Course Booklet

Connecting Networks

ciscopress.com

Cisco | Networking Academy®
Mind Wide Open™

Connecting Networks Course Booklet

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

Printed in the United States of America

First Printing December 2013

Library of Congress data is on file.

ISBN-13: 978-1-58713-330-5

ISBN-10: 1-58713-330-X

Warning and Disclaimer

This book is designed to provide information about Cisco Networking Academy 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.

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Business Operations Manager, Cisco Press
Jan Cornelssen

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Project Editor
Seth Kerney

Editorial Assistant
Vanessa Evans

Cover Designer
Louisa Adair

Interior Designer
Mark Shirar

Composition
Bronkella Publishing, LLC

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.

Trademark Acknowledgments

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

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.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.**

Contents at a Glance

Contents

Command Syntax Conventions

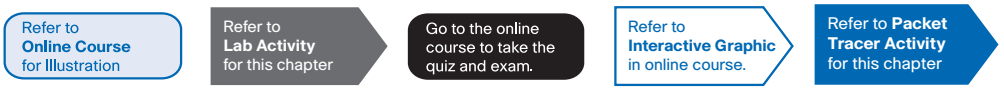
The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **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.

About This Course Booklet

Your Cisco Networking Academy Course Booklet is designed as a study resource you can easily read, highlight, and review on the go, wherever the Internet is not available or practical:

- The text is extracted directly, word-for-word, from the online course so you can highlight important points and take notes in the "Your Chapter Notes" section.
- Headings with the exact page correlations provide a quick reference to the online course for your classroom discussions and exam preparation.
- An icon system directs you to the online curriculum to take full advantage of the images imbedded within the Networking Academy online course interface and reminds you to perform the labs, Class activities, Interactive activities, Packet Tracer activities, and chapter quizzes and exams.



The *Course Booklet* is a basic, economical paper-based resource to help you succeed with the Cisco Networking Academy online course.

Companion Guide

Looking for more than the online curriculum? The Companion Guide is fully aligned to Networking Academy's online course chapters and offers additional book-based pedagogy to reinforce key concepts, enhance student comprehension, and promote retention. Using this full-fledged textbook, students can focus scarce study time, organize review for quizzes and exams, and get the day-to-day reference answers they're looking for.

The Companion Guide also offers instructors additional opportunities to assign take-home reading or vocabulary homework, helping students prepare more for in-class lab work and discussions.

Available in print and all major eBook formats (Book: 9781587133329 eBook: 9780133476521)

CHAPTER 0

Introduction to Course

0.0 Connecting Networks

0.0.1 Message to the Student

0.0.1.1 Welcome

Welcome to the CCNA R&S Connecting Networks course. The goal of this course is to introduce you to fundamental networking concepts and technologies. These online course materials will assist you in developing the skills necessary to plan and implement small networks across a range of applications. The specific skills covered in each chapter are described at the start of each chapter.

You can use your smart phone, tablet, laptop, or desktop to access your course, participate in discussions with your instructor, view your grades, read or review text, and practice using interactive media. However, some media are complex and must be viewed on a PC, as well as Packet Tracer activities, quizzes, and exams.

Refer to **Online Course** for Illustration

0.0.1.2 A Global Community

When you participate in the Networking Academy, you are joining a global community linked by common goals and technologies. Schools, colleges, universities, and other entities in over 160 countries participate in the program. A visualization of the global Networking Academy community is available at http://www.academynetspace.com.

Look for the Cisco Networking Academy official site on Facebook© and LinkedIn©. The Facebook site is where you can meet and engage with other Networking Academy students from around the world. The Cisco Networking Academy LinkedIn site connects you with job postings, and you can see how others are effectively communicating their skills.

Refer to **Online Course** for Illustration

0.0.1.3 More Than Just Information

The NetSpace learning environment is an important part of the overall course experience for students and instructors in the Networking Academy. These online course materials include course text and related interactive media, Packet Tracer simulation activities, real equipment labs, remote access labs, and many different types of quizzes. All of these materials provide important feedback to help you assess your progress throughout the course.

The material in this course encompasses a broad range of technologies that facilitate how people work, live, play, and learn by communicating with voice, video, and other data. Networking and the internet affect people differently in different parts of the world. Although we have worked with instructors from around the world to create these materials, it is important that you work with your instructor and fellow students to make the material in this course applicable to your local situation.

Refer to **Online Course** for Illustration

0.0.1.4 How We Teach

E-doing is a design philosophy that applies the principle that people learn best by doing. The curriculum includes embedded, highly interactive e-doing activities to help stimulate learning, increase knowledge retention, and make the whole learning experience much richer – and that makes understanding the content much easier.

Refer to **Online Course** for Illustration

0.0.1.5 Practice Leads to Mastery

In a typical lesson, after learning about a topic for the first time, you will check your understanding with some interactive media items. If there are new commands to learn, you will practice them with the Syntax Checker before using the commands to configure or troubleshoot a network in Packet Tracer, the Networking Academy network simulation tool. Next, you will do practice activities on real equipment in your classroom or accessed remotely over the internet.

Packet Tracer can also provide additional practice any time by creating your own activities or you may want to competitively test your skills with classmates in multi-user games. Packet Tracer skills assessments and skills integration labs give you rich feedback on the skills you are able to demonstrate and are great practice for chapter, checkpoint, and final exams.

Refer to **Online Course** for Illustration

0.0.1.6 Mind Wide Open

An important goal in education is to enrich you, the student, by expanding what you know and can do. It is important to realize, however, that the instructional materials and the instructor can only facilitate the process. You must make the commitment yourself to learn new skills. The following pages share a few suggestions to help you learn and prepare for transitioning your new skills to the workplace.

Refer to **Online Course** for Illustration

0.0.1.7 Engineering Journals

Professionals in the networking field often keep Engineering Journals in which they write down the things they observe and learn such as how to use protocols and commands. Keeping an Engineering Journal creates a reference you can use at work in your ICT job. Writing is one way to reinforce your learning – along with Reading, Seeing, and Practicing.

A sample entry for implementing a technology could include the necessary software commands, the purpose of the commands, command variables, and a topology diagram indicating the context for using the commands to configure the technology.

Refer to **Online Course** for Illustration

0.0.1.8 Explore the World of Networking

Packet Tracer is a networking learning tool that supports a wide range of physical and logical simulations. It also provides visualization tools to help you understand the internal workings of a network.

The pre-made Packet Tracer activities consist of network simulations, games, activities, and challenges that provide a broad range of learning experiences. These tools will help you develop an understanding of how data flows in a network.

Refer to **Online Course** for Illustration

0.0.1.9 Create Your Own Worlds

You can also use Packet Tracer to create your own experiments and networking scenarios. We hope that, over time, you consider using Packet Tracer - not only for experiencing the pre-built activities, but also to become an author, explorer, and experimenter.

The online course materials have embedded Packet Tracer activities that will launch on computers running Windows® operating systems, if Packet Tracer is installed. This integration may also work on other operating systems using Windows emulation.

Refer to **Online Course** for Illustration

0.0.1.10 How Packet Tracer Helps Master Concepts

Educational Games

Packet Tracer Multi-User games enable you or a team to compete with other students to see who can accurately complete a series of networking tasks the fastest. It is an excellent way to practice the skills you are learning in Packet Tracer activities and hands-on labs.

Cisco Aspire is a single-player, standalone strategic simulation game. Players test their networking skills by completing contracts in a virtual city. The Networking Academy Edition is specifically designed to help you prepare for the CCENT certification exam. It also incorporates business and communication skills ICT employers seek in job candidates.

Performance-Based Assessments

The Networking Academy performance-based assessments have you do Packet Tracer activities like you have been doing all along, only now integrated with an online assessment engine that will automatically score your results and provide you with immediate feedback. This feedback helps you to more accurately identify the knowledge and skills you have mastered and where you need more practice. There are also questions on chapter quizzes and exams that use Packet Tracer activities to give you additional feedback on your progress.

Refer to **Online Course** for Illustration

0.0.1.11 Course Overview

As the course title states, the focus of this course is on the WAN technologies and network services required by converged applications in a complex network. In this course, you will learn the selection criteria of network devices and WAN technologies to meet network requirements. You will do the following:

- Describe different WAN technologies and their benefits
- Describe the operations and benefits of virtual private networks (VPNs) and tunneling
- Configure and troubleshoot serial connections
- Configure and troubleshoot broadband connections
- Configure and troubleshoot IPsec tunneling operations
- Monitor and troubleshoot network operations using syslog, SNMP, and NetFlow
- Describe network architectures

By the end of this course, you will be able to configure and troubleshoot network devices and resolve common issues with data link protocols. Students will also develop the knowledge and skills needed to implement IPsec and virtual private network (VPN) operations in a complex network.

Refer to **Interactive Graphic** in online course.

0.1.1.1 Course GUI Tutorial

Go to the online course to take the quiz and exam.

Chapter 0 Quiz

This quiz is designed to provide an additional opportunity to practice the skills and knowledge presented in the chapter and to prepare for the chapter exam. You will be allowed multiple attempts and the grade does not appear in the gradebook.

Chapter 0 Exam

The chapter exam assesses your knowledge of the chapter content.

Your Chapter Notes

CHAPTER 1

Hierarchical Network Design

1.0 Hierarchical Network Design

1.0.1.1 Introduction

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.

Refer to **Lab Activity** for this chapter

1.0.1.2 Class Activity - Design Hierarchy

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

Refer to **Interactive Graphic** in online course.

1.1 Hierarchical Network Design Overview

1.1.1 Enterprise Network Campus Design

1.1.1.1 Network Requirements

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-sized network**- Provides services for 200 to 1000 devices.
- **Large network**- Provides services for 1000+ 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 the figure. 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.

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.

Refer to **Online Course** for Illustration

1.1.1.2 Structured Engineering Principles

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 fork-lift 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.

Refer to **Online Course** for Illustration

1.1.2 Hierarchical Network Design

1.1.2.1 Network Hierarchy

In networking, a hierarchical 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.

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.

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.

Layer 2 devices in a flat network provide little opportunity to control broadcasts or to filter undesirable traffic. As more devices and applications are added to a flat network, response times degrade until the network becomes unusable.

Click play in Figure 1 to view a transition of a flat network to a hierarchical network design.

Another sample three-layer hierarchical network design is displayed in Figure 2. Notice that each building is using the same hierarchical network model that includes the access, distribution, and core layers.

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.

Refer to **Online Course** for Illustration

1.1.2.2 The Access Layer

In a LAN environment, the access layer 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 the figure, the access layer for a small business network generally incorporates Layer 2 switches and access points providing connectivity between workstations and servers.

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

Refer to **Online Course** for Illustration

1.1.2.3 The Distribution Layer

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 the figure, the distribution layer is the boundary between the Layer 2 domains and the Layer 3 routed network.

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

Refer to **Online Course** for Illustration

1.1.2.4 The Core Layer

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 the figure, the core layer is critical for interconnectivity between distribution layer devices; for example, interconnecting the distribution block to the WAN and Internet edge. 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 later 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

Refer to **Online Course** for Illustration

1.1.2.5 Two-Tier Collapsed Core Design

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 the figure has collapsed the distribution layer and core layer functionality into multilayer switch devices.

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

Refer to **Interactive Graphic** in online course.

1.1.2.6 Activity - Identify Hierarchical Network Characteristics

Refer to **Online Course** for Illustration

1.2 Cisco Enterprise Architecture

1.2.1 Modular Network Design

1.2.1.1 Modular Design

While the hierarchical network design works well within the campus infrastructure, networks have expanded beyond these borders. As shown in the figure, networks have become more sophisticated and complex, with some requiring connections to dedicated data centers, often off-site. Branch sites often require connectivity to the campus backbones, and employees wanted to be able to work from home offices or other remote locations. 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.

Refer to **Online Course** for Illustration

1.2.1.2 Modules in the Enterprise Architecture

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. (Figure 1).
- **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. (Figure 2).
- **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. (Figure 3).
- **Enterprise Edge**- Consists of the Internet Edge and the WAN Edge. These blocks offer connectivity to voice, video, and data services outside the enterprise. (Figure 4).

Refer to **Interactive Graphic** in online course.

1.2.1.3 Activity - Identify Modules in a Network Design

Refer to **Online Course** for Illustration

1.2.2 Cisco Enterprise Architecture Model

1.2.2.1 Cisco Enterprise Architecture Model

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 into the architecture allows flexibility in network design and facilitates implementation and troubleshooting.

As shown in the figure, the following are the primary Cisco Enterprise Architecture modules:

- Enterprise Campus
- Enterprise Edge
- Service Provider Edge

Connected to the Service Provider Edge are additional modules including:

- Enterprise Data Center
- Enterprise Branch
- Enterprise Teleworker

Refer to **Online Course** for Illustration

1.2.2.2 Cisco Enterprise Campus

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.

The enterprise campus module consists of the following submodules:

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

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.

Click the enterprise campus module in the figure for more information.

Refer to **Online Course** for Illustration

1.2.2.3 Cisco Enterprise Edge

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.

The enterprise edge module consists of the following submodules:

- **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 (ISP) 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.

Click the Enterprise Edge module in the figure for more information.

Refer to **Online Course** for Illustration

1.2.2.4 Service Provider Edge

Enterprises use Service Providers (SPs) to link to other sites. As shown in Figure 1, 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

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

Click the Service Provider Edge in Figure 1 for more information.

When acquiring Internet services from an ISP, redundancy or failover should be considered. As shown in Figure 2, 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

Alternatively, it is possible to set up redundancy using multiple ISPs, as shown in Figure 3. Options for connecting to multiple ISPs include:

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

Refer to **Online Course** for Illustration

1.2.2.5 Remote Functional Area

The remote functional area is responsible for remote connectivity options and includes several modules:

Enterprise Branch

The enterprise branch module includes remote branches that allow employees to work at non-campus 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 the figure 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 into 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.

Refer to **Interactive Graphic** in online course.

1.2.2.6 Activity - Identify Modules of the Cisco Enterprise Architecture

Refer to **Online Course** for Illustration

1.3 Evolving Network Architectures

1.3.1 Cisco Enterprise Architectures

1.3.1.1 IT Challenges

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.

Refer to **Online Course** for Illustration

1.3.1.2 Emerging Enterprise Architectures

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, as shown in the figure:

- 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.

Refer to **Online Course** for Illustration

1.3.2 Emerging Network Architectures

1.3.2.1 Cisco Borderless Networks

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 shown in Figure 1, 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 smart phones. It removes the location and device borders, providing unified access to wired and wireless devices. Endpoint / 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 the figure. For example, most smart phones 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 shown in Figure 2, Borderless network services unify the approach to securely delivering 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.

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.

Refer to **Online Course** for Illustration

1.3.2.2 Collaboration Architecture

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 the figure, 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.

Refer to **Online Course** for Illustration

1.3.2.3 Data Center and Virtualization

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:

- **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).

Click Play in Figure 2 to see a short video on the Cisco Unified Fabric.

Refer to **Online Course** for Illustration

1.3.2.4 Expanding the Network

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.

Click Play in the figure to view the evolution of a network to a WAN infrastructure.

Refer to **Interactive Graphic** in online course.

1.3.2.5 Activity - Identify Evolving Network Architecture Terminology

Refer to **Online Course** for Illustration

1.4 Summary

Refer to **Lab Activity** for this chapter

1.4.1.1 Class Activity - Borderless Innovations - Everywhere

Borderless Innovations - Everywhere

You are the network administrator for your small- to medium-sized 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

Refer to **Packet Tracer Activity** for this chapter

1.4.1.2 Packet Tracer - Skills Integration Challenge - OSPF

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

Background/Scenario

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.

Refer to **Packet Tracer Activity** for this chapter

1.4.1.3 Packet Tracer - Skills Integration Challenge - EIGRP

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

Background/Scenario

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.

Refer to **Online Course** for Illustration

1.4.1.4 Summary

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.

Go to the online course to take the quiz and exam.

Chapter 1 Quiz

This quiz is designed to provide an additional opportunity to practice the skills and knowledge presented in the chapter and to prepare for the chapter exam. You will be allowed multiple attempts and the grade does not appear in the gradebook.

Chapter 1 Exam

The chapter exam assesses your knowledge of the chapter content.

Your Chapter Notes

CHAPTER 2

Connecting to the WAN

2.0 Connecting to the WAN

2.0.1.1 Introduction

Businesses must connect 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.

Refer to **Lab Activity** for this chapter

2.0.1.2 Class Activity - Branching Out

Branching Out

Your medium-sized 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.

Refer to **Interactive Graphic** in online course.

2.1 WAN Technologies Overview

2.1.1 Purpose of WANs

2.1.1.1 Why a WAN?

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

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.

Refer to **Online Course** for Illustration

2.1.1.2 Are WANs Necessary?

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.

Refer to **Online Course** for Illustration

2.1.1.3 Evolving Networks

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. Watch how its network requirements change as the company grows from a small local business into a global enterprise.

Refer to **Online Course** for Illustration

2.1.1.4 Small Office

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

Connection to the Internet is through a common broadband service called 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.

The figure shows an example of a small office and its network.

Refer to **Online Course** for Illustration

2.1.1.5 Campus Network

Five years later, SPAN Engineering has grown rapidly. The company was contracted to design and implement a full-sized 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-sized 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 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 network, or campus, 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.

The figure shows an example of SPAN's campus network.

Refer to **Online Course** for Illustration

2.1.1.6 Branch Networks

Another six 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.

For its branch offices that are in nearby cities, the company decides to use private dedicated lines through their local service provider. However, for those offices that are located in other countries, 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.

Refer to **Online Course** for Illustration

2.1.1.7 Distributed Network

SPAN Engineering has now been in business for 20 years and has grown to thousands of employees distributed in offices worldwide, as shown in Figure 1. 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.

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 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.

Refer to **Interactive Graphic** in online course.

2.1.1.8 Activity - Identify WAN Topologies

Refer to **Online Course** for Illustration

2.1.2 WAN Operations

2.1.2.1 WANs in the OSI Model

WAN operations focus primarily on the physical layer (OSI Layer 1) and the data link layer (OSI 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 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.

Refer to **Online Course** for Illustration

2.1.2.2 Common WAN Terminology

One primary difference between a WAN and a LAN is that a company or organization must subscribe to an outside WAN service provider to use WAN carrier network services. 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. The figure illustrates the terminology commonly used to describe WAN connections, including:

- **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.

Refer to **Online Course** for Illustration

2.1.2.3 WAN Devices

There are many types of devices that are specific to WAN environments, including:

- **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**- Concentrates dialup modem, dial-in and dial-out user communications. 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.
- **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**- Provides internetworking and WAN access interface ports that are 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**- A router or multilayer switch that resides within the middle or backbone of the WAN, rather than at its periphery. To fulfill this role, a router or multilayer switch must be able to support multiple telecommunications interfaces of the highest speed used in the WAN core. It must also be able to forward IP packets

at full speed on all of those interfaces. The router or multilayer switch must also support the routing protocols being used in the core.

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

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

2.1.2.4 Circuit Switching

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

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).

Click the Play button in the figure to see how circuit switching works.

Refer to **Online Course** for Illustration

2.1.2.5 Packet Switching

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 switches 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 switch 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 switch 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 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.

Click the Play button in the figure to see a packet-switching example. 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.

Refer to **Interactive Graphic** in online course.

2.1.2.6 Activity - Identify WAN Terminology

Refer to **Online Course** for Illustration

2.2 Selecting a WAN Technology

2.2.1 WAN Services

2.2.1.1 WAN Link Connection Options

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 shown in Figure 1, 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 travelling between corporate sites over the public WAN infrastructure should be protected using VPNs.

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

Refer to **Online Course** for Illustration

2.2.1.2 Service Provider Network Infrastructure

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 shown in Figure 1.

Specifically, DWDM:

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

DWDM circuits are used in all modern submarine communications cable systems and other long-haul circuits, as shown in Figure 2.

Refer to **Interactive Graphic** in online course.

2.2.1.3 Activity - Classify WAN Access Options

Refer to **Online Course** for Illustration

2.2.2 Private WAN Infrastructures

2.2.2.1 Leased Lines

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 the figure. For instance, a T1 link supports 1.544 Mb/s, an E1 supports 2.048 Mb/s, a T3 supports 43.7 Mb/s, and an E3 connection supports 34.368 Mb/s. 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.

Refer to **Online Course** for Illustration

2.2.2.2 Dialup

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, called 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 kb/s.

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.

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

Refer to **Online Course** for Illustration

2.2.2.3 ISDN

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 1 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.

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 kb/s 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 kb/s B channels and a 16 kb/s D channel. The BRI D channel is designed for control and often underused, because it has only two B channels to control (Figure 2).
- **Primary Rate Interface (PRI)**– ISDN is also available for larger installations. In North America, PRI delivers 23 B channels with 64 kb/s and one D channel with 64 kb/s for a total bit rate of up to 1.544 Mb/s. This includes some additional overhead for synchronization. In Europe, Australia, and other parts of the world, ISDN PRI provides 30 B channels and one D channel, for a total bit rate of up to 2.048 Mb/s, including synchronization overhead (Figure 3).

BRI has a call setup time that is less than a second, and the 64 kb/s 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 kb/s. 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.

Refer to **Online Course** for Illustration

2.2.2.4 Frame Relay

Frame Relay is a simple Layer 2 non-broadcast 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 Mb/s, 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 figure, R1 will use DLCI 102 to reach R2 while R2 will use DLCI 201 to reach R1.

Refer to **Online Course** for Illustration

2.2.2.5 ATM

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 Mb/s) 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.

Refer to **Online Course** for Illustration

2.2.2.6 Ethernet WAN

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).

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.

Refer to **Online Course** for Illustration

2.2.2.7 MPLS

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 which 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 the figure illustrates how MPLS is used. 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.

Refer to **Online Course** for Illustration

2.2.2.8 VSAT

All private WAN technologies discussed so far used either copper or fiber optics media. What if an organization needed 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 which is pointed to a service provider's satellite in a geosynchronous orbit in space. The signals must travel approximately 35,786 kilometers (22,236 miles) to the satellite and back.

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

Refer to **Interactive Graphic** in online course.

2.2.2.9 Activity - Identify Private WAN Infrastructure Terminology

Refer to **Online Course** for Illustration

2.2.3 Public WAN Infrastructure

2.2.3.1 DSL

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 the figure displays a sample DSL WAN connection.

Refer to **Online Course** for Illustration

2.2.3.2 Cable

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 the figure displays a sample cable WAN connection.

Refer to **Online Course** for Illustration

2.2.3.3 Wireless

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 kb/s 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.

The figure displays an example of a WiMAX network.

Refer to **Online Course** for Illustration

2.2.3.4 3G/4G Cellular

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 smart phones 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. These devices use radio waves to communicate through a nearby mobile phone tower. 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 3rd generation and 4th 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.

Refer to **Online Course** for Illustration

2.2.3.5 VPN Technology

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 1. 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.
- **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.

Refer to **Interactive Graphic** in online course.

2.2.3.6 Activity - Identify Public WAN Infrastructure Terminology

Refer to **Online Course** for Illustration

2.2.4 Selecting WAN Services

2.2.4.1 Choosing a WAN Link Connection

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.

Refer to **Online Course** for Illustration

2.2.4.2 Choosing a WAN Link Connection, cont.

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 above, 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.

Refer to **Lab Activity** for this chapter

2.2.4.3 Lab - 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

Refer to **Online Course** for Illustration

2.3 Summary

Refer to **Lab Activity** for this chapter

2.3.1.1 Class Activity - WAN Device Modules

WAN Device Modules

Your medium-sized 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

Refer to
Online Course
for Illustration

2.3.1.2 Summary

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).

Go to the online course to take the quiz and exam.

Chapter 2 Quiz

This quiz is designed to provide an additional opportunity to practice the skills and knowledge presented in the chapter and to prepare for the chapter exam. You will be allowed multiple attempts and the grade does not appear in the gradebook.

Chapter 2 Exam

The chapter exam assesses your knowledge of the chapter content.

Your Chapter Notes