CHAPTER 1

Exploring the Network

1.0 Exploring the Network

1.0.1.1 Introduction

We now stand at a critical turning point in the use of technology to extend and empower our ability to communicate. The globalization of the Internet has succeeded faster than anyone could have imagined. The manner in which social, commercial, political and personal interactions occur is rapidly changing to keep up with the evolution of this global network. In the next stage of our development, innovators will use the Internet as a starting point for their efforts - creating new products and services specifically designed to take advantage of the network capabilities. As developers push the limits of what is possible, the capabilities of the interconnected networks that form the Internet will play an increasing role in the success of these projects.

This chapter introduces the platform of data networks upon which our social and business relationships increasingly depend. The material lays the groundwork for exploring the services, technologies, and issues encountered by network professionals as they design, build, and maintain the modern network.

Refer to **Lab Activity** for this chapter

1.0.1.2 Class Activity - Draw Your Concept of the Internet

Welcome to a new component of our Networking Academy curriculum: Modeling Activities! You will find them at the beginning and end of each chapter.

Some activities can be completed individually (at home or in class), and some will require group or learning-community interaction. Your instructor will be facilitating so that you can obtain the most from these introductory activities.

These activities will help you enhance your understanding by providing an opportunity to visualize some of the abstract concepts that you will be learning in this course. Be creative and enjoy these activities!

Here is your first modeling activity:

Draw Your Concept of the Internet

Draw and label a map of the Internet as you interpret it now. Include your home or school/university location and its respective cabling, equipment, devices, etc. Some items you may wish to include:

- Devices/Equipment
- Media (cabling)
- Link Addresses or Names

- Sources & Destinations
- Internet Service Providers

Upon completion, be sure to save your work in a hard-copy format, as it will be used for future reference at the end of this chapter. If it is an electronic document, save it to a server location provided by your instructor. Be prepared to share and explain your work in class.

For an example to get you started, please visit http://www.kk.org/internet-mapping/.

Refer to **Online Course** for Illustration

1.1 Globally Connected

1.1.1 Networking Today

1.1.1.1 Networks in Our Daily Lives

Among all of the essentials for human existence, the need to interact with others ranks just below our need to sustain life. Communication is almost as important to us as our reliance on air, water, food, and shelter.

The methods that we use to communicate are constantly changing and evolving. Whereas we were once limited to face-to-face interactions, breakthroughs in technology have significantly extended the reach of our communications. From cave paintings to the printing press to radio and television, each new development has improved and enhanced our ability to connect and communicate with others.

The creation and interconnection of robust data networks has had a profound effect on communication, and has become the new platform on which modern communications occur.

In today's world, through the use of networks, we are connected like never before. People with ideas can communicate instantly with others to make those ideas a reality. News events and discoveries are known worldwide in seconds. Individuals can even connect and play games with friends separated by oceans and continents.

Networks connect people and promote unregulated communication. Everyone can connect, share, and make a difference.

1.1.1.2 Technology Then and Now

Imagine a world without the Internet. No more Google, YouTube, instant messaging, Facebook, Wikipedia, online gaming, Netflix, iTunes, and easy access to current information. No more price comparison websites, avoiding lines by shopping online, or quickly looking up phone numbers and map directions to various locations at the click of a finger. How different would our lives be without all of this? That was the world we lived in just 15 to 20 years ago. But over the years, data networks have slowly expanded and been repurposed to improve the quality of life for people everywhere.

In the course of a day, resources that are available through the Internet can help you:

- Post and share your photographs, home videos, and experiences with friends or with the world.
- Access and submit school work.

- Communicate with friends, family, and peers using email, instant messaging, or Internet phone calls.
- Watch videos, movies, or television episodes on demand.
- Play online games with friends.
- Decide what to wear using online current weather conditions.
- Find the least congested route to your destination, displaying weather and traffic video from webcams.
- Check your bank balance and pay bills electronically.

Innovators are figuring out ways to use the Internet more every day. As developers push the limits of what is possible, the capabilities of the Internet and the role the Internet plays in our lives will expand broader and broader. Consider the changes that have happened over the last 25 years, as depicted in the figure. Now consider what changes will happen within the next 25 years. This future holds the Internet of Everything (IoE).

The IoE is bringing together people, process, data, and things to make networked connections more relevant and valuable. It is turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for individuals, businesses, and countries.

What else do you think we will be able to do using the network as the platform?

Refer to **Online Course** for Illustration

1.1.1.3 The Global Community

Advancements in networking technologies are perhaps the most significant change agents in the world today. They are helping to create a world in which national borders, geographic distances, and physical limitations become less relevant, and present ever-diminishing obstacles.

The Internet has changed the manner in which social, commercial, political, and personal interactions occur. The immediate nature of communications over the Internet encourages the creation of global communities. Global communities allow for social interaction that is independent of location or time zone. The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities across the globe.

Cisco refers to this as the human network. The human network centers on the impact of the Internet and networks on people and businesses.

How has the human network affected you?

Refer to **Online Course** for Illustration

1.1.1.4 Networks Support the Way We Learn

Networks and the Internet have changed everything we do, from the way we learn, to the way we communicate, to how we work, and even how we play.

Changing the way we learn

Communication, collaboration, and engagement are fundamental building blocks of education. Institutions are continually striving to enhance these processes to maximize the dissemination of knowledge. Traditional learning methods provide primarily two sources of expertise from which the student can obtain information: the textbook and the instructor. These two sources are limited, both in the format and the timing of the presentation.

Networks have changed the way we learn. Robust and reliable networks support and enrich student learning experiences. They deliver learning material in a wide range of formats including interactive activities, assessments, and feedback. As shown in Figure 1, networks now:

- Support the creation of virtual classrooms
- Provide on-demand video
- Enable collaborative learning spaces
- Enable mobile learning

Access to high quality instruction is no longer restricted to students living in proximity to where that instruction is being delivered. Online distance learning has removed geographic barriers and improved student opportunity. Online (e-learning) courses can now be delivered over a network. These courses can contain data (text, links), voice, and video available to the students at any time from any place. Online discussion groups and message boards enable a student to collaborate with the instructor, with other students in the class, or even with students across the world. Blended courses can combine instructor-led classes with online courseware to provide the best of both delivery methods. Figure 2 is a video about the ways that the classroom has expanded.

In addition to the benefits for the student, networks have improved the management and administration of courses as well. Some of these online functions include student enrollment, assessment delivery, and progress tracking.

Refer to **Online Course** for Illustration

1.1.1.5 Networks Support the Way We Communicate

Changing the way we communicate

The globalization of the Internet has ushered in new forms of communication that empower individuals to create information that can be accessed by a global audience.

Some forms of communication include:

- **Instant Messaging (IM) / Texting –** IM and texting both enable instant real-time communication between two or more people. Many IM and texting applications incorporate features such as file transfer. IM applications can offer additional features such as voice and video communication.
- **Social Media –** Social media consists of interactive websites where people and communities create and share user-generated content with friends, family, peers, and the world.
- **Collaboration Tools -** Collaboration tools give people the opportunity to work together on shared documents. Without the constraints of location or time zone, individuals connected to a shared system can speak to each other, often across real-time interactive video. Across the network they can share text and graphics, and edit documents together. With collaboration tools always available, organizations can move quickly to share information and pursue goals. The broad distribution of data networks means that people in remote locations can contribute on an equal basis with people at the heart of large population centers.
- **Weblogs (blogs) -** Weblogs are web pages that are easy to update and edit. Unlike commercial websites, which are created by professional communications experts,

blogs give anyone a means to communicate their thoughts to a global audience without technical knowledge of web design. There are blogs on nearly every topic one can think of, and communities of people often form around popular blog authors.

- **Wikis -** Wikis are web pages that groups of people can edit and view together. Whereas a blog is more of an individual, personal journal, a wiki is a group creation. As such, it may be subject to more extensive review and editing. Like blogs, wikis can be created in stages, and by anyone, without the sponsorship of a major commercial enterprise. Wikipedia has become a comprehensive resource - an online encyclopedia - of publicly-contributed topics. Private organizations and individuals can also build their own wikis to capture collected knowledge on a particular subject. Many businesses use wikis as their internal collaboration tool. With the global Internet, people of all walks of life can participate in wikis and add their own perspectives and knowledge to a shared resource.
- **Podcasting -** Podcasting is an audio-based medium that originally enabled people to record audio and convert it for use. Podcasting allows people to deliver their recordings to a wide audience. The audio file is placed on a website (or blog or wiki) where others can download it and play the recording on their computers, laptops, and other mobile devices.
- **Peer-to-Peer (P2P) File Sharing –** Peer-to-Peer file sharing allows people to share files with each other without having to store and download them from a central server. The user joins the P2P network by simply installing the P2P software. This lets them locate and share files with others in the P2P network. The widespread digitization of media files, such as music and video files has increased the interest in P2P file sharing. P2P file sharing has not been embraced by everyone. Many people are concerned about violating the laws of copyrighted materials.

What other sites or tools do you use to share your thoughts?

Refer to **Online Course** for Illustration

1.1.1.6 Networks Support the Way We Work

Changing the way we work

In the business world, data networks were initially used by businesses to internally record and manage financial information, customer information, and employee payroll systems. These business networks evolved to enable the transmission of many different types of information services, including email, video, messaging, and telephony.

The use of networks to provide efficient and cost-effective employee training is increasing in acceptance. Online learning opportunities can decrease time-consuming and costly travel yet still ensure that all employees are adequately trained to perform their jobs in a safe and productive manner.

There are many success stories illustrating innovative ways networks are being used to make us more successful in the workplace. Some of these scenarios are available through the Cisco web site at http://www.cisco.com.

Refer to **Online Course** for Illustration

1.1.1.7 Networks Support the Way We Play

Changing the way we play

The widespread adoption of the Internet by the entertainment and travel industries enhances the ability to enjoy and share many forms of recreation, regardless of location. It is possible

to explore places interactively that previously we could only dream of visiting, as well as preview the actual destinations before making a trip. Travelers can post the details and photographs from their adventures online for others to view.

In addition, the Internet is used for traditional forms of entertainment. We listen to recording artists, preview or view motion pictures, read entire books, and download material for future offline access. Live sporting events and concerts can be experienced as they are happening, or recorded and viewed on demand.

Networks enable the creation of new forms of entertainment, such as online games. Players participate in any kind of online competition that game designers can imagine. We compete with friends and foes around the world in the same manner as if they were in the same room.

Even offline activities are enhanced using network collaboration services. Global communities of interest have grown rapidly. We share common experiences and hobbies well beyond our local neighborhood, city, or region. Sports fans share opinions and facts about their favorite teams. Collectors display prized collections and get expert feedback about them.

Online markets and auction sites provide the opportunity to buy, sell, and trade all types of merchandise.

Whatever form of recreation we enjoy in the human network, networks are improving our experience.

How do you play on the Internet?

Refer to **Lab Activity** for this chapter

1.1.1.8 Lab - Researching Network Collaboration Tools

In this lab, you will complete the following objectives:

- Part 1: Use Collaboration Tools
- Part 2: Share Documents with Google Drive
- Part 3: Explore Conferencing and Web Meetings
- Part 4: Create Wiki Pages

Refer to **Online Course** for Illustration

1.1.2 Providing Resources in a Network

1.1.2.1 Networks of Many Sizes

Networks come in all sizes. They can range from simple networks consisting of two computers to networks connecting millions of devices.

Simple networks installed in homes enable sharing of resources, such as printers, documents, pictures and music between a few local computers.

Home office networks and small office networks are often set up by individuals that work from a home or remote office and need to connect to a corporate network or other centralized resources. Additionally, many self-employed entrepreneurs use home office and small office networks to advertise and sell products, order supplies and communicate with customers. Communication over a network is usually more efficient and less expensive than traditional forms of communication, such as regular mail or long distance phone calls.

In businesses and large organizations, networks can be used on an even broader scale to allow employees to provide consolidation, storage, and access to information on network servers. Networks also allow for rapid communication such as email, instant messaging, and collaboration among employees. In addition to internal organizational benefits, many organizations use their networks to provide products and services to customers through their connection to the Internet.

The Internet is the largest network in existence. In fact, the term Internet means a 'network of networks'. The Internet is literally a collection of interconnected private and public networks, such as the ones described above. Businesses, small office networks, and even home networks usually provide a shared connection to the Internet.

It is incredible how quickly the Internet has become an integral part of our daily routines.

Refer to **Online Course** for Illustration

1.1.2.2 Clients and Servers

All computers connected to a network that participate directly in network communication are classified as hosts or end devices. Hosts can send and receive messages on the network. In modern networks, end devices can act as a client, a server, or both. The software installed on the computer determines which role the computer plays.

Servers are hosts that have software installed that enable them to provide information, like email or web pages, to other hosts on the network. Each service requires separate server software. For example, a host requires web server software in order to provide web services to the network.

Clients are computer hosts that have software installed that enable them to request and display the information obtained from the server. An example of client software is a web browser, like Internet Explorer.

Refer to **Online Course** for Illustration

1.1.2.3 Clients and Servers (Cont.)

A computer with server software can provide services simultaneously to one or many clients.

Additionally, a single computer can run multiple types of server software. In a home or small business, it may be necessary for one computer to act as a file server, a web server, and an email server.

A single computer can also run multiple types of client software. There must be client software for every service required. With multiple clients installed, a host can connect to multiple servers at the same time. For example, a user can check email and view a web page while instant messaging and listening to Internet radio.

1.1.2.4 Peer-to-Peer

Client and server software usually runs on separate computers, but it is also possible for one computer to carry out both roles at the same time. In small businesses and homes, many computers function as the servers and clients on the network. This type of network is called a peer-to-peer network.

The simplest peer-to-peer network consists of two directly connected computers using a wired or wireless connection.

Multiple PCs can also be connected to create a larger peer-to-peer network but this requires a network device, such as a hub, to interconnect the computers.

The main disadvantage of a peer-to-peer environment is that the performance of a host can be slowed down if it is acting as both a client and a server at the same time.

In larger businesses, due to the potential for high amounts of network traffic, it is often necessary to have dedicated servers to support the number of service requests.

Refer to **Online Course** for Illustration

1.2 LANs, WANs, and the Internet

1.2.1 Components of a Network

1.2.1.1 Components of the Network

The path that a message takes from source to destination can be as simple as a single cable connecting one computer to another or as complex as a network that literally spans the globe. This network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which our communications can occur.

The network infrastructure contains three categories of network components:

- Devices
- Media
- Services

Click each button in the figure to highlight the corresponding network components.

Devices and media are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices. Occasionally, some components may not be so visible. In the case of wireless media, messages are transmitted through the air using invisible radio frequency or infrared waves.

Network components are used to provide services and processes. These are the communication programs, called software, that run on the networked devices. A network service provides information in response to a request. Services include many of the common network applications people use every day, like email hosting services and web hosting services. Processes provide the functionality that directs and moves the messages through the network. Processes are less obvious to us but are critical to the operation of networks.

Refer to **Online Course** for Illustration

1.2.1.2 End Devices

The network devices that people are most familiar with are called end devices, or hosts. These devices form the interface between users and the underlying communication network.

Some examples of end devices are:

- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- TelePresence endpoint

- Security cameras
- Mobile handheld devices (such as smartphones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners)

A host device is either the source or destination of a message transmitted over the network, as shown in the animation. In order to distinguish one host from another, each host on a network is identified by an address. When a host initiates communication, it uses the address of the destination host to specify where the message should be sent.

Refer to **Online Course** for Illustration

1.2.1.3 Intermediary Network Devices

Intermediary devices interconnect end devices. These devices provide connectivity and work behind the scenes to ensure that data flows across the network, as shown in the animation. Intermediary devices connect the individual hosts to the network and can connect multiple individual networks to form an internetwork.

Examples of intermediary network devices are:

- Network Access (switches and wireless access points)
- Internetworking (routers)
- Security (firewalls)

The management of data as it flows through the network is also a role of the intermediary devices. These devices use the destination host address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network.

Processes running on the intermediary network devices perform these functions:

- Regenerate and retransmit data signals
- Maintain information about what pathways exist through the network and internetwork
- Notify other devices of errors and communication failures
- Direct data along alternate pathways when there is a link failure
- Classify and direct messages according to Quality of Service (QoS) priorities
- Permit or deny the flow of data, based on security settings

Refer to **Online Course** for Illustration

1.2.1.4 Network Media

Communication across a network is carried on a medium. The medium provides the channel over which the message travels from source to destination.

Modern networks primarily use three types of media to interconnect devices and to provide the pathway over which data can be transmitted. As shown in the figure, these media are:

- Metallic wires within cables
- Glass or plastic fibers (fiber optic cable)
- Wireless transmission

The signal encoding that must occur for the message to be transmitted is different for each media type. On metallic wires, the data is encoded into electrical impulses that match specific patterns. Fiber optic transmissions rely on pulses of light, within either infrared or visible light ranges. In wireless transmission, patterns of electromagnetic waves depict the various bit values.

Different types of network media have different features and benefits. Not all network media has the same characteristics and is appropriate for the same purpose. The criteria for choosing network media are:

- The distance the media can successfully carry a signal
- The environment in which the media is to be installed
- The amount of data and the speed at which it must be transmitted
- The cost of the media and installation

Refer to **Online Course** for Illustration

1.2.1.5 Network Representations

When conveying complex information such as displaying all the devices and medium in a large internetwork, it is helpful to use visual representations. A diagram provides an easy way to understand the way the devices in a large network are connected. Such a diagram uses symbols to represent the different devices and connections that make up a network. This type of "picture" of a network is known as a topology diagram.

Like any other language, the language of networking uses a common set of symbols to represent the different end devices, network devices, and media, as shown in the figure. The ability to recognize the logical representations of the physical networking components is critical to being able to visualize the organization and operation of a network. Throughout this course and labs, you will learn both how these devices operate and how to perform basic configuration tasks on these devices.

In addition to these representations, specialized terminology is used when discussing how each of these devices and media connect to each other. Important terms to remember are:

- **Network Interface Card -** A NIC, or LAN adapter, provides the physical connection to the network at the PC or other host device. The media connecting the PC to the networking device plugs directly into the NIC.
- **Physical Port -** A connector or outlet on a networking device where the media is connected to a host or other networking device.
- **Interface -** Specialized ports on an internetworking device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to network interfaces.

Refer to **Online Course** for Illustration

1.2.1.6 Topology Diagrams

Topology diagrams are mandatory for anyone working with a network. It provides a visual map of how the network is connected.

There are two types of topology diagrams including:

- **Physical topology diagrams -** Identify the physical location of intermediary devices, configured ports, and cable installation.
- **Logical topology diagrams -** Identify devices, ports, and IP addressing scheme.

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

1.2.1.7 Activity - Network Component Representations and Functions

Refer to **Online Course** for Illustration

1.2.2 LANs and WANs

1.2.2.1 Types of Networks

Network infrastructures can vary greatly in terms of:

- Size of the area covered
- Number of users connected
- Number and types of services available

The figure illustrates the two most common types of network infrastructures:

- **Local Area Network (LAN) -** A network infrastructure that provides access to users and end devices in a small geographical area.
- **Wide Area Network (WAN) -** A network infrastructure that provides access to other networks over a wide geographical area.

Other types of networks include:

- **Metropolitan Area Network (MAN) -** A network infrastructure that spans a physical area larger than a LAN but smaller than a WAN (e.g., a city). MANs are typically operated by a single entity such as a large organization.
- **Wireless LAN (WLAN) -** Similar to a LAN but wirelessly interconnects users and end points in a small geographical area.
- **Storage Area Network (SAN) -** A network infrastructure designed to support file servers and provide data storage, retrieval, and replication. It involves high-end servers, multiple disk arrays (called blocks), and Fibre Channel interconnection technology.

Refer to **Online Course** for Illustration

1.2.2.2 Local Area Networks

Local Area Networks (LANs) are a network infrastructure that spans a small geographical area. Specific features of LANs include:

- LANs interconnect end devices in a limited area such as a home, school, office building, or campus.
- A LAN is usually administered by a single organization or individual. The administrative control that governs the security and access control policies are enforced on the network level.
- LANs provide high speed bandwidth to internal end devices and intermediary devices.

Refer to **Online Course** for Illustration

1.2.2.3 Wide Area Networks

Wide Area Networks (WANs) are a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SP) or Internet Service Providers (ISP).

Specific features of WANs include:

- WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
- WANs are usually administered by multiple service providers.
- WANs typically provide slower speed links between LANs.

Refer to **Online Course** for Illustration

1.2.3 The Internet

1.2.3.1 The Internet

Although there are benefits to using a LAN or WAN, most individuals need to communicate with a resource on another network, outside of the local network within the home, campus, or organization. This is done using the Internet.

As shown in the figure, the Internet is a worldwide collection of interconnected networks (internetworks or internet for short), cooperating with each other to exchange information using common standards. Through telephone wires, fiber optic cables, wireless transmissions, and satellite links, Internet users can exchange information in a variety of forms.

The Internet is a conglomerate of networks and is not owned by any individual or group. Ensuring effective communication across this diverse infrastructure requires the application of consistent and commonly recognized technologies and standards as well as the cooperation of many network administration agencies. There are organizations that have been developed for the purpose of helping to maintain structure and standardization of Internet protocols and processes. These organizations include the Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Architecture Board (IAB), plus many others.

Note The term internet (with a lower case "i") is used to describe multiple networks interconnected. When referring to the global system of interconnected computer networks or the World Wide Web, the term Internet (with a capital "I") is used.

Refer to **Online Course** for Illustration

1.2.3.2 Intranet and Extranet

There are two other terms which are similar to the term Internet:

- Intranet
- Extranet

Intranet is a term often used to refer to a private connection of LANs and WANs that belongs to an organization, and is designed to be accessible only by the organization's members, employees, or others with authorization. Intranets are basically an internet which is usually only accessible from within the organization.

Organizations may publish web pages on an intranet about internal events, health and safety policies, staff newsletters, and staff phone directories. For example, schools may have intranets that include information on class schedules, online curriculum, and discussion forums. Intranets usually help eliminate paperwork and speed up workflows. The intranet

may be accessible to staff working outside of the organization by using secure connections to the internal network.

An organization may use an extranet to provide secure and safe access to individuals who work for a different organizations, but require company data. Examples of extranets include:

- A company providing access to outside suppliers/contractors.
- A hospital providing a booking system to doctors so they can make appointments for their patients.
- A local office of education providing budget and personnel information to the schools in its district.

Refer to **Lab Activity** for this chapter

1.2.3.3 Lab - Researching Converged Network Services

In this lab, you will complete the following objectives:

- Part 1: Survey Your Understanding of Convergence
- Part 2: Research ISPs Offering Converged Services
- Part 3: Research Local ISPs Offering Converged Services
- Part 4: Select Best Local ISP Converged Service
- Part 5: Research Local Company or Public Institution Using Convergence Technologies

Refer to **Online Course** for Illustration

1.2.4 Connecting to the Internet

1.2.4.1 Internet Access Technologies

There are many different ways to connect users and organizations to the Internet.

Home users, teleworkers (remote workers), and small offices typically require a connection to an Internet Service Provider (ISP) to access the Internet. Connection options vary greatly between ISP and geographical location. However, popular choices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.

Organizations typically require access to other corporate sites and the Internet. Fast connections are required to support business services including IP phones, video conferencing, and data center storage.

Business-class interconnections are usually provided by service providers (SP). Popular business-class services include business DSL, leased lines, and Metro Ethernet.

1.2.4.2 Connecting Remote Users to the Internet

The figure illustrates common connection options for small office and home office users, which include:

- **Cable** - Typically offered by cable television service providers, the Internet data signal is carried on the same coaxial cable that delivers cable television. It provides a high bandwidth, always on, connection to the Internet. A special cable modem separates

the Internet data signal from the other signals carried on the cable and provides an Ethernet connection to a host computer or LAN.

- **DSL -** Provides a high bandwidth, always on, connection to the Internet. It requires a special high-speed modem that separates the DSL signal from the telephone signal and provides an Ethernet connection to a host computer or LAN. DSL runs over a telephone line, with the line split into three channels. One channel is used for voice telephone calls. This channel allows an individual to receive phone calls without disconnecting from the Internet. A second channel is a faster download channel, used to receive information from the Internet. The third channel is used for sending or uploading information. This channel is usually slightly slower than the download channel. The quality and speed of the DSL connection depends mainly on the quality of the phone line and the distance from your phone company's central office. The farther you are from the central office, the slower the connection.
- **Cellular -** Cellular Internet access uses a cell phone network to connect. Wherever you can get a cellular signal, you can get cellular Internet access. Performance will be limited by the capabilities of the phone and the cell tower to which it is connected. The availability of cellular Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all, or for those constantly on the go.
- **Satellite -** Satellite service is a good option for homes or offices that do not have access to DSL or cable. Satellite dishes require a clear line of sight to the satellite and so might be difficult in heavily wooded areas or places with other overhead obstructions. Speeds will vary depending on the contract, though they are generally good. Equipment and installation costs can be high (although check the provider for special deals), with a moderate monthly fee thereafter. The availability of satellite Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all.
- **Dial-up Telephone -** An inexpensive option that uses any phone line and a modem. To connect to the ISP, a user calls the ISP access phone number. The low bandwidth provided by a dial-up modem connection is usually not sufficient for large data transfer, although it is useful for mobile access while traveling. A modem dial-up connection should only be considered when higher speed connection options are not available.

Many homes and small offices are more commonly being connected directly with fibre optic cables. This enables an Internet service provider to provide higher bandwidth speeds and support more services such as Internet, phone, and TV.

The choice of connection varies depending on geographical location and service provider availability.

What are your options for connecting to the Internet?

Refer to **Online Course** for Illustration

1.2.4.3 Connecting Businesses to the Internet

Corporate connection options differ from home user options. Businesses may require higher bandwidth, dedicated bandwidth, and managed services. Connection options available differ depending on the number of service providers located nearby.

The figure illustrates common connection options for organizations, which include:

- **Dedicated Leased Line -** This is a dedicated connection from the service provider to the customer premise. Leased lines are actually reserved circuits that connect geographically

separated offices for private voice and/or data networking. The circuits are typically rented at a monthly or yearly rate which tends to make it expensive. In North America, common leased line circuits include T1 (1.54 Mb/s) and T3 (44.7 Mb/s) while in other parts of the world they are available in E1 (2 Mb/s) and E3 (34 Mb/s).

- **Metro Ethernet -** Metro Ethernet is typically available from a provider to the customer premise over a dedicated copper or fiber connection providing bandwidth speeds of 10 Mb/s to 10 Gb/s. Ethernet over Copper (EoC) is more economical than fiber optic Ethernet service in many cases, quite widely available, and reaches speeds of up to 40 Mbps. However, Ethernet over Copper is limited by distance. Fiber optic Ethernet service delivers the fastest connections available at an economical price per megabit. Unfortunately, there are still many areas where this service is unavailable.
- **DSL -** Business DSL is available in various formats. A popular choice is Symmetric Digital Subscriber Lines (SDSL) which is similar to Asymmetric Digital Subscriber Line (ADSL), but provides the same upload and download speeds. ADSL is designed to deliver bandwidth at different rates downstream than upstream. For example, a customer getting Internet access may have downstream rates that range from 1.5 to 9 Mbps, whereas upstream bandwidth ranges are from 16 to 640 kbps. ADSL transmissions work at distances up to 18,000 feet (5,488 meters) over a single copper twisted pair.
- **Satellite -** Satellite service can provide a connection when a wired solution is not available. Satellite dishes require a clear line of sight to the satellite. Equipment and installation costs can be high, with a moderate monthly fee thereafter. Connections tend to be slower and less reliable than its terrestrial competition, which makes it less attractive than other alternatives.

The choice of connection varies depending on geographical location and service provider availability.

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

1.2.4.4 Packet Tracer - Network Representation

Packet Tracer is a fun, take-home, flexible software program which will help you with your Cisco Certified Network Associate (CCNA) studies. Packet Tracer allows you to experiment with network behavior, build network models, and ask "what if" questions. In this activity, you will explore a relatively complex network that highlights a few of Packet Tracer's features. While doing so, you will learn how to access Help and the tutorials. You will also learn how to switch between various modes and workspaces. Finally, you will explore how Packet Tracer serves as a modeling tool for network representations.

Refer to **Online Course** for Illustration

1.3 The Network as a Platform

1.3.1 Converged Networks

1.3.1.1 The Converging Network

Modern networks are constantly evolving to meet user demands. Early data networks were limited to exchanging character-based information between connected computer systems. Traditional telephone, radio, and television networks were maintained separately from

data networks. In the past, every one of these services required a dedicated network, with different communication channels and different technologies to carry a particular communication signal. Each service had its own set of rules and standards to ensure successful communication.

Consider a school built forty years ago. Back then, classrooms were cabled for the data network, telephone network, and video network for televisions. These separate networks were disparate; meaning that they could not communicate with each other, as shown in Figure 1.

Advances in technology are enabling us to consolidate these different kinds of networks onto one platform referred to as the "converged network". Unlike dedicated networks, converged networks are capable of delivering voice, video streams, text, and graphics between many different types of devices over the same communication channel and network structure, as shown in Figure 2. Previously separate and distinct communication forms have converged onto a common platform. This platform provides access to a wide range of alternative and new communication methods that enable people to interact directly with each other almost instantaneously.

On a converged network there are still many points of contact and many specialized devices such as, personal computers, phones, TVs, and tablet computers, but there is one common network infrastructure. This network infrastructure uses the same set of rules, agreements, and implementation standards.

Refer to **Online Course** for Illustration

1.3.1.2 Planning for the Future

The convergence of the different types of communications networks onto one platform represents the first phase in building the intelligent information network. We are currently in this phase of network evolution. The next phase will be to consolidate not only the different types of messages onto a single network, but to also consolidate the applications that generate, transmit, and secure the messages onto integrated network devices.

Not only will voice and video be transmitted over the same network, the devices that perform the telephone switching and video broadcasting will be the same devices that route the messages through the network. The resulting communications platform will provide high quality application functionality at a reduced cost.

The pace at which the development of exciting new converged network applications is occurring can be attributed to the rapid growth and expansion of the Internet. With only about 10 billion of the 1.5 trillion things currently connected globally, there is vast potential to connect the unconnected via the IoE. This expansion has created a wider audience for whatever message, product, or service can be delivered.

The underlying mechanics and processes that drive this explosive growth have resulted in a network architecture that is both capable of supporting changes and able to grow. As the supporting technology platform for living, learning, working, and playing in the human network, the network architecture of the Internet must adapt to constantly changing requirements for a high quality of service and security.

Refer to **Lab Activity** for this chapter

1.3.1.3 Lab - Mapping the Internet

In this lab, you will complete the following objectives:

- Part 1: Test Network Connectivity Using Ping
- Part 2: Trace a Route to a Remote Server Using Windows Tracert

- Part 3: Trace a Route to a Remote Server Using Web-Based and Software Tools
- Part 4: Compare Traceroute Results

Refer to **Online Course** for Illustration

1.3.2 Reliable Network

1.3.2.1 The Supporting Network Architecture

Networks must support a wide range of applications and services, as well as operate over many different types of cables and devices, which make up the physical infrastructure. The term network architecture, in this context, refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move messages across the network.

As networks evolve, we are discovering that there are four basic characteristics that the underlying architectures need to address in order to meet user expectations:

- Fault Tolerance (Figure 1)
- Scalability (Figure 2)
- Quality of Service (QoS) (Figure 3)
- Security (Figure 4)

1.3.2.2 Fault Tolerance in Circuit Switched Networks

Fault Tolerance

The expectation is that the Internet is always available to the millions of users who rely on it. This requires a network architecture that is built to be fault tolerant. A fault tolerant network is one that limits the impact of a failure, so that the fewest number of devices are affected by it. It is also built in a way that allows quick recovery when such a failure occurs. These networks depend on multiple paths between the source and destination of a message. If one path fails, the messages can be instantly sent over a different link. Having multiple paths to a destination is known as redundancy.

Circuit-Switched Connection-Oriented Networks

To understand the need for redundancy, we can look at how early telephone systems worked. When a person made a call using a traditional telephone set, the call first went through a setup process. This process identified the telephone switching locations between the person making the call (the source) and the phone set receiving the call (the destination). A temporary path, or circuit, was created for the duration of the telephone call. If any link or device in the circuit failed, the call was dropped. To reconnect, a new call had to be made, with a new circuit. This connection process is referred to as a circuit-switched process and is illustrated in the figure.

Many circuit-switched networks give priority to existing circuit connections at the expense of new circuit requests. After a circuit is established, even if no communication is occurring between the persons on either end of the call, the circuit remains connected and resources used until one of the parties disconnects the call. Because there are only so many circuits that can be created, it is possible to get a message that all circuits are busy

and a call cannot be placed. The cost to create many alternate paths with enough capacity to support a large number of simultaneous circuits, and the technologies necessary to dynamically recreate dropped circuits in the event of a failure, is why circuit switched technology was not optimal for the Internet.

Refer to **Online Course** for Illustration

1.3.2.3 Fault Tolerance in Packet-Switched Networks

Packet-Switched Networks

In the search for a network that was more fault tolerant, the early Internet designers researched packet switched networks. The premise for this type of network is that a single message can be broken into multiple message blocks, with each message block containing addressing information to indicate the origination point and final destination. Using this embedded information, these message blocks, called packets, can be sent through the network along various paths, and can be reassembled into the original message when reaching their destination, as illustrated in the figure.

The devices within the network itself are typically unaware of the content of the individual packets. Only visible is the address of the final destination. These addresses are often referred to as IP addresses, represented in a dotted decimal format such as 10.10.10.10. Each packet is sent independently from one location to another. At each location, a routing decision is made as to which path to use to forward the packet towards its final destination. This would be like writing a long message to a friend using ten postcards. Each postcard has the destination address of the recipient. As the postcards are forwarded through the postal system, the destination address is used to determine the next path that postcard should take. Eventually, they will be delivered to the address on the postcards.

If a previously used path is no longer available, the routing function can dynamically choose the next best available path. Because the messages are sent in pieces, rather than as a single complete message, the few packets that may be lost can be retransmitted to the destination along a different path. In many cases, the destination device is unaware that any failure or rerouting occurred. Using our postcard analogy, if one of the postcards is lost along the way, only that postcard needs to be mailed again.

The need for a single, reserved circuit from end-to-end does not exist in a packet switched network. Any piece of a message can be sent through the network using any available path. Additionally, packets containing pieces of messages from different sources can travel the network at the same time. By providing a method to dynamically use redundant paths, without intervention by the user, the Internet has become a fault tolerant method of communication. In our mail analogy, as our postcard travels through the postal system they will share transportation with other postcards, letters and packages. For example, one of the postcards may be placed on an airplane, along with lots of other packages and letters that are being transported toward their final destination.

Although packet-switched connectionless networks are the primary infrastructure for today's Internet, there are some benefits to a connection-oriented system like the circuit-switched telephone system. Because resources at the various switching locations are dedicated to providing a finite number of circuits, the quality and consistency of messages transmitted across a connection-oriented network can be guaranteed. Another benefit is that the provider of the service can charge the users of the network for the period of time that the connection is active. The ability to charge users for active connections through the network is a fundamental premise of the telecommunication service industry.

Refer to **Online Course** for Illustration

1.3.2.4 Scalable Networks

Scalability

Thousands of new users and service providers connect to the Internet each week. In order for the Internet to support this rapid amount of growth, it must be scalable. A scalable network can expand quickly to support new users and applications without impacting the performance of the service being delivered to existing users. The figures show the structure of the Internet.

The fact that the Internet is able to expand at the rate that it is, without seriously impacting the performance experienced by individual users, is a function of the design of the protocols and underlying technologies on which it is built. The Internet has a hierarchical layered structure for addressing, for naming, and for connectivity services. As a result, network traffic that is destined for local or regional services does not need to traverse to a central point for distribution. Common services can be duplicated in different regions, thereby keeping traffic off the higher level backbone networks.

Scalability also refers to the ability to accept new products and applications. Although there is no single organization that regulates the Internet, the many individual networks that provide Internet connectivity cooperate to follow accepted standards and protocols. The adherence to standards enables the manufacturers of hardware and software to concentrate on product development and improvements in the areas of performance and capacity, knowing that the new products can integrate with and enhance the existing infrastructure.

The current Internet architecture, while highly scalable, may not always be able to keep up with the pace of user demand. New protocols and addressing structures are under development to meet the increasing rate at which Internet applications and services are being added.

Refer to **Online Course** for Illustration

1.3.2.5 Providing QoS

Quality of Service

Quality of Service (QoS) is also an ever increasing requirement of networks today. New applications available to users over internetworks, such as voice and live video transmissions, as shown in Figure 1, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses?

Networks must provide predictable, measurable, and at times, guaranteed services. The packet-switched network architecture does not guarantee that all packets that comprise a particular message will arrive on time, in their correct order, or even that they will arrive at all.

Networks also need mechanisms to manage congested network traffic. Network bandwidth is the measure of the data carrying capacity of the network. In other words, how much information can be transmitted within a specific amount of time? Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps). When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion. The network simply has more bits to transmit than what the bandwidth of the communication channel can deliver.

In most cases, when the volume of packets is greater than what can be transported across the network, devices queue, or hold, the packets in memory until resources become available to transmit them, as shown in Figure 2. Queuing packets causes delay because new packets cannot be transmitted until previous packets have been processed. If the number of packets to be queued continues to increase, the memory queues fill up and packets are dropped.

Achieving the required QoS by managing the delay and packet loss parameters on a network becomes the secret to a successful end-to-end application quality solution. One way this can be accomplished is through classification. To create QoS classifications of data, we use a combination of communication characteristics and the relative importance assigned to the application, as shown in Figure 3. We then treat all data within the same classification according to the same rules. For example, communication that is time-sensitive, such as voice transmissions, would be classified differently from communication that can tolerate delay, such as file transfers.

Examples of priority decisions for an organization might include:

- **Time-sensitive communication -** increase priority for services like telephony or video distribution
- **Non time-sensitive communication -** decrease priority for web page retrieval or email
- **High importance to organization -** increase priority for production control or business transaction data
- **Undesirable communication -** decrease priority or block unwanted activity, like peer-to-peer file sharing or live entertainment

Refer to **Online Course** for Illustration

1.3.2.6 Providing Network Security

Security

The Internet has evolved from a tightly controlled internetwork of educational and government organizations to a widely accessible means for transmission of business and personal communications. As a result, the security requirements of the network have changed. The network infrastructure, services, and the data contained on network attached devices are crucial personal and business assets. Compromising the integrity of these assets could have serious consequences, such as:

- Network outages that prevent communications and transactions from occurring, with consequent loss of business
- Intellectual property (research ideas, patents, or designs) that is stolen and used by a competitor
- Personal or private information that is compromised or made public without the users consent
- Misdirection and loss of personal or business funds
- Loss of important data that takes a significant labor to replace, or is irreplaceable

There are two types of network security concerns that must be addressed: network infrastructure security and information security.

Securing a network infrastructure includes the physical securing of devices that provide network connectivity, and preventing unauthorized access to the management software that resides on them.

Information security refers to protecting the information contained within the packets being transmitted over the network and the information stored on network attached devices. Security measures taken in a network should:

- Prevent unauthorized disclosure
- Prevent theft of information (Figure 1)
- Prevent unauthorized modification of information
- Prevent Denial of Service (DoS)

In order to achieve the goals of network security, there are three primary requirements, as shown in Figure 2:

- **Ensuring confidentiality -** Data confidentiality means that only the intended and authorized recipients - individuals, processes, or devices – can access and read data. This is accomplished by having a strong system for user authentication, enforcing passwords that are difficult to guess, and requiring users to change them frequently. Encrypting data, so that only the intended recipient can read it, is also part of confidentiality.
- **Maintaining communication integrity -** Data integrity means having the assurance that the information has not been altered in transmission, from origin to destination. Data integrity can be compromised when information has been corrupted - willfully or accidentally. Data integrity is made possible by requiring validation of the sender as well as using mechanisms to validate that the packet has not changed during transmission.
- **Ensuring availability -** Availability means having the assurance of timely and reliable access to data services for authorized users. Network firewall devices, along with desktop and server antivirus software can ensure system reliability and the robustness to detect, repel, and cope with such attacks. Building fully redundant network infrastructures, with few single points of failure, can reduce the impact of these threats.

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

1.3.2.7 Activity - Reliable Networks

Refer to **Online Course** for Illustration

1.4 The Changing Network Environment

1.4.1 Network Trends

1.4.1.1 New Trends

When you look at how the Internet has changed so many of the things people do daily, it is hard to believe that it has only been around for most people for about 20 years. It has truly transformed the way individuals and organizations communicate. For example, before the Internet became so widely available, organizations and small businesses largely

relied on print marketing to make consumers aware of their products. It was difficult for businesses to determine which households were potential customers, so businesses relied on mass print marketing programs. These programs were expensive and varied in effectiveness. Compare that to how consumers are reached today. Most businesses have an Internet presence where consumers can learn about their products, read reviews from other customers, and order products directly from the web site. Social networking sites partner with businesses to promote products and services. Bloggers partner with businesses to highlight and endorse products and services. Most of this product placement is targeted to the potential consumer, rather than to the masses. Figure 1 shows several predictions for the Internet in the near future.

As new technologies and end user devices come to market, businesses and consumers must continue to adjust to this ever-changing environment. The role of the network is transforming to enable the connections of people, devices, and information. There are several new networking trends that will effect organizations and consumers. Some of the top trends include:

- Any device, to any content, any way
- Online collaboration
- Video
- Cloud computing

These trends are interconnected and will continue to build off of one another in the coming years. The next couple of topics will cover these trends in more detail.

But keep in mind, new trends are being dreamed up and engineered every day. How do you think the Internet will change in the next 10 years? 20 years? Figure 2 is a video that shows some of Cisco's thoughts on future developments.

Refer to **Online Course** for Illustration

1.4.1.2 BYOD

Bring Your Own Device (BYOD)

The concept of any device, to any content, in anyway is a major global trend that requires significant changes to the way devices are used. This trend is known as Bring Your Own Device (BYOD).

BYOD is about end users having the freedom to use personal tools to access information and communicate across a business or campus network. With the growth of consumer devices, and the related drop in cost, employees and students can be expected to have some of the most advanced computing and networking tools for personal use. These personal tools include laptops, netbooks, tablets, smartphones, and e-readers. These can be devices purchased by the company or school, purchased by the individual, or both.

BYOD means any device, with any ownership, used anywhere. For example, in the past, a student who needed to access the campus network or the Internet had to use one of the school's computers. These devices were typically limited and seen as tools only for work done in the classroom or in the library. Extended connectivity through mobile and remote access to the campus network gives students tremendous flexibility and more learning opportunities for the student.

BYOD is an influential trend that has or will touch every IT organization.

Refer to **Online Course** for Illustration

1.4.1.3 Online Collaboration

Online Collaboration

Individuals want to connect to the network, not only for access to data applications, but also to collaborate with one another. Collaboration is defined as "the act of working with another or others on a joint project."

For businesses, collaboration is a critical and strategic priority. To remain competitive, organizations must answer three primary collaboration questions:

- How can they get everyone on the same page?
- With decreased budgets and personnel, how can they balance resources to be in more places at once?
- How can they maintain face-to-face relationships with a growing network of colleagues, customers, partners, and peers in an environment that is more dependent on 24-hour connectivity?

Collaboration is also a priority in education. Students need to collaborate to assist each other in learning, to develop team skills used in the work force, and to work together on team-based projects.

One way to answer these questions and meet these demands in today's environment is through online collaboration tools. In traditional workspaces, and with BYOD environments alike, individuals are taking advantage of voice, video, and conferencing services in collaboration efforts.

The ability to collaborate online is changing business processes. New and expanding collaboration tools allow individuals to quickly and easily collaborate, regardless of physical location. Organizations have much more flexibility in the way they are organized. Individuals are no longer restricted to physical locations. Expert knowledge is easier to access than ever before. Expansions in collaboration allow organizations to improve their information gathering, innovation, and productivity. The figure lists some of the benefits of online collaboration.

Collaboration tools give employees, students, teachers, customers, and partners a way to instantly connect, interact, and conduct business, through whatever communications channels they prefer, and achieve their objectives.

Refer to **Online Course** for Illustration

1.4.1.4 Video Communication

Video Communication

Another trend in networking that is critical in the communication and collaboration effort is video. Video is being used for communications, collaboration, and entertainment. Video calls are becoming more popular, facilitating communications as part of the human network. Video calls can be made to and from anywhere with an Internet connection, including from home or at work.

Video calls and video conferencing is proving particularly powerful for sales processes and for doing business. Video is a useful tool for conducting business at a distance, both locally and globally. Today, businesses are using video to transform the way they do business. Video helps businesses create a competitive advantage, lower costs and reduce the impact on the environment by reducing the need travel. Figure 1 shows the trend of video in communication.

Both consumers and businesses are driving this change. Video is becoming a key requirement for effective collaboration as organizations extend across geographic and cultural boundaries. Video users now demand the ability to view any content, on any device, anywhere.

Businesses are also recognizing the role of video to enhance the human network. The growth of media, and the new uses to which it is being put, is driving the need to integrate audio and video into many forms of communication. The audio conference will coexist with the video conference. Collaboration tools designed to link distributed employees will integrate desktop video to bring teams closer together.

There are many drivers and benefits for including a strategy for using video. Each organization is unique. The exact mix, and nature of the drivers for adopting video, will vary from organization to organization, and by business function. Marketing, for example, may focus on globalization, and fast-changing consumer tastes; while the Chief Information Officer's (CIO) focus may be on cost savings by reducing travel costs of employees needing to meet face-to-face. Figure 2 lists some of the drivers for organizations to develop and implement a video solution strategy.

Figure 3 is a video that gives a closer look at how TelePresence using video can be incorporated into everyday life and business.

Another trend in video is video-on-demand and streaming live video. Delivering video over the network lets us see movies and television programs when we want and where we want.

Refer to **Online Course** for Illustration

1.4.1.5 Cloud Computing

Cloud Computing

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network. A company uses the hardware and software in the cloud and a service fee is charged.

Local computers no longer have to do all the "heavy lifting" when it comes to running network applications. The network of computers that make up the cloud handles them instead. The hardware and software requirements of the user are decreased. The user's computer must interface with the cloud using software, which may be a web browser, and the cloud's network takes care of the rest.

Cloud computing is another global trend changing the way we access and store data. Cloud computing encompasses any subscription-based or pay-per-use service, in real time over the Internet. Cloud computing allows us to store personal files, even backup our entire hard disk drive on servers over the Internet. Applications such as word processing and photo editing can be accessed using the cloud.

For businesses, cloud computing extends IT's capabilities without requiring investment in new infrastructure, training new personnel, or licensing new software. These services are available on demand and delivered economically to any device anywhere in the world without compromising security or function.

The term "cloud computing" really refers to web-based computing. Online banking, online retail stores, and online music downloading are all examples of cloud computing. Cloud applications are usually delivered to the user through a web browser. Users do not need to have any software installed on their end device. This allows many different kinds of devices to connect to the cloud.

Cloud computing offers the following potential benefits:

- **Organizational flexibility -** Users can access the information anytime and anyplace using a web browser.
- **Agility and rapid deployment -** IT department can focus on delivering the tools to mine, analyze, and share the information and knowledge from databases, files, and people.
- **Reduced cost of infrastructure -** Technology is moved from on-site to a cloud provider, eliminating the cost of hardware and applications.
- **Refocus of IT resources -** Cost savings of hardware and applications can be applied elsewhere.
- **Creation of new business models -** Applications and resources are easily accessible, so companies can react quickly to customer needs. This helps them set strategies to promote innovation while potentially entering new markets.

There are four primary types of clouds, as shown in Figure 2. Click each cloud to learn more.

Refer to **Online Course** for Illustration

1.4.1.6 Data Centers

Cloud computing is possible because of data centers. A data center is a facility used to house computer systems and associated components including:

- Redundant data communications connections
- High-speed virtual servers (sometimes referred to as server farms or server clusters)
- Redundant storage systems (typically uses SAN technology)
- Redundant or backup power supplies
- Environmental controls (e.g., air conditioning, fire suppression)
- Security devices

A data center can occupy one room of a building, one or more floors, or an entire building. Modern data centers make use of cloud computing and virtualization to efficiently handle large data transactions. Virtualization is the creation of a virtual version of something, such as a hardware platform, operating system (OS), storage device, or network resources. While a physical computer is an actual discrete device, a virtual machine consists of a set of files and programs running on an actual physical system. Unlike multitasking, which involves running several programs on the same OS; virtualization runs several different OSs in parallel on a single CPU. This drastically reduces administrative and cost overheads.

Data centers are typically very expensive to build and maintain. For this reason only large organizations use privately built data centers to house their data and provide services to users. For example, a large hospital may own a separate data center where patient records are maintained electronically. Smaller organizations, that cannot afford to maintain their own private data center, can reduce the overall cost of ownership by leasing server and storage services from a larger data center organization in the cloud.

The figure is a video about the growing use of cloud computing and data center services.

1.4.2 Networking Technologies for the Home

1.4.2.1 Technology Trends in the Home

Networking trends are not only affecting the way we communicate at work and at school, they are also changing just about every aspect of the home.

The newest home trends include 'smart home technology'. Smart home technology is technology that is integrated into every-day appliances allowing them to interconnect with other devices, making them more 'smart' or automated. For example, imagine being able to prepare a dish and place it in the oven for cooking prior to leaving the house for the day. Imagine if the oven was 'aware' of the dish it was cooking and was connected to your 'calendar of events' so that it could determine what time you should be available to eat, and adjust start times and length of cooking accordingly. It could even adjust cooking times and temperatures based on changes in schedule. Additionally, a smartphone or tablet connection allows the user the ability to connect to the oven directly, to make any desired adjustments. When the dish is "available", the oven sends an alert message to a specified end user device that the dish is done and warming.

This scenario is not long off. In fact, smart home technology is currently being developed for all rooms within a house. Smart home technology will become more of a reality as home networking and high-speed Internet technology becomes more widespread in homes. New home networking technologies are being developed daily to meet these types of growing technology needs.

Refer to **Online Course** for Illustration

1.4.2.2 Powerline Networking

Powerline networking is an emerging trend for home networking that uses existing electrical wiring to connect devices, as shown in the figure. The concept of "no new wires" means the ability to connect a device to the network wherever there is an electrical outlet. This saves the cost of installing data cables and without any additional cost to the electrical bill. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies similar to the same technology used for DSL.

Using a HomePlug standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet. Powerline networking is especially useful when wireless access points cannot be used or cannot reach all the devices in the home. Powerline networking is not designed to be a substitute for dedicated cabling for data networks. However, it is an alternative when data network cables or wireless communications are not a viable option.

Refer to **Online Course** for Illustration

1.4.2.3 Wireless Broadband

Connecting to the Internet is vital in smart home technology. DSL and cable are common technologies used to connect homes and small businesses to the Internet. However, wireless may be another option in many areas.

Wireless Internet Service Provider (WISP)

Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to a designated access point or hot spot using similar wireless technologies found in home wireless local area networks (WLANs). WISPs are more commonly found in rural environments where DSL or cable services are not available.

Although a separate transmission tower may be installed for the antenna, it is common that the antenna is attached to an existing elevated structure such as a water tower or a radio tower. A small dish or antenna is installed on the subscriber's roof in range of the WISP transmitter. The subscriber's access unit is connected to the wired network inside the home. From the perspective of the home user the setup isn't much different than DSL or cable service. The main difference is the connection from the home to the ISP is wireless instead of a physical cable.

Wireless Broadband Service

Another wireless solution for the home and small businesses is wireless broadband. This uses the same cellular technology used to access the Internet with a smart phone or tablet. An antenna is installed outside the house providing either wireless or wired connectivity for devices in the home. In many areas, home wireless broadband is competing directly with DSL and cable services.

Refer to **Online Course** for Illustration

1.4.3 Network Security

1.4.3.1 Security threats

Network security is an integral part of computer networking, regardless of whether the network is limited to a home environment with a single connection to the Internet, or as large as a corporation with thousands of users. The network security implemented must take into account the environment, as well as the tools and requirements of the network. It must be able to secure data, while still allowing for the quality of service that is expected of the network.

Securing a network involves protocols, technologies, devices, tools, and techniques to secure data and mitigate threats. Many external network security threats today are spread over the Internet. The most common external threats to networks include:

- **Viruses, worms, and Trojan horses -** malicious software and arbitrary code running on a user device
- **Spyware and adware -** software installed on a user device that secretly collects information about the user
- **Zero-day attacks, also called zero-hour attacks -** an attack that occurs on the first day that a vulnerability becomes known
- **Hacker attacks -** an attack by a knowledgeable person to user devices or network resources
- **Denial of service attacks -** attacks designed to slow or crash applications and processes on a network device
- **Data interception and theft -** an attack to capture private information from an organization's network
- **Identity theft -** an attack to steal the login credentials of a user in order to access private data

It is equally important to consider internal threats. There have been many studies that show that the most common data breaches happen because of internal users of the network. This can be attributed to lost or stolen devices, accidental misuse by employees, and in

the business environment, even malicious employees. With the evolving BYOD strategies, corporate data is much more vulnerable. Therefore, when developing a security policy, it is important to address both external and internal security threats.

Refer to **Online Course** for Illustration

1.4.3.2 Security Solutions

No single solution can protect the network from the variety of threats that exist. For this reason, security should be implemented in multiple layers, using more than one security solution. If one security component fails to identify and protect the network, others still stand.

A home network security implementation is usually rather basic. It is generally implemented on the connecting host devices, as well as at the point of connection to the Internet, and can even rely on contracted services from the ISP.

In contrast the network security implementation for a corporate network usually consists of many components built into the network to monitor and filter traffic. Ideally, all components work together, which minimizes maintenance and improves security.

Network security components for a home or small office network should include, at a minimum:

- **Antivirus and antispyware -** to protect user devices from malicious software
- **Firewall filtering -** to block unauthorized access to the network. This may include a host-based firewall system that is implemented to prevent unauthorized access to the host device, or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.

In addition to the above, larger networks and corporate networks often have other security requirements:

- **Dedicated firewall systems -** to provide more advanced firewall capability that can filter large amounts of traffic with more granularity
- **Access control lists (ACL) -** to further filter access and traffic forwarding
- **Intrusion prevention systems (IPS) -** to identify fast-spreading threats, such as zero-day or zero-hour attacks
- **Virtual private networks (VPN) -** to provide secure access to remote workers

Network security requirements must take into account the network environment, as well as the various applications, and computing requirements. Both home environments and businesses must be able to secure their data, while still allowing for the quality of service that is expected of each technology. Additionally, the security solution implemented must be adaptable to the growing and changing trends of the network.

The study of network security threats and mitigation techniques starts with a clear understanding of the underlying switching and routing infrastructure used to organize network services.

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

1.4.3.3 Activity - Network Security Terminology

Refer to **Online Course** for Illustration

1.4.4 Network Architectures

1.4.4.1 Cisco Network Architectures

The role of the network has changed from a data-only network, to a system that enables the connections of people, devices, and information in a media rich, converged network environment. In order for networks to function efficiently and grow in this type of environment, the network must be built upon a standard network architecture.

The network architecture refers to the devices, connections, and products that are integrated to support the necessary technologies and applications. A well-planned network technology architecture helps ensure the connection of any device across any combination of networks. While ensuring connectivity, it also increases cost efficiency by integrating network security and management, and improves business processes. At the foundation of all network architectures, and in fact, at the foundation of the Internet itself, are routers and switches. Routers and switches transport data, voice, and video communications, as well as allow for wireless access, and provide for security.

Building networks that support our needs of today and the needs and trends of the future starts with a clear understanding of the underlying switching and routing infrastructure. After a basic routing and switching network infrastructure is built, individuals, small businesses, and organizations can grow their network over time, adding features and functionality in an integrated solution.

Refer to **Online Course** for Illustration

1.4.4.2 CCNA

As the use of these integrated, expanding networks increase, so does the need for training for individuals who implement and manage network solutions. This training must begin with the routing and switching foundation. Achieving Cisco Certified Network Associate (CCNA) certification is the first step in helping an individual prepare for a career in networking.

CCNA certification validates an individual's ability to install, configure, operate, and troubleshoot medium-size route and switched networks, including implementation and verification of connections to remote sites in a WAN. CCNA curriculum also includes basic mitigation of security threats, introduction to wireless networking concepts and terminology, and performance-based skills. This CCNA curriculum includes the use of various protocols, such as: IP, Open Shortest Path First (OSPF), Serial Line Interface Protocol, Frame Relay, VLANs, Ethernet, access control lists (ACLs) and others.

This course helps set the stage for networking concepts and basic routing and switching configurations and is a start on your path for CCNA certification.

Refer to **Lab Activity** for this chapter

1.4.4.3 Lab - Researching IT and Networking Job Opportunities

In this lab, you will complete the following objectives:

- Part 1: Research Job Opportunities
- Part 2: Reflect on Research

1.5 Summary

Refer to
Lab Activity
for this chapter

1.5.1.1 Class Activity - Draw Your Concept of the Internet Now

Draw Your Concept of the Internet Now

In this activity, you will use the knowledge you have acquired throughout Chapter 1, and the modeling activity document that you prepared at the beginning of this chapter. You may also refer to the other activities completed in this chapter, including Packet Tracer activities.

Draw a map of the Internet as you see it now. Use the icons presented in the chapter for media, end devices, and intermediary devices.

In your revised drawing, you may wish to include some of the following:

- WANs
- LANs
- Cloud computing
- Internet Service Providers (tiers)

Save your drawing in hard-copy format. If it is an electronic document, save it to a server location provided by your instructor. Be prepared to share and explain your revised work in class.

Refer to
Online Course
for Illustration

1.5.1.2 Summary

Networks and the Internet have changed the way we communicate, learn, work, and even play.

Networks come in all sizes. They can range from simple networks consisting of two computers, to networks connecting millions of devices.

The Internet is the largest network in existence. In fact, the term Internet means a 'network of networks'. The Internet provides the services that enable us to connect and communicate with our families, friends, work, and interests.

The network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which communication can occur. It is made up of network components including end devices, intermediate device, and network media.

Networks must be reliable. This means the network must be fault tolerant, scalable, provide quality of service, and ensure security of the information and resources on the network. Network security is an integral part of computer networking, regardless of whether the network is limited to a home environment with a single connection to the Internet, or as large as a corporation with thousands of users. No single solution can protect the network from the variety of threats that exist. For this reason, security should be implemented in multiple layers, using more than one security solution.

The network infrastructure can vary greatly in terms of size, number of users, and number and types of services that are supported on it. The network infrastructure must grow and adjust to support the way the network is used. The routing and switching platform is the foundation of any network infrastructure.

This chapter focused on networking as a primary platform for supporting communication. The next chapter will introduce you to the Cisco Internet Operating System (IOS) used to enable routing and switching in a Cisco network environment.

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