.

Common cellular industry terms include

- *3G/4G Wireless*: Abbreviation for third-generation and fourth-generation cellular access. These technologies support wireless Internet access.
- *Long Term Evolution (LTE)*: Refers to a newer and faster technology and is considered to be part of fourth generation (4G) technology.

VPN Technology (2.2.3.5)

Security risks are incurred when a teleworker or a remote office worker uses broadband services to access the corporate WAN over the Internet. To address security concerns, broadband services provide capabilities for using VPN connections to a VPN server, which is typically located at the corporate site.

A VPN is an encrypted connection between private networks over a public network, such as the Internet. Instead of using a dedicated Layer 2 connection, such as a leased line, a VPN uses virtual connections called VPN tunnels, which are routed through the Internet from the private network of the company to the remote site or employee host.

Benefits of VPN include the following:

- **Cost savings**: VPNs enable organizations to use the global Internet to connect remote offices and remote users to the main corporate site, thus eliminating expensive dedicated WAN links and modem banks.
- **Security**: VPNs provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.
- **Scalability**: Because VPNs use the Internet infrastructure within ISPs and devices, it is easy to add new users. Corporations are able to add large amounts of capacity without adding significant infrastructure.
- **Compatibility with broadband technology**: VPN technology is supported by broadband service providers such as DSL and cable, so mobile workers and telecommuters can take advantage of their home high-speed Internet service to access their corporate networks. Business-grade high-speed broadband connections can also provide a cost-effective solution for connecting remote offices.

There are two types of VPN access:

- *Site-to-site VPNs*: Site-to-site VPNs connect entire networks to each other; for example, they can connect a branch office network to a company headquarters network, as shown in Figure 2-27. Each site is equipped with a VPN gateway, such as a router, firewall, VPN concentrator, or security appliance. In the figure, a remote branch office uses a site-to-site-VPN to connect with the corporate head office.

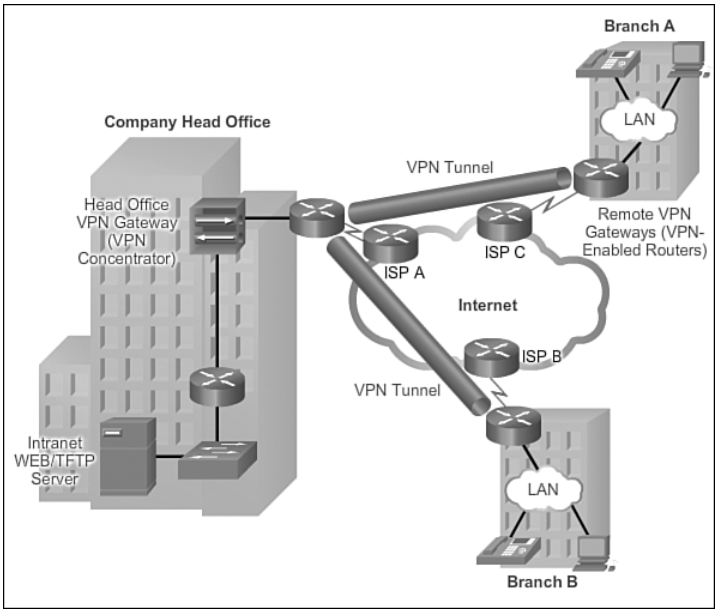


Figure 2-27 Sample Site-to-Site VPN Topology

- *Remote-access VPNs*: Remote-access VPNs enable individual hosts, such as telecommuters, mobile users, and extranet consumers, to access a company network securely over the Internet. Each host (Teleworker 1 and Teleworker 2) typically has VPN client software loaded or uses a web-based client, as shown in Figure 2-28.

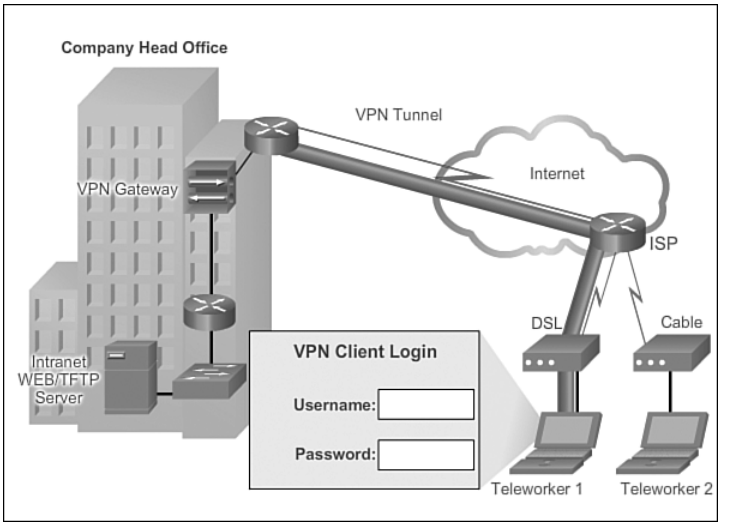


Figure 2-28 Sample Remote-Access VPN Topology

Interactive Graphic

Activity 2.2.3.6: Identify Public WAN Infrastructure Terminology

Go to the course online to perform this practice activity.

Selecting WAN Services (2.2.4)

Many factors influence the choice of service provider. This topic discusses how the purpose of the WAN, the geographic scope of the WAN, and the traffic requirements all factor in when choosing service providers.

Choosing a WAN Link Connection (2.2.4.1, 2.2.4.2)

There are many important factors to consider when choosing an appropriate WAN connection. For a network administrator to decide which WAN technology best meets the requirements of their specific business, they must answer the following questions:

What Is the Purpose of the WAN?

Considerations include

- Will the enterprise connect local branches in the same city area, connect remote branches, or connect to a single branch?
- Will the WAN be used to connect internal employees, or external business partners and customers, or all three?
- Will the enterprise connect to customers, connect to business partners, connect to employees, or some combination of these?
- Will the WAN provide authorized users limited or full access to the company intranet?

What Is the Geographic Scope?

Considerations include

- Is the WAN local, regional, or global?
- Is the WAN one to one (single branch), one to many branches, or many to many (distributed)?

What Are the Traffic Requirements?

Considerations include

- What type of traffic must be supported (data only, VoIP, video, large files, streaming files)? This determines the quality and performance requirements.
- What volume of traffic type (voice, video, or data) must be supported for each destination? This determines the bandwidth capacity required for the WAN connection to the ISP.
- What quality of service is required? This may limit the choices. If the traffic is highly sensitive to latency and jitter, eliminate any WAN connection options that cannot provide the required quality.
- What are the security requirements (data integrity, confidentiality, and security)? These are important factors if the traffic is of a highly confidential nature, or if it provides essential services, such as emergency response.

In addition to gathering information about the scope of the WAN, the administrator must also determine

- **Should the WAN use a private or public infrastructure?** A private infrastructure offers the best security and confidentiality, whereas the public Internet infrastructure offers the most flexibility and lowest ongoing expense. The choice depends on the purpose of the WAN, the types of traffic it carries, and available operating budget. For example, if the purpose is to provide a nearby branch with high-speed, secure services, a private dedicated or switched connection may be best. If the purpose is to connect many remote offices, a public WAN using the Internet may be the best choice. For distributed operations, a combination of options may be the solution.
- **For a private WAN, should it be dedicated or switched?** Real-time high-volume transactions have special requirements that could favor a dedicated line, such as traffic flowing between the data center and the corporate head office. If the enterprise is connecting to a local single branch, a dedicated leased line could be used. However, that option would become very expensive for a WAN connecting multiple offices. In that case, a switched connection might be better.
- **For a public WAN, what type of VPN access is required?** If the purpose of the WAN is to connect a remote office, a site-to-site VPN may be the best choice. To connect teleworkers or customers, remote-access VPNs are a better option. If the WAN is serving a mixture of remote offices, teleworkers, and authorized customers, such as a global company with distributed operations, a combination of VPN options may be required.

- **Which connection options are available locally?** In some areas, not all WAN connection options are available. In this case, the selection process is simplified, although the resulting WAN may provide less-than-optimal performance. For example, in a rural or remote area, the only option may be VSAT or cellular access.
- **What is the cost of the available connection options?** Depending on the option chosen, the WAN can be a significant ongoing expense. The cost of a particular option must be weighed against how well it meets the other requirements. For example, a dedicated leased line is the most expensive option, but the expense may be justified if it is critical to ensure secure transmission of high volumes of real-time data. For less-demanding applications, a less-expensive switched or Internet connection option may be more suitable.

Using the guidelines described here, as well as those described by the Cisco Enterprise Architecture, a network administrator should be able to choose an appropriate WAN connection to meet the requirements of different business scenarios.

Lab 2.2.4.3: Researching WAN Technologies

In this lab, you will complete the following objectives:

- Part 1: Investigate Dedicated WAN Technologies and Providers
- Part 2: Investigate a Dedicated Leased Line Service Provider in Your Area

Summary (2.3)

Class Activity 2.3.1.1: WAN Device Modules

Your medium-size company is upgrading its network. To make the most of the equipment currently in use, you decide to purchase WAN modules instead of new equipment.

All branch offices use either Cisco 1900 or 2911 series ISRs. You will be updating these routers in several locations. Each branch has its own ISP requirements to consider.

To update the devices, focus on the following WAN modules access types:

- Ethernet
- Broadband
- T1/E1 and ISDN PRI
- BRI
- Serial
- T1 and E1 trunk voice and WAN
- Wireless LANs and WANs

A business can use private lines or the public network infrastructure for WAN connections. A public infrastructure connection can be a cost-effective alternative to a private connection between LANs, as long as security is also planned.

WAN access standards operate at Layers 1 and 2 of the OSI model, and are defined and managed by the TIA/EIA, ISO, and IEEE. A WAN may be circuit switched or packet switched.

There is common terminology used to identify the physical components of WAN connections and who, the service provider or the customer, is responsible for which components.

Service provider networks are complex and the service provider's backbone networks consist primarily of high-bandwidth fiber-optic media. The device used for interconnection to a customer is specific to the WAN technology that is implemented.

Permanent, dedicated, point-to-point connections are provided by using leased lines. Dialup access, although slow, is still viable for remote areas with limited WAN options. Other private connection options include ISDN, Frame Relay, ATM, Ethernet WAN, MPLS, and VSAT.

Public infrastructure connections include DSL, cable, wireless, and 3G/4G cellular. Security over public infrastructure connections can be provided by using remote-access or site-to-site virtual private networks (VPNs).

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Connecting Networks Lab Manual* (978-1-58713-331-2).

Class Activities

Class Activity 2.0.1.2: Branching Out

Class Activity 2.3.1.1: WAN Device Modules

Labs

Lab 2.2.4.3: Researching WAN Technologies

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix, "Answers to the 'Check Your Understanding' Questions," lists the answers.

1. A broadband service such as DSL available through a local Internet service provider is suitable for what type of organization?

   A. A small company with 10 employees that uses a single LAN to share information

   B. A medium-size company with 500 employees that uses multiple LANs to share information

   C. A large company with 2,000 employees, in multiple locations and in a multi-LAN environment.

2. Which device is a data terminal equipment?

   A. Cable modem

   B. CSU/DSU

   C. Dialup modem

   D. DSL modem

   E. Router

3. Which two devices are used when digital leased lines interconnect a client with a provider? (Choose two.)

   A. Access server
   B. Channel service unit (CSU)
   C. Data service unit (DSU)
   D. Dialup modem
   E. Layer 2 switch
   F. Router

4. Which statements are true regarding connection-orientated packet-switched networks? (Choose three.)

   A. A virtual circuit is created for the duration of the packet delivery.
   B. Each packet has to carry only an identifier.
   C. Ethernet is an example.
   D. Full addressing information must be carried in each data packet.
   E. The Internet is an example.
   F. The network predetermines the route for each packet.

5. Which technology supports long distance SONET and SDH connections using fiber-optic media?

   A. ATM
   B. DSL
   C. DWDM
   D. Frame Relay
   E. ISDN
   F. MPLS
   G. Municipal Wi-Fi
   H. VPN
   I. VSAT
   J. WiMAX

6. What WAN technology is designed to deliver data, voice, and video simultaneously built on a cell-based architecture?

   A. ATM
   B. DSL
   C. DWDM
   D. Frame Relay
   E. ISDN
   F. MPLS
   G. Municipal Wi-Fi
   H. VPN
   I. VSAT
   J. WiMAX

7. ISDN PRI is composed of how many B channels in North America?

   A. 2
   B. 16
   C. 23
   D. 30
   E. 64

8. The ability to connect securely to a private network over a public network is provided by which WAN technology?

   A. ATM
   B. DSL
   C. DWDM
   D. Frame Relay
   E. ISDN
   F. MPLS
   G. VPN
   H. VSAT
   I. WiMAX

9. What term describes the cabling that connects the customer site to the nearest exchange of the WAN service provider?

   A. CO
   B. DCE
   C. DTE
   D. Local loop

10. Which two statements about a circuit-switched network are true? (Choose two.)

    A. A dedicated secure circuit is established between each pair of communicating nodes.
    B. A connection through the service provider network is established quickly before communications start.
    C. Multiple pairs of nodes can communicate over the same network channel.
    D. The communication costs are lower.

This page intentionally left blank

CHAPTER 3

Point-to-Point Connections

Objectives

Upon completion of this chapter

- What are the fundamentals of point-to-point serial communications across a WAN?
- How do you configure HDLC encapsulation on a point-to-point serial link?
- What are the benefits of using PPP over HDLC in a WAN?
- What is the PPP layered architecture and the functions of LCP and NCP?
- How is a PPP session established?
- How do you configure PPP encapsulation on a point-to-point serial link?
- How do you configure PPP authentication protocols?
- How are the **show** and **debug** commands used to troubleshoot PPP?

Key Terms

This chapter uses the following key terms. You can find the definitions in the glossary.

point-to-point connections *page 80*

clock skew *page 82*

time-division multiplexing (TDM) *page 85*

statistical time-division multiplexing (STDM) *page 85*

data stream *page 85*

transmission link *page 85*

demarcation point *page 88*

null modem *page 91*

DS (digital signal level) *page 94*

E1 *page 95*

E3 *page 95*

bit-oriented *page 97*

Synchronous Data Link Control (SDLC) *page 97*

primary station *page 99*

Cisco 7000 *page 103*

trunk lines *page 105*

Link Control Protocol (LCP) *page 105*

Network Control Protocols (NCPs) *page 105*

Novell IPX *page 105*

SNA Control Protocol *page 105*

Password Authentication Protocol (PAP) *page 119*

Challenge Handshake Authentication Protocol (CHAP) *page 119*

fragmentation *page 119*

reassembly *page 119*

message digest 5 (MD5) *page 130*

TACACS/TACACS+ *page 135*

Introduction (3.0.1.1)

One of the most common types of WAN connections, especially in long-distance communications, is a *point-to-point connection*, also called a serial or leased line connection. Because these connections are typically provided by a carrier, such as a telephone company, boundaries between what is managed by the carrier and what is managed by the customer must be clearly established.

This chapter covers the terms, technology, and protocols used in serial connections. The High-Level Data Link Control (HDLC) and Point-to-Point Protocol (PPP) are introduced. PPP is a protocol that is able to handle authentication, compression, error detection, monitor link quality, and logically bundles multiple serial connections together to share the load.

Class Activity 3.0.1.2: PPP Persuasion

Your network engineering supervisor recently attended a networking conference where Layer 2 protocols were discussed. He knows that you have Cisco equipment on the premises, but he would also like to offer security and advanced TCP/IP options and controls on that same equipment by using the Point-to-Point Protocol (PPP).

After researching the PPP protocol, you find it offers some advantages over the HDLC protocol, currently used on your network.

Create a matrix listing the advantages and disadvantages of using the HDLC vs. PPP protocols. When comparing the two protocols, include

- Ease of configuration
- Adaptability to non-proprietary network equipment
- Security options
- Bandwidth usage and compression
- Bandwidth consolidation

Share your chart with another student or class. Justify whether or not you would suggest sharing the matrix with the network engineering supervisor to justify a change being made from HDLC to PPP for Layer 2 network connectivity.

Serial Point-to-Point Overview (3.1)

This section gives an overview of point-to-point serial communications. A basic understanding of point-to-point serial communications is essential to understanding protocols that are used over these types of serial links. HDLC encapsulation and configuration is discussed later in this section.

Serial Communications (3.1.1)

The earliest form of computer communications involved serial links between mainframe computers. Serial communications is still a widely used method of connecting two networks usually over long distances.

Serial and Parallel Ports (3.1.1.1)

One of the most common types of WAN connections is the point-to-point connection. As shown in Figure 3-1, point-to-point connections are used to connect LANs to service provider WANs, and to connect LAN segments within an enterprise network.

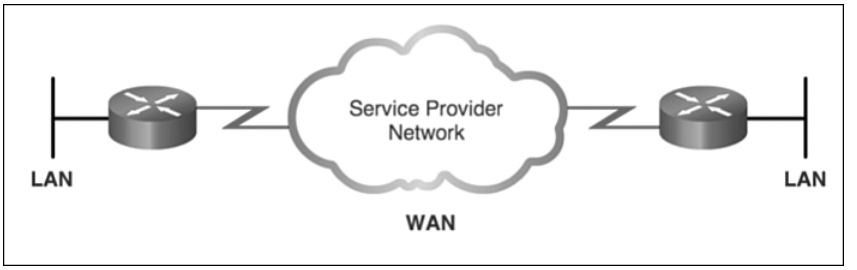


Figure 3-1 Serial Point-to-Point Communications

A LAN-to-WAN point-to-point connection is also referred to as a serial connection or leased line connection. This is because the lines are leased from a carrier (usually a telephone company) and are dedicated for use by the company leasing the lines. Companies pay for a continuous connection between two remote sites, and the line is continuously active and available. Leased lines are a frequently used type of WAN access, and they are generally priced based on the bandwidth required and the distance between the two connected points.

Understanding how point-to-point serial communication across a leased line works is important to an overall understanding of how WANs function.

Communications across a serial connection is a method of data transmission in which the bits are transmitted sequentially over a single channel. This is equivalent to a pipe only wide enough to fit one ball at a time. Multiple balls can go into the pipe, but only one at a time, and they only have one exit point, the other end of the pipe. A serial port is bidirectional, and often referred to as a bidirectional port or a communications port.

This is in contrast to parallel communications in which bits can be transmitted simultaneously over multiple wires. As shown in Figure 3-2, a parallel connection theoretically transfers data eight times faster than a serial connection. Based on this theory, a parallel connection sends a byte (eight bits) in the time that a serial connection sends a single bit. However, parallel communications do have issues with crosstalk across

wires, especially as the wire length increases. *Clock skew* is also an issue with parallel communications. Clock skew occurs when data across the various wires does not arrive at the same time, creating synchronization issues. Finally, most parallel communications support only one-direction, outbound-only communication from the hard drive.

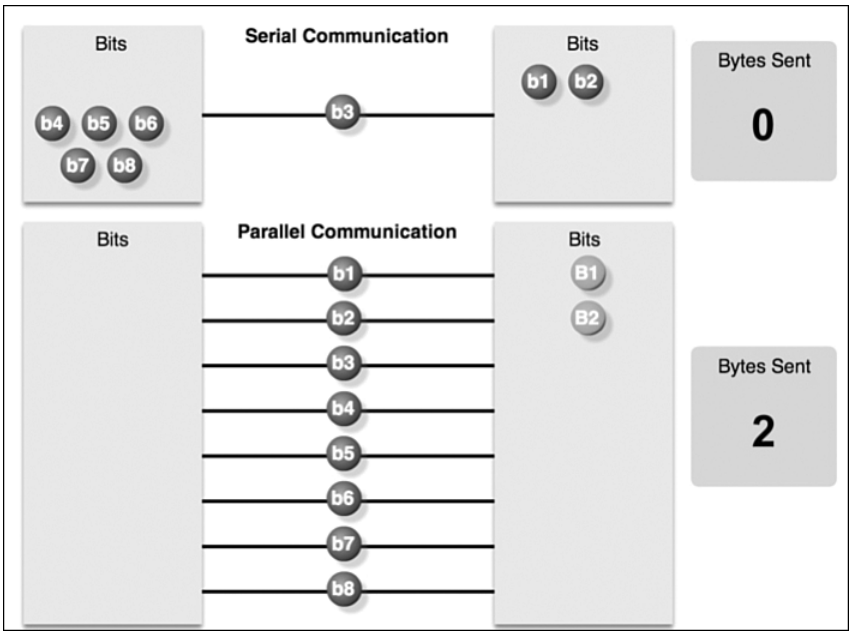


Figure 3-2 Serial and Parallel Communications

At one time, most PCs included both serial and parallel ports. Parallel ports were used to connect printers, computers, and other devices that required relatively high bandwidth. Parallel ports were also used between interior components. For external communications, a serial bus was primarily used for signal conversion. Because of their bidirectional ability, serial communications are considerably less expensive to implement. Serial communications use fewer wires, cheaper cables, and fewer connector pins.

On most PCs, parallel ports and RS-232 serial ports have been replaced by the higher speed serial Universal Serial Bus (USB) interfaces. However, for long-distance communication, many WANs use still serial transmission.

Serial Communication (3.1.1.2)

Figure 3-3 shows a simple representation of a serial communication across a WAN. Data is encapsulated by the communications protocol used by the sending router. The encapsulated frame is sent on a physical medium to the WAN. There are various ways to traverse the WAN, but the receiving router uses the same communications protocol to de-encapsulate the frame when it arrives.

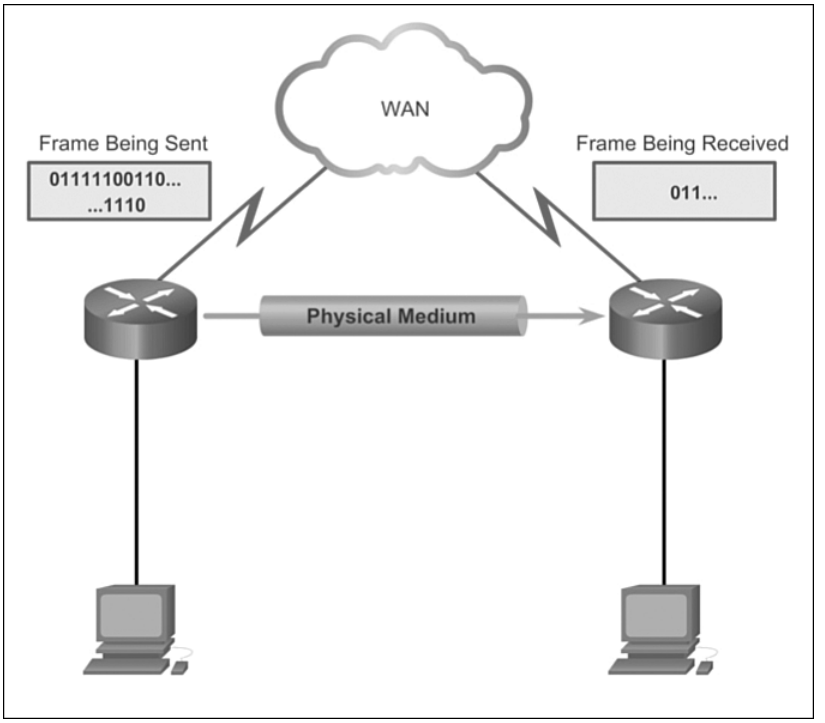


Figure 3-3 Serial Communication Process

There are many different serial communication standards, each one using a different signaling method. There are three important serial communication standards affecting LAN-to-WAN connections:

- **RS-232**: Most serial ports on personal computers conform to the RS-232C or newer RS-422 and RS-423 standards. Both 9-pin and 25-pin connectors are used. A serial port is a general-purpose interface that can be used for almost any type of device, including modems, mice, and printers. These types of peripheral devices for computers have been replaced by new and faster standards such as USB but many network devices use RJ-45 connectors that conform to the original RS-232 standard.
- **V.35**: Typically used for modem-to-multiplexer communication, this ITU standard for high-speed, synchronous data exchange combines the bandwidth of several telephone circuits. In the U.S., V.35 is the interface standard used by most routers and DSUs that connect to T1 carriers. V.35 cables are high-speed serial assemblies designed to support higher data rates and connectivity between DTEs and DCEs over digital lines. There is more on DTEs and DCEs later in this section.

- **HSSI:** A High-Speed Serial Interface (HSSI) supports transmission rates up to 52 Mbps. Engineers use HSSI to connect routers on LANs with WANs over high-speed lines, such as T3 lines. Engineers also use HSSI to provide high-speed connectivity between LANs, using Token Ring or Ethernet. HSSI is a DTE/DCE interface developed by Cisco Systems and T3 Plus Networking to address the need for high-speed communication over WAN links.

Point-to-Point Communication Links (3.1.1.3)

When permanent dedicated connections are required, a point-to-point link is used to provide a single, pre-established WAN communications path from the customer premises, through the provider network, to a remote destination, as shown in Figure 3-4.

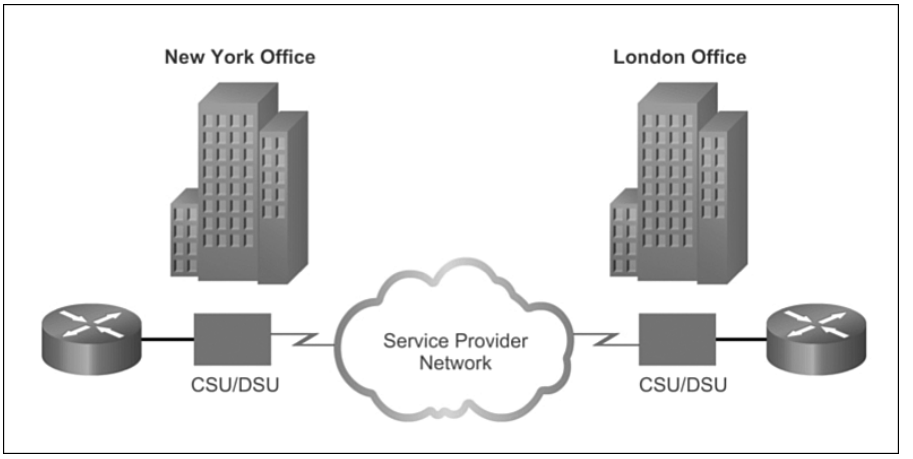


Figure 3-4 Point-to-Point Communication Links

A point-to-point link can connect two geographically distant sites, such as a corporate office in New York and a regional office in London. For a point-to-point line, the carrier dedicates specific resources for a line that is leased by the customer (leased line).

Note

Point-to-point connections are not limited to connections that cross land. There are hundreds of thousands of miles of undersea fiber-optic cables that connect countries and continents worldwide. An Internet search of "undersea Internet cable map" produces several cable maps of these undersea connections.

Point-to-point links are usually more expensive than shared services. The cost of leased line solutions can become significant when used to connect many sites over increasing distances. However, there are times when the benefits outweigh the cost of the leased line. The dedicated capacity removes latency or jitter between the endpoints. Constant availability is essential for some applications such as VoIP or video over IP.

Time-Division Multiplexing (3.1.1.4)

With a leased line, despite the fact that customers are paying for dedicated services, and dedicated bandwidth is provided to the customer, the carrier still uses multiplexing technologies within the network. Multiplexing refers to a scheme that allows multiple logical signals to share a single physical channel. Two common types of multiplexing are ***time-division multiplexing (TDM)*** and ***statistical time-division multiplexing (STDM)***.

TDM

Bell Laboratories originally invented TDM to maximize the amount of voice traffic carried over a medium. Before multiplexing, each telephone call required its own physical link. This was an expensive and unscalable solution. TDM divides the bandwidth of a single link into separate time slots. TDM transmits two or more channels (***data stream***) over the same link by allocating a different time slot for the transmission of each channel. In effect, the channels take turns using the link.

TDM is a physical layer concept. It has no regard for the nature of the information that is multiplexed on to the output channel. TDM is independent of the Layer 2 protocol that has been used by the input channels.

TDM can be explained by an analogy to highway traffic. To transport traffic from four roads to another city, all traffic can be sent on one lane if the roads are equally serviced and the traffic is synchronized. If each of the four roads puts a car on to the main highway every four seconds, the highway gets a car at the rate of one each second. As long as the speed of all the cars is synchronized, there is no collision. At the destination, the reverse happens and the cars are taken off the highway and fed to the local roads by the same synchronous mechanism.

This is the principle used in synchronous TDM when sending data over a link. TDM increases the capacity of the ***transmission link*** by dividing transmission time into smaller, equal intervals so that the link carries the bits from multiple input sources.

In Figure 3-5, a multiplexer (MUX) at the transmitter accepts three separate signals. The MUX breaks each signal into segments. The MUX puts each segment into a single channel by inserting each segment into a time slot.

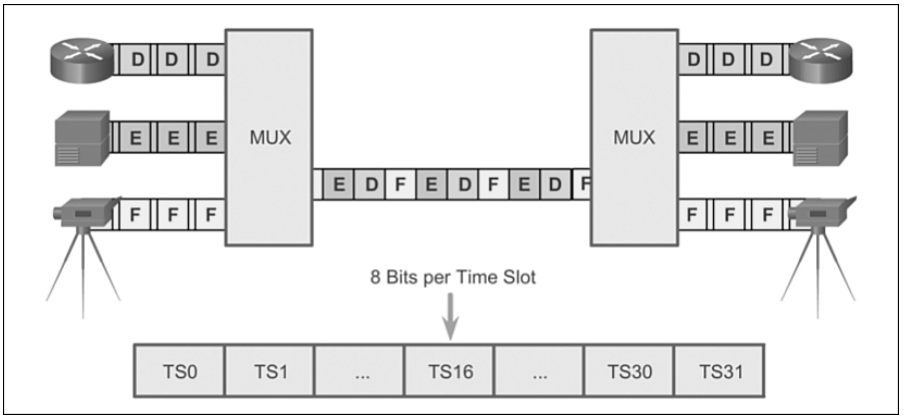


Figure 3-5 Time-Division Multiplexing

A MUX at the receiving end reassembles the TDM stream into the three separate data streams based only on the timing of the arrival of each bit. A technique called bit interleaving keeps track of the number and sequence of the bits from each specific transmission so that they can be quickly and efficiently reassembled into their original form upon receipt. Byte interleaving performs the same functions, but because there are eight bits in each byte, the process needs a bigger or longer time slot.

The operations of TDM are summarized as follows:

- TDM shares available transmission time on a medium by assigning a time slot to users.
- The MUX accepts input from attached devices in an alternating sequence (round-robin) and transmits the data in a recurrent pattern.
- T1/E1 and ISDN telephone lines are common examples of synchronous TDM.

Statistical Time-Division Multiplexing (3.1.1.5)

In another analogy, compare TDM to a train with 32 railroad cars. Each car is owned by a different freight company, and every day the train leaves with the 32 cars attached. If one of the companies has cargo to send, the car is loaded. If the company has nothing to send, the car remains empty, but stays on the train. Shipping empty containers is not very efficient. TDM shares this inefficiency when traffic is intermittent, because the time slot is still allocated even when the channel has no data to transmit.

STDM

STDM was developed to overcome this inefficiency. As shown in Figure 3-6, STDM uses a variable time slot length allowing channels to compete for any free slot space. It employs a buffer memory that temporarily stores the data during periods of peak traffic. STDM does not waste high-speed line time with inactive channels using this scheme. STDM requires each transmission to carry identification information or a channel identifier.

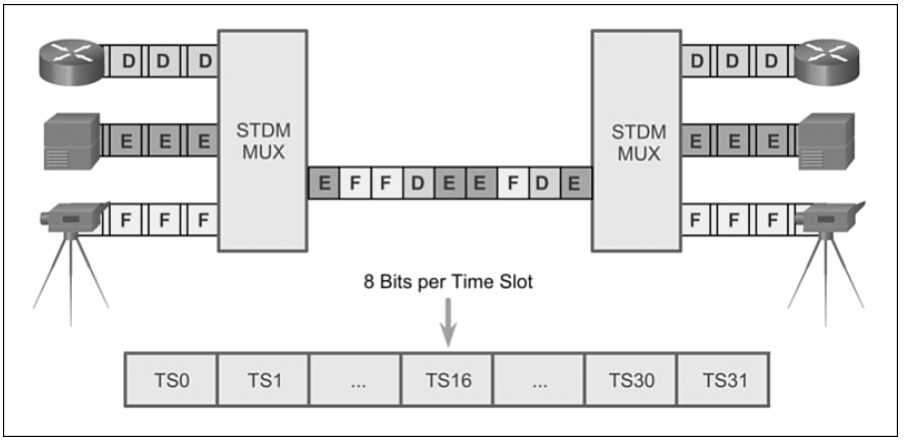


Figure 3-6 Statistical Time-Division Multiplexing

TDM Examples – Sonet and SDM (3.1.1.6)

On a larger scale, the telecommunications industry uses the Synchronous Optical Networking (SONET) or Synchronous Digital Hierarchy (SDH) standard for optical transport of TDM data. SONET, used in North America, and SDH, used elsewhere, are two closely related standards that specify interface parameters, rates, framing formats, multiplexing methods, and management for synchronous TDM over fiber.

Figure 3-7 displays SONET, which is an example of STDM. SONET/SDH takes *n* bit streams, multiplexes them, and optically modulates the signals. It then sends the signals out using a light emitting device over fiber with a bit rate equal to (incoming bit rate) ´ *n*. Thus, traffic arriving at the SONET multiplexer from four places at 2.5 Gbps goes out as a single stream at 4 ´ 2.5 Gbps, or 10 Gbps. This principle is illustrated in the figure, which shows an increase in the bit rate by a factor of four in time slot T.

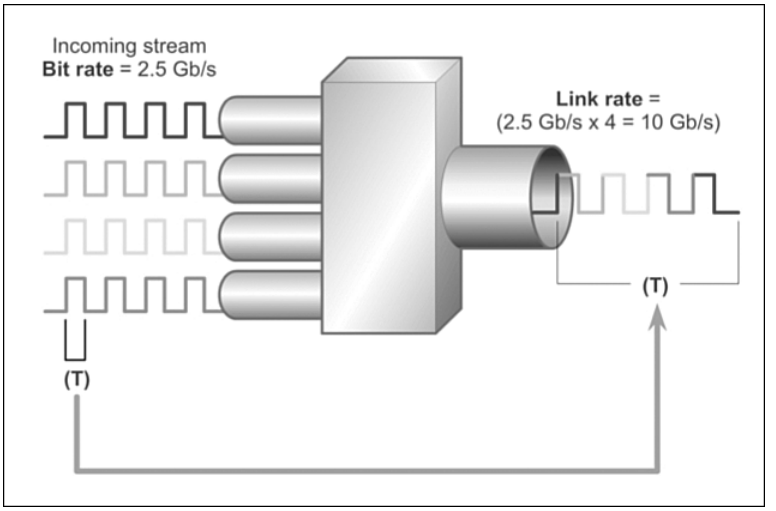


Figure 3-7 TDM Example: SONET

Demarcation Point (3.1.1.7)

Prior to deregulation in North America and other countries, telephone companies owned the local loop, including the wiring and equipment on the premises of the customers. The local loop refers to the line from the premises of a telephone subscriber to the telephone company central office. Deregulation forced telephone companies to unbundle their local loop infrastructure to allow other suppliers to provide equipment and services. This led to a need to delineate which part of the network the telephone company owned and which part the customer owned. This point of delineation is the ***demarcation point***, or demarc. The demarcation point marks the point where your network interfaces with a network that is owned by another organization. In telephone terminology, this is the interface between customer premises equipment (CPE) and network service provider equipment. The demarcation point is the point in the network where the responsibility of the service provider ends, as shown in Figure 3-8.

The differences in demarcation points can best be shown using ISDN. In the United States, a service provider provides the local loop into the customer premises, and the customer provides the active equipment such as the channel service unit / data service unit (CSU/DSU) on which the local loop is terminated. This termination often occurs in a telecommunications closet, and the customer is responsible for maintaining, replacing, or repairing the equipment. In other countries, the network terminating unit (NTU)

is provided and managed by the service provider. This allows the service provider to actively manage and troubleshoot the local loop with the demarcation point occurring after the NTU. The customer connects a CPE device, such as a router or Frame Relay access device, to the NTU using a V.35 or RS-232 serial interface.

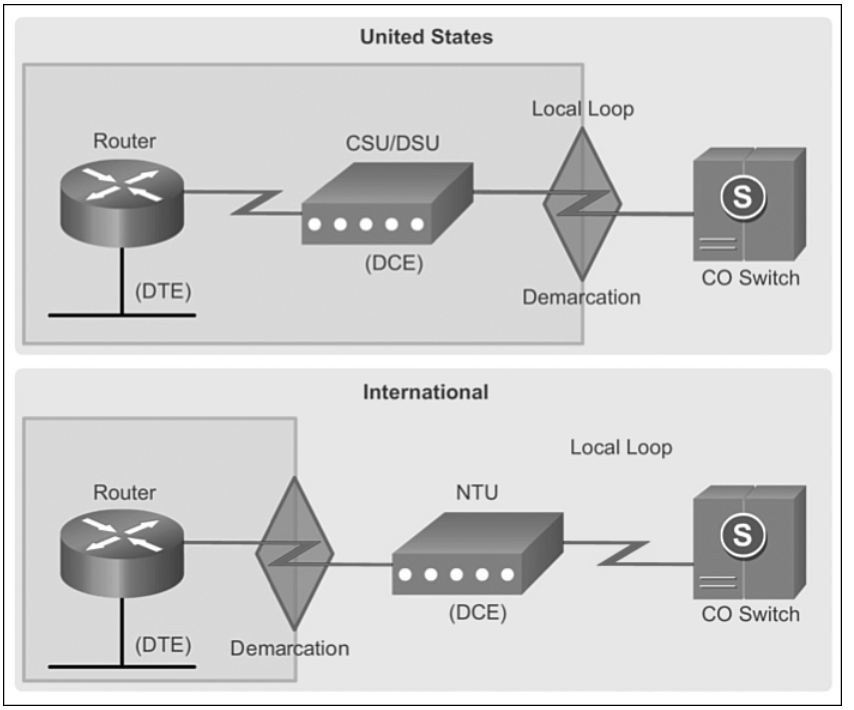


Figure 3-8 Demarcation Point

A router serial port is required for each leased line connection. If the underlying network is based on the T-carrier or E-carrier technologies, the leased line connects to the network of the carrier through a CSU/DSU. The purpose of the CSU/DSU is to provide a clocking signal to the customer equipment interface from the DSU and terminate the channelized transport media of the carrier on the CSU. The CSU also provides diagnostic functions such as a loopback test.

As shown in Figure 3-9, most T1 or E1 TDM interfaces on current routers include CSU/DSU capabilities. A separate CSU/DSU is not required because this functionality is embedded in the interface. IOS commands are used to configure the CSU/DSU operations.

Figure 3-9 T1/E1 with Embedded CSU/DSU

DTE-DCE (3.1.1.8)

From the point of view of connecting to the WAN, a serial connection has a data terminal equipment (DTE) device at one end of the connection and a data circuit-terminating equipment or data communications equipment (DCE) device at the other end. The connection between the two DCE devices is the WAN service provider transmission network, as shown in Figure 3-10. In this example

- The CPE, which is generally a router, is the DTE. The DTE could also be a terminal, computer, printer, or fax machine if they connect directly to the service provider network.
- The DCE, commonly a modem or CSU/DSU, is the device used to convert the user data from the DTE into a form acceptable to the WAN service provider transmission link. This signal is received at the remote DCE, which decodes the signal back into a sequence of bits. The remote DCE then signals this sequence to the remote DTE.

The Electronics Industry Association (EIA) and the International Telecommunication Union Telecommunications Standardization Sector (ITU-T) have been most active in the development of standards that allow DTEs to communicate with DCEs.

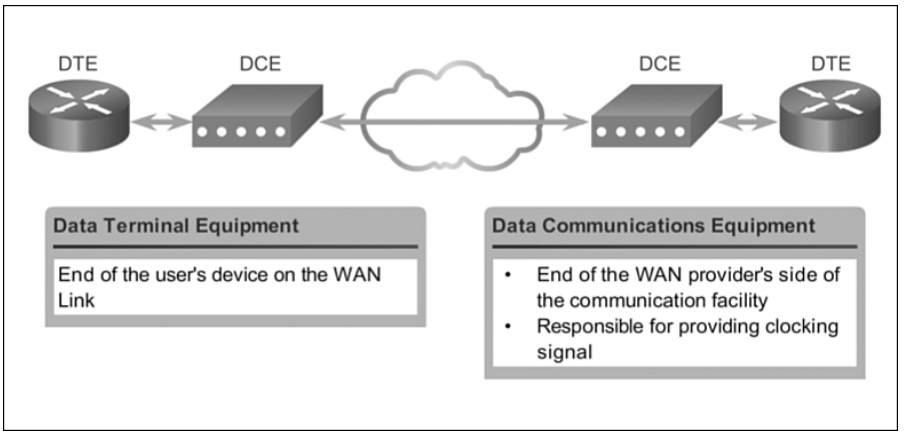


Figure 3-10 Serial DCE and DTE WAN Connections

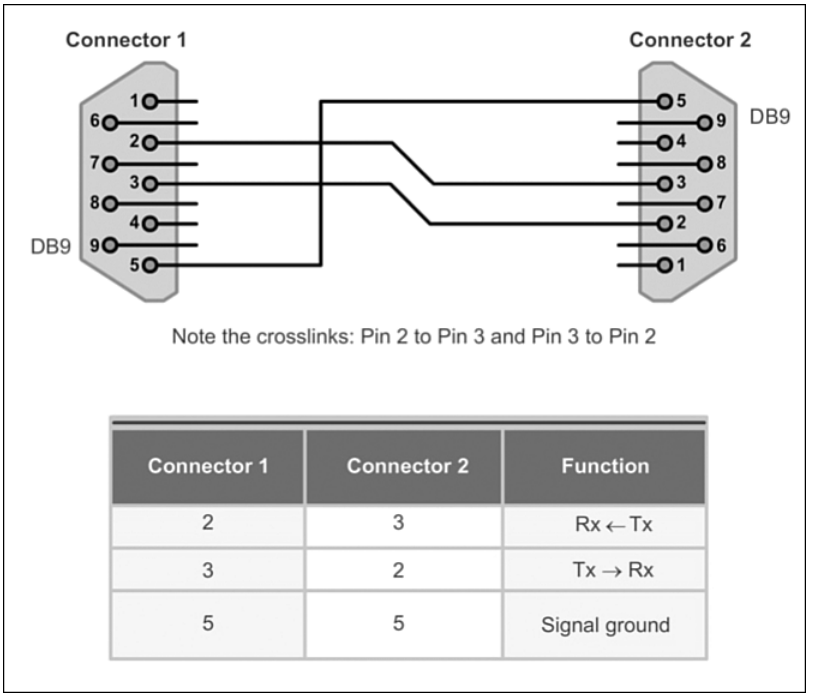
Serial Cables (3.1.1.9)

Originally, the concept of DCEs and DTEs was based on two types of equipment: terminal equipment that generated or received data, and the communication equipment that only relayed data. In the development of the RS-232 standard, there were reasons why 25-pin RS-232 connectors on these two types of equipment must be wired differently. These reasons are no longer significant, but there are two different types of cables remaining: one for connecting a DTE to a DCE, and another for connecting two DTEs directly to each other.

The DTE/DCE interface for a particular standard defines the following specifications:

- **Mechanical/physical:** Number of pins and connector type
- **Electrical:** Defines voltage levels for 0 and 1
- **Functional:** Specifies the functions that are performed by assigning meanings to each of the signaling lines in the interface
- **Procedural:** Specifies the sequence of events for transmitting data

The original RS-232 standard only defined the connection of DTEs with DCEs, which were modems. However, to connect two DTEs, such as two computers or two routers in a lab, a special cable called a null modem eliminates the need for a DCE. In other words, the two devices can be connected without a modem. A ***null modem*** is a communication method to directly connect two DTEs using an RS-232 serial cable. With a null modem connection, the transmit (Tx) and receive (Rx) lines are cross-linked, as shown in Figure 3-11.



Connector 1	Connector 2	Function
2	3	Rx ← Tx
3	2	Tx → Rx
5	5	Signal ground

Figure 3-11 Null Modem to Connect Two DTEs

The cable for the DTE to DCE connection is a shielded serial transition cable. The router end of the shielded serial transition cable may be a DB-60 connector, which connects to the DB-60 port on a serial WAN interface card, as shown in Figure 3-12. The other end of the serial transition cable is available with the connector appropriate for the standard that is to be used. The WAN provider or the CSU/DSU usually dictates this cable type. Cisco devices support the EIA/TIA-232, EIA/TIA-449, V.35, X.21, and EIA/TIA-530 serial standards, as shown in Figure 3-13.

Figure 3-12 DB-60 Router Connection

To support higher port densities in a smaller form factor, Cisco has introduced a Smart Serial cable, as shown in Figure 3-14. The router interface end of the Smart Serial cable is a 26-pin connector that is significantly more compact than the DB-60 connector.

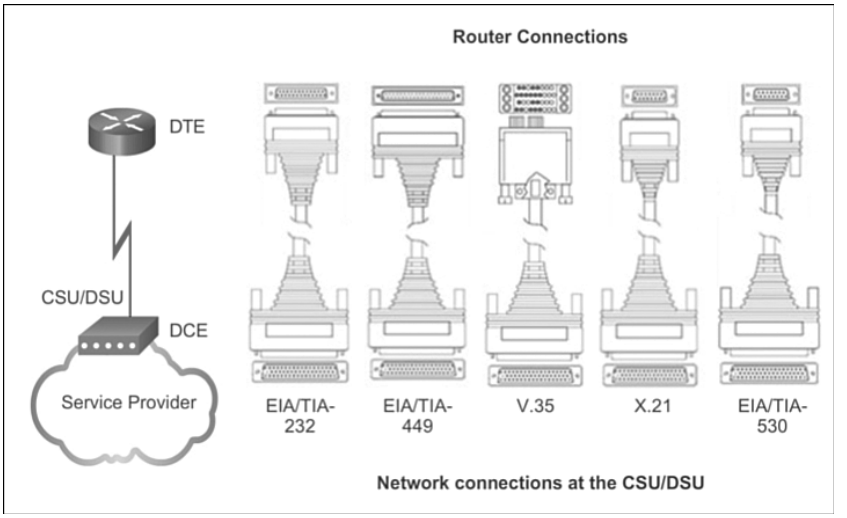


Figure 3-13 WAN Serial Connection Options

Figure 3-14 Smart Serial Connector

When using a null modem, synchronous connections require a clock signal. An external device can generate the signal, or one of the DTEs can generate the clock signal. When a DTE and DCE are connected, the serial port on a router is the DTE end of the connection, by default, and the clock signal is typically provided by a CSU/DSU, or similar DCE device. However, when using a null modem cable in a router-to-router connection, one of the serial interfaces must be configured as the DCE end to provide the clock signal for the connection, as shown in Figure 3-15.

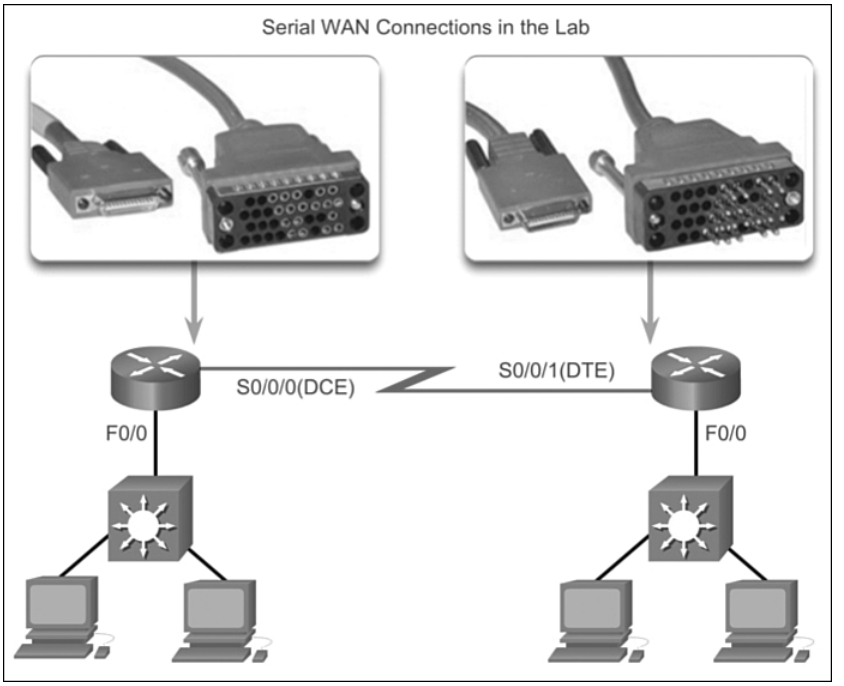


Figure 3-15 Smart Serial Connections in the Lab

Serial Bandwidth (3.1.1.10)

Bandwidth refers to the rate at which data is transferred over the communication link. The underlying carrier technology depends on the bandwidth available. There is a difference in bandwidth points between the North American (T-carrier) specification and the European (E-carrier) system. Optical networks also use a different bandwidth hierarchy, which again differs between North America and Europe. In the United States, Optical Carrier (OC) defines the bandwidth points.

In North America, the bandwidth is usually expressed as a *DS (digital signal level)* number (DS0, DS1, etc.), which refers to the rate and format of the signal. The most fundamental line speed is 64 Kbps, or DS-0, which is the bandwidth required for an uncompressed, digitized phone call. Serial connection bandwidths can be incrementally increased to accommodate the need for faster transmission. For example, 24 DS0s can be bundled to get a DS1 line (also called a T1 line) with a speed of 1.544 Mbps. Also, 28 DS1s can be bundled to get a DS3 line (also called a T3 line) with a speed of 44.736 Mbps. Leased lines are available in different capacities and are generally priced based on the bandwidth required and the distance between the two connected points.

OC transmission rates are a set of standardized specifications for the transmission of digital signals carried on SONET fiber-optic networks. The designation uses OC, followed by an integer value representing the base transmission rate of 51.84 Mbps. For example, OC-1 has a transmission capacity of 51.84 Mbps, whereas an OC-3 transmission medium would be three times 51.84 Mbps, or 155.52 Mbps.

Table 3-1 lists the most common line types and the associated bit rate capacity of each.

Table 3-1 Carrier Transmission Rates

Line Type	Bit Rate Capacity
56	56 Kbps
64	64 Kbps
T1	1.544 Mbps
E1	2.048 Mbps
J1	2.048 Mbps
E3	34.064 Mbps
T3	44.736 Mbps
OC-1	51.84 Mbps
OC-3	155.54 Mbps
OC-9	466.56 Mbps
OC-12	622.08 Mbps
OC-18	933.12 Mbps
OC-24	1.244 Gbps
OC-36	1.866 Gbps
OC-48	2.488 Gbps
OC-96	4.976 Gbps
OC-192	9.954 Gbps
OC-768	39.813 Gbps

Note

E1 (2.048 Mbps) and *E3* (34.368 Mbps) are European standards like T1 and T3, but with different bandwidths and frame structures.

Interactive Graphic

Activity 3.1.1.11: Identify the Serial Communications Terminology

Go to the course online to perform this practice activity.

HDLC Encapsulation (3.1.2)

HDLC is a synchronous data link layer protocol developed by the International Organization for Standardization (ISO). Although HDLC can be used for point-to-multipoint connections, the most common usage of HDLC is for point-to-point serial communications.

WAN Encapsulation Protocols (3.1.2.1)

On each WAN connection, data is encapsulated into frames before crossing the WAN link. To ensure that the correct protocol is used, the appropriate Layer 2 encapsulation type must be configured. The choice of protocol depends on the WAN technology and the communicating equipment. Figure 3-16 displays the more common WAN protocols and where they are used. The following are short descriptions of each type of WAN protocol:

- **HDLC**: The default encapsulation type on point-to-point connections, dedicated links, and circuit-switched connections when the link uses two Cisco devices. HDLC is now the basis for synchronous PPP used by many servers to connect to a WAN, most commonly the Internet.
- **PPP**: Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP works with several network layer protocols, such as IPv4 and IPv6. PPP uses the HDLC encapsulation protocol, but also has built-in security mechanisms such as PAP and CHAP.
- **Serial Line Internet Protocol (SLIP)**: A standard protocol for point-to-point serial connections using TCP/IP. SLIP has been largely displaced by PPP.
- **X.25/Link Access Procedure, Balanced (LAPB)**: An ITU-T standard that defines how connections between a DTE and DCE are maintained for remote terminal access and computer communications in public data networks. X.25 specifies LAPB, a data link layer protocol. X.25 is a predecessor to Frame Relay.
- **Frame Relay**: An industry standard, switched, data link layer protocol that handles multiple virtual circuits. Frame Relay is a next-generation protocol after X.25. Frame Relay eliminates some of the time-consuming processes (such as error correction and flow control) employed in X.25.
- **ATM**: The international standard for cell relay in which devices send multiple service types, such as voice, video, or data, in fixed-length (53-byte) cells. Fixed-length cells allow processing to occur in hardware; thereby, reducing transit delays. ATM takes advantage of high-speed transmission media such as E3, SONET, and T3.

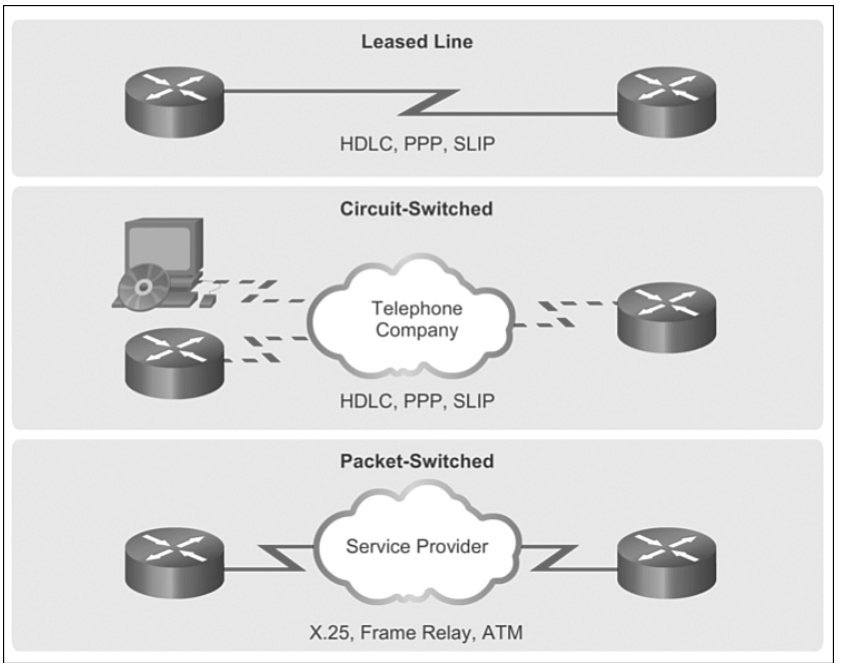


Figure 3-16 WAN Encapsulation Protocols

HDLC Encapsulation (3.1.2.2)

HDLC is a *bit-oriented* synchronous data link layer protocol developed by the International Organization for Standardization (ISO). The current standard for HDLC is ISO 13239. HDLC was developed from the *Synchronous Data Link Control (SDLC)* standard proposed in the 1970s. HDLC provides both connection-oriented and connectionless service.

HDLC uses synchronous serial transmission to provide error-free communication between two points. HDLC defines a Layer 2 framing structure that allows for flow control and error control through the use of acknowledgments. Each frame has the same format, whether it is a data frame or a control frame.

When frames are transmitted over synchronous or asynchronous links, those links have no mechanism to mark the beginning or end of frames. For this reason, HDLC uses a frame delimiter, or flag, to mark the beginning and the end of each frame.

Cisco has developed an extension to the HLDC protocol to solve the inability to provide multiprotocol support. Although Cisco HLDC (also referred to as cHDLC) is proprietary, Cisco has allowed many other network equipment vendors to implement it. Cisco HDLC frames contain a field for identifying the network protocol being encapsulated. Figure 3-17 compares standard HLDC to Cisco HLDC.

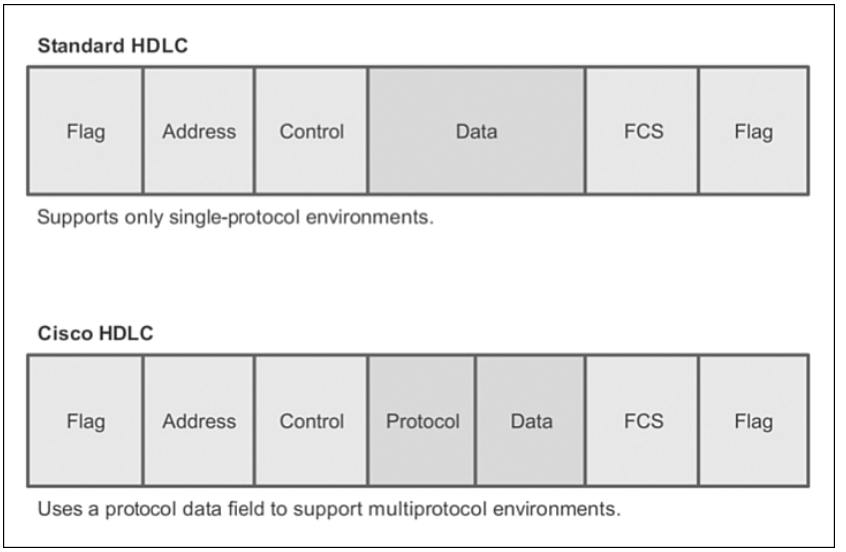


Figure 3-17 Standard and Cisco HLDC Frame Format

HDLC Frame Types (3.1.2.3)

HDLC defines three types of frames, each with a different control field format.

Flag

The Flag field initiates and terminates error checking. The frame always starts and ends with an 8-bit Flag field. The bit pattern is 01111110. Because there is a likelihood that this pattern occurs in the actual data, the sending HDLC system always inserts a 0 bit after every five consecutive 1s in the data field, so in practice the flag sequence can only occur at the frame ends. The receiving system strips out the inserted bits. When frames are transmitted consecutively, the end flag of the first frame is used as the start flag of the next frame.

Address

The Address field contains the HDLC address of the secondary station. This address can contain a specific address, a group address, or a broadcast address. A primary address is either a communication source or a destination, which eliminates the need to include the address of the primary.

Control

The Control field, shown in Figure 3-18, uses three different formats, depending on the type of HDLC frame used:

- **Information (I) frame:** I-frames carry upper layer information and some control information. This frame sends and receives sequence numbers, and the poll final (P/F) bit performs flow and error control. The send sequence number refers to the number of the frame to be sent next. The receive sequence number provides the number of the frame to be received next. Both sender and receiver maintain send and receive sequence numbers. A *primary station* uses the P/F bit to tell the secondary whether it requires an immediate response. A secondary station uses the P/F bit to tell the primary whether the current frame is the last in its current response.
- **Supervisory (S) frame:** S-frames provide control information. An S-frame can request and suspend transmission, report on status, and acknowledge receipt of I-frames. S-frames do not have an information field.
- **Unnumbered (U) frame:** U-frames support control purposes and are not sequenced. Depending on the function of the U-frame, its Control field is 1 or 2 bytes. Some U-frames have an Information field.

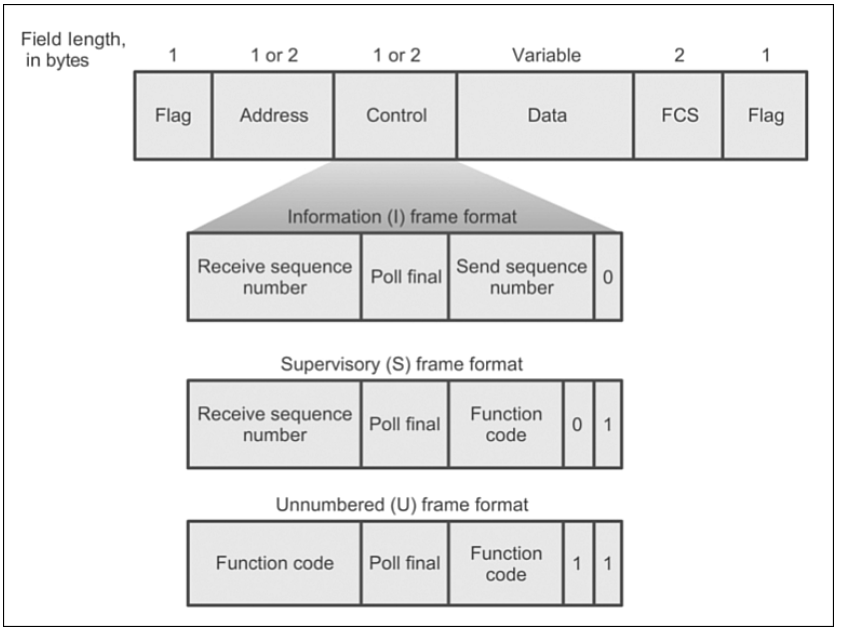


Figure 3-18 HDLC Frame Types

Protocol

Only used in Cisco HDLC. This field specifies the protocol type encapsulated within the frame (e.g., 0x0800 for IP).

Data

The Data field contains a path information unit (PIU) or exchange identification (XID) information.

Frame Check Sequence (FCS)

The FCS precedes the ending flag delimiter and is usually a cyclic redundancy check (CRC) calculation remainder. The CRC calculation is redone in the receiver. If the result differs from the value in the original frame, an error is assumed.

Configuring HDLC Encapsulation (3.1.2.4)

Cisco HDLC is the default encapsulation method used by Cisco devices on synchronous serial lines.

Use Cisco HDLC as a point-to-point protocol on leased lines between two Cisco devices. If connecting non-Cisco devices, use synchronous PPP.

If the default encapsulation method has been changed, use the **encapsulation hdlc** command in privileged EXEC mode to reenable HDLC.

There are two steps to re-enable HDLC encapsulation:

Step 1. Enter the interface configuration mode of the serial interface.

Step 2. Enter the **encapsulation hdlc** command to specify the encapsulation protocol on the interface.

The following shows an example of HDLC reenabled on a serial interface:

```
R2(config)# interface s0/0/0
R2(config-if)# encapsulation hdlc
```

Troubleshooting a Serial Interface (3.1.2.5)

The output of the **show interfaces serial** command displays information specific to serial interfaces. When HDLC is configured, **encapsulation HDLC** should be reflected in the output, as highlighted in Example 3-1. **Serial 0/0/0 is up, line protocol is up** indicates that the line is up and functioning; **encapsulation HDLC** indicates that the default serial encapsulation (HDLC) is enabled.

Example 3-1 Displaying Serial Interface Information

```
R1# show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
```

```
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
CRC checking enabled
<Output omitted for brevity>
```

The **show interfaces serial** command returns one of six possible states:

- Serial *x* is up, line protocol is up.
- Serial *x* is down, line protocol is down.
- Serial *x* is up, line protocol is down.
- Serial *x* is up, line protocol is up (looped).
- Serial *x* is up, line protocol is down (disabled).
- Serial *x* is administratively down, line protocol is down.

Of the six possible states, there are five problem states. Table 3-2 lists the five problem states, the issues associated with that state, and how to troubleshoot the issue.

Table 3-2 Troubleshooting a Serial Interface

Status Line Condition	Possible Problem	Solution
Serial *x* is up, line protocol is up.	This is proper status line condition.	No action is required.
Serial *x* is down, line protocol is down.	The router is not sensing a carrier detect (CD) signal (that is, the CD is not active). The line is down or is not connected on the far end. Cabling is faulty or incorrect. Hardware failure has occurred (CSU/DSU).	1. Check the CD LEDs on the CSU/DSU to see whether the CD is active, or insert a breakout box on the line to check for the CD signal. 2. Verify that the proper cable and interface are being used by looking at the hardware installation documentation. 3. Insert a breakout box and check all control leads. 4. Contact the leased line or other carrier service to see whether there is a problem. 5. Swap faulty parts. 6. If you suspect faulty router hardware, change the serial line to another port. If the connection comes up, the previously connected interface has a problem.

Status Line Condition	Possible Problem	Solution
Serial x is up, line protocol is down (DCE mode).	The **clock rate** interface configuration command is missing. The DTE device does not support or is not set up for SCTE mode (terminal timing). The remote CSU or DSU has failed.	1. Add the **clockrate** interface configuration command on the serial interface. Syntax: **clock rate** *bps* Syntax Description: ■ *bps*: Desired clock rate in bits per second: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000, or 8000000. 2. If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU or DSU. 3. Verify that the correct cable is being used. 4. If the line protocol is still down, there is a possible hardware failure or cabling problem. Insert a breakout box and observe leads. 5. Replace faulty parts as necessary.
Serial *x* is up, line protocol is up (looped).	A loop exists in the circuit. The sequence number in the keepalive packet changes to a random number when a loop is initially detected. If the same random number is returned over the link, a loop exists.	1. Use the **show running-config** privileged exec command to look for any **loopback** interface configuration command entries. 2. If you find a **loopback** interface configuration command entry, use the **no loopback** interface configuration command to remove the loop. 3. If you do not find the **loopback** interface configuration command, examine the CSU/DSU to determine whether they are configured in manual loopback mode. If they are, disable manual loopback. 4. Reset the CSU/DSU, and inspect the line status. If the line protocol comes up, no other action is needed. 5. If the CSU/DSU is not configured in manual loopback mode, contact the leased line or other carrier service for line troubleshooting assistance.

Status Line Condition	Possible Problem	Solution
Serial *x* is up, line protocol is down (disabled) .	A high error rate has occurred due to a remote device problem. A CSU or DSU hardware problem has occurred. Router hardware (interface) is bad.	1. Troubleshoot the line with a serial analyzer and breakout box. Look for toggling CTS and DSR signals. 2. Loop CSU/DSU (DTE loop). If the problem continues, it is likely that there is a hardware problem. If the problem does not continue, it is likely that there is a telephone company problem. 3. Swap out bad hardware, as required (CSU, DSU, switch, local or remote router).
Serial *x* is administratively down, line protocol is down.	The router configuration includes the `shutdown` interface configuration command. A duplicate IP address exists.	1. Check the router configuration for the **shutdown** command. 2. Use the **no shutdown** interface configuration command to remove the **shutdown** command. 3. Verify that there are no identical IP addresses using the **show running-config** privileged exec command or the **show interfaces** exec command. 4. If there are duplicate addresses, resolve the conflict by changing one of the IP addresses.

The **show controllers** command is another important diagnostic tool when troubleshooting serial lines, as shown in Example 3-2. The output indicates the state of the interface channels and whether a cable is attached to the interface. In example 3-2, interface serial 0/0/0 has a V.35 DCE cable attached. The command syntax varies depending on the platform. *Cisco 7000* series routers use a cBus controller card for connecting serial links. With these routers, use the **show controllers cbus** command.

If the electrical interface output displays as `UNKNOWN` instead of `V.35`, `EIA/TIA-449`, or some other electrical interface type, the likely problem is an improperly connected cable. A problem with the internal wiring of the card is also possible. If the electrical interface is unknown, the corresponding display for the **show interfaces serial** command shows that the interface and line protocol are down.

Example 3-2 Displaying Controller Hardware Information on a Serial Interface

```
R1# show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is GT96K
DCE V.35, clock rate 64000
idb at 0x66855120, driver data structure at 0x6685C93C
wic_info 0x6685CF68
```

```
Physical Port 0, SCC Num 0
MPSC Registers:
<Output omitted for brevity>
```

Interactive Graphic

Activity 3.1.2.6: Troubleshooting a Serial Interface

Go to the course online to use the Syntax Checker to perform troubleshooting on a serial interface.

Packet Tracer Activity

Packet Tracer Activity 3.1.2.7: Troubleshooting Serial Interfaces

Background/Scenario

You have been asked to troubleshoot WAN connections for a local telephone company (Telco). The Telco router is supposed to communicate with four remote sites, but none of them are working. Use your knowledge of the OSI model and a few general rules to identify and repair the errors in the network.

PPP Operation (3.2)

This section discusses the PPP operations, including the benefits of PPP, LCP, and NCP protocols, and establishing a PPP session.

Benefits of PPP (3.2.1)

PPP has several advantages over its predecessor HDLC. In this section, PPP is introduced along with examining the benefits of PPP.

Introducing PPP (3.2.1.1)

Recall that HDLC is the default serial encapsulation method when connecting two Cisco routers. With an added protocol type field, the Cisco version of HDLC is proprietary. Thus, Cisco HDLC can only work with other Cisco devices. However, when there is a need to connect to a non-Cisco router, PPP encapsulation should be used, as shown in the Figure 3-19.

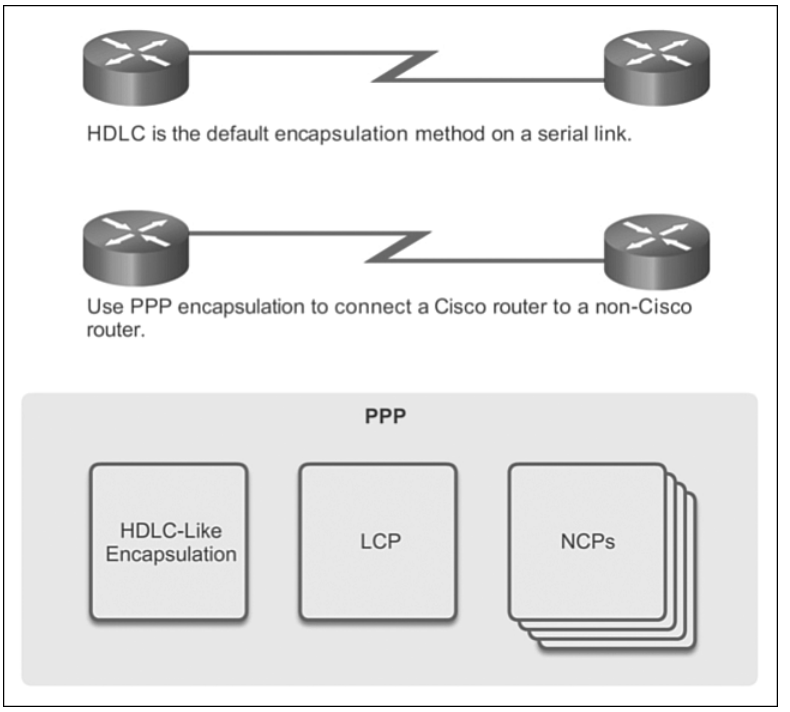


Figure 3-19 What is PPP?

PPP encapsulation has been carefully designed to retain compatibility with most commonly used supporting hardware. PPP encapsulates data frames for transmission over Layer 2 physical links. PPP establishes a direct connection using serial cables, phone lines, ***trunk lines***, cellular telephones, specialized radio links, or fiber-optic links.

PPP contains three main components:

- HDLC-like framing for transporting multiprotocol packets over point-to-point links.
- Extensible ***Link Control Protocol (LCP)*** for establishing, configuring, and testing the data-link connection.
- Family of ***Network Control Protocols (NCPs)*** for establishing and configuring different network layer protocols. PPP allows the simultaneous use of multiple network layer protocols. Some of the more common NCPs are Internet Protocol (IPv4) Control Protocol, IPv6 Control Protocol, AppleTalk Control Protocol, ***Novell IPX*** Control Protocol, Cisco Systems Control Protocol, ***SNA Control Protocol***, and Compression Control Protocol.

Advantages of PPP (3.2.1.2)

PPP originally emerged as an encapsulation protocol for transporting IPv4 traffic over point-to-point links. PPP provides a standard method for transporting multiprotocol packets over point-to-point links.

There are many advantages to using PPP including the fact that it is not proprietary. PPP includes many features not available in HDLC:

- The link quality management feature, as shown in Figure 3-20, monitors the quality of the link. If too many errors are detected, PPP takes the link down.
- PPP supports PAP and CHAP authentication. This feature is explained and practiced in a later section.

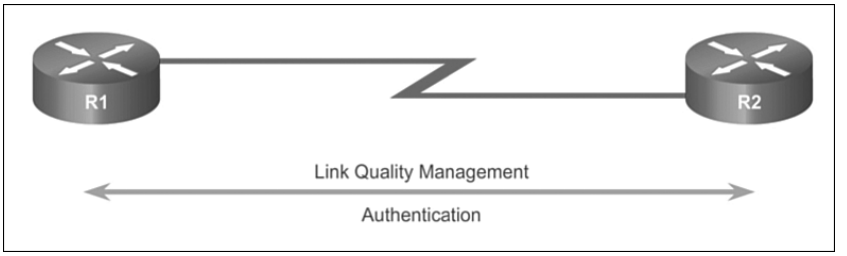


Figure 3-20 Advantages of PPP

LCP and NCP (3.2.2)

LCP and NCP are two key components to PPP. An understanding of these two protocols will help you understand and troubleshoot PPP operations.

PPP Layered Architecture (3.2.2.1)

A layered architecture is a logical model, design, or blueprint that aids in communication between interconnecting layers. Figure 3-21 maps the layered architecture of PPP against the Open System Interconnection (OSI) model. PPP and OSI share the same physical layer, but PPP distributes the functions of LCP and NCP differently.

At the physical layer, you can configure PPP on a range of interfaces, including

- Asynchronous serial, such as leased line services
- Synchronous serial, such as those that use basic telephone service for modem dialup connections
- HSSI
- ISDN

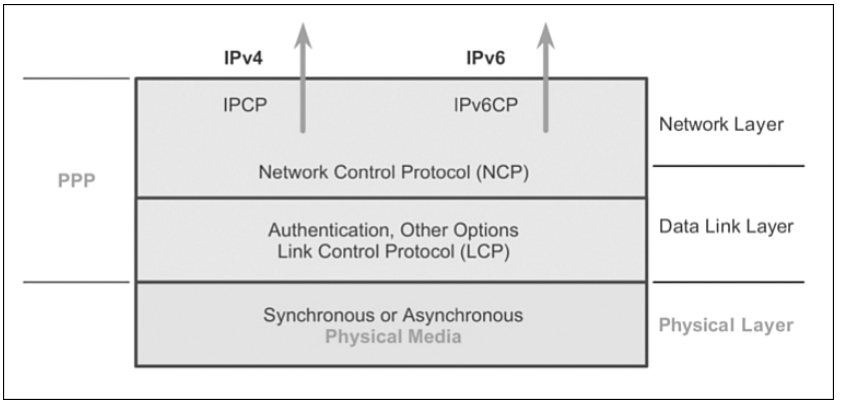


Figure 3-21 PPP Layered Architecture

PPP operates across any DTE/DCE interface (RS-232-C, RS-422, RS-423, or V.35). The only absolute requirement imposed by PPP is a full-duplex circuit, either dedicated or switched, that can operate in either an asynchronous or synchronous bit-serial mode, transparent to PPP link layer frames. PPP does not impose any restrictions regarding transmission rate other than those imposed by the particular DTE/DCE interface in use.

Most of the work done by PPP is at the data link and network layers by the LCP and NCPs. The LCP sets up the PPP connection and its parameters, the NCPs handle higher layer protocol configurations, and the LCP terminates the PPP connection.

PPP – Link Control Protocol (LCP) (3.2.2.2)

The LCP functions within the data link layer and has a role in establishing, configuring, and testing the data-link connection. The LCP establishes the point-to-point link. The LCP also negotiates and sets up control options on the WAN data link, which are handled by the NCPs.

The LCP provides automatic configuration of the interfaces at each end, including

- Handling varying limits on packet size
- Detecting common misconfiguration errors
- Terminating the link
- Determining when a link is functioning properly or when it is failing

After the link is established, PPP also uses the LCP to agree automatically on encapsulation formats such as authentication, compression, and error detection. Figure 3-21 shows the relationship of LCP to the physical layer and NCP.

PPP – Network Control Protocol (NCP) (3.2.2.3)

PPP permits multiple network layer protocols to operate on the same communications link. For every network layer protocol used, PPP uses a separate NCP, as shown in Figure 3-21. For example, IPv4 uses the IP Control Protocol (IPCP) and IPv6 uses IPv6 Control Protocol (IPv6CP).

NCPs include functional fields containing standardized codes to indicate the network layer protocol that PPP encapsulates. Table 3-3 lists the PPP protocol field numbers. Each NCP manages the specific needs required by its respective network layer protocols. The various NCP components encapsulate and negotiate options for multiple network layer protocols.

Table 3-3 Protocol Fields

Value (in hex)	Protocol Name
8021	Internet Protocol (IPv4) Control Protocol
8057	Internet Protocol Version 6 (IPv6) Control Protocol
8023	OSI Network Layer Control Protocol
8029	Appletalk Control Protocol
802b	Novell IPX Control Protocol
c021	Link Control Protocol
c023	Password Authentication Protocol
c223	Challenge Handshake Authentication Protocol

PPP Frame Structure (3.2.2.4)

A PPP frame consists of six fields. The following descriptions summarize the PPP frame fields illustrated in Figure 3-22:

- **Flag:** A single byte that indicates the beginning or end of a frame. The Flag field consists of the binary sequence 01111110. In successive PPP frames, only a single Flag character is used.
- **Address:** A single byte that contains the binary sequence 11111111, the standard broadcast address. PPP does not assign individual station addresses.
- **Control:** A single byte that contains the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame. This provides a connectionless link service that does require the establishment of data links or links stations. On a point-to-point link, the destination node does not need to

be addressed. Therefore, for PPP, the Address field is set to 0xFF, the broadcast address. If both PPP peers agree to perform Address and Control field compression during the LCP negotiation, the Address field is not included.

- **Protocol**: Two bytes that identify the protocol encapsulated in the information field of the frame. The 2-byte Protocol field identifies the protocol of the PPP payload. If both PPP peers agree to perform Protocol field compression during LCP negotiation, the Protocol field is 1 byte for the protocol identification in the range 0x00-00 to 0x00-FF. The most up-to-date values of the Protocol field are specified in the most recent Assigned Numbers Request For Comments (RFC).
- **Data**: Zero or more bytes that contain the datagram for the protocol specified in the Protocol field. The end of the Information field is found by locating the closing flag sequence and allowing 2 bytes for the FCS field. The default maximum length of the Information field is 1500 bytes. By prior agreement, consenting PPP implementations can use other values for the maximum Information field length.
- **Frame Check Sequence (FCS)**: Normally 16 bits (2 bytes). By prior agreement, consenting PPP implementations can use a 32-bit (4-byte) FCS for improved error detection. If the receiver's calculation of the FCS does not match the FCS in the PPP frame, the PPP frame is silently discarded.

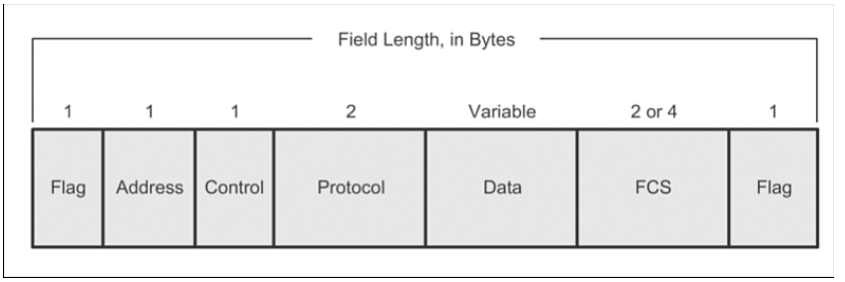


Figure 3-22 PPP Frame Fields

LCPs can negotiate modifications to the standard PPP frame structure. Modified frames, however, are always distinguishable from standard frames.

Interactive Graphic

Activity 3.2.2.5: Troubleshooting a Serial Interface

Go to the course online to perform this practice activity.

PPP Sessions (3.2.3)

Understanding PPP session establishment, LCP and NCP are important parts of implementing and troubleshooting PPP. These topics are discussed next.

Establishing a PPP Session (3.2.3.1)

There are three phases of establishing a PPP session, as shown in Figure 3-23:

- **Phase 1: Link establishment and configuration negotiation**: Before PPP exchanges any network layer datagrams, such as IP, the LCP must first open the connection and negotiate configuration options. This phase is complete when the receiving router sends a configuration-acknowledgment frame back to the router initiating the connection.
- **Phase 2: Link quality determination (optional)**: The LCP tests the link to determine whether the link quality is sufficient to bring up network layer protocols. The LCP can delay transmission of network layer protocol information until this phase is complete.
- **Phase 3: Network layer protocol configuration negotiation**: After the LCP has finished the link quality determination phase, the appropriate NCP can separately configure the network layer protocols, and bring them up and take them down at any time. If the LCP closes the link, it informs the network layer protocols so that they can take appropriate action.

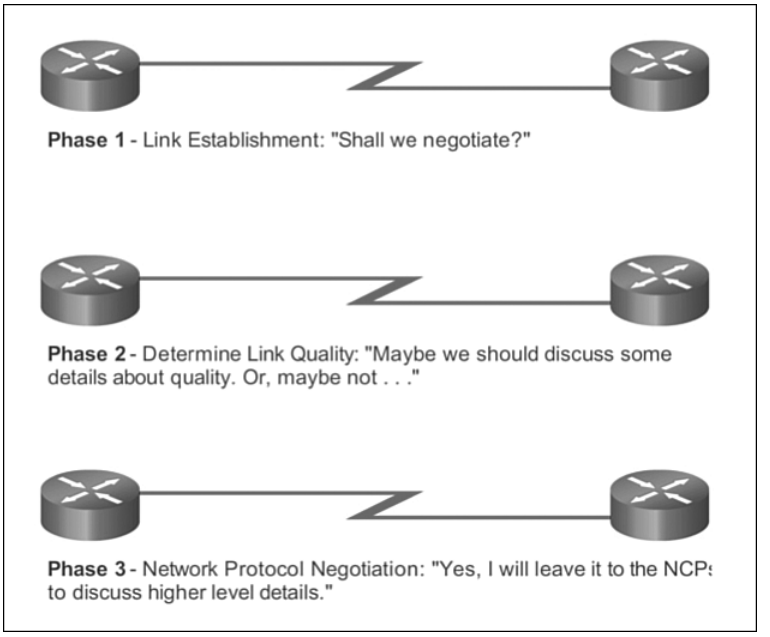


Figure 3-23 Establishing a PPP Session

The link remains configured for communications until explicit LCP or NCP frames close the link, or until some external event occurs such as an inactivity timer expiring, or an administrator intervening.

The LCP can terminate the link at any time. This is usually done when one of the routers requests termination, but can happen because of a physical event, such as the loss of a carrier or the expiration of an idle-period timer.

LCP Operation (3.2.3.2)

LCP operation includes provisions for link establishment, link maintenance, and link termination. LCP operation uses three classes of LCP frames to accomplish the work of each of the LCP phases:

- Link-establishment frames establish and configure a link (Configure-Request, Configure-Ack, Configure-Nak, and Configure-Reject).
- Link-maintenance frames manage and debug a link (Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply, and Discard-Request).
- Link-termination frames terminate a link (Terminate-Request and Terminate-Ack).

Link Establishment

Link establishment is the first phase of LCP operation, as seen in Figure 3-24. This phase must complete successfully, before any network layer packets can be exchanged. During link establishment, the LCP opens the connection and negotiates the configuration parameters. The link establishment process starts with the initiating device sending a Configure-Request frame to the responder. The Configure-Request frame includes a variable number of configuration options needed to set up on the link.

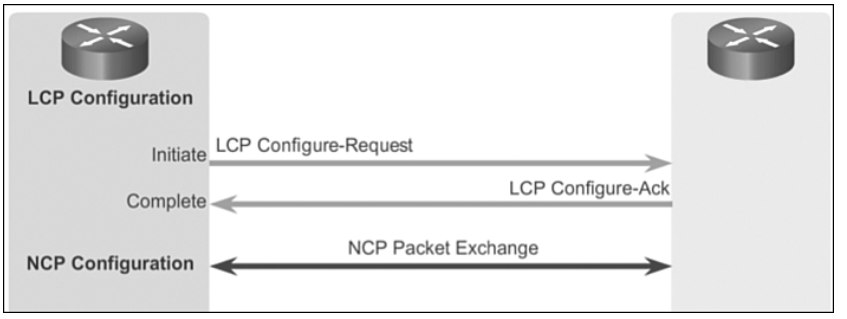


Figure 3-24 PPP Link Establishment

The initiator includes the options for how it wants the link created, including protocol or authentication parameters. The responder processes the request:

- If the options are not acceptable or not recognized, the responder sends a Configure-Nak or Configure-Reject message. If this occurs and the negotiation fails, the initiator must restart the process with new options.

- If the options are acceptable, the responder responds with a Configure-Ack message and the process moves on to the authentication stage. The operation of the link is handed over to the NCP.

When NCP has completed all necessary configurations, including validating authentication if configured, the line is available for data transfer. During the exchange of data, LCP transitions into link maintenance.

Link Maintenance

During link maintenance, LCP can use messages to provide feedback and test the link, as shown in Figure 3-25.

- **Echo-Request, Echo-Reply, and Discard-Request:** These frames can be used for testing the link.
- **Code-Reject and Protocol-Reject:** These frame types provide feedback when one device receives an invalid frame due to either an unrecognized LCP code (LCP frame type) or a bad protocol identifier. For example, if an uninterpretable packet is received from the peer, a Code-Reject packet is sent in response. The sending device will resend the packet.

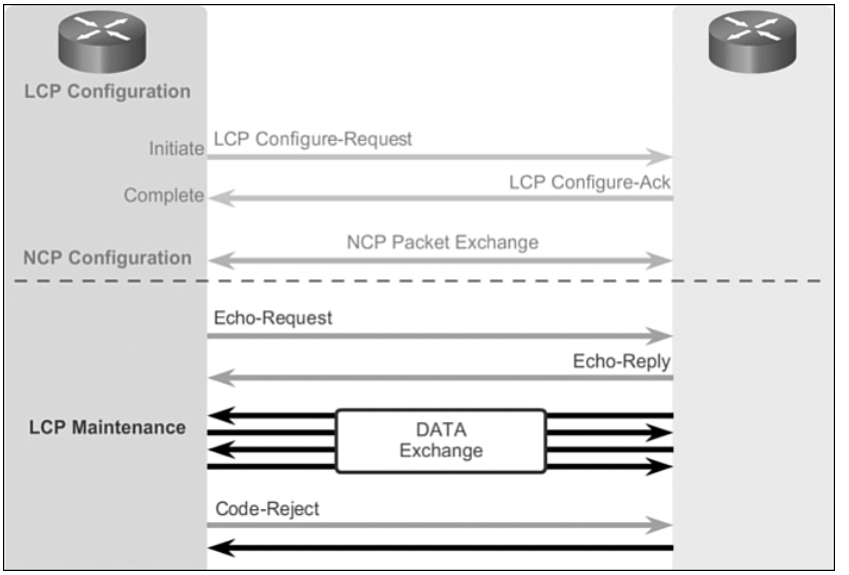


Figure 3-25 PPP Link Maintenance

Link Termination

After the transfer of data at the network layer completes, the LCP terminates the link, as shown in Figure 3-26. NCP only terminates the network layer and NCP link. The link remains open until the LCP terminates it. If the LCP terminates the link before NCP, the NCP session is also terminated.

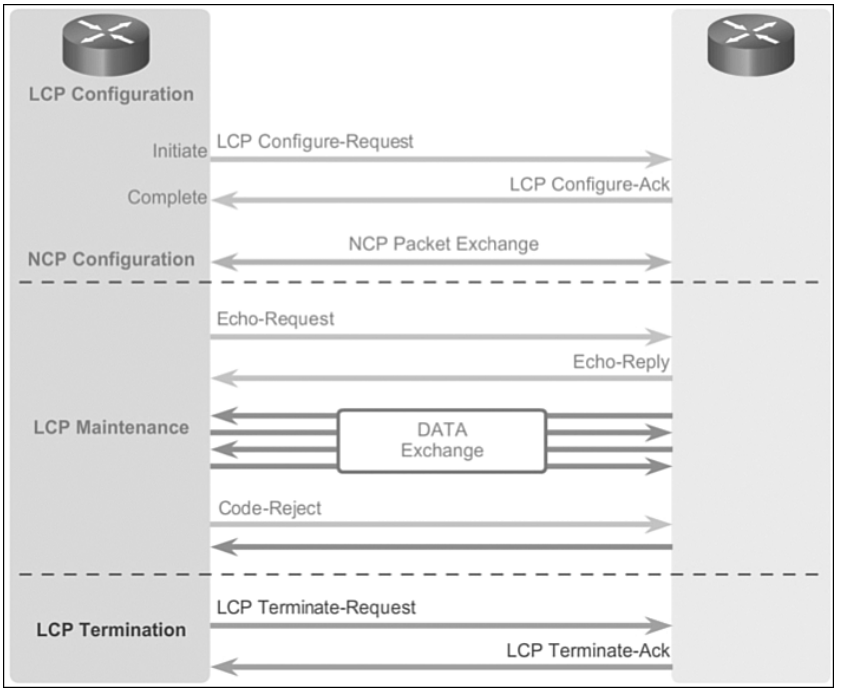


Figure 3-26 PPP Link Termination

PPP can terminate the link at any time. This might happen because of the loss of the carrier, authentication failure, link quality failure, the expiration of an idle-period timer, or the administrative closing of the link. The LCP closes the link by exchanging Terminate packets. The device initiating the shutdown sends a Terminate-Request message. The other device replies with a Terminate-Ack. A termination request indicates that the device sending it needs to close the link. When the link is closing, PPP informs the network layer protocols so that they may take appropriate action.

LCP Packet (3.2.3.3)

Figure 3-27 shows the fields in an LCP packet:

- **Code:** The Code field is 1 byte in length and identifies the type of LCP packet.
- **Identifier:** The Identifier field is 1 byte in length and is used to match packet requests and replies.

- **Length:** The Length field is 2 bytes in length and indicates the total length (including all fields) of the LCP packet.
- **Data:** The Data field is 0 or more bytes as indicated by the length field. The format of this field is determined by the code.

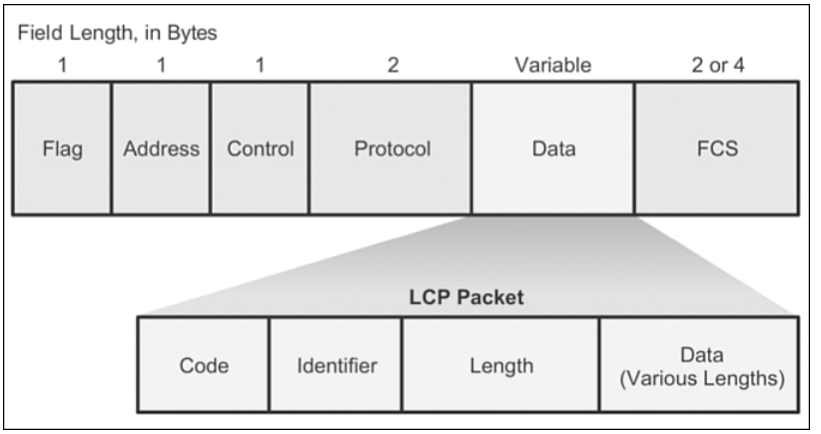


Figure 3-27 LCP Packet Codes

Each LCP packet is a single LCP message consisting of an LCP Code field identifying the type of LCP packet, an identifier field so that requests and replies can be matched, and a Length field indicating the size of the LCP packet and LCP packet type-specific data.

Each LCP packet has a specific function in the exchange of configuration information depending on its packet type. The Code field of the LCP packet identifies the packet type according to Table 3-4.

Table 3-4 LCP Packet Fields

LCP Code	LCP Packet Type	Description
1	Configure-Request	Sent to open or reset a PPP connection. Configure-Request contains a list of LCP options with changes to default option values.
2	Configure-Ack	Sent when all of the values of all of the LCP options in the last Configure-Request received are recognized and acceptable. When both PPP peers send and receive Configure-Acks, the LCP negotiation is complete.
3	Configure-Nak	Sent when all the LCP options are recognized, but the values of some options are not acceptable. Configure-Nak includes the mismatching options and their acceptable values.

LCP Code	LCP Packet Type	Description
4	Configure-Reject	Set when LCP options are not recognized or not acceptable for negotiation. Configure-Reject includes the unrecognized or non-negotiable options.
5	Terminate-Request	Optionally sent to close the PPP connection.
6	Terminate-Ack	Sent in response to a Terminate-Request.
7	Code-Reject	Sent when the LCP code is unknown. The Code-Request message includes the rejected LCP packet.
8	Protocol-Reject	Sent when the PPP frame contains an unknown Protocol ID. The Protocol-Reject message includes the rejected LCP packet. Protocol-Reject is typically sent by a PPP peer in response to PPP NCP for a LAN protocol not enabled on the PPP peer.
9	Echo-Request	Optionally sent to test PPP connection.
10	Echo-Reply	Sent in response to an Echo-Request. The PPP Echo-Request and Echo-Reply are not related to the ICMP Echo Request and Echo Reply messages.
11	Discard-Request	Optionally sent to exercise the link in the outbound direction.

PPP Configuration Options (3.2.3.4)

PPP can be configured to support various optional functions, as shown in Figure 3-28. These optional functions include

- Authentication using either PAP or CHAP
- Compression using either Stacker or Predictor
- Multilink that combines two or more channels to increase the WAN bandwidth

To negotiate the use of these PPP options, the LCP link-establishment frames contain option information in the data field of the LCP frame, as shown in Figure 3-29. If a configuration option is not included in an LCP frame, the default value for that configuration option is assumed.

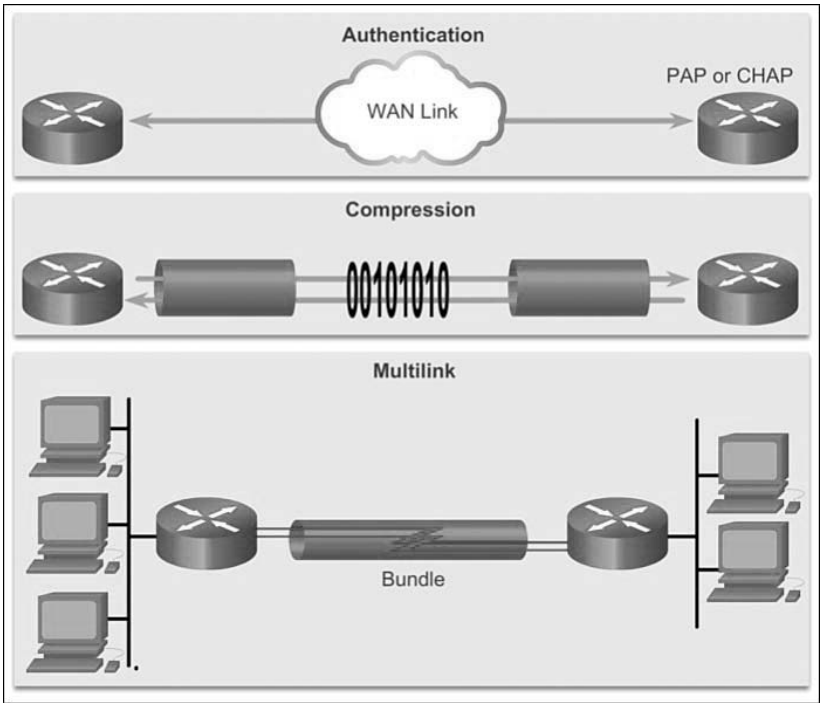


Figure 3-28 PPP Configuration Options

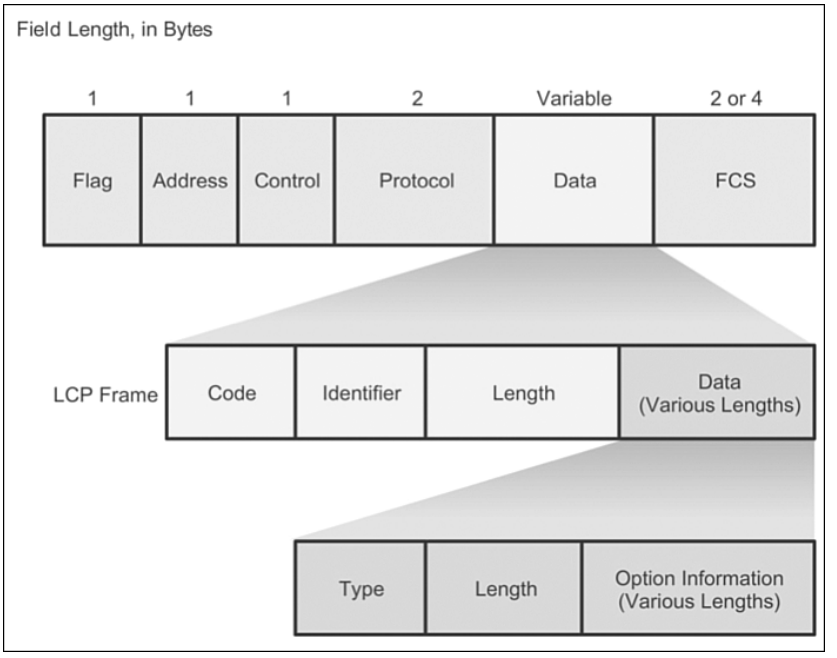


Figure 3-29 LCP Option Fields

This phase is complete when a configuration acknowledgment frame has been sent and received.

NCP Explained (3.2.3.5)

After the link has been initiated, the LCP passes control to the appropriate NCP.

NCP Process

Although initially designed for IP packets, PPP can carry data from multiple network layer protocols by using a modular approach in its implementation. PPP's modular model allows LCP to set up the link and then transfer the details of a network protocol to a specific NCP. Each network protocol has a corresponding NCP and each NCP has a corresponding RFC.

There are NCPs for IPv4, IPv6, IPX, AppleTalk, and many others. NCPs use the same packet format as the LCPs.

After the LCP has configured and authenticated the basic link, the appropriate NCP is invoked to complete the specific configuration of the network layer protocol being used. When the NCP has successfully configured the network layer protocol, the network protocol is in the open state on the established LCP link. At this point, PPP can carry the corresponding network layer protocol packets.

IPCP Example

As an example of how the NCP layer works, the NCP configuration of IPv4, which is the most common Layer 3 protocol, is shown in Figure 3-30. After LCP has established the link, the routers exchange IPCP messages, negotiating options specific to the IPv4 protocol. IPCP is responsible for configuring, enabling, and disabling the IPv4 modules on both ends of the link. IPv6CP is an NCP with the same responsibilities for IPv6.

IPCP negotiates two options:

- **Compression:** Allows devices to negotiate an algorithm to compress TCP and IP headers and save bandwidth. The Van Jacobson TCP/IP header compression reduces the size of the TCP/IP headers to as few as 3 bytes. This can be a significant improvement on slow serial lines, particularly for interactive traffic.
- **IPv4-Address:** Allows the initiating device to specify an IPv4 address to use for routing IP over the PPP link, or to request an IPv4 address for the responder. Prior to the advent of broadband technologies such as DSL and cable modem services, dialup network links commonly used the IPv4 address option.

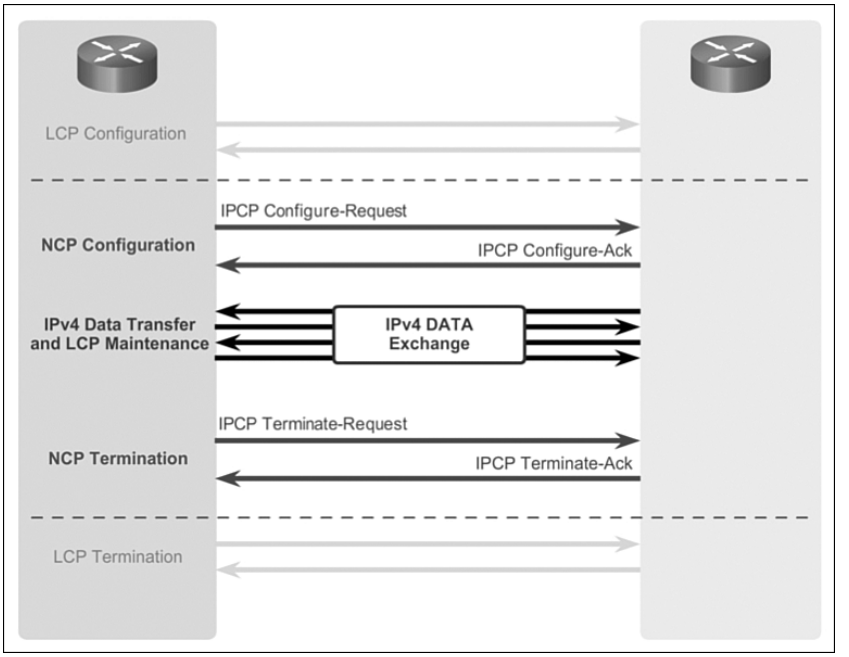


Figure 3-30 PPP NCP Operation

After the NCP process is complete, the link goes into the open state, and LCP takes over again in a link maintenance phase. Link traffic consists of any possible combination of LCP, NCP, and network layer protocol packets. When data transfer is complete, NCP terminates the protocol link; LCP terminates the PPP connection.

Interactive Graphic

Activity 3.2.3.6: Identify the Steps in the LCP Link Negotiation Process

Go to the course online to perform this practice activity.

Configure PPP (3.3)

This section describes the configuration of PPP. Basic PPP configuration is discussed along with optional PPP features and PPP authentication.

Configure PPP (3.3.1)

Basic PPP configuration commands are discussed next along with PPP compression, PPP quality link monitoring, and PPP Multilink.

PPP Configuration Options (3.3.1.1)

In the previous section, configurable LCP options were introduced to meet specific WAN connection requirements. PPP may include the following LCP options:

- **Authentication:** Peer routers exchange authentication messages. Two authentication choices are *Password Authentication Protocol (PAP)* and *Challenge Handshake Authentication Protocol (CHAP)*.
- **Compression:** Increases the effective throughput on PPP connections by reducing the amount of data in the frame that must travel across the link. The protocol decompresses the frame at its destination. Two compression protocols available in Cisco routers are Stacker and Predictor.
- **Error detection:** Identifies fault conditions. The Quality and Magic Number options help ensure a reliable, loop-free data link. The Magic Number field helps in detecting links that are in a looped-back condition. Until the Magic-Number Configuration Option has been successfully negotiated, the Magic-Number must be transmitted as zero. Magic numbers are generated randomly at each end of the connection.
- **PPP Callback:** PPP callback is used to enhance security. With this LCP option, a Cisco router can act as a callback client or a callback server. The client makes the initial call, requests that the server call it back, and terminates its initial call. The callback router answers the initial call and makes the return call to the client based on its configuration statements. The command is **ppp callback [accept | request]**.
- **Multilink:** This alternative provides load balancing over the router interfaces that PPP uses. Multilink PPP, also referred to as MP, MPPP, MLP, or Multilink, provides a method for spreading traffic across multiple physical WAN links while providing packet *fragmentation* and *reassembly*, proper sequencing, multivendor interoperability, and load balancing on inbound and outbound traffic.

When options are configured, a corresponding field value is inserted into the LCP option field, shown in Table 3-5.

Table 3-5 Configurable Options Field Codes

Option Name	Option Type	Option Length	Description
Authentication Protocol	3	5 or 6	This field indicates the authentication protocol, either PAP or CHAP.
Protocol Compression	7	2	A flag indicating that the PPP protocol ID be compressed to a single octet when the 2-byte protocol field is in the range of 0x00-00 to 0x00-FF.

Option Name	Option Type	Option Length	Description
Address and Control Field Compression	8	2	A flag indicating that the PPP Address field (always set to 0xFF) and the PPP Control field (always set to 0x03) be removed from the PPP header.
Magic Number (Error Detection)	5	6	This is a random number chosen to distinguish a peer and detect looped back lines.
Callback	13 or 0x0D	3	A 1-octet indicator of how callback is to be determined.

PPP Basic Configuration Command (3.3.1.2)

Basic PPP configuration is very straightforward. After PPP is configured on an interface the network administrator can then apply one or more PPP options.

Enabling PPP on an Interface

To set PPP as the encapsulation method used by a serial interface, use the **encapsulation ppp** interface configuration command.

The following example enables PPP encapsulation on interface serial 0/0/0:

```
R3# configure terminal
R3(config)# interface serial 0/0/0
R3(config-if)# encapsulation ppp
```

The **encapsulation ppp** interface command has no arguments. Remember that if PPP is not configured on a Cisco router, the default encapsulation for serial interfaces is HDLC.

Figure 3-31 and the listing that follows, shows that routers R1 and R2 have been configured with both an IPv4 and an IPv6 address on the serial interfaces. PPP is a Layer 2 encapsulation that supports various Layer 3 protocols including IPv4 and IPv6.

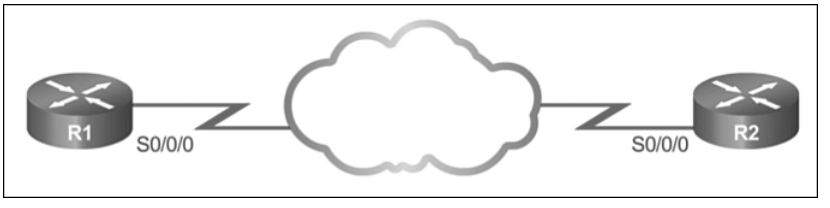


Figure 3-31 PPP Basic Configuration

Partial running-config for R1

```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
```

Parital running-config for R2

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
```

PPP Compression Commands (3.3.1.3)

Point-to-point software compression on serial interfaces can be configured after PPP encapsulation is enabled. Because this option invokes a software compression process, it can affect system performance. If the traffic already consists of compressed files, such as .zip, .tar, or .mpeg, do not use this option. The command syntax for the **compress** command is

```
Router(config-if)# compress [ predictor | stac ]
```

- **predictor** (optional): Specifies that a predictor compression algorithm will be used
- **stac** (optional): Specifies that a Stacker (LZS) compression algorithm will be used

To configure compression over PPP, enter the following commands:

```
R2(config)# interface serial 0/0/0
R2(config-if)# encapsulation ppp
R2(config-if)# compress [ predictor | stac ]
```

The following example shows predictor compression used between R1 and R2:

Partial running-config for R1

```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
```

```
 encapsulation ppp
 compress predictor
```

Partial running-config for R2

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 compress predictor
```

PPP Link Quality Monitoring Command (3.3.1.4)

Recall that LCP provides an optional link quality determination phase. In this phase, LCP tests the link to determine whether the link quality is sufficient to use Layer 3 protocols. The **ppp quality** *percentage* command ensures that the link meets the quality requirement set; otherwise, the link closes down. The command syntax for the **ppp quality** command is

```
Router(config-if)# ppp quality percentage
```

- *percentage*: Specifies the link quality threshold. Range is 1 to 100.

The percentages are calculated for both incoming and outgoing directions. The outgoing quality is calculated by comparing the total number of packets and bytes sent to the total number of packets and bytes received by the destination node. The incoming quality is calculated by comparing the total number of packets and bytes received to the total number of packets and bytes sent by the destination node.

If the link quality percentage is not maintained, the link is deemed to be of poor quality and is taken down. Link Quality Monitoring (LQM) implements a time lag so that the link does not bounce up and down.

The following configuration example monitors the data dropped on the link and avoids frame looping:

```
R2(config)# interface serial 0/0/0
R2(config-if)# encapsulation ppp
R2(config-if)# ppp quality 80
```

Use the **no ppp quality** command to disable LQM. The following example shows link quality being used between R1 and R2:

Partial running-config for R1

```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
 ppp quality 80
```

Partial running-config for R2

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp quality 80
```

Interactive Graphic

Activity 3.3.1.4: PPP Link Quality Monitoring Command

Go to the course online to use the checker to LQM on R1's serial 0/0/1 interface.

PPP Multilink Commands (3.3.1.5)

Multilink PPP (also referred to as MP, MPPP, MLP, or Multilink) provides a method for spreading traffic across multiple physical WAN links, as shown in Figure 3-32. Multilink PPP also provides packet fragmentation and reassembly, proper sequencing, multivendor interoperability, and load balancing on inbound and outbound traffic.

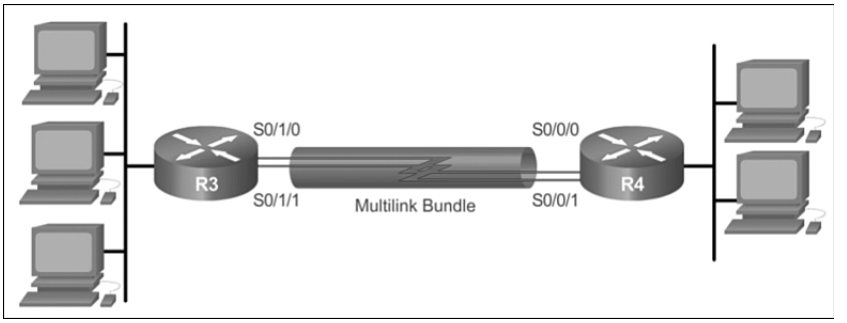


Figure 3-32 PPP Multilink

MPPP allows packets to be fragmented and sends these fragments simultaneously over multiple point-to-point links to the same remote address. The multiple physical links come up in response to a user-defined load threshold. MPPP can measure the

load on just inbound traffic, or on just outbound traffic, but not on the combined load of both inbound and outbound traffic.

Configuring MPPP requires two steps.

Step 1. Create a multilink bundle.

The **interface multilink** *number* command creates the multilink interface.

In interface configuration mode, an IP address is assigned to the multilink interface. In this example, both IPv4 and IPv6 addresses are configured on routers R3 and R4.

The interface is enabled for multilink PPP.

The interface is assigned a multilink group number.

Step 2. Assign interfaces to the multilink bundle. Each interface that is part of the multilink group:

Is enabled for PPP encapsulation.

Is enabled for multilink PPP.

Is bound to the multilink bundle using the multilink group number configured in Step 1.

The following example shows multilink PPP configured between R3 and R4:

Partial running-config for R3

```
hostname R3
!
interface Multilink 1
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

Partial running-config for R4

```
hostname R4
!
interface Multilink 1
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

To disable PPP multilink, use the **no ppp multilink** command.

Verifying PPP Configuration (3.3.1.6)

Use the **show interfaces serial** command to verify proper configuration of HDLC or PPP encapsulation. Example 3-3 shows a PPP configuration.

Example 3-3 Using **show interfaces serial** to Verify a PPP Encapsulation

```
R2#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.0.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, IPV6CP, CCP, CDPCP,, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
<Output omitted for brevity>
```

When you configure HDLC, the output of the **show interfaces serial** command should display **encapsulation HDLC**. When PPP is configured, the LCP and NCP states also display. Notice that NCPs IPCP and IPv6CP are open for IPv4 and IPv6 because R1 and R2 were configured with both IPv4 and IPv6 addresses.

Table 3-6 summarizes commands used when verifying PPP.

Table 3-6 Verifying PPP Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.
show interfaces serial	Displays information about a serial interface.
show ppp multilink	Displays information about a PPP multilink interface.

The **show ppp multilink** command verifies that PPP multilink is enabled on R3, as shown in Example 3-4. The output indicates the interface Multilink 1, the hostnames of both the local and remote endpoints, and the serial interfaces assigned to the multilink bundle.

Example 3-4 Verifying PPP Multilink

```
R3# show ppp multilink
Multilink1
  Bundle name: R4
  Remote Endpoint Discriminator: [1] R4
  Local Endpoint Discriminator: [1] R3
  Bundle up for 00:01:20, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x2 received sequence, 0x2 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se0/1/1, since 00:01:20
    Se0/1/0, since 00:01:06
No inactive multilink interfaces
R3#
```

PPP Authentication (3.3.2)

PPP authentication protocols and configuration of PPP authentication is discussed in this section.

PPP Authentication Protocols (3.3.2.1)

PPP defines an extensible LCP that allows negotiation of an authentication protocol for authenticating its peer before allowing network layer protocols to transmit over the link. RFC 1334 defines two protocols for authentication, PAP and CHAP, as shown in Figure 3-33.

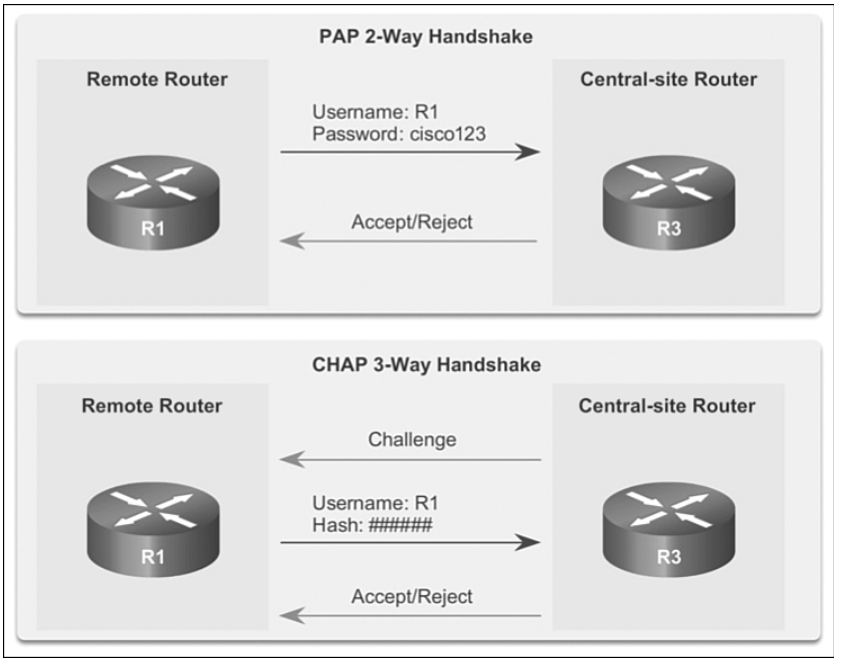


Figure 3-33 PPP Authentication Protocols

PAP is a very basic two-way process. There is no encryption. The username and password are sent in plaintext. If it is accepted, the connection is allowed. CHAP is more secure than PAP. It involves a three-way exchange of a shared secret.

The authentication phase of a PPP session is optional. If used, the peer is authenticated after LCP establishes the link and chooses the authentication protocol. If it is used, authentication takes place before the network layer protocol configuration phase begins.

The authentication options require that the calling side of the link enter authentication information. This helps to ensure that the user has the permission of the network administrator to make the call. Peer routers exchange authentication messages.

Password Authentication Protocol (PAP) (3.3.2.2)

One of the many features of PPP is that it performs Layer 2 authentication in addition to other layers of authentication, encryption, access control, and general security procedures.

Initiating PAP

PAP provides a simple method for a remote node to establish its identity using a two-way handshake. PAP is not interactive. When the **ppp authentication pap** command is used, the username and password are sent as one LCP data package, rather than the server sending a login prompt and waiting for a response, as shown in Figure 3-34. After PPP completes the link establishment phase, the remote node repeatedly sends a username-password pair across the link until the receiving node acknowledges it or terminates the connection.

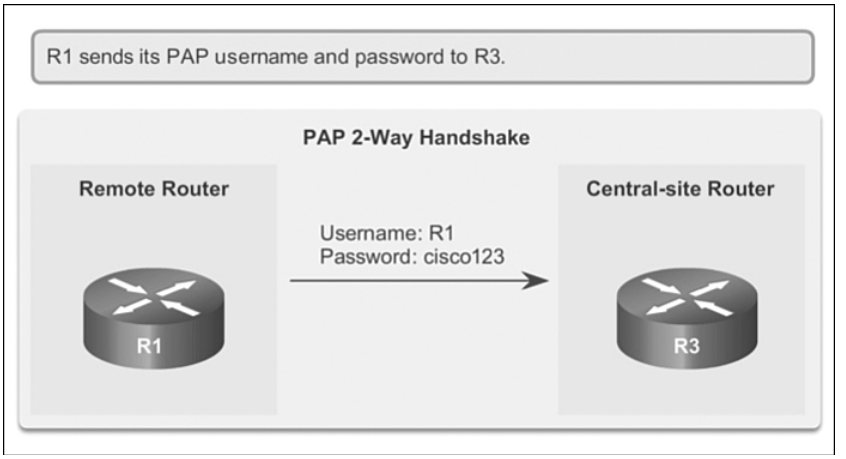


Figure 3-34 Initiating PAP

Completing PAP

At the receiving node, the username-password is checked by an authentication server that either allows or denies the connection. An accept or reject message is returned to the requester, as shown in Figure 3-35.

PAP is not a strong authentication protocol. Using PAP, passwords are sent across the link in plaintext, and there is no protection from playback or repeated trial-and-error attacks. The remote node is in control of the frequency and timing of the login attempts.

Nonetheless, there are times when using PAP can be justified. For example, despite its shortcomings, PAP may be used in the following environments:

- A large installed base of client applications that do not support CHAP
- Incompatibilities between different vendor implementations of CHAP
- Situations where a plaintext password must be available to simulate a login at the remote host

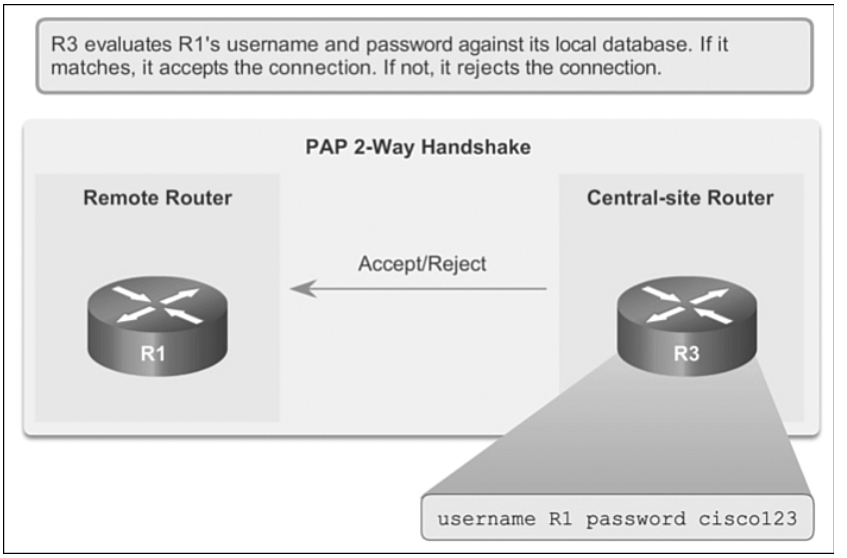


Figure 3-35 Completing PAP

Challenge Handshake Authentication Protocol (CHAP) (3.3.2.3)

After authentication is established with PAP, it does not reauthenticate. This leaves the network vulnerable to attack. Unlike PAP, which only authenticates once, CHAP conducts periodic challenges to make sure that the remote node still has a valid password value. The password value is variable and changes unpredictably while the link exists.

After the PPP link establishment phase is complete, the local router sends a challenge message to the remote node, as shown in Figure 3-36.

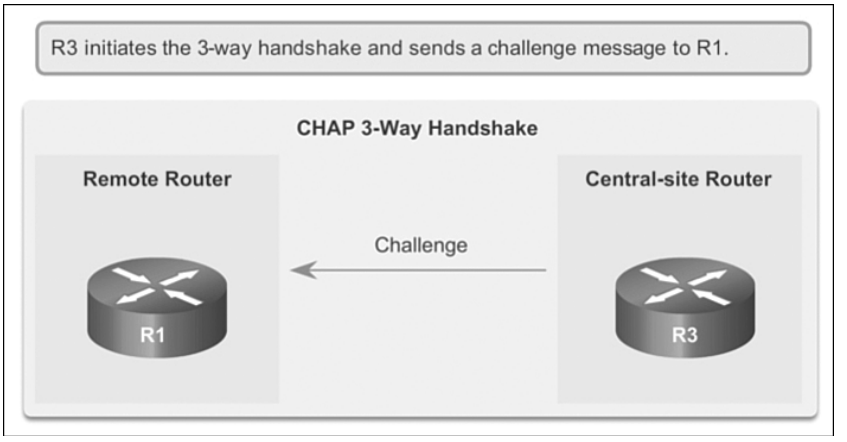


Figure 3-36 Initiating CHAP

The remote node responds with a value calculated using a one-way hash function, which is typically *message digest 5 (MD5)* based on the password and challenge message, as shown in Figure 3-37.

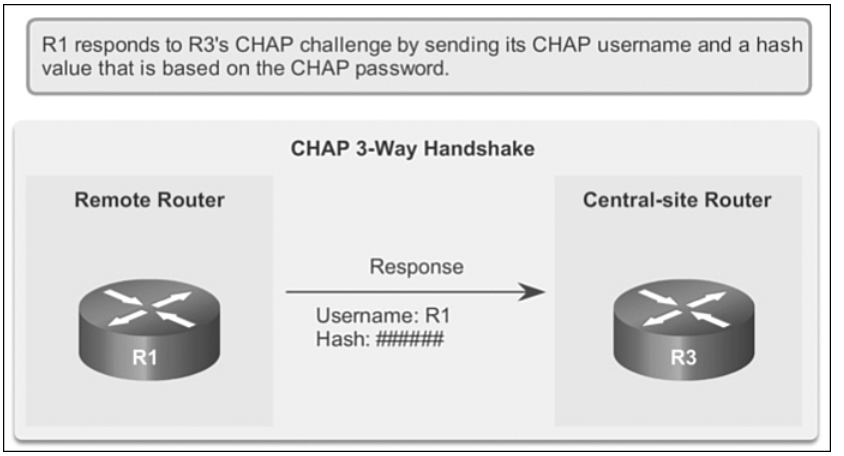


Figure 3-37 Responding CHAP

The local router checks the response against its own calculation of the expected hash value. If the values match, the initiating node acknowledges the authentication, as shown in Figure 3-38. If the value does not match, the initiating node immediately terminates the connection.

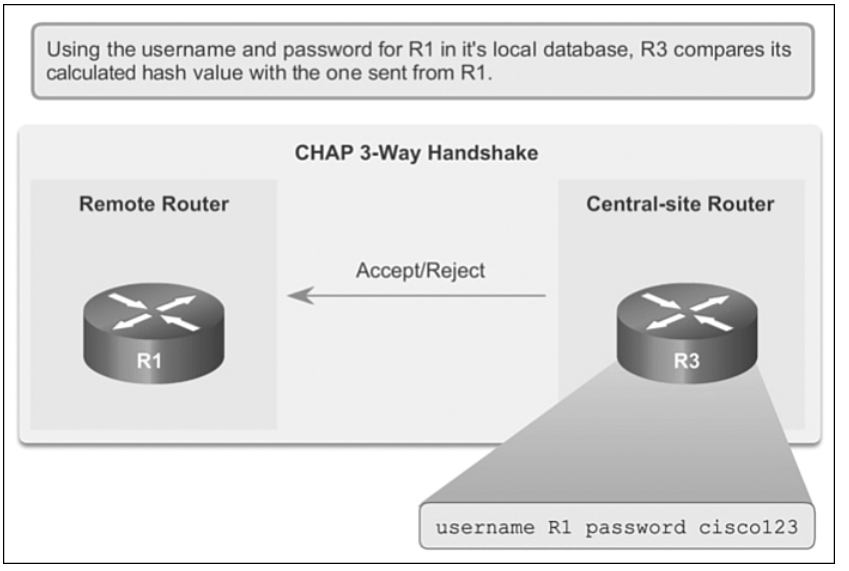


Figure 3-38 Completing CHAP

CHAP provides protection against playback attack by using a variable challenge value that is unique and unpredictable. Because the challenge is unique and random, the resulting hash value is also unique and random. The use of repeated challenges limits the time of exposure to any single attack. The local router or a third-party authentication server is in control of the frequency and timing of the challenges.

PPP Encapsulation and Authentication Process (3.3.2.4)

The flowchart in Figure 3-39 can be used to help understand the PPP authentication process when configuring PPP. The flowchart provides a visual example of the logic decisions made by PPP.

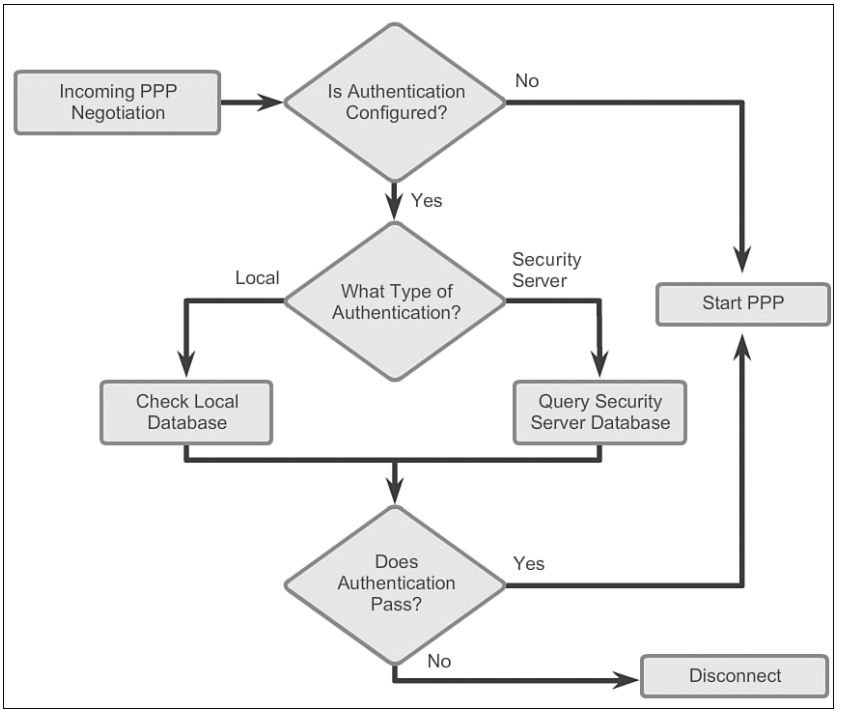


Figure 3-39 PPP Encapsulation and Authentication Process

For example, if an incoming PPP request requires no authentication, then PPP progresses to the next level. If an incoming PPP request requires authentication, then it can be authenticated using either the local database or a security server. As illustrated in the flowchart, successful authentication progresses to the next level, while an authentication failure disconnects and drops the incoming PPP request.

Follow the steps to view R1 establishing an authenticated PPP CHAP connection with R2.

Step 1. As shown in Figure 3-40, R1 initially negotiates the link connection using LCP with router R2 and the two systems agree to use CHAP authentication during the PPP LCP negotiation.

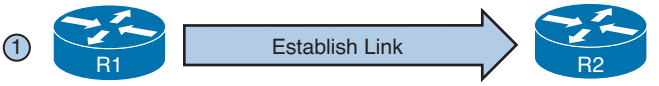


Figure 3-40 Establishing a Link

Step 2. As shown in Figure 3-41, R2 generates an ID and a random number, and sends that and its username as a CHAP challenge packet to R1.

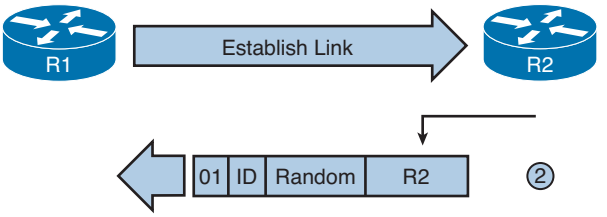


Figure 3-41 Sending a CHAP Challenge to R1

Step 3. As shown in Figure 3-42, R1 uses the username of the challenger (R2) and cross references it with its local database to find its associated password. R1 then generates a unique MD5 hash number using the R2's username, ID, random number and the shared secret password. In this example, the shared secret password is boardwalk.

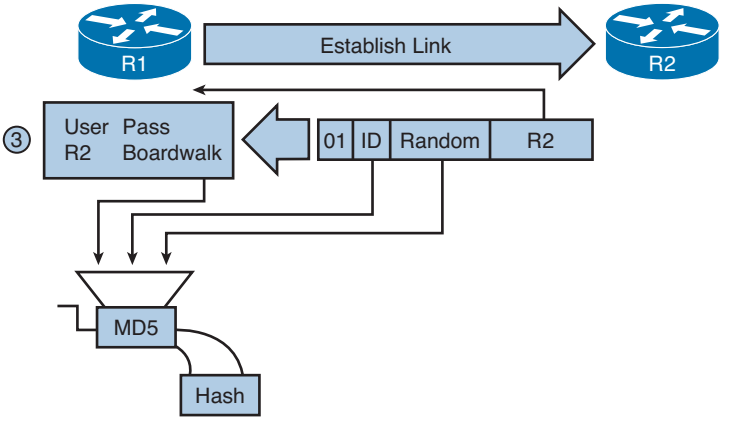


Figure 3-42 R1 Validates R2

Step 4. As shown in Figure 3-43, Router R1 then sends the challenge ID, the hashed value, and its username (R1) to R2.

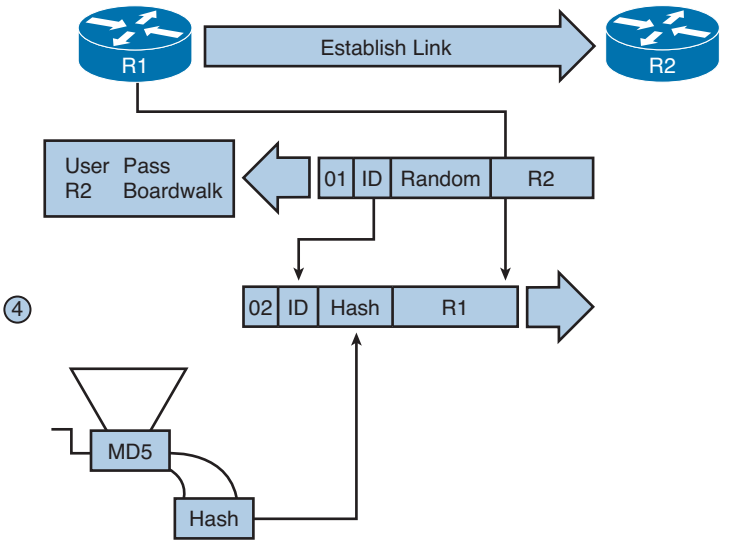


Figure 3-43 R1 Sends the Challenge to R2

Step 5. As shown in Figure 3-44, R2 generates its own hash value using the ID, the shared secret password, and the random number it originally sent to R1.

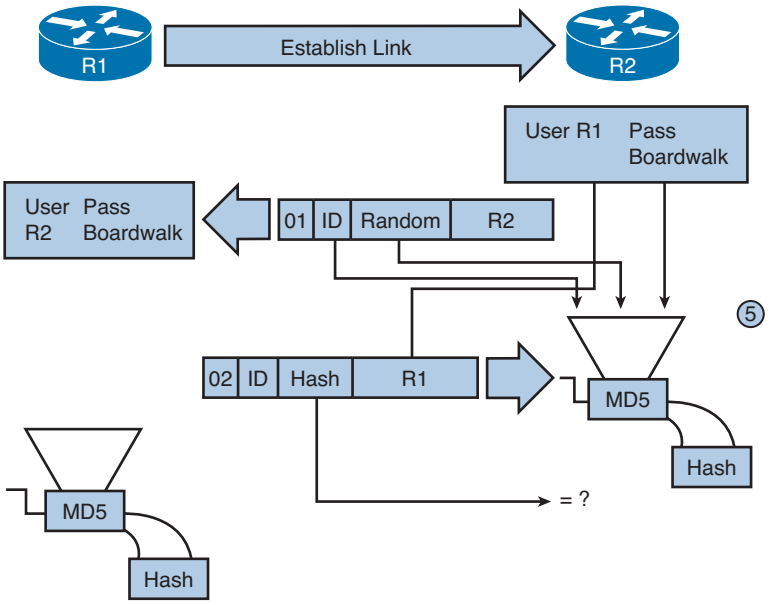


Figure 3-44 R2 Validates R1

Step 6. As shown in Figure 3-45, R2 compares its hash value with the hash value sent by R1. If the values are the same, R2 sends a link established response to R1.

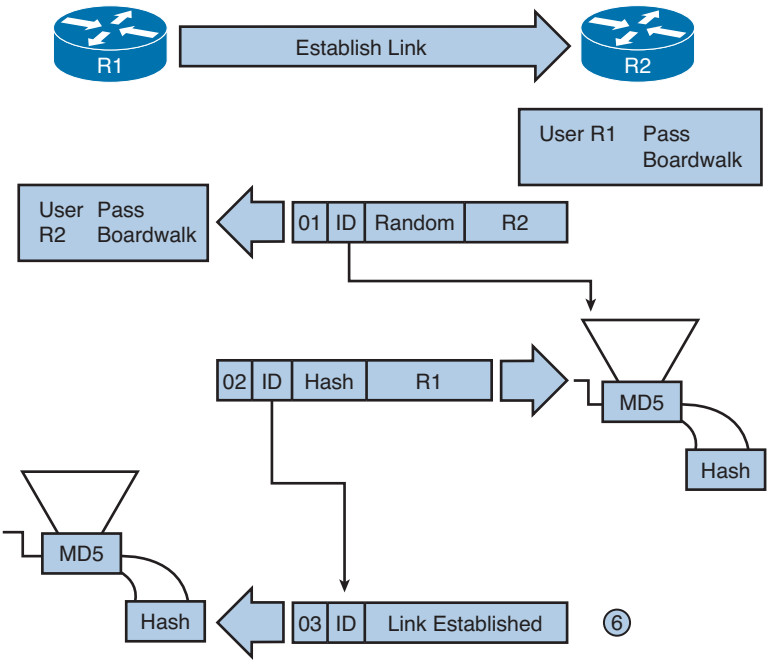


Figure 3-45 R2 Establishes the Link

If the authentication failed, a CHAP failure packet is built from the following components:

- 04 = CHAP failure message type
- id = copied from the response packet
- "Authentication failure" or some similar text message, which is meant to be a user-readable explanation

The shared secret password must be identical on R1 and R2.

Configuring PPP Authentication (3.3.2.5)

To specify the order in which the CHAP or PAP protocols are requested on the interface, use the **ppp authentication** interface configuration command:

```
Router(config-if)# ppp authentication {chap | chap pap | pap chap | pap} [if needed]
   [list-name | default] [callin]
```

- Use the **no** form of the command to disable this authentication.

Table 3-7 explains the syntax for the **ppp authentication** interface configuration command.

Table 3-7 PPP Command Syntax

`chap`	Enables CHAP on serial interface.
`pap`	Enables PAP on serial interface.
`chap pap`	Enables both CHAP and PAP on serial interface, and performs CHAP authentication before PAP.
`pap chap`	Enables both CHAP and PAP on serial interface, and performs PAP authentication before CHAP.
if-needed (Optional)	Used with TACACS and XTACACS. Do not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.
list-name (Optional)	Used with AAA/TACACS+. Specifies the name of a list of TACACS+ methods of authentication to use. If no list name is specified, the system uses the default. Lists are created with the **aaa authentication ppp** command.
default (Optional)	Used with AAA/TACACS+. Created with the **aaa authentication ppp** command.
Callin	Specifies authentication on incoming (received) calls only.

After you have enabled CHAP or PAP authentication, or both, the local router requires the remote device to prove its identity before allowing data traffic to flow. This is done as follows:

- PAP authentication requires the remote device to send a name and password to be checked against a matching entry in the local username database or in the remote *TACACS/TACACS+* database.
- CHAP authentication sends a challenge to the remote device. The remote device must encrypt the challenge value with a shared secret and return the encrypted value and its name to the local router in a response message. The local router uses the name of the remote device to look up the appropriate secret in the local username or remote TACACS/TACACS+ database. It uses the looked-up secret to encrypt the original challenge and verify that the encrypted values match.

Note

Authentication, authorization, and accounting (AAA)/TACACS is a dedicated server used to authenticate users. TACACS clients send a query to a TACACS authentication server. The server can authenticate the user, authorize what the user can do, and track what the user has done.

Either PAP or CHAP or both can be enabled. If both methods are enabled, the first method specified is requested during link negotiation. If the peer suggests using the

second method or simply refuses the first method, the second method should be tried. Some remote devices support CHAP only and some PAP only. The order in which you specify the methods is based on your concerns about the ability of the remote device to correctly negotiate the appropriate method as well as your concern about data line security. PAP usernames and passwords are sent as plaintext strings and can be intercepted and reused. CHAP has eliminated most of the known security holes.

Configuring PPP with Authentication (3.3.2.6)

The procedure outlined in the table describes how to configure PPP encapsulation and PAP/CHAP authentication protocols. Correct configuration is essential, because PAP and CHAP use these parameters to authenticate.

Configuring PAP Authentication

Figure 3-46 shows the topology used in an example of a two-way PAP authentication configuration, with the configuration in the following listing. Both routers authenticate and are authenticated, so the PAP authentication commands mirror each other. The PAP username and password that each router sends must match those specified with the **username** *name* **password** *password* command of the other router.

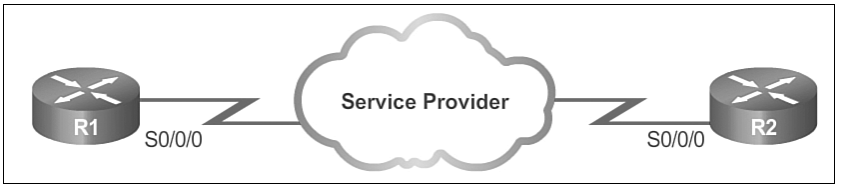


Figure 3-46 Topology for PPP

Partial running-config for R1

```
hostname R1
username R2 password sameone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R2 password sameone
```

Partial running-config for R2

```
hostname R2
username R1 password 0 sameone
!
interface Serial 0/0/0
```

```
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R2 password sameone
```

PAP provides a simple method for a remote node to establish its identity using a two-way handshake. This is done only on initial link establishment. The hostname on one router must match the username the other router has configured for PPP. The passwords must also match. Specify the username and password parameters, use the following command: **ppp pap sent-username** *name* **password** *password*.

Interactive Graphic

Activity 3.3.2.6: PPP PAP Authentication

Go to the course online to use the Syntax Checker to configure PAP authentication on router R1's serial 0/0/1 interface.

Configuring CHAP Authentication

CHAP periodically verifies the identity of the remote node using a three-way handshake. The hostname on one router must match the username the other router has configured. The passwords must also match. This occurs on initial link establishment and can be repeated any time after the link has been established. The following is an example of a CHAP configuration.

Partial running-config for R1

```
hostname R1
username R2 password sameone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication chap
```

Partial running-config for R2

```
hostname R2
username R1 password 0 sameone
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication chap
```

Interactive Graphic

Activity 3.3.2.6: PPP CHAP Authentication

Go to the course online to use the Syntax Checker to configure CHAP authentication on router R1's serial 0/0/1 interface.

Packet Tracer Activity

Packet Tracer Activity 3.3.2.7: Configuring PAP and CHAP Authentication

Background/Scenario

In this activity, you will practice configuring PPP encapsulation on serial links. You will also configure PPP PAP authentication and PPP CHAP authentication.

Lab 3.3.2.8: Configuring Basic PPP with Authentication

In this lab, you will complete the following objectives:

- Part 1: Configure Basic Device Settings
- Part 2: Configure PPP Encapsulation
- Part 3: Configure PPP CHAP Authentication

Troubleshoot WAN Connectivity (3.4)

Troubleshooting is an important component to understanding and implementing any technology. This section discusses troubleshooting WAN connectivity, specifically point-to-point serial communications using PPP.

Troubleshoot PPP (3.4.1)

Similar to other protocols implemented on a router, troubleshooting PPP involves a combination of **debug** and **show** commands. This section discusses how to use these commands to troubleshoot PPP negotiation and authentication.

Troubleshooting PPP Serial Encapsulation (3.4.1.1)

Recall that the **debug** command is used for troubleshooting and is accessed from privileged EXEC mode of the command-line interface. A **debug** output displays information about various router operations, related traffic generated or received by the router, and any error messages. It can consume a significant amount of resources, and the router is forced to process-switch the packets being debugged. The **debug** command must not be used as a monitoring tool; rather, it is meant to be used for a short period of time for troubleshooting.

Use the **debug ppp** command to display information about the operation of PPP.

```
Router# debug ppp {packet | negotiation | error | authentication | compression |
   cbcp}
```

Table 3-8 shows the command syntax. Use the `no` form of this command to disable debugging output.

Table 3-8 `debug ppp` Command Parameters

Parameter	Usage
packet	Displays PPP packets being sent and received. (This command displays low-level packet dumps.)
negotiation	Displays PPP packets transmitted during PPP startup, where PPP options are negotiated.
error	Displays protocol errors and error statistics associated with PPP connection negotiation and operation.
authentication	Displays authentication protocol messages, including Challenge Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges.
compression	Displays information specific to the exchange of PPP connections using MPPC. This command is useful for obtaining incorrect packet sequence number information where MPPC compression is enabled.
cbcp	Displays protocol errors and statistics associated with PPP connection negotiations using MSCB.

Use the **debug ppp** command when trying to search the following:

- NCPs that are supported on either end of a PPP connection
- Any loops that might exist in a PPP internetwork
- Nodes that are (or are not) properly negotiating PPP connections
- Errors that have occurred over the PPP connection
- Causes for CHAP session failures
- Causes for PAP session failures
- Information specific to the exchange of PPP connections using the Callback Control Protocol (CBCP), used by Microsoft clients
- Incorrect packet sequence number information where MPPC compression is enabled

Debug PPP (3.4.1.2)

In addition to the **debug ppp** command, there are other commands that are available for troubleshooting a PPP connection.

A good command to use when troubleshooting serial interface encapsulation is the **debug ppp packet** command, as shown in Example 3-5. The example depicts packet exchanges under normal PPP operation, including LCP state, LQM procedures, and the LCP magic number.

Example 3-5 Output of **debug ppp packet** Command

```
R1# debug ppp packet
PPP packet display debugging is on
R1#
*Apr  1 16:15:17.471: Se0/0/0 LQM: O state Open magic 0x1EFC37C3 len 48
*Apr  1 16:15:17.471: Se0/0/0 LQM:     LastOutLQRs 70 LastOutPackets/Octets 194/9735
*Apr  1 16:15:17.471: Se0/0/0 LQM:     PeerInLQRs 70 PeerInPackets/Discards/Errors/
  Octets 0/0/0/0
*Apr  1 16:15:17.471: Se0/0/0 LQM:     PeerOutLQRs 71 PeerOutPackets/Octets 197/9839
*Apr  1 16:15:17.487: Se0/0/0 PPP: I pkt type 0xC025, datagramsize 52 link[ppp]
*Apr  1 16:15:17.487: Se0/0/0 LQM: I state Open magic 0xFE83D624 len 48
*Apr  1 16:15:17.487: Se0/0/0 LQM:     LastOutLQRs 71 LastOutPackets/Octets 197/9839
*Apr  1 16:15:17.487: Se0/0/0 LQM:     PeerInLQRs 71 PeerInPackets/Discards/Errors/
  Octets 0/0/0/0
*Apr  1 16:15:17.487: Se0/0/0 LQM:     PeerOutLQRs 71 PeerOutPackets/Octets 196/9809
*Apr  1 16:15:17.535: Se0/0/0 LCP: O ECHOREQ [Open] id 36 len 12 magic 0x1EFC37C3
*Apr  1 16:15:17.539: Se0/0/0 LCP-FS: I ECHOREP [Open] id 36 len 12 magic 0xFE83D624
*Apr  1 16:15:17.539: Se0/0/0 LCP-FS: Received id 36, sent id 36, line up
R1# undebug all
```

Example 3-6 displays the **debug ppp negotiation** command in a normal negotiation, where both sides agree on NCP parameters. In this case, protocol types IPv4 and IPv6 are proposed and acknowledged. The **debug ppp negotiation** command enables the network administrator to view the PPP negotiation transactions, identify the problem or stage when the error occurs, and develop a resolution. The output includes the LCP negotiation, authentication, and NCP negotiation.

Example 3-6 Output of **debug ppp negotiation** Command

```
R1# debug ppp negotiation
PPP protocol negotiation debugging is on
R1#
*Apr  1 18:42:29.831: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
*Apr  1 18:42:29.831: Se0/0/0 PPP: Sending cstate UP notification
*Apr  1 18:42:29.831: Se0/0/0 PPP: Processing CstateUp message
```

```
*Apr  1 18:42:29.835: PPP: Alloc Context [66A27824]
*Apr  1 18:42:29.835: ppp2 PPP: Phase is ESTABLISHING
*Apr  1 18:42:29.835: Se0/0/0 PPP: Using default call direction
*Apr  1 18:42:29.835: Se0/0/0 PPP: Treating connection as a dedicated line
*Apr  1 18:42:29.835: Se0/0/0 PPP: Session handle[4000002] Session id[2]
*Apr  1 18:42:29.835: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
*Apr  1 18:42:29.835: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 23
*Apr  1 18:42:29.835: Se0/0/0 LCP:    AuthProto CHAP (0x0305C22305)
*Apr  1 18:42:29.835: Se0/0/0 LCP:    QualityType 0xC025 period 1000
  (0x0408C025000003E8)
*Apr  1 18:42:29.835: Se0/0/0 LCP:    MagicNumber 0x1F887DD3 (0x05061F887DD3)
<Output omitted>
*Apr  1 18:42:29.855: Se0/0/0 PPP: Phase is AUTHENTICATING, by both
*Apr  1 18:42:29.855: Se0/0/0 CHAP: O CHALLENGE id 1 len 23 from "R1"
<Output omitted>
*Apr  1 18:42:29.871: Se0/0/0 IPCP: Authorizing CP
*Apr  1 18:42:29.871: Se0/0/0 IPCP: CP stalled on event[Authorize CP]
*Apr  1 18:42:29.871: Se0/0/0 IPCP: CP unstall
<Output omitted>
*Apr  1 18:42:29.875: Se0/0/0 CHAP: O SUCCESS id 1 len 4
*Apr  1 18:42:29.879: Se0/0/0 CHAP: I SUCCESS id 1 len 4
*Apr  1 18:42:29.879: Se0/0/0 PPP: Phase is UP
*Apr  1 18:42:29.879: Se0/0/0 IPCP: Protocol configured, start CP. state[Initial]
*Apr  1 18:42:29.879: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
*Apr  1 18:42:29.879: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
*Apr  1 18:42:29.879: Se0/0/0 IPCP:    Address 10.0.1.1 (0x03060A000101)
*Apr  1 18:42:29.879: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
*Apr  1 18:42:29.879: Se0/0/0 IPV6CP: Protocol configured, start CP. state[Initial]
*Apr  1 18:42:29.883: Se0/0/0 IPV6CP: Event[OPEN] State[Initial to Starting]
*Apr  1 18:42:29.883: Se0/0/0 IPV6CP: Authorizing CP
*Apr  1 18:42:29.883: Se0/0/0 IPV6CP: CP stalled on event[Authorize CP]
<Output omitted>
*Apr  1 18:42:29.919: Se0/0/0 IPCP: State is Open
*Apr  1 18:42:29.919: Se0/0/0 IPV6CP: State is Open
*Apr  1 18:42:29.919: Se0/0/0 CDPCP: State is Open
*Apr  1 18:42:29.923: Se0/0/0 CCP: State is Open
*Apr  1 18:42:29.927: Se0/0/0 Added to neighbor route AVL tree: topoid 0, address
  10.0.1.2
*Apr  1 18:42:29.927: Se0/0/0 IPCP: Install route to 10.0.1.2
*Apr  1 18:42:39.871: Se0/0/0 LQM: O state Open magic 0x1F887DD3 len 48
*Apr  1 18:42:39.871: Se0/0/0 LQM:    LastOutLQRs 0 LastOutPackets/Octets 0/0
*Apr  1 18:42:39.871: Se0/0/0 LQM:    PeerInLQRs 0 PeerInPackets/Discards/Errors/
  Octets 0/0/0/0
*Apr  1 18:42:39.871: Se0/0/0 LQM:    PeerOutLQRs 1 PeerOutPackets/Octets 3907/155488
*Apr  1 18:42:39.879: Se0/0/0 LQM: I state Open magic 0xFF101A5B len 48
*Apr  1 18:42:39.879: Se0/0/0 LQM:    LastOutLQRs 0 LastOutPackets/Octets 0/0
```

```
*Apr  1 18:42:39.879: Se0/0/0 LQM:     PeerInLQRs 0 PeerInPackets/Discards/Errors/
  Octets 0/0/0/0
*Apr  1 18:42:39.879: Se0/0/0 LQM:     PeerOutLQRs 1 PeerOutPackets/Octets 3909/155225
<Output omitted>
```

The **debug ppp error** command is used to display protocol errors and error statistics associated with PPP connection negotiation and operation, as shown in Example 3-7. These messages might appear when the Quality Protocol option is enabled on an interface that is already running PPP.

Example 3-7 Output of **debug ppp error** Command

```
R1# debug ppp error

PPP Serial3(i): rlqr receive failure. successes = 15
PPP: myrcvdiffp = 159 peerxmitdiffp = 41091
PPP: myrcvdiffo = 2183 peerxmitdiffo = 1714439
PPP: threshold = 25
PPP Serial4(i): rlqr transmit failure. successes = 15
PPP: myxmitdiffp = 41091 peerrcvdiffp = 159
PPP: myxmitdiffo = 1714439 peerrcvdiffo = 2183
PPP: l->OutLQRs = 1 LastOutLQRs = 1
PPP: threshold = 25
PPP Serial3(i): lqr_protrej() Stop sending LQRs.
PPP Serial3(i): The link appears to be looped back.
```

Troubleshooting a PPP Configuration with Authentication (3.4.1.3)

Authentication is a feature that needs to be implemented correctly or the security of your serial connection may be compromised. Always verify your configuration with the **show interfaces serial** command, in the same way as you did without authentication.

Note

Never assume your authentication configuration works without testing it. Debugging allows you to confirm your configuration and correct any deficiencies. For debugging PPP authentication, use the **debug ppp authentication** command.

Example 3-8 shows an example output of the **debug ppp authentication** command.

Example 3-8 Troubleshooting a PPP Configuration with Authentication

```
R2# debug ppp authentication

Serial0/0/0: Unable to authenticate. No name received from peer
Serial0/0/0: Unable to validate CHAP response. USERNAME pioneer not found.
Serial0/0/0: Unable to validate CHAP response. No password defined for USERNAME pio-
  neer
Serial0/0/0: Failed CHAP authentication with remote.
Remote message is Unknown name
Serial0/0/0: remote passed CHAP authentication.
Serial0/0/0: Passed CHAP authentication with remote.
Serial0/0/0: CHAP input code = 4 id = 3 len = 48
```

The following is an interpretation of the output:

Line 1 says that the router is unable to authenticate on interface Serial0/0/0 because the peer did not send a name.

Line 2 says the router was unable to validate the CHAP response because username pioneer was not found.

Line 3 says no password was found for pioneer. Other possible responses at this line might have been no name received to authenticate, unknown name, no secret for given name, short MD5 response received, or MD5 compare failed.

In the last line, the code 4 means that a failure has occurred. Other code values are as follows:

- **1**: Challenge.
- **2**: Response.
- **3**: Success.
- **4**: Failure.
- **id**: 3 is the ID number per LCP packet format.
- **len**: 48 is the packet length without the header.

Packet Tracer Activity 3.4.1.4: Troubleshooting PPP with Authentication

Background/Scenario

The routers at your company were configured by an inexperienced network engineer. Several errors in the configuration have resulted in connectivity issues. Your boss has asked you to troubleshoot and correct the configuration errors and document your work. Using your knowledge of PPP and standard testing methods, find and correct the errors. Make sure that all of the serial links use PPP CHAP authentication, and that all of the networks are reachable. The passwords are cisco and class.

Lab 3.4.1.5: Troubleshooting Basic PPP with Authentication

In this lab, you will complete the following objectives:

Part 1: Build the Network and Load Device Configurations

Part 2: Troubleshoot the Data Link Layer

Part 3: Troubleshoot the Network Layer

Summary (3.5)

Class Activity 3.5.1.1: PPP Validation

Three friends who are enrolled in the Cisco Networking Academy want to check their knowledge of PPP network configuration.

They set up a contest where each person will be tested on configuring PPP with defined PPP scenario requirements and varying options. Each person devises a different configuration scenario.

The next day they get together and test each other's configuration using their PPP scenario requirements.

Packet Tracer Activity

Packet Tracer Activity 3.5.1.2: Skills Integration Challenge

Background/Scenario

This activity allows you to practice a variety of skills including configuring VLANs, PPP with CHAP, static and default routing, using IPv4 and IPv6. Due to the sheer number of graded elements, feel free to click Check Results and Assessment Items to see if you correctly entered a graded command. Use the passwords cisco and class to access EXEC modes of the CLI for routers and switches.

Serial transmissions sequentially send 1 bit at a time over a single channel. A serial port is bidirectional. Synchronous serial communications require a clocking signal.

Point-to-Point links are usually more expensive than shared services; however, the benefits may outweigh the costs. Constant availability is important for some protocols, such as VoIP.

SONET is an optical network standard that uses STDM for efficient use of bandwidth. In the United States, OC transmission rates are standardized specifications for SONET.

The bandwidth hierarchy used by carriers is different in North America (T-carrier) and Europe (E-carrier). In North America, the fundamental line speed is 64 Kbps, or DS0. Multiple DS0s are bundled together to provide higher line speeds.

The demarcation point is the point in the network where the responsibility of the service provider ends and the responsibility of the customer begins. The CPE, usually a router, is the DTE device. The DCE is usually a modem or CSU/DSU.

A null modem cable is used to connect two DTE devices together without the need for a DCE device by crossing the Tx and Rx lines. When using this cable between routers in a lab, one of the routers must provide the clocking signal.

Cisco HDLC is a bit-oriented synchronous data link layer protocol extension of HDLC and is used by many vendors to provide multiprotocol support. This is the default encapsulation method used on Cisco synchronous serial lines.

Synchronous PPP is used to connect to non-Cisco devices, to monitor link quality, provide authentication, or bundle links for shared use. PPP uses HDLC for encapsulating datagrams. LCP is the PPP protocol used to establish, configure, test, and terminate the data link connection. LCP can optionally authenticate a peer using PAP or CHAP. A family of NCPs are used by the PPP protocol to simultaneously support multiple network layer protocols. Multilink PPP spreads traffic across bundled links by fragmenting packets and simultaneously sending these fragments over multiple links to the same remote address, where they are reassembled.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion Introduction to Connecting Networks Lab Manual (978-1-58713-331-2). The Packet Tracer Activity PKA files are found in the online course.

Class Activities

Class Activity 3.0.1.2: PPP Persuasion

Class Activity 3.5.1.1: PPP Validation

Labs

Lab 3.3.2.8: Configuring Basic PPP with Authentication

Lab 3.4.1.5: Troubleshooting Basic PPP with Authentication

Packet Tracer Activities

Packet Tracer Activity 3.1.2.7: Troubleshooting Serial Interfaces

Packet Tracer Activity 3.3.2.7: Configuring PAP and CHAP Authentication

Packet Tracer Activity 3.4.1.4: Troubleshooting PPP with Authentication

Packet Tracer Activity 3.5.1.2: Skills Integration Challenge

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix, "Answers to the 'Check Your Understanding' Questions," lists the answers.

1. Match each PPP establishment step with its appropriate sequence number:

   Step 1:

   Step 2:

   Step 3:

   Step 4:

   Step 5:

   A. Test link quality (optional).
   B. Negotiate Layer 3 protocol options.
   C. Send link-establishment frames to negotiate options such as MTU size, compression, and authentication.
   D. Send configuration-acknowledgment frames.
   E. NCP reaches Open state.

2. Which output from the **show interfaces s0/0/0** command indicates that the far end of a point-to-point link has a different encapsulation set than the local router?

   A. Serial 0/0/0 is down, line protocol is down.
   B. Serial 0/0/0 is up, line protocol is down.
   C. Serial 0/0/0 is up, line protocol is up (looped).
   D. Serial 0/0/0 is up, line protocol is down (disabled).
   E. Serial 0/0/0 is administratively down, line protocol is down.

3. What is the default encapsulation for serial interfaces on a Cisco router?

   A. HDLC
   B. PPP
   C. Frame Relay
   D. X.25

4. What is the function of the Protocol field in a PPP frame?

   A. It identifies the application layer protocol that will process the frame.
   B. It identifies the transport layer protocol that will process the frame.
   C. It identifies the data link layer protocol encapsulation in the frame's Data field.
   D. It identifies the network layer protocol encapsulated in the frame's Data field.

5. Match each description with its corresponding term:

   Error control:

   Authentication protocols:

   Allows load balancing:

   Compression protocols:

   A. Stacker/predictor
   B. Magic number
   C. Multilink
   D. CHAP/PAP
   E. Call in

6. Which of the following statements describe the function of statistical time-division multiplexing (STDM)? (Choose three.)

   A. Multiple data streams share one common channel.
   B. Bit interleaving controls the timing mechanism that places data on the channel.
   C. Time slots are used on a first-come, first-served basis.
   D. STDM was developed to overcome the inefficiency caused by time slots still being allocated even when the channel has no data to transmit.
   E. Sources of data alternate during transmission and are reconstructed at the receiving end.
   F. Priority can be dedicated to one data source.

7. Which of the following describes the serial connection between two routers using the High-level Data Link Control (HDLC) protocol?

   A. Synchronous or asynchronous bit-oriented transmissions using a universal frame format
   B. Synchronous bit-oriented transmissions using a frame format that allows flow control and error detection
   C. Asynchronous bit-oriented transmissions using a frame format derived from the Synchronous Data Link Control (SDLC) protocol
   D. Asynchronous bit-oriented transmissions using a V.35 DTE/DCE interface

8. If an authentication protocol is configured for PPP operation, when is the client or user workstation authenticated?

   A. Before link establishment
   B. During the link establishment phase
   C. Before the network layer protocol configuration begins
   D. After the network layer protocol configuration has ended

9. Why are Network Control Protocols used in PPP?

   A. To establish and terminate data links
   B. To provide authentication capabilities to PPP
   C. To manage network congestion and to allow quality testing of the link
   D. To allow multiple Layer 3 protocols to operate over the same physical link

10. Which statement describes the PAP authentication protocol?

    A. It sends encrypted passwords by default.
    B. It uses a two-way handshake to establish identity.
    C. It protects against repeated trial-and-error attacks.
    D. It requires the same username to be configured on every router.

11. A technician testing the functionality of a recently installed router is unable to ping the serial interface of a remote router. The technician executes the **show interfaces serial 0/0/0** command on the local router and sees the following line in the router:

    Serial0/0/0 is down, line protocol is down

    What are two possible causes of this command output?

    A. The **clock rate** command is missing.
    B. The carrier detect signal is not sensed.
    C. Keepalives are not being sent.
    D. The interface is disabled due to a high error rate.
    E. The interface is shut down.
    F. The cabling is faulty or incorrect.

12. The network administrator is configuring Router1 to connect to Router2 using three-way handshake authentication. Match each description with the command necessary to configure Router1:

Configure the username and password:

Enter interface configuration mode:

Specify the encapsulation type:

Configure authentication:

A. **username Router2 password cisco**
B. **username Router1 password cisco**
C. **interface serial 0/1/0**
D. encapsulation ppp
E. **encapsulation hdlc**
F. **ppp authentication pap**
G. **ppp authentication chap**

13. What is required to successfully establish a connection between two routers using CHAP authentication?

A. The hostnames of both routers must be the same.
B. The usernames of both routers must be the same.
C. The enable secret passwords configured on both routers must be the same.
D. The password configured with the router's username must be the same on both routers.
E. The **ppp chap sent-username** command must be configured the same on both routers.

14. For each characteristic, indicate whether it is associated with PAP or CHAP:

Two-way handshake:

Three-way handshake:

Open to trial-and-error attacks:

Password sent in cleartext:

Periodic verification:

Uses a one-way hash function:

15. For each description, indicate whether it is associated with LCP or NCP:

    Negotiates link establishment parameters:

    Negotiates Layer 3 protocol parameters:

    Maintains/debugs a link:

    Can negotiate multiple Layer 3 protocols:

    Terminates a link:

16. Describe the functions of LCP and NCP.

17. Describe the five configurable LCP encapsulation options.

18. Refer to the following configurations for Router R1 and Router R3:

```
hostname R1
username R1 password cisco123
!
int serial 0/0
ip address 128.0.1.1 255.255.255.0
encapsulation ppp
ppp authentication pap
----------------------------
hostname R3
username R1 password cisco
!
int serial 0/0
ip address 128.0.1.2 255.255.255.0
encapsulation ppp
ppp authentication CHAP
```

    Router R1 is unable to connect with Router R3. On the basis of the information presented, which configuration changes on Router R1 would correct the problem?

This page intentionally left blank

Index

NUMBERS

A

B

C

D

E

F

G-H

I

J-K-L

M

N

O

P

Q-R

S

T

U-V

W

X-Y-Z