Course Booklet

CCNA Exploration Accessing the WAN

Version 4.0

ciscopress.com

Cisco | Networking Academy
Mind Wide Open

CCNA Exploration Course Booklet Accessing the WAN, Version 4.0

Cisco Networking Academy

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

Printed in the United States of America

First Printing September 2009

Library of Congress Cataloging-in-Publication Data is available upon request

ISBN-13: 978-1-58713-255-1

ISBN-10: 1-58713-255-9

Warning and Disclaimer

This book is designed to provide information about accessing the WAN. 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

Cisco Representative
Erik Ullanderson

Cisco Press Program Manager
Anand Sundaram

Executive Editor
Mary Beth Ray

Managing Editor
Patrick Kanouse

Project Editor
Bethany Wall

Editorial Assistant
Vanessa Evans

Cover Designer
Louisa Adair

Composition
Mark Shirar

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.**

Course Introduction

Welcome

Welcome to the CCNA Exploration Accessing the WAN 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.

More than just information

This computer-based learning environment is an important part of the overall course experience for students and instructors in the Networking Academy. These online course materials are designed to be used along with several other instructional tools and activities. These include:

- Class presentation, discussion, and practice with your instructor
- Hands-on labs that use networking equipment within the Networking Academy classroom
- Online scored assessments and a matching grade book
- Packet Tracer simulation tool
- Additional software for classroom activities

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. You can see an interactive network map of the global Networking Academy community at http://www.academynetspace.com.

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.

Keep in Touch

These online instructional materials, as well as the rest of the course tools, are part of the larger Networking Academy. The portal for the program is located at http://cisco.netacad.net. There you will obtain access to the other tools in the program such as the assessment server and student grade book), as well as informational updates and other relevant links.

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. Below are a few suggestions to help you learn and grow.

1. Take notes. Professionals in the networking field often keep Engineering Journals in which they write down the things they observe and learn. Taking notes is an important way to help your understanding grow over time.
2. Think about it. The course provides information both to change what you know and what you can do. As you go through the course, ask yourself what makes sense and what doesn't. Stop and ask questions when you are confused. Try to find out more about topics that interest you. If you are not sure why something is being taught, consider asking your instructor or a friend. Think about how the different parts of the course fit together.
3. Practice. Learning new skills requires practice. We believe this is so important to e-learning that we have a special name for it. We call it e-doing. It is very important that you complete the activities in the online instructional materials and that you also complete the hands-on labs and Packet Tracer® activities.
4. Practice again. Have you ever thought that you knew how to do something and then, when it was time to show it on a test or at work, you discovered that you really hadn't mastered it? Just like learning any new skill like a sport, game, or language, learning a professional skill requires patience and repeated practice before you can say you have truly learned it. The online instructional materials in this course provide opportunities for repeated practice for many skills. Take full advantage of them. You can also work with your instructor to extend Packet Tracer, and other tools, for additional practice as needed.
5. Teach it. Teaching a friend or colleague is often a good way to reinforce your own learning. To teach well, you will have to work through details that you may have overlooked on your first reading. Conversations about the course material with fellow students, colleagues, and the instructor can help solidify your understanding of networking concepts.
6. Make changes as you go. The course is designed to provide feedback through interactive activities and quizzes, the online assessment system, and through interactions with your instructor. You can use this feedback to better understand where your strengths and weaknesses are. If there is an area that you are having trouble with, focus on studying or practicing more in that area. Seek additional feedback from your instructor and other students.

Explore the world of networking

This version of the course includes a special tool called Packet Tracer 4.1®. 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 to understand the internal workings of a network.

The Packet Tracer activities included in the course consist of network simulations, games, activities, and challenges that provide a broad range of learning experiences.

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 activities included in the course, 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.

Course Overview

The primary focus of this course is on accessing wide area networks (WAN). The goal is to develop an understanding of various WAN technologies to connect small- to medium-sized business networks.

The course introduces WAN converged applications and quality of service (QoS). It focuses on WAN technologies including PPP, Frame Relay, and broadband links. WAN security concepts are discussed in detail, including types of threats, how to analyze network vulnerabilities, general methods for mitigating common security threats and types of security appliances and applications. The course then explains the principles of traffic control and access control lists (ACLs) and describes how to implement IP addressing services for an Enterprise network, including how to configure NAT and DHCP. IPv6 addressing concepts are also discussed. During the course, you will learn how to use Cisco Router and Security Device Manager (SDM) to secure a router and implement IP addressing services. Finally, students learn how to detect, troubleshoot and correct common Enterprise network implementation issues.

The labs and Packet Tracer activities used in this course are designed to help you develop an understanding of how to configure routing operations while reinforcing the concepts learned in each chapter.

Chapter 1 Introduction to WANs - In Chapter 1, you will learn the fundamentals enterprise WANs, the technologies available to implement them, and the terminology used to discuss them. You will learn how the Cisco enterprise architecture provides integrated services over an enterprise network and how to select the appropriate WAN technology to meet different enterprise business requirements.

Chapter 2 PPP - Chapter 2 focuses on serial point-to-point communications and the Point-to-Point Protocol (PPP). Understanding how point-to-point communication links function to provide access to a WAN is important to an overall understanding of how WANs function. Various aspects of PPP are discussed including securing PPP using either Password Authentication Protocol (PAP) or the more effective Challenge Handshake Authentication Protocol (CHAP).

Chapter 3 Frame Relay - Chapter 3 focuses on the high-performance Frame Relay WAN protocol. You will learn how to implement Frame Relay for use between LANs over a WAN.

Chapter 4 Network Security - Chapter 4 introduces network security which has moved to the forefront of network management and implementation. The overall security challenge is to find a balance between two important requirements: the need to open networks to support evolving business opportunities, and the need to protect private, personal, and strategic business information. You will learn to identify security threats to enterprise networks and mitigation techniques. You will also learn how to configure basic router security, disable unused resources and interfaces. Finally you will learn to manage configurations and IOS files.

Chapter 5 ACLs - Chapter 5 builds on the concepts introduced in Chapter 4 and focuses on the application of ACLs. One of the most important skills a network administrator needs is mastery of access control lists (ACLs). You will learn how to create firewalls using standard and extended ACLs. Finally, you learn about advanced ACL features including dynamic, reflexive and timed ACLs.

Chapter 6 Teleworker Services - Chapter 6 discusses broadband technologies from a telecommuter's perspective. Specifically, you will learn about cable, DSL, and wireless broadband options. You will also explore how VPNs are utilized to secure broadband connections.

Chapter 7 IP Addressing Services - Chapter 7 discusses how a branch site can provide IP addressing services to users. You will identify teleworker requirements and recommend architectures for providing teleworking services. Specifically, you will learn how to configure a router to be a Dynamic Host Configuration Protocol (DHCP) server and how to integrate private addresses and Network Address Translation (NAT). You will finish with an overview of IPv6 and how to configure routers to exchange IPv6 routes using RIPng.

Chapter 8 Network Troubleshooting - Chapter 8 is the capstone chapter for this course. You will learn how to establish a network baseline and develop network documentation to help in network troubleshooting. You will also develop your network troubleshooting skills by reviewing troubleshooting methodology. You will learn to identify and troubleshoot common enterprise network implementation issues using a layered model approach.

CHAPTER 1

Introduction to WANs

Chapter Introduction

Refer to **Figure** in online course

When an enterprise grows to include branch offices, e-commerce services, or global operations, a single ***LAN network*** is no longer sufficient to meet its business requirements. Wide-area network (***WAN***) access has become essential for larger businesses today.

There are a variety of WAN technologies to meet the different needs of businesses and many ways to scale the network. Adding WAN access introduces other considerations, such as network security and ***address*** management. Consequently, designing a WAN and choosing the correct carrier network services is not a simple matter.

In this chapter, you will begin exploring some of the options available for designing enterprise WANs, the technologies available to implement them, and the terminology used to discuss them. You will learn about selecting the appropriate WAN technologies, services, and ***devices*** to meet the changing business requirements of an evolving enterprise. The activities and labs confirm and reinforce your learning.

Upon completion of this chapter, you will be able to identify and describe the appropriate WAN technologies to enable integrated WAN services over a multilocation ***enterprise network***.

1.1 Providing Integrated Services to the Enterprise

1.1.1 Introducing Wide Area Networks (WANs)

Refer to **Figure** in online course

What is a WAN?

A WAN is a ***data communications*** network that operates beyond the geographic scope of a LAN.

WANs are different from LANs in several ways. While a LAN connects computers, peripherals, and other devices in a single building or other small geographic area, a WAN allows the transmission of data across greater geographic distances. In addition, an enterprise must subscribe to a WAN service provider to use WAN carrier network services. LANs are typically owned by the company or organization that uses them.

WANs use facilities provided by a service provider, or carrier, such as a telephone or cable company, to connect the locations of an organization to each other, to locations of other organizations, to external services, and to remote users. WANs generally carry a variety of traffic types, such as voice, data, and video.

Here are the three major characteristics of WANs:

- WANs generally connect devices that are separated by a broader geographical area than can be served by a LAN.

- WANs use the services of carriers, such as telephone companies, cable companies, satellite systems, and network providers.
- WANs use serial connections of various types to provide access to ***bandwidth*** over large geographic areas.

Why Are WANs Necessary?

LAN technologies provide both speed and cost-efficiency for the transmission of data in organizations over relatively small geographic areas. However, there are other business needs that require communication among remote sites, including the following:

- People in the regional or branch offices of an organization need to be able to communicate and share data with the central site.
- Organizations often want to share information with other organizations across large distances. For example, software manufacturers routinely communicate product and promotion 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.

In addition, home computer users need to send and receive data across increasingly larger distances. Here are some examples:

- It is now common in many households for consumers to communicate with banks, stores, and a variety of providers of goods and services via computers.
- 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.

Since it is obviously not feasible to connect computers across a country or around the world in the same way that computers are connected in a LAN with cables, different technologies have evolved to support this need. Increasingly, the ***Internet*** is being used as an inexpensive alternative to using an enterprise WAN for some applications. 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.

1.1.2 The Evolving Enterprise

Refer to **Figure** in online course

Businesses and Their Networks

As companies grow, they hire more employees, open branch offices, and expand into global markets. These changes also influence their requirements for integrated services and drive their network requirements. In this topic, we will explore how company networks change to accommodate their changing business requirements.

Every business is unique and how an organization grows depends on many factors, such as the type of products or services 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.

To illustrate, let us look at an example of a fictitious company called Span Engineering, and watch how its network requirements change as the company grows from a small local business into a global enterprise.

Click the tabs in the figure to see each growth stage and the associated network topology.

Small Office (Single LAN)

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 hoping that they will have full scale projects 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 Digital Subscriber Line (DSL), which is supplied by their local telephone service provider. With so few employees, bandwidth is not a significant problem.

The company cannot afford in-house information technology (IT) support staff, and uses support services purchased from the same service provider. The company also uses a hosting service rather than purchasing and operating its own ***FTP*** and ***e-mail servers***. The figure shows an example of a small office and its network.

Campus (Multiple LANs)

Five years later, Span Engineering has grown rapidly. As the owners had hoped, 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, other projects have also been won 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 are 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 servers for e-mail, data transfer and file storage, web-based productivity tools and applications, as well as for the company intranet to provide in-house documents and information to employees. In addition, the company has an extranet that provides project information only to designated customers.

Branch (WAN)

Another five years later, Span Engineering has been so successful with its patented process that demand for its services has skyrocketed, and new projects are now being built in other 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 now needs to 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 now an attractive WAN connection option. Although connecting offices through the Internet is economical, it introduces security and privacy issues that the IT team must address.

Distributed (Global)

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

To increase profitability, Span Engineering needs to 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 we have seen from this example, the 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 needs to 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 techniques we teach in this series of courses. The next topic describes a network model for designing networks that can accommodate the changing needs of today's evolving businesses.

1.1.3 The Evolving Network Model

Refer to **Figure** in online course

The Hierarchical Design Model

The hierarchical network model is a useful high-level tool for designing a reliable network infrastructure. It provides a modular view of a network, making it easier to design and build a scalable network.

The Hierarchical Network Model

As you may recall from CCNA Exploration: LAN Switching and Wireless, the hierarchical network model divides a network into three layers:

- ***Access layer-*** Grants user access to network devices. In a network campus, the access layer generally incorporates switched LAN devices with ***ports*** that provide connectivity to

workstations and servers. In the WAN environment, it may provide ***teleworkers*** or remote sites access to the corporate network across WAN technology.

- ***Distribution layer-*** Aggregates the ***wiring closets***, using ***switches*** to ***segment workgroups*** and isolate network problems in a campus environment. Similarly, the distribution layer aggregates WAN connections at the edge of the campus and provides policy-based connectivity.
- ***Core layer (also referred to as the backbone***) - A high-speed backbone that is designed to switch ***packets*** as fast as possible. Because the core is critical for connectivity, it must provide a high level of availability and adapt to changes very quickly. It also provides scalability and fast ***convergence***.

Click Example *Topology* button in the figure.

The figure represents the Hierarchical Network Model in campus environments. The Hierarchical Network Model provides a modular framework that allows flexibility in network design, and facilitates ease of implementation and troubleshooting in the infrastructure. However, it is important to understand that the network infrastructure is only the foundation to a comprehensive architecture.

Networking technologies have advanced considerably in recent years, resulting in networks that are increasingly intelligent. The current network elements are more aware of traffic characteristics and can be configured to deliver specialized services based on such things as the types of data they carry, the priority of the data, and even the security needs. Although most of these various infrastructure services are outside the scope of this course, it is important to understand that they influence network design. In the next topic, we will explore the Cisco Enterprise Architecture, which expands upon the hierarchical model by making use of network intelligence to address the network infrastructure.

Refer to **Figure** in online course

The Enterprise Architecture

As described earlier, different businesses need different types of networks, depending on how the business is organized and its business goals. Unfortunately, all too often networks grow in a haphazard way as new components are added in response to immediate needs. Over time, those networks become complex and expensive to manage. Because the network is a mixture of newer and older technologies, it can be difficult to support and maintain. Outages and poor performance are a constant source of trouble for ***network administrators***.

To help prevent this situation, Cisco has developed a recommended architecture called the Cisco Enterprise Architecture that has relevance to the different stages of growth of a business. This architecture is designed to provide network planners with a roadmap for network growth as the business moves through different stages. By following the suggested roadmap, IT managers can plan for future network upgrades that will integrate seamlessly into the existing network and support the ever-growing need for services.

The following are some examples of the modules within the architecture that are relevant to the Span Engineering scenario described earlier:

- Enterprise Campus Architecture
- Enterprise Branch Architecture
- Enterprise Data Center Architecture
- Enterprise Teleworker Architecture

Refer to **Figure** in online course

Modules in the Enterprise Architecture

The Cisco Enterprise Architecture consists of modules representing focused views that target each place in the network. Each module has a distinct network infrastructure with services and network applications that extend across the modules. The Cisco Enterprise Architecture includes the following modules.

Roll over each module in the figure.

Enterprise Campus Architecture

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. In the Span Engineering example, the campus spanned multiple floors of the same building.

The Enterprise Campus Architecture 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.

Enterprise Edge Architecture

This module offers connectivity to voice, video, and data services outside the enterprise. This module enables the enterprise to use Internet and partner resources, and provide resources for its customers. This module often functions as a liaison between the campus module and the other modules in the Enterprise Architecture. The Enterprise WAN and Metropolitan-Area Network (***MAN***) Architecture, which the technologies covered later in this course are relevant to, are considered part of this module.

Enterprise Branch Architecture

This module allows businesses to extend the applications and services found at the campus to thousands of remote locations and users or to a small group of branches. Much of this course focuses on the technologies that are often implemented in this module.

Enterprise Data Center Architecture

Data centers are responsible for managing and maintaining the 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. Over the last decade, the rise of Internet and web-based technologies has made the data center more important than ever, improving productivity, enhancing business processes, and accelerating change.

Enterprise Teleworker Architecture

Many businesses today offer a flexible work environment to their employees, allowing them to telecommute from home offices. To telecommute is to leverage the network resources of the enterprise from home. The teleworker module recommends that connections from home using broadband services such as cable ***modem*** or DSL connect to the Internet and from there to the corporate network. Because the Internet introduces significant security risks to businesses, special measures need to be taken to ensure that teleworker communications are secure and private.

Click the Example Topology button in the figure.

The figure shows an example of how these Enterprise Architecture modules can be used to build a business network topology.

Refer to **Figure** in online course

Acitvity: Providing Integrated Services to the Enterprise

1.2 WAN Technology Concepts

1.2.1 WAN Technology Overview

Refer to **Figure** in online course

WANs and the OSI Model

As described in relation to the ***OSI*** reference model, WAN operations focus primarily on Layer 1 and Layer 2. WAN access ***standards*** typically describe both ***Physical layer*** delivery methods and ***Data Link layer*** requirements, including ***physical addressing***, ***flow control***, and ***encapsulation***. WAN access standards are defined and managed by a number of recognized authorities, including the International Organization for Standardization (***ISO***), the Telecommunication Industry Association (***TIA***), and the Electronic Industries Alliance (***EIA***).

The Physical layer (OSI Layer 1) protocols describe how to provide electrical, mechanical, operational, and functional connections to the services of a communications service provider.

The Data Link layer (OSI 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 ***Frame Relay*** and ***ATM***. Some of these protocols use the same basic framing mechanism, High-Level Data Link Control (***HDLC***), an ISO standard, or one of its subsets or variants.

1.2.2 WAN Physical Layer Concepts

Refer to **Figure** in online course

WAN Physical Layer 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 the locations of an organization to each other, to locations of other organizations, to external services, and to remote users. The WAN access Physical layer describes the physical connection between the company network and the service provider network. The figure illustrates the terminology commonly used to describe physical WAN connections, including:

- ***Customer Premises Equipment (CPE)***- The devices and inside wiring located at the premises of the subscriber and connected with a telecommunication ***channel*** of a carrier. 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 or carrier.
- ***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. This is very important because when problems arise, it is necessary to determine whether the user or the service provider is responsible for troubleshooting or repair.
- ***Local Loop***- The copper or fiber telephone ***cable*** that connects the CPE at the subscriber site to the CO of the service provider. The local loop is also sometimes called the "last-mile."

- ***Central Office (CO)***- A local service provider facility or building where local telephone cables link to long-haul, all-digital, fiber-optic ***communications lines*** through a system of switches and other equipment.

Refer to **Figure** in online course

WAN Devices

WANs use numerous types of devices that are specific to WAN environments, including:

- ***Modem-*** Modulates an analog carrier signal to encode digital information, and also demodulates the carrier signal to decode the transmitted information. A voiceband modem converts 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*** for input to a computer or network connection. Faster modems, such as cable modems and DSL modems, transmit using higher broadband frequencies.
- ***CSU/DSU-*** Digital lines, such as ***T1*** or ***T3*** carrier lines, require a channel service unit (***CSU***) and a data service unit (***DSU***). The two are often combined into a single piece of equipment, called the CSU/DSU. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the ***T-carrier*** line frames into frames that the LAN can interpret and vice versa.
- ***Access server***- Concentrates dial-in and dial-out user communications. An access server may have a mixture of analog and digital interfaces and support hundreds of simultaneous users.
- ***WAN switch-*** A multiport internetworking device used in carrier networks. These devices typically switch traffic such as Frame Relay, ATM, or ***X.25***, and operate at the Data Link layer of the OSI reference model. Public switched telephone network (***PSTN***) switches may also be used within the cloud for circuit-switched connections like Integrated Services Digital Network (***ISDN***) or analog dialup.
- ***Router***- Provides ***internetworking*** and WAN access interface ports that are used to connect to the service provider network. These interfaces may be serial connections 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 point of presence (***POP***) of the service provider.
- ***Core router***- A router that resides within the middle or backbone of the WAN rather than at its periphery. To fulfill this role, a router must be able to support multiple ***telecommunications*** interfaces of the highest speed in use in the WAN core, and it must be able to forward IP packets at full speed on all of those interfaces. The router must also support the ***routing*** protocols being used in the core.

Refer to **Figure** in online course

WAN Physical Layer Standards

WAN Physical layer ***protocols*** describe how to provide electrical, mechanical, operational, and functional connections for WAN services. The WAN Physical layer also describes the interface between the DTE and the DCE. The DTE/DCE interface uses various Physical layer protocols, including:

- ***EIA/TIA-232***- This protocol allows signal speeds of up to 64 kb/s on a 25-pin D-connector over short distances. It was formerly known as ***RS-232***. The ***ITU-T V.24*** specification is effectively the same.
- ***EIA/TIA-449***/530- This protocol is a faster (up to 2 Mb/s) version of EIA/TIA-232. It uses a 36-pin D-connector and is capable of longer cable runs. There are several versions. This standard is also known as RS422 and ***RS-423***.

- ***EIA/TIA-612/613-*** This standard describes the High-Speed Serial Interface (***HSSI***) protocol, which provides access to services up to 52 Mb/s on a 60-pin D-connector.
- ***V.35***- This is the ITU-T standard for synchronous communications between a network access device and a packet network. Originally specified to support data rates of 48 kb/s, it now supports speeds of up to 2.048 Mb/s using a 34-pin rectangular connector.
- ***X.21***- This protocol is an ITU-T standard for synchronous digital communications. It uses a 15-pin D-connector.

These protocols establish the codes and electrical parameters the devices use to communicate with each other. Choosing a protocol is largely determined by the service provider's method of facilitation.

Click the WAN Cable Connectors button in the figure to see the types of cable connectors associated with each Physical layer protocol.

1.2.3 WAN Data Link Layer Concepts

Refer to **Figure** in online course

Data Link Protocols

In addition to Physical layer devices, WANs require Data Link layer protocols to establish the link across the communication line from the sending to the receiving device. This topic describes the common data link protocols that are used in today's enterprise networks to implement WAN connections.

Data Link layer protocols define how data is encapsulated for transmission to remote sites and the mechanisms for transferring the resulting frames. A variety of different technologies, such as ISDN, Frame Relay, or ATM, are used. Many of these protocols use the same basic framing mechanism, HDLC, an ISO standard, or one of its subsets or variants. ATM is different from the others, because it uses small fixed-size cells of 53 ***bytes*** (48 bytes for data), unlike the other packet-switched technologies, which use variable-sized packets.

The most common WAN data-link protocols are:

- HDLC
- ***PPP***
- Frame Relay
- ATM

ISDN and X.25 are older data-link protocols that are less frequently used today. However, ISDN is still covered in this course because of its use when provisioning VoIP network using PRI links. X.25 is mentioned to help explain the relevance of Frame Relay. As well, X.25 is still in use in developing countries where packet data networks (PDN) are used to transmit credit card and debit card transactions from retailers.

Note: Another Data Link layer protocol is the Multiprotocol Label Switching (MPLS) protocol. MPLS is increasingly being deployed by service providers to provide an economical solution to carry circuit-switched as well as packet-switched network traffic. It can operate over any existing infrastructure, such as IP, Frame Relay, ATM, or ***Ethernet***. It sits between Layer 2 and Layer 3 and is sometimes referred to as a Layer 2.5 protocol. However, MPLS is beyond the scope of this course but is covered in the CCNP: Implementing Secure Converged Wide-area Networks.

Refer to **Figure** in online course

WAN Encapsulation

Data from the ***Network layer*** is passed to the Data Link layer for delivery on a physical link, which is normally point-to-point on a WAN connection. The Data Link layer builds a frame around the Network layer data so that the necessary checks and controls can be applied. Each

WAN connection type uses a Layer 2 protocol to encapsulate a packet while it is crossing the WAN link. To ensure that the correct encapsulation protocol is used, the Layer 2 encapsulation type used for each router serial interface must be configured. The choice of encapsulation protocols depends on the WAN technology and the equipment. HDLC was first proposed in 1979 and for this reason, most framing protocols which were developed afterwards are based on it.

Click the Play button in the figure to view how WAN data-link protocols encapsulate traffic.

Refer to **Figure** in online course

WAN Frame Encapsulation Formats

Examining the header portion of an HDLC frame will help identify common fields used by many WAN encapsulation protocols. The frame always starts and ends with an 8-***bit*** flag field. The bit pattern is 01111110. The address field is not needed for WAN links, which are almost always point-to-point. The address field is still present and may be 1 or 2 bytes long. The control field is protocol dependent, but usually indicates whether the content of the data is control information or Network layer data. The control field is normally 1 byte.

Together the address and control fields are called the frame ***header***. The encapsulated data follows the control field. Then a frame check sequence (***FCS***) uses the cyclic redundancy check (***CRC***) mechanism to establish a 2 or 4 byte field.

Several data-link protocols are used, including subsets and proprietary versions of HDLC. Both PPP and the Cisco version of HDLC have an extra field in the header to identify the Network layer protocol of the encapsulated data.

1.2.4 WAN Switching Concepts

Refer to **Figure** in online course

Circuit Switching

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

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.

The internal path taken by the circuit between exchanges is shared by a number of conversations. Time-division ***multiplexing*** (***TDM***) gives each conversation a share of the connection in turn. TDM assures that a fixed capacity connection is made available to the subscriber.

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.

PSTN and ISDN are two types of circuit-switching technology that may be used to implement a WAN in an enterprise setting.

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

Refer to **Figure** in online course

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*** determine which link the packet must be sent on next from the addressing information in each packet. There are two approaches to this link determination, ***connectionless*** or ***connection-oriented***.

- Connectionless systems, such as the Internet, carry full addressing information in each packet. Each switch must evaluate the address to determine where to send the packet.
- Connection-oriented systems predetermine the route for a packet, and each packet only has to carry an identifier. In the case of Frame Relay, these are called Data Link Connection Identifiers (***DLCIs***). 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. If this circuit is only physically in existence while a packet is traveling through it, it is called a virtual circuit (***VC***).

Because the internal links between the switches are shared between many users, the costs of packet switching are lower than those of circuit switching. ***Delays*** (***latency***) and variability of delay (***jitter***) are greater in packet-switched 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 even video communications on these networks.

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

Server A is sending data to server B. 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 server B.

Virtual Circuits

Packet-switched networks may establish routes through the switches for particular end-to-end connections. These routes are called virtual circuits. A VC is a logical circuit created within a shared network between two network devices. Two types of VCs exist:

- ***Permanent Virtual Circuit (PVC)***- A permanently established virtual circuit that consists of one mode: data transfer. PVCs are used in situations in which data transfer between devices is constant. PVCs decrease the bandwidth use associated with establishing and terminating VCs, but they increase costs because of constant virtual circuit availability. PVCs are generally configured by the service provider when an order is placed for service.
- ***Switched Virtual Circuit (SVC)***- A VC that is dynamically established on demand and terminated when transmission is complete. Communication over an SVC consists of three phases: circuit establishment, data transfer, and circuit termination. The establishment phase involves creating the VC between the source and destination devices. Data transfer involves transmitting data between the devices over the VC, and the circuit termination phase involves tearing down the VC between the source and destination devices. SVCs are used in situations in which data transmission between devices is intermittent, largely to save costs. SVCs release the circuit when transmission is complete, which results in less expensive connection charges than those incurred by PVCs, which maintain constant virtual circuit availability.

Connecting to a Packet-Switched Network

To connect to a packet-switched network, a subscriber needs a local loop to the nearest location where the provider makes the service available. This is called the point-of-presence (POP) of the service. Normally this is a dedicated leased line. This line is much shorter than a leased line directly connected to the subscriber locations, and often carries several VCs. Because it is likely that not all

the VCs require maximum demand simultaneously, the capacity of the ***leased line*** can be smaller than the sum of the individual VCs. Examples of packet- or cell-switched connections include:

- X.25
- Frame Relay
- ATM

Refer to **Figure** in online course

Practice: WAN Technology Concepts

1.3 WAN Connection Options

1.3.1 WAN Link Connection Options

Refer to **Figure** in online course

Many options for implementing WAN solutions are currently available. They differ in technology, speed, and cost. Familiarity with these technologies is an important part of network design and evaluation.

WAN connections can be either over a private infrastructure or over a public infrastructure, such as the Internet.

Private WAN Connection Options

Private WAN connections include both dedicated and switched communication link options.

Dedicated communication links

When permanent dedicated connections are required, point-to-point lines are used with various capacities that are limited only by the underlying physical facilities and the willingness of users to pay for these dedicated lines. A point-to-point link provides a pre-established WAN communications path from the customer premises through the provider network to a remote destination. Point-to-point lines are usually leased from a carrier and are also called leased lines.

Switched communication links

Switched communication links can be either circuit switched or packet switched.

- ***Circuit-switched communication links-*** 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. Examples of circuit-switched communication links are analog dialup (PSTN) and ISDN.
- ***Packet-switched communication links-*** Many WAN users do not make efficient use of the fixed bandwidth that is available with dedicated, switched, or permanent circuits because the data flow fluctuates. Communications providers have data networks available to more appropriately service these users. In packet-switched networks, the data is transmitted in labeled frames, cells, or packets. Packet-switched communication links include Frame Relay, ATM, X.25, and Metro Ethernet.

Public WAN Connection Options

Public connections use the global Internet infrastructure. Until recently, the Internet was not a viable networking option for many businesses because of the significant security risks and lack of adequate performance guarantees in an end-to end Internet connection. With the development of VPN technology, however, the Internet is now an inexpensive and secure option for connecting to teleworkers and remote offices where performance guarantees are not critical. Internet WAN con-

nection links are through broadband services such as DSL, cable modem, and broadband wireless, and combined with VPN technology to provide privacy across the Internet.

1.3.2 Dedicated Connection Link Options

Refer to **Figure** in online course

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 through the provider network to a remote destination. Point-to-point lines are usually leased from a carrier and are called leased lines. This topic describes how enterprises use leased lines to provide a dedicated WAN connection.

Click the Line Types and Bandwidth button in the figure to view a list of the available leased line types and their ***bit rate*** capacities.

Leased lines are available in different capacities and are generally priced based on the bandwidth required and the distance between the two connected points.

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

A router serial port is required for each leased line connection. A CSU/DSU and the actual circuit from the service provider are also required.

Leased lines provide permanent dedicated capacity and are used extensively for building WANs. They have been the traditional connection of choice but have a number of disadvantages. Leased lines have a fixed capacity; however, WAN traffic is often variable leaving some of the capacity unused. In addition, each endpoint needs a separate physical interface on the router, which increases equipment costs. Any changes to the leased line generally require a site visit by the carrier.

Refer to **Figure** in online course

Practice: WAN Technologies - Leased Lines

1.3.3 Circuit Switched Connection Options

Refer to **Figure** in online course

Analog Dialup

When intermittent, low-volume data transfers are needed, modems and analog dialed telephone lines provide low capacity and dedicated switched connections. This topic describes the pros and cons of using analog dialup connection options, and identifies the types of business scenarios that benefit most from this type of option.

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, analog.

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 e-mail. Using automatic dialup at night or on weekends for large file transfers and data backup can take advantage of lower off-peak tariffs (line 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.

Refer to **Figure** in online course

Integrated Services Digital Network

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 are taking turns on the channel. A data block of subchannel 1 is transmitted during timeslot 1, subchannel 2 during timeslot 2, and so on. One TDM frame consists of one timeslot per subchannel. TDM is described in more detail in Chapter 2, PPP.

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 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. Therefore, some providers allow the D channel to carry data at low bit rates, such as X.25 connections at 9.6 kb/s.
- ***Primary Rate Interface (PRI)***- ISDN is also available for larger installations. PRI delivers 23 B channels with 64 kb/s and one D channel with 64 kb/s in North America, 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. In North America, PRI corresponds to a T1 connection. The rate of international PRI corresponds to an ***E1*** or J1 connection.

For small WANs, the BRI ISDN can provide an ideal connection mechanism. 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 **Figure** in online course

Practice: WAN Technologies - Circuit Switching

1.3.4 Packet Switched Connection Options

Refer to **Figure** in online course

Common Packet Switching WAN Technologies

The most common packet-switching technologies used in today's enterprise WAN networks include Frame Relay, ATM, and legacy X.25.

Click the X.25 button in the figure.

X.25

X.25 is a legacy Network layer protocol that provides subscribers with a ***network address***. Virtual circuits can be established through the network with call request packets to the target address. The resulting SVC is identified by a channel number. Data packets labeled with the channel number are delivered to the corresponding address. Multiple channels can be active on a single connection.

Typical X.25 applications are point-of-sale card readers. These readers use X.25 in dialup mode to validate transactions on a central computer. For these applications, the low bandwidth and high latency are not a concern, and the low cost makes X.25 affordable.

X.25 link speeds vary from 2400 b/s up to 2 Mb/s. However, public networks are usually low capacity with speeds rarely exceeding above 64 kb/s.

X.25 networks are now in dramatic decline being replaced by newer Layer 2 technologies such as Frame Relay, ATM, and ADSL. However, they are still in use in many portions of the developing world, where there is limited access to newer technologies.

Click the Frame Relay button in the figure.

Frame Relay

Although the network layout appears similar to X.25, Frame Relay differs from X.25 in several ways. Most importantly, it is a much simpler protocol that works at the Data Link layer rather than the Network layer. Frame Relay implements no error or flow control. The simplified handling of frames leads to reduced latency, and measures taken to avoid frame build-up at intermediate switches help reduce jitter. Frame Relay offers data rates up to 4 Mb/s, with some providers offering even higher rates.

Frame Relay VCs are uniquely identified by a DLCI, which ensures bidirectional communication from one DTE device to another. Most Frame Relay connections are PVCs rather than SVCs.

Frame Relay provides permanent, shared, medium-bandwidth connectivity that carries both voice and data traffic. Frame Relay is ideal for connecting enterprise LANs. The router on the LAN needs only a single interface, even when multiple VCs are used. The short-leased line to the Frame Relay network edge allows cost-effective connections between widely scattered LANs.

Frame Relay is described in more detail in Chapter 3, "Frame Relay."

Click the ATM button in the figure.

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 a larger data packet to be transmitted.

The 53 byte ATM cell is less efficient than the bigger frames and packets of Frame Relay and X.25. 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 can support link speeds of T1/E1 to OC-12 (622 Mb/s) and higher.

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

Refer to **Figure** in online course

Practice: WAN Technologies - Packet Switching

1.3.5 Internet Connection Options

Refer to **Figure** in online course

Broadband Services

Broadband connection options are typically used to connect telecommuting employees to a corporate site over the Internet. These options include cable, DSL, and wireless.

Click the DSL button in the figure.

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 data rates of up to 8.192 Mb/s.

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.

Click the Cable Modem button in the figure.

Cable Modem

Coaxial cable is widely used in urban areas to distribute television signals. Network access is available from some ***cable television*** networks. 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.

Click the Broadband Wireless button in the figure.

Broadband 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 WiFi-*** 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 WiFi, 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 WiFi hotspots. WiMAX operates in a similar way to WiFi, 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 10 miles of their location. They also need a WiMAX-enabled computer 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 satellite dish 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.

DSL, cable, and wireless broadband services are described in more detail in Chapter 6, "Teleworker Services."

Refer to **Figure** in online course

VPN Technology

Security risks are incurred when a teleworker or remote office uses broadband services to access the corporate WAN over the Internet. To address security concerns, broadband services provide capabilities for using Virtual Private Network (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.

VPN Benefits

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.

Types of VPN Access

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 the figure. 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 typically has VPN ***client*** software loaded or uses a web-based client.

Click the Remote Access VPN button or the Site-to-Site VPN button in the figure to see an example of each type of VPN connection.

Refer to **Figure** in online course

Metro Ethernet

Metro Ethernet is a rapidly maturing networking technology that broadens Ethernet to the public networks run by telecommunications companies. IP-aware Ethernet switches enable service providers to offer enterprises converged voice, data, and video services such as IP telephony, video streaming, imaging, and data storage. By extending Ethernet to the metropolitan area, companies can provide their remote offices with reliable access to applications and data on the corporate headquarters LAN.

Benefits of Metro Ethernet include:

- ***Reduced expenses and administration-*** Metro Ethernet 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 ATM and Frame Relay. 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-*** Metro Ethernet connects easily to existing Ethernet LANs, reducing installation costs and time.
- ***Enhanced business productivity-*** Metro Ethernet 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.

Refer to **Figure** in online course

Choosing a WAN Link Connection

Now that we have looked at the variety of WAN connection options, how do you choose the best technology to meet the requirements of a specific business? The figure compares the advantages and disadvantages of the WAN connection options that we have discussed in this chapter. This information is a good start. In addition, to help in the decision-making process, here are some questions to ask yourself when choosing a WAN connection option.

What is the purpose of the WAN?

Do you want to connect local branches in the same city area, connect remote branches, connect to a single branch, connect to customers, connect to business partners, or some combination of these? If the WAN is for providing authorized customers or business partners limited access to the company intranet, what is the best option?

What is the geographic scope?

Is it local, regional, global, one-to-one (single branch), one-to-many branches, many-to-many (distributed)? Depending on the range, some WAN connection options may be better than others.

What are the traffic requirements?

Traffic requirements to consider include:

- Traffic type (data only, VoIP, video, large files, streaming files) determines the quality and performance requirements. For example, if you are sending a lot of voice or streaming video traffic, ATM may be the best choice.
- Traffic volumes depending on type (voice, video, or data) for each destination determine the bandwidth capacity required for the WAN connection to the ISP.
- Quality requirements may limit your choices. If your traffic is highly sensitive to latency and jitter, you can eliminate any WAN connection options that cannot provide the required quality.
- Security requirements (data integrity, confidentiality, and security) is an important factor if the traffic is of a highly confidential nature or if provides essential services, such as emergency response.

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. Your 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, an 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 you are connecting to a local single branch, you could use a dedicated leased line. 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 do you need?

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, your 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 broadband satellite Internet access.

What is the cost of the available connection options?

Depending on the option you choose, the WAN can be a significant ongoing expense. The cost of a particular option must be weighed against how well it meets your 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 cheaper switched or Internet connection option may be more suitable.

As you can see, there are many important factors to consider when choosing an appropriate WAN connection. Following the guidelines described above, as well as those described by the Cisco Enterprise Architecture, you should now be able to choose an appropriate WAN connection to meet the requirements of different business scenarios.

Refer to **Figure** in online course

Activity: Using Appropriate WAN in the ECNM

1.4 Chapter Labs

1.4.1 Challenge Review

Refer to **Lab Activity** for this chapter

In this lab, you will review basic routing and switching concepts. Try to do as much on your own as possible. Refer back to previous material when you cannot proceed on your own.

Note: Configuring three separate routing protocols-***RIP***, OSPF, and ***EIGRP***-to route the same network is emphatically not a best practice. It should be considered a worst practice and is not something that would be done in a production network. It is done here so that you can review the major routing protocols before proceeding, and see a dramatic illustration of the concept of ***administrative distance***.

Chapter Summary

Refer to **Figure** in online course

A WAN is a data communications network that operates beyond the geographic scope of a LAN.

As companies grow, adding more employees, opening branch offices, and expanding into global markets, their requirements for integrated services change. These business requirements drive their network requirements.

The Cisco Enterprise Architecture expands upon the Hierarchical Design Model by further dividing the enterprise network into physical, logical, and functional areas.

Implementation of a Cisco Enterprise Architecture provides a secure, robust network with high availability that facilitates the deployment of converged networks.

WANs operate in relation to the OSI reference model, primarily on Layer 1 and Layer 2.

Devices that put data on the local loop are called data circuit-terminating equipment, or data communications equipment (DCE). The customer devices that pass the data to the DCE are called data terminal equipment (DTE). The DCE primarily provides an interface for the DTE into the communication link on the WAN cloud.

The physical demarcation point is the place where the responsibility for the connection changes from the enterprise to the service provider.

Data Link layer protocols define how data is encapsulated for transmission to remote sites and the mechanisms for transferring the resulting frames.

A circuit-switching network establishes a dedicated circuit (or channel) between nodes and terminals before the users may communicate.

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

A point-to-point link provides a pre-established WAN communications path from the customer premises through the provider network to a remote destination. Point-to-point links use leased lines to provide a dedicated connection.

Circuit-switching WAN options include analog dialup and ISDN. Packet-switching WAN options include X.25, Frame Relay, and ATM. ATM transmits data in 53-byte cells rather than frames. ATM is most suited to video traffic.

Internet WAN connection options include broadband services, such as DSL, cable modem or broadband wireless, and Metro Ethernet. VPN technology enables businesses to provide secure teleworker access through the Internet over broadband services.

Refer to **Figure** in online course

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

This activity covers many of the skills you acquired in the first three Exploration courses. Skills include building a network, applying an addressing scheme, configuring routing, `VLANs`, `STP` and `VTP`, and testing connectivity. You should review those skills before proceeding. In addition, this activity provides you an opportunity to review the basics of the Packet Tracer program. Packet Tracer is integrated throughout this course. You must know how to navigate the Packet Tracer environment to complete this course. Use the tutorials if you need a review of Packet Tracer fundamentals. The tutorials are located in the Packet Tracer Help menu.

Detailed instructions are provided within the activity as well as in the PDF link below.

Activity Instructions (PDF)

Go to
the online course
to take the quiz.

Chapter Quiz

Take the chapter quiz to test your knowledge.

Your Chapter Notes