College of Computer Science and Information Technology
Department of Information Systems

IS 356 Computer Networks

Dr. Haider M. Al-Mashhadi

Course Name	**ISC356 Computer Networks**
Course Objective	**This course introduces the architecture, structure, functions, components, and models of the Internet and other computer networks. The principles and structure of IP addressing and the fundamentals of Ethernet concepts, media, and operations are introduced to provide a foundation for the curriculum. By the end of the course, students will be able to build simple LANs, perform basic configurations for routers and switches, and implement IP addressing schemes.**
Course contents	**Course Key Topic Area Includes:** **1 Explore the Network** **2 Configure a Network Operating System** **3 Network Protocols and Communications** **4 Network Access** **5 Ethernet** **6 Network Layer** **7 IP Addressing** **8 Subnetting IP Networks** **9 Transport Layer** **10 Application Layer** **11 Build a Small Network**
Learning outcomes	**At the end of the program the trainees will be able to:** **• Understand and describe the devices and services used to support communications in data networks and the Internet** **• Understand and describe the role of protocol layers in data networks** **• Understand and describe the importance of addressing**

	and naming schemes at various layers of data networks in IPv4 and IPv6 environments **• Design, calculate, and apply subnet masks and addresses to fulfill given requirements in IPv4 and IPv6 networks** **• Explain fundamental Ethernet concepts, such as media, services, and operations** **• Build a simple Ethernet network using routers and switches** **• Use Cisco command-line interface (CLI) commands to perform basic router and switch configurations** **• Utilize common network utilities to verify small network operations and analyze data traffic**

Chapter 1: Exploring the Network

1.0. 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.

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.

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.

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.

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?

1.1.1.3 No Boundaries

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.

1.1.1.4 Networks Support the Way we learn

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.

- 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. 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.

1.1.1.5 Networks Support 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.

1.1.1.6 Networks Support 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.

1.1.1.7 Networks Support 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.

1.1 Globally Connected

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. 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. 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.

Small Home Networks

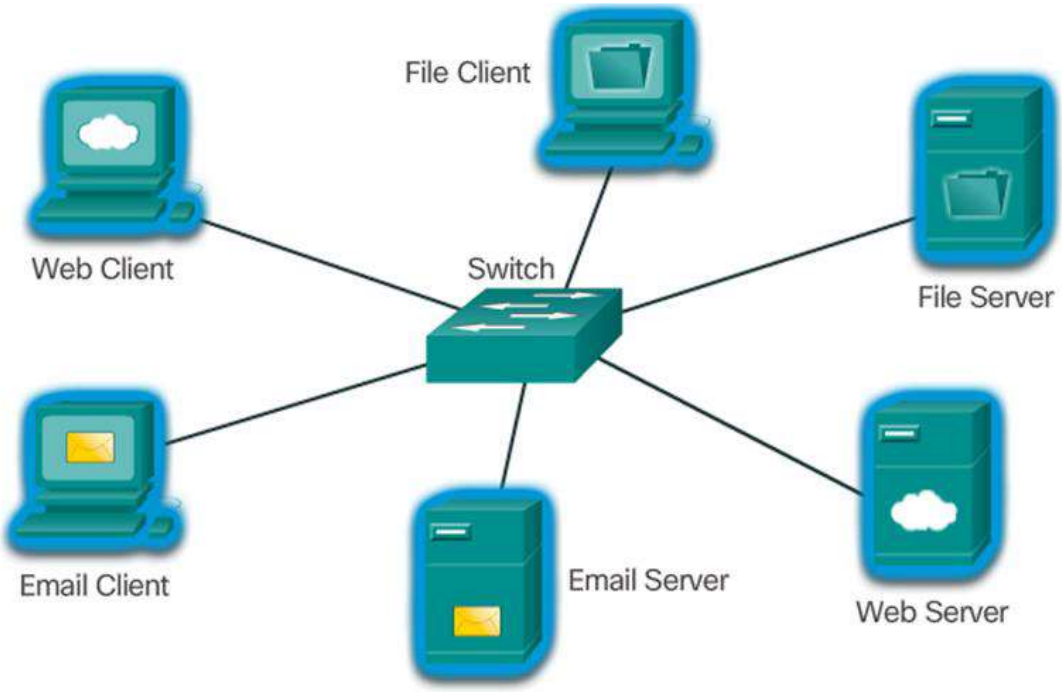
Small Office/Home Office Networks

Medium to Large Networks

World Wide Networks

1.1.2.2 Clients and Servers

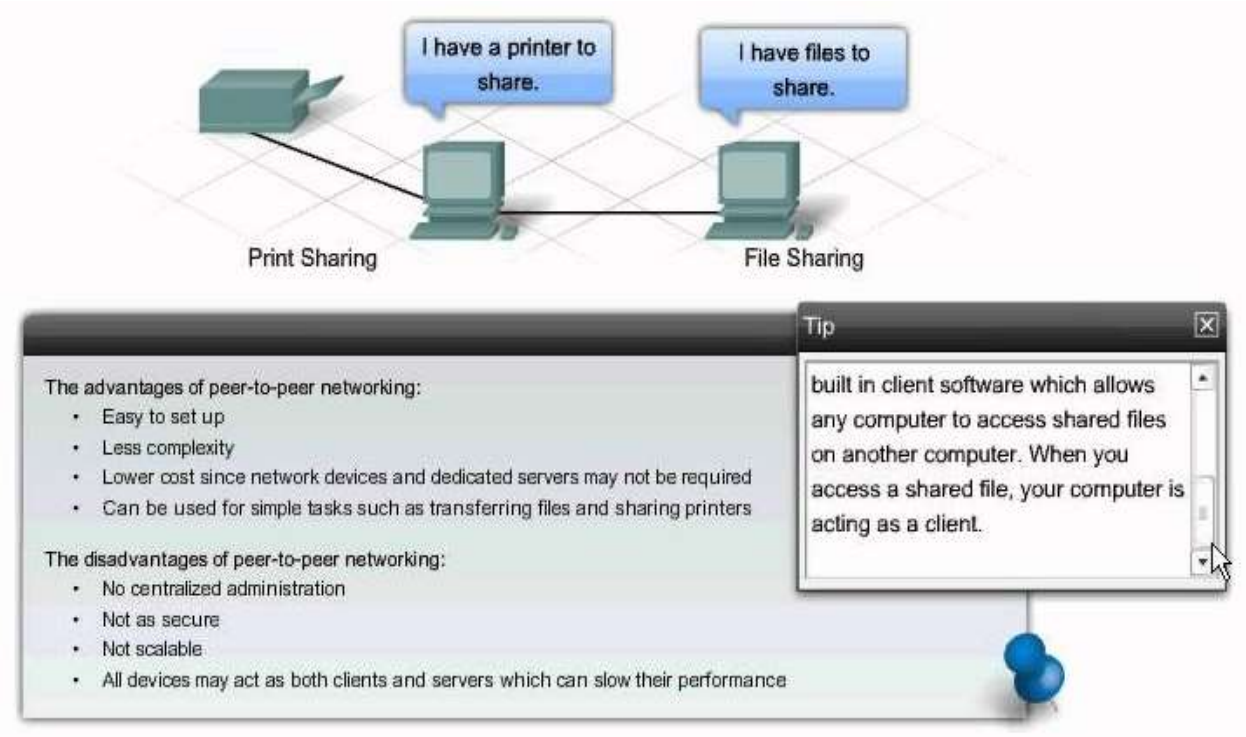
All computers connected to a network that participate directly in network communication are classified as hosts or end devices. Hosts can send and receive messages on the network. In modern networks, end devices can act as a client, a server, or both. The software installed on the computer determines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



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.

1.1.2.3 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.



1.2 LANs, WANs, and the Internet

1.2.1 Network Components

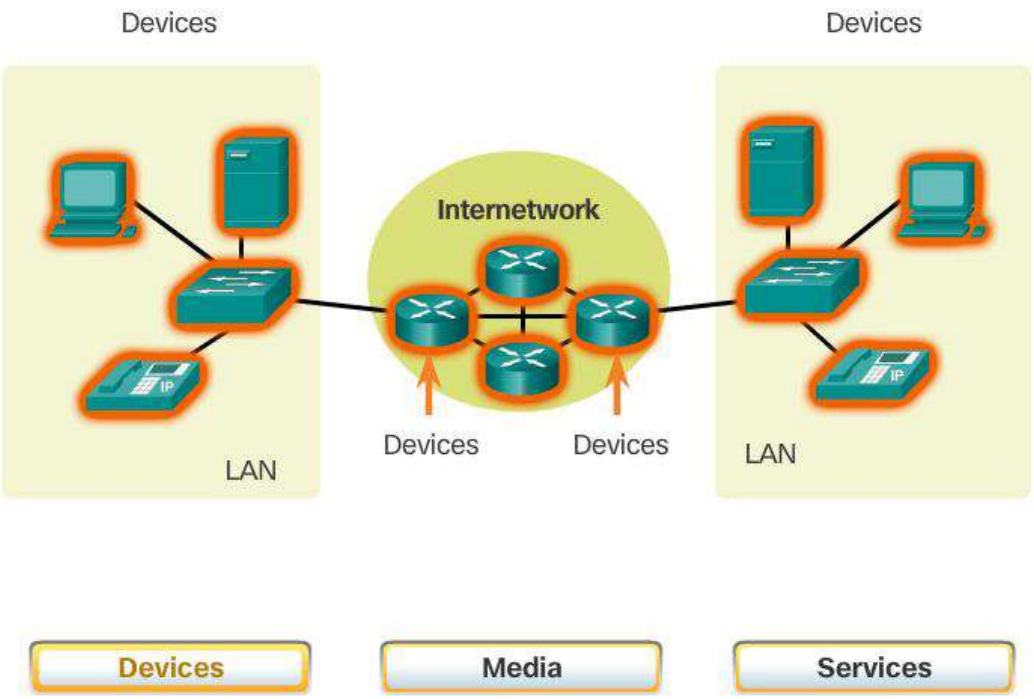
1.2.1.1 Overview of Network Components

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.

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.



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 smart phones, 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. 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.

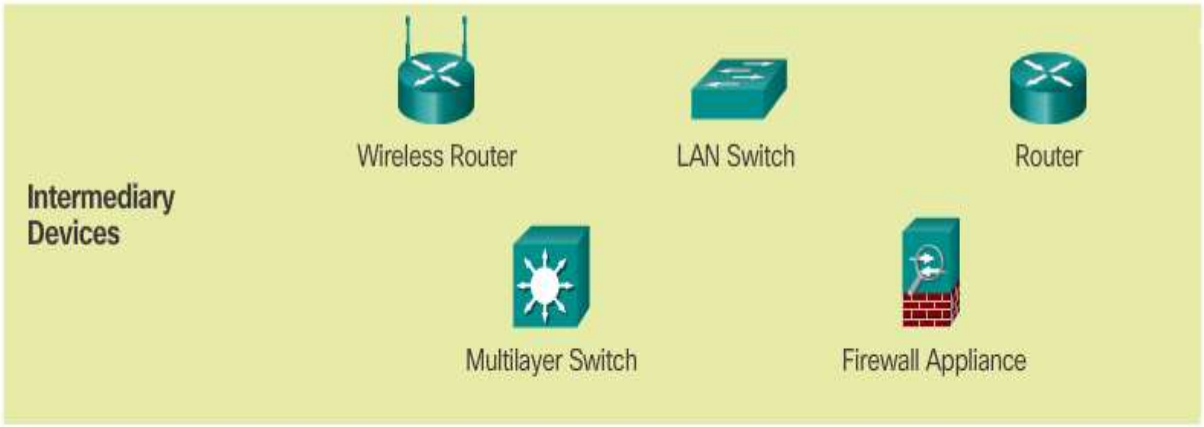
1.2.1.3 Intermediary Network Devices

Intermediary devices interconnect end devices. These devices provide connectivity and work behind the scenes to ensure that data flows across the network. 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.



Intermediary network devices perform some or all of 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 priorities
- Permit or deny the flow of data, based on security settings

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.

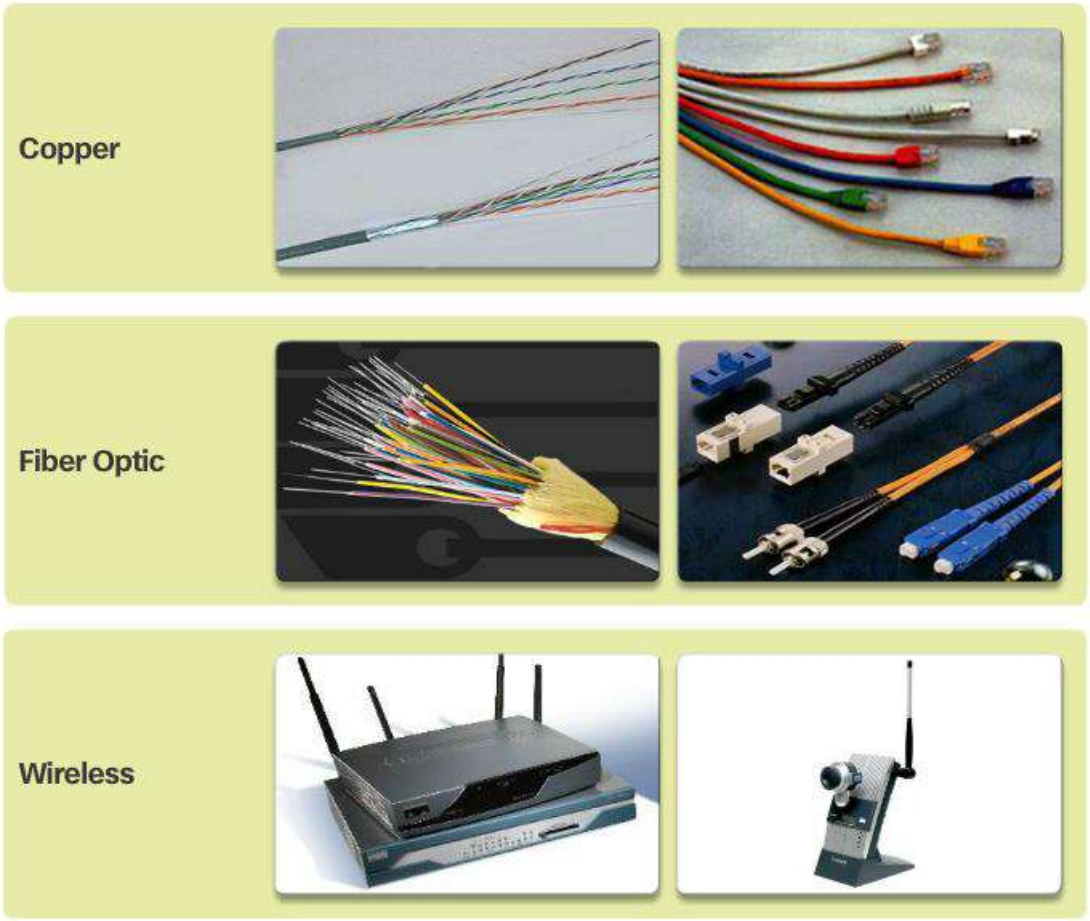
These media are:

- 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.



1.2.1.5 Network Representations

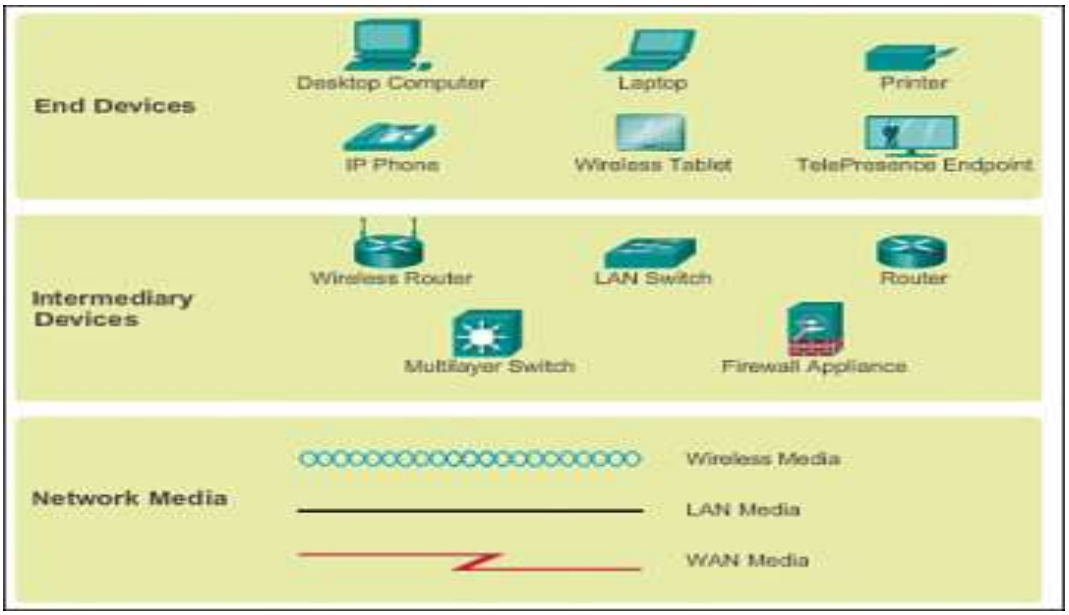
When conveying complex information such as displaying all the devices and medium in a large internetwork, it is helpful to use visual representations. A diagram provides an easy way to understand the way the devices in a large network are connected. Such a diagram uses symbols to represent the different 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. 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.

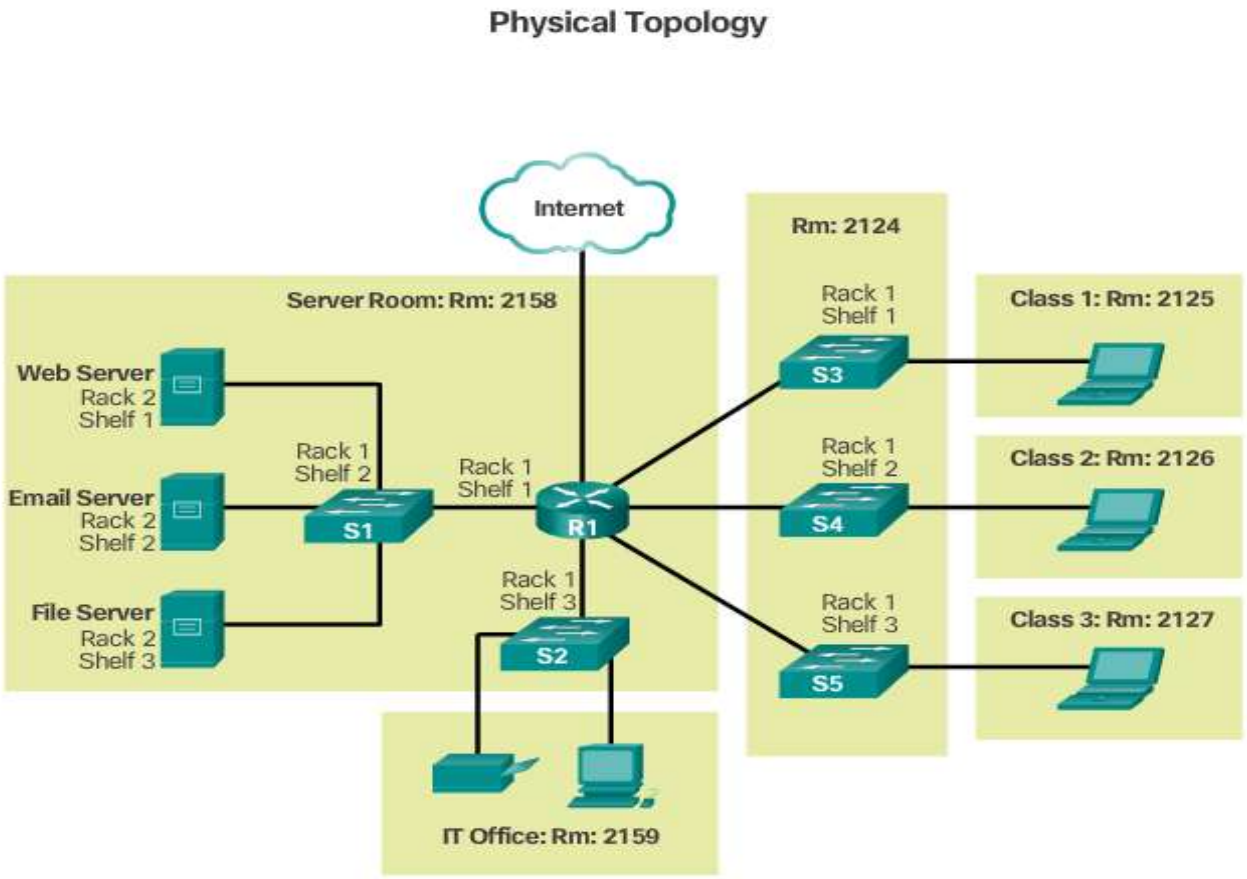
- **Interface** - Specialized ports on an internetworking device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to network interfaces.



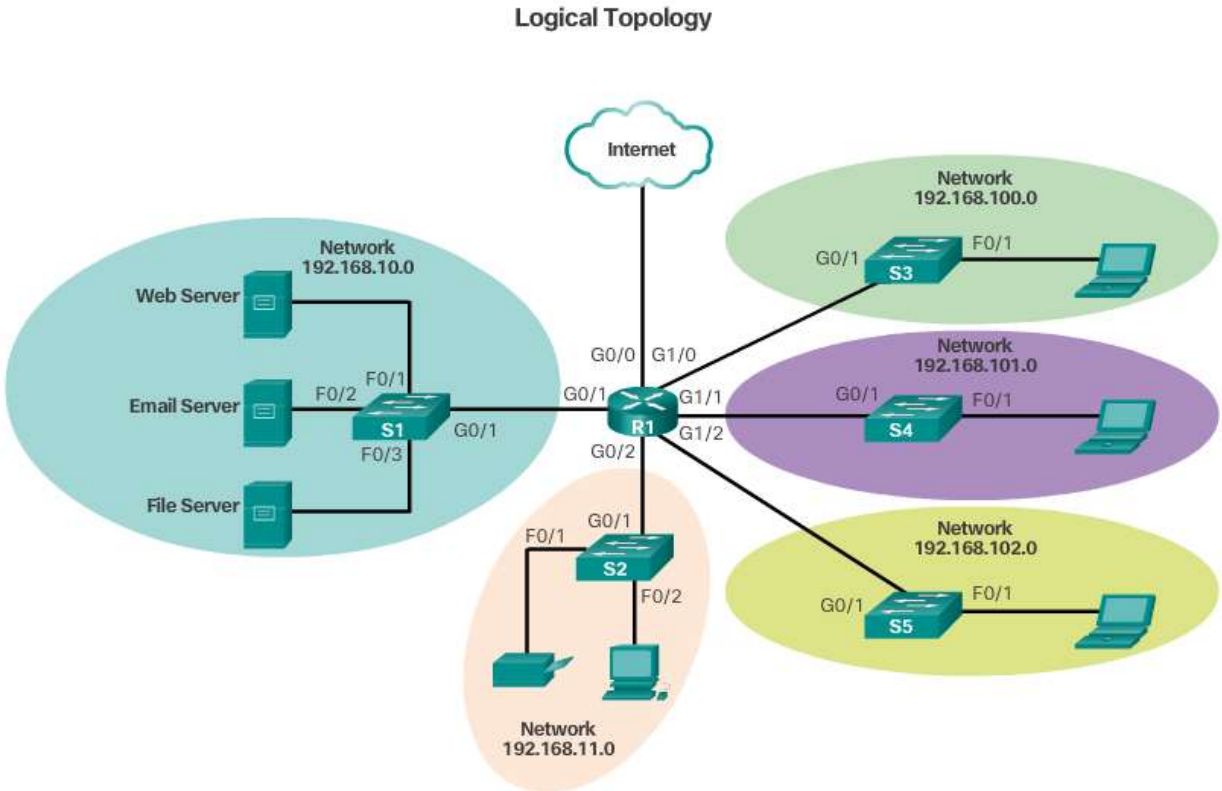
1.2.1.6 Topology Diagrams

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.

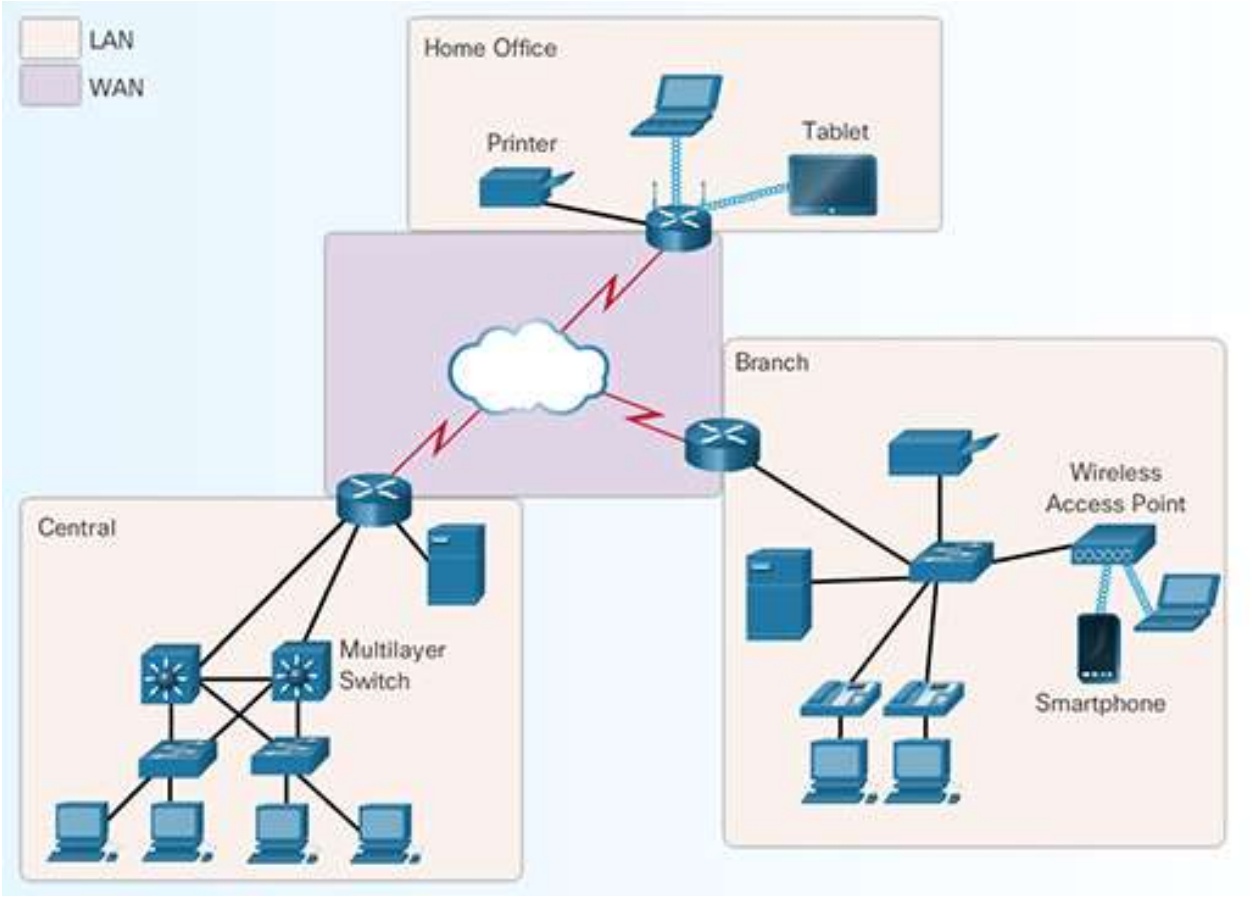


- **Logical topology diagrams** - Identify devices, ports, and IP addressing scheme.



LANs, WANs, and the Internet 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.

There are 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.

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.

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.

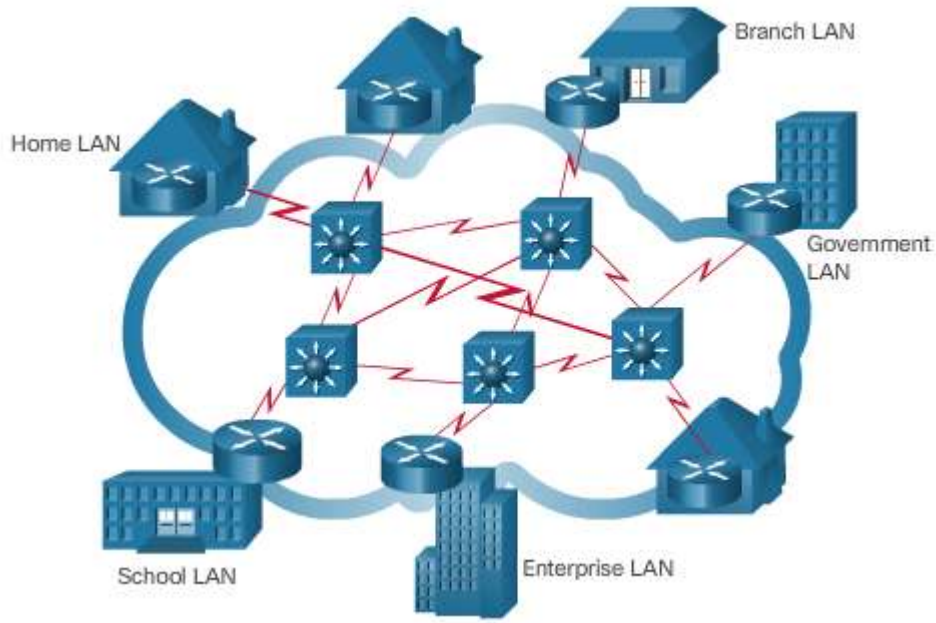
- WANs are usually administered by multiple service providers.

- WANs typically provide slower speed links between LANs.

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.

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.

1.2.3.2 Intranet and Extranet

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

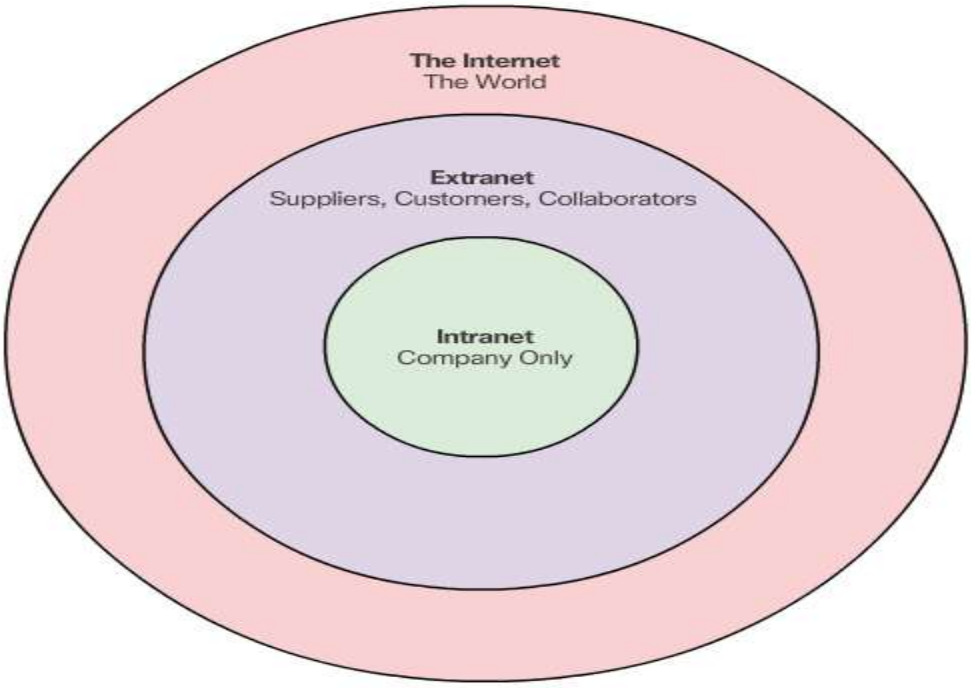
- Intranet.
- Extranet.

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.

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.

LANs, WANs, and the Internet 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 Home and Small Office Internet Connections

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.

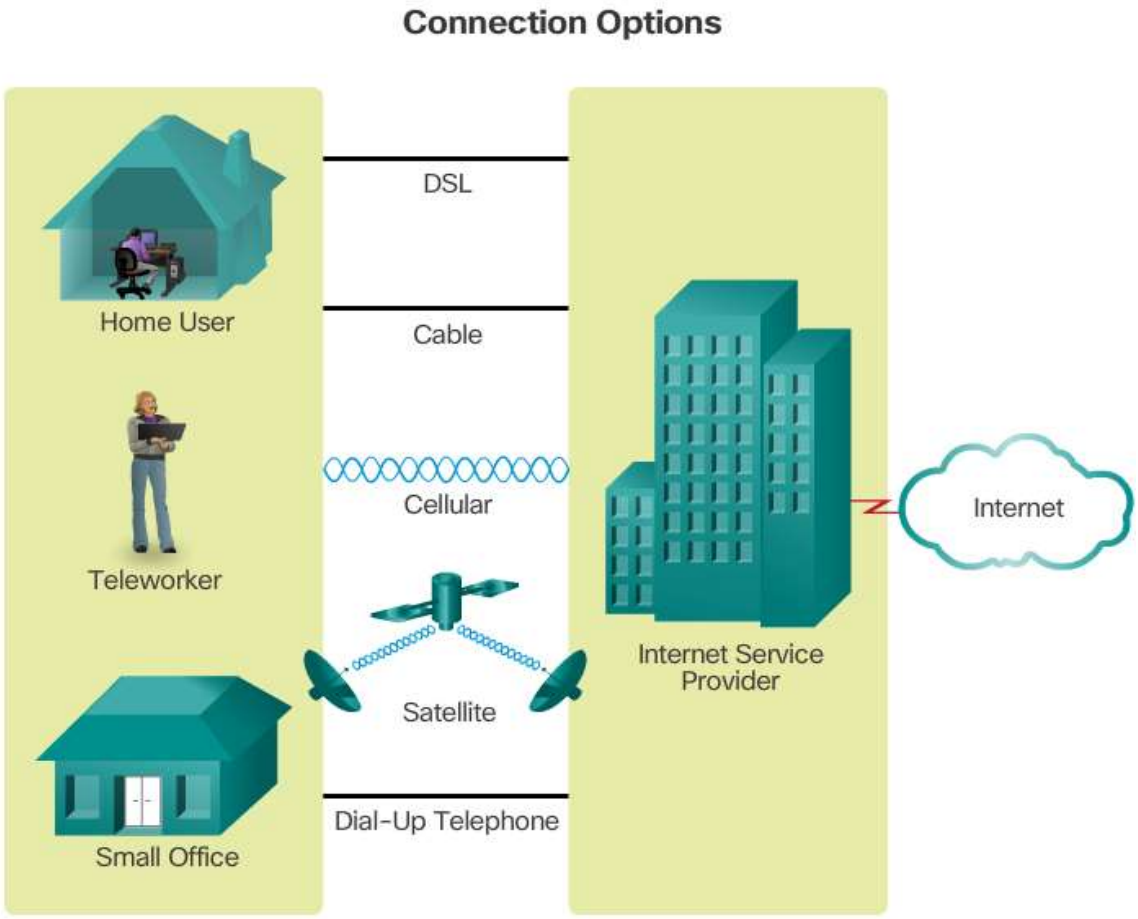
- **DSL** - Digital Subscriber Lines provide a high bandwidth, always on, connection to the Internet. DSL runs over a telephone line. In general, small office and home office users connect using Asymmetrical DSL (ADSL), which means that the download speed is faster than the upload speed.

- **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.
- **Satellite** - The availability of satellite Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all. Satellite dishes require a clear line of sight to the satellite.

- **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.

Many homes and small offices are more commonly being connected directly with *fiber 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.



1.2.4.3 Businesses Internet Connection

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. Common connection options for organizations, which include:

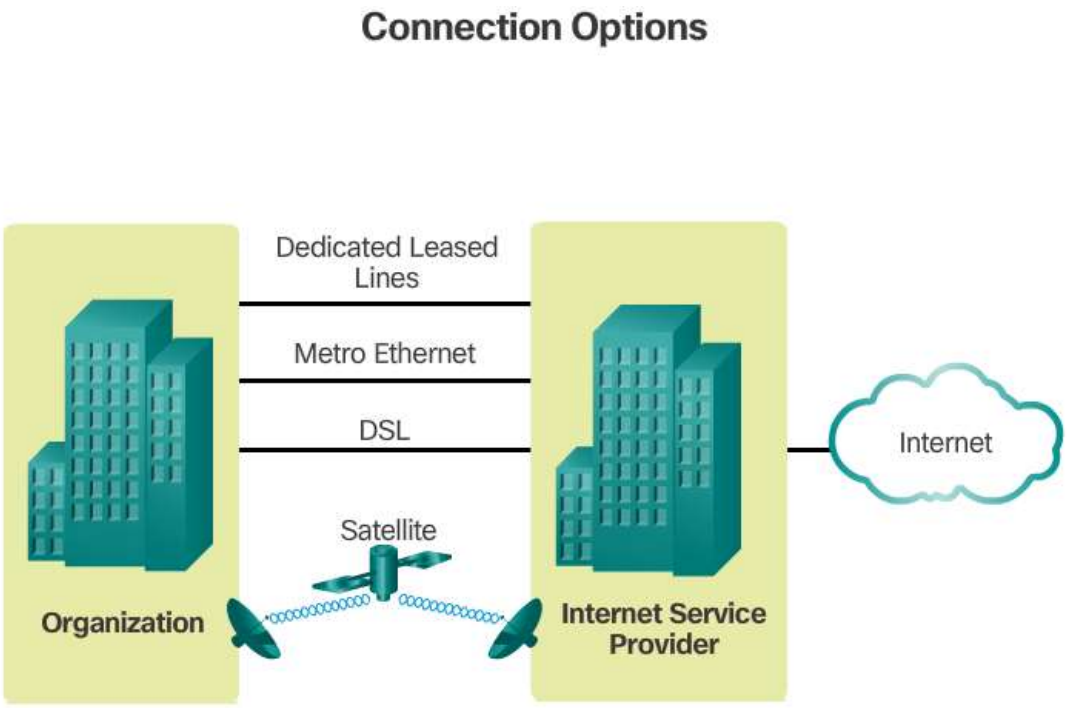
- **Dedicated Leased Line** - Leased lines are actually reserved circuits within the service provider's network that connect geographically separated offices for private voice and/or data networking. The circuits are typically rented at a monthly or yearly rate. They can be expensive.

- **Ethernet WAN**- Ethernet WANs extend LAN access technology into the WAN. The benefits of Ethernet are now being extended into the WAN.

- **DSL** - Business DSL is available in various formats. A popular choice is Symmetric Digital Subscriber Lines (SDSL) which is similar to the consumer version of DSL, but provides uploads and downloads at the same speeds.

- **Satellite** - Similar to small office and home office users, satellite service can provide a connection when a wired solution is not available.

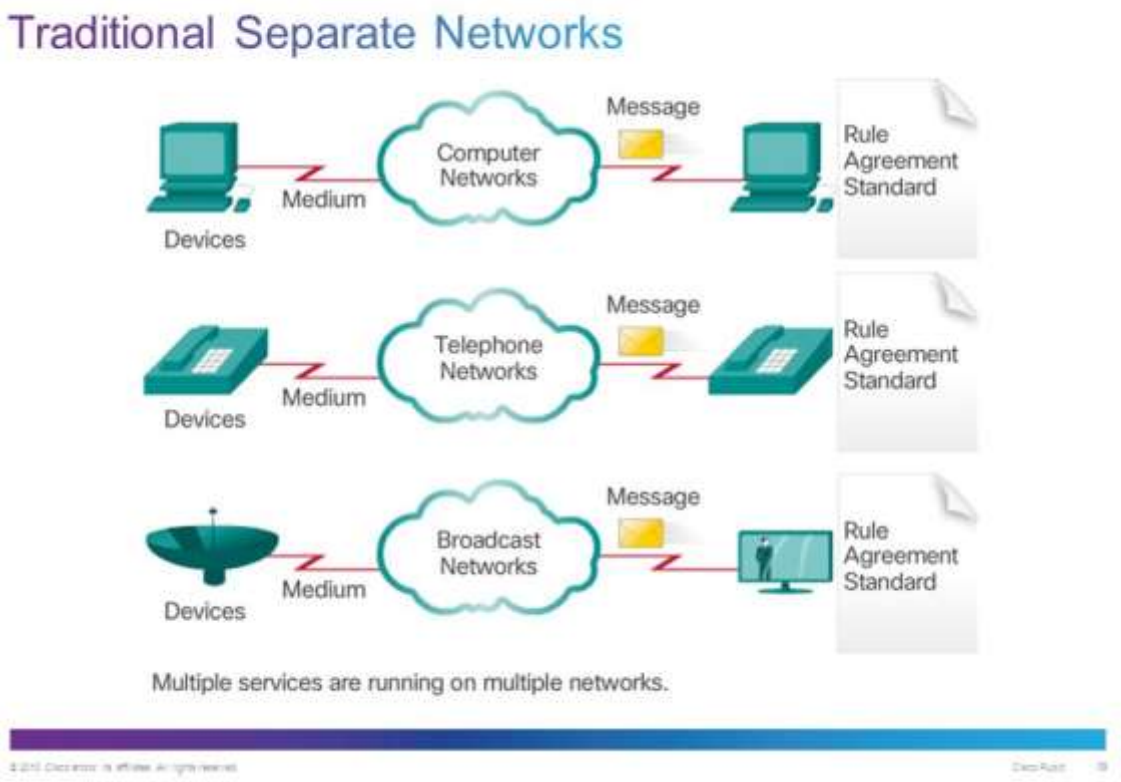
The choice of connection varies depending on geographical location and service provider availability.



1.3 The Network as a Platform

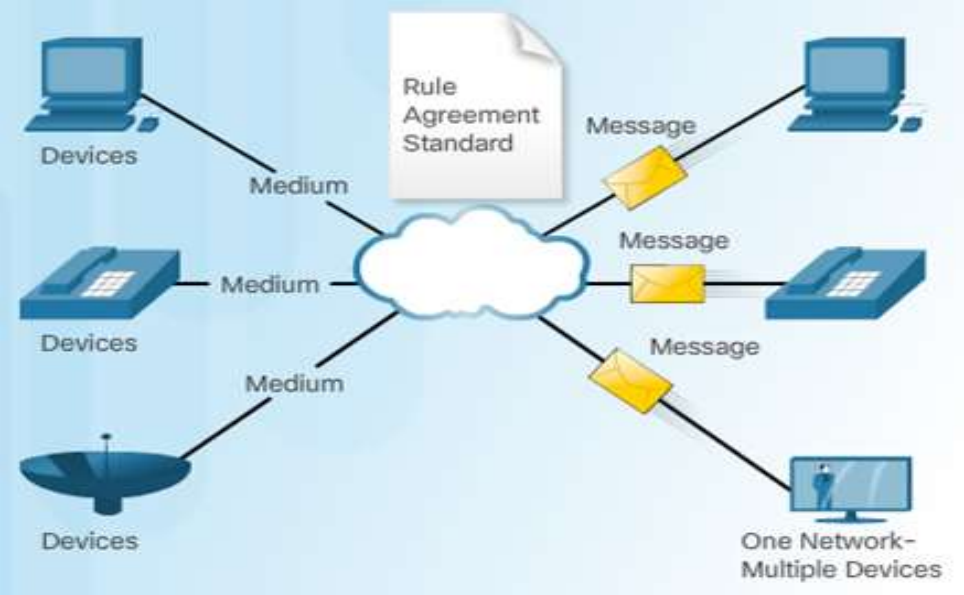
1.3.1 Converged Network

1.3.1.1 Traditional Separate Networks



Consider a school built thirty years ago. Back then, some classrooms were cabled for the data network, telephone network, and video network for televisions. These separate networks could not communicate with each other, as shown in the figure. Each network used different technologies to carry the communication signal. Each network had its own set of rules and standards to ensure successful communication.

1.3.1.2 The Converging Networks

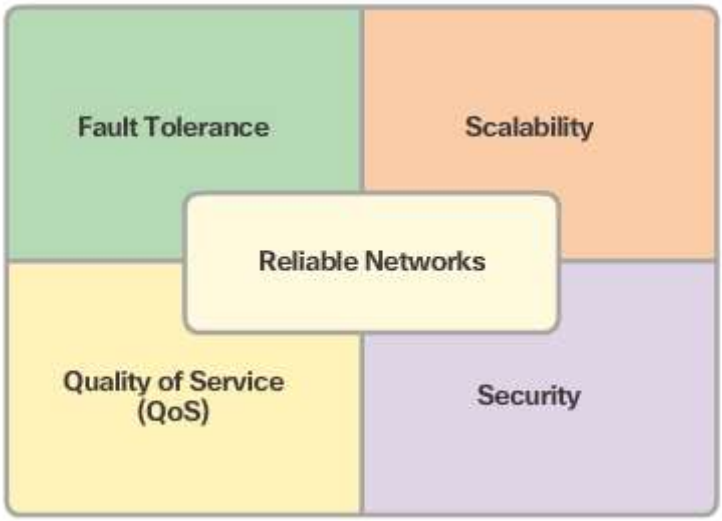


Today, the separate data, telephone, and video networks are converging. Unlike dedicated networks, converged networks are capable of delivering data, voice, and video between many different types of devices over the same network infrastructure, as shown in the figure. This network infrastructure uses the same set of rules, agreements, and implementation standards

1.3.2.1 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.
- Scalability.
- Quality of Service (QoS).
- Security**.**

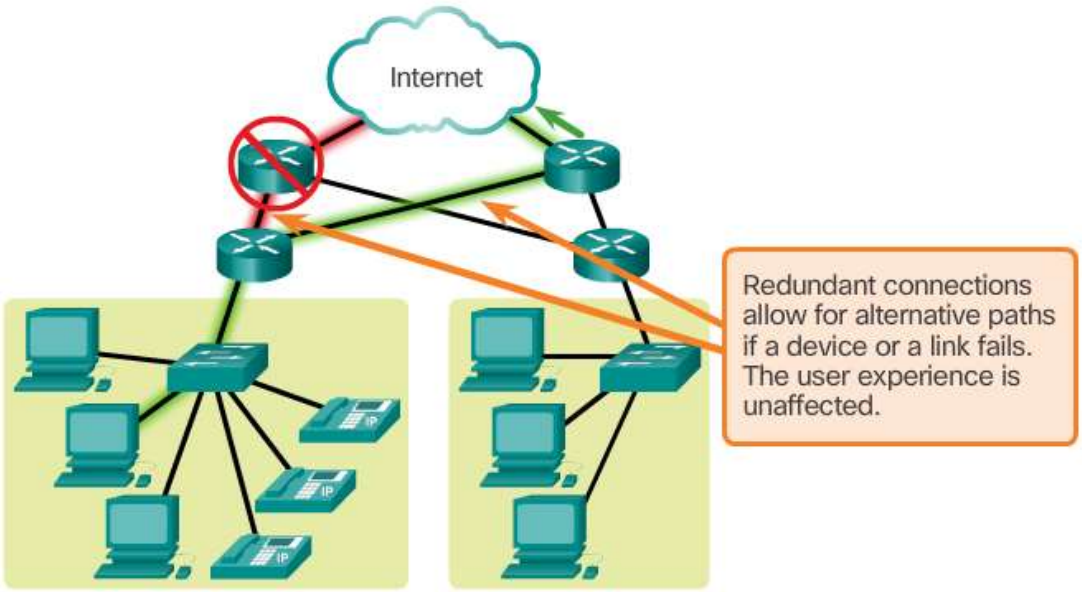


1.3.2.2 Fault Tolerance

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. 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.

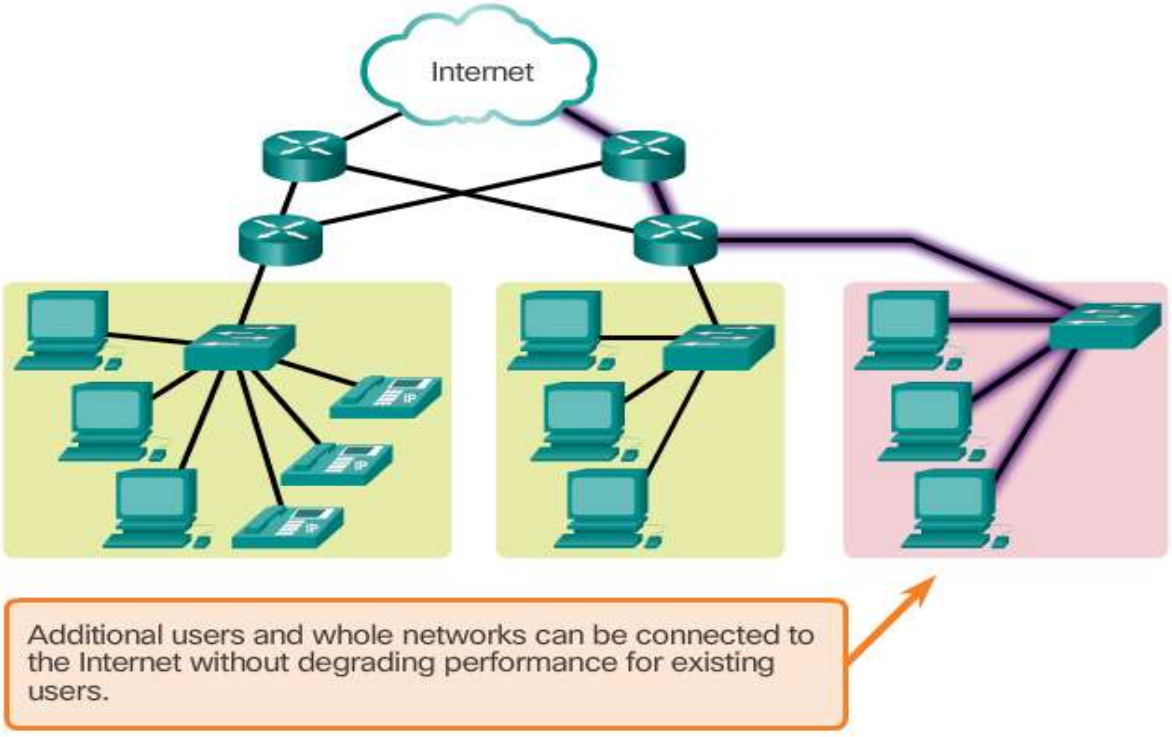
One way reliable networks provide redundancy is by implementing a packet-switched network. Packet switching splits traffic into packets that are routed over a shared network. A single message, such as an email or a video stream, is broken into multiple message blocks, called packets. Each packet has the necessary addressing information of the source and destination of the message. The routers within the network switch the packets based on the condition of the network at that moment. This means that all the packets in a single message could take very different paths to the destination. In the figure, the user is not aware and is unaffected by the router dynamically changing the route when a link fails.

This is not the case in circuit-switched networks traditionally used for voice communications. A circuit-switched network is one that establishes a dedicated circuit between the source and destination before the users may communicate. If the call is unexpectedly terminated, the users must initiate a new connection.



1.3.2.3 Scalability

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 figure shows how a new network can be easily added to an existing network. In addition, networks are scalable because the designers follow accepted standards and protocols. This allows software and hardware vendors to focus on improving products and services without worrying about designing a new set of rules for operating within the network.



1.3.2.5 Quality of Service

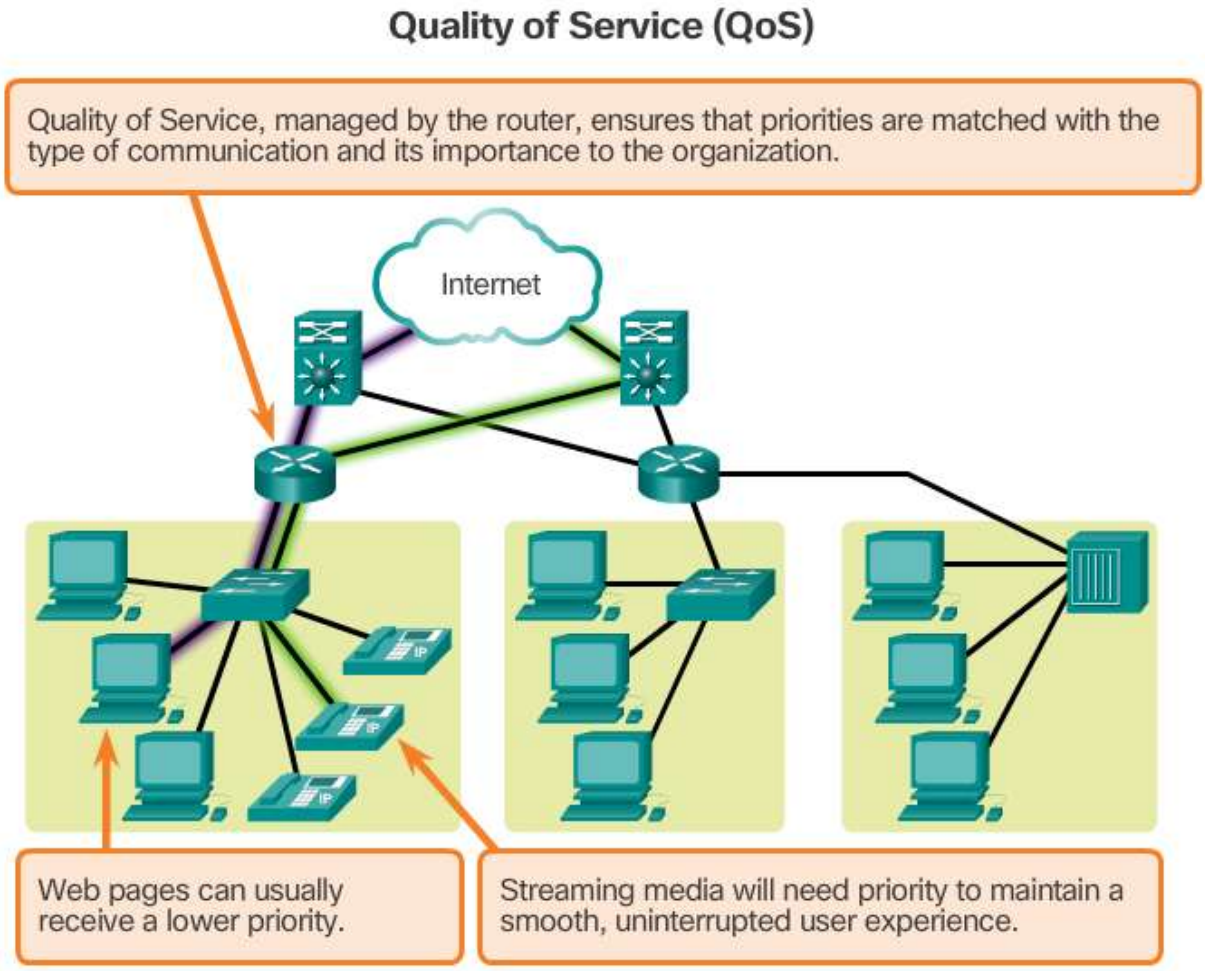
Providing QoS *Quality of Service (QoS) is also an ever increasing requirement of networks today. New application available to users over internetworks, such as voice and live video transmissions, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video 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. 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. 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.



1.3.2.6 Security

The network infrastructure, services, and the data contained on network-attached devices are crucial personal and business assets. There are two types of network security concerns that must be addressed: network infrastructure security and information security.

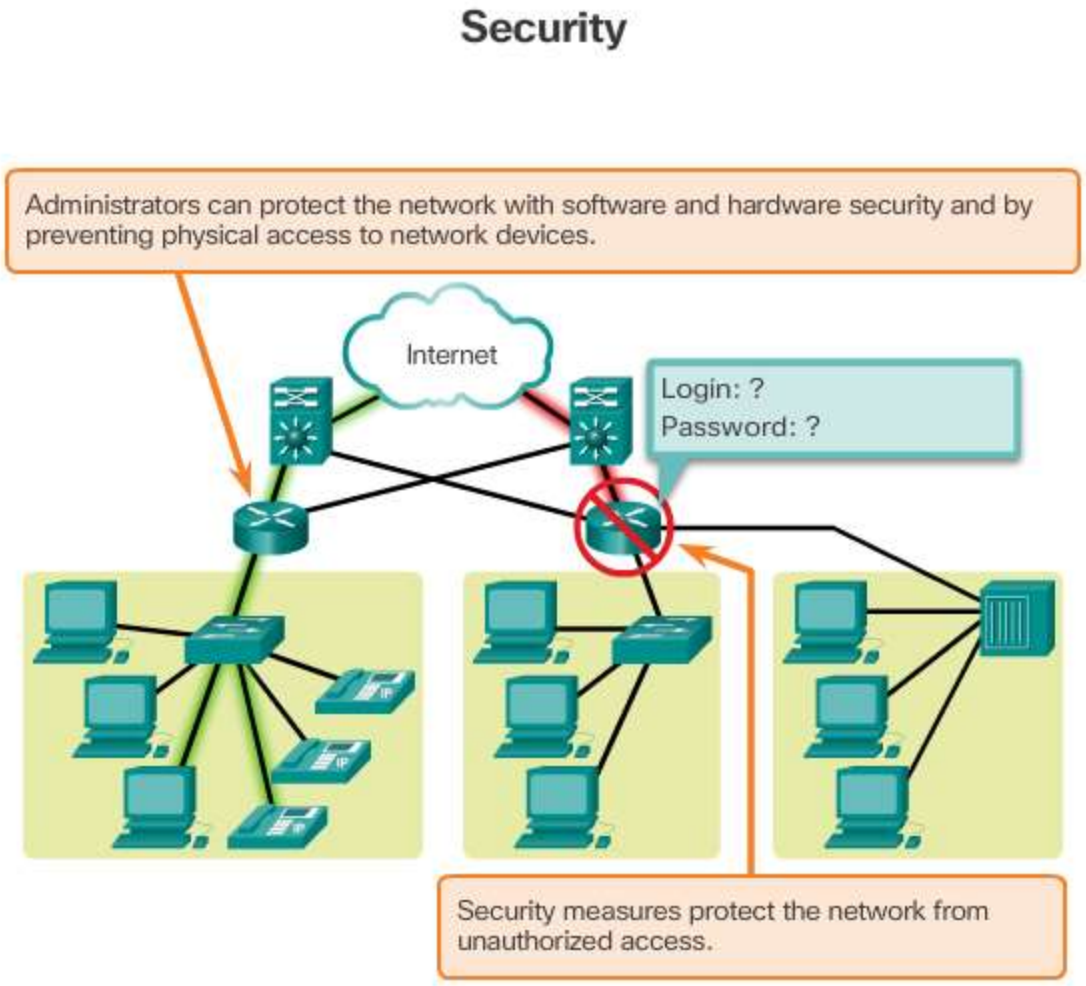
Securing a network infrastructure includes the physical securing of devices that provide network connectivity, and preventing unauthorized access to the management software that resides on them, as shown in Figure 1.

Information security refers to protecting the information contained within the packets being transmitted over the network and the information stored on network attached devices. In order to achieve the goals of network security, there are three primary requirements, as shown in Figure 2:

- **Confidentiality** - Data confidentiality means that only the intended and authorized recipients can access and read data.

- **Integrity** - Data integrity means having the assurance that the information has not been altered in transmission, from origin to destination.

- **Availability** - Data availability means having the assurance of timely and reliable access to data services for authorized users.



1.4 The Changing Network Environment

1.4.1 Network Trends

1.4.1.1 New Trends

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 between people, devices, and information. There are several new networking trends that will effect organizations and consumers. Some of the top trends include:

- Bring Your Own Device (BYOD)
- Online collaboration
- Video communications
- Cloud computing

1.4.1.2 Bring Your Own Device

The concept of any device, to any content, in any manner, 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.

1.4.1.3 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 that organizations are using to remain competitive. 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.

1.4.1.4 Video Communication

Another trend in networking that is critical to the communication and collaboration effort is video. Video is being used for communications, collaboration, and entertainment. Video calls can be made to and from anywhere with an Internet connection.

Video conferencing is a powerful tool for communicating with others at a distance, both locally and globally. Video is becoming a critical requirement for effective collaboration as organizations extend across geographic and cultural boundaries.

1.4.1.5 Cloud Computing

Cloud computing is another global trend changing the way we access and store data. 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.

There are four primary types of Clouds, as shown in the figure: Public Clouds, Private Clouds, Hybrid Clouds, and Custom Clouds.

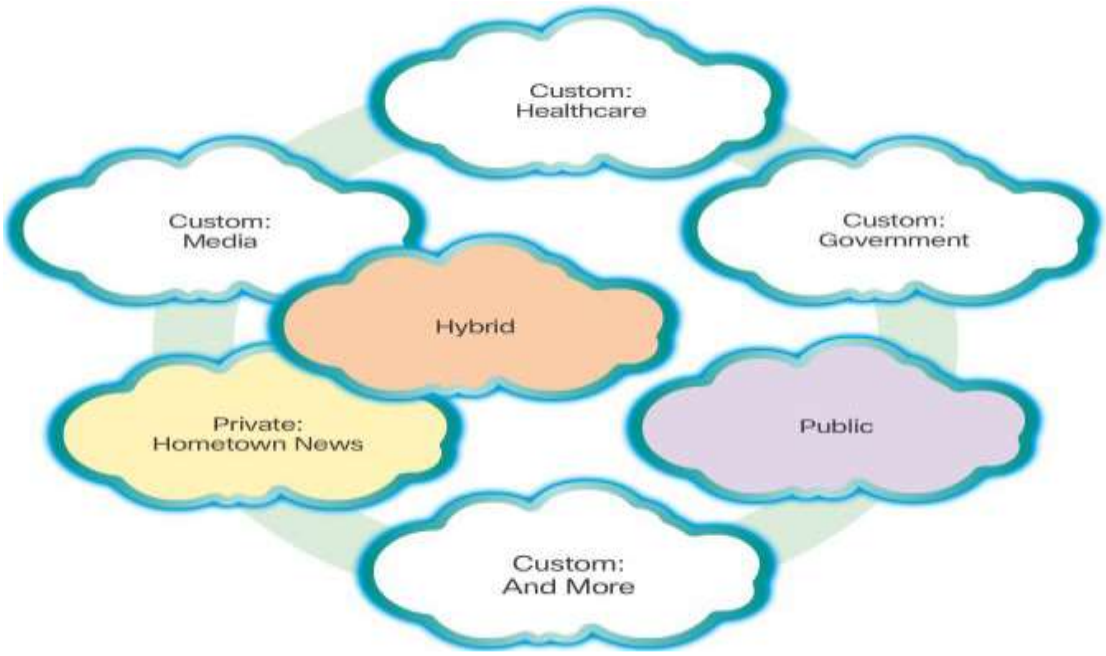
Cloud computing is possible because of data centers. A data center is a facility used to house computer systems and associated components. A data center can occupy one room of a building, one or more floors, or an entire building. Data centers are typically very expensive to build and maintain. For this reason, only large organizations use privately built data centers to house their data and provide services to users. 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.

Cloud computing offers the following potential benefits:

- **Organizational flexibility** - Users can access the information anytime and anyplace using a web browser.

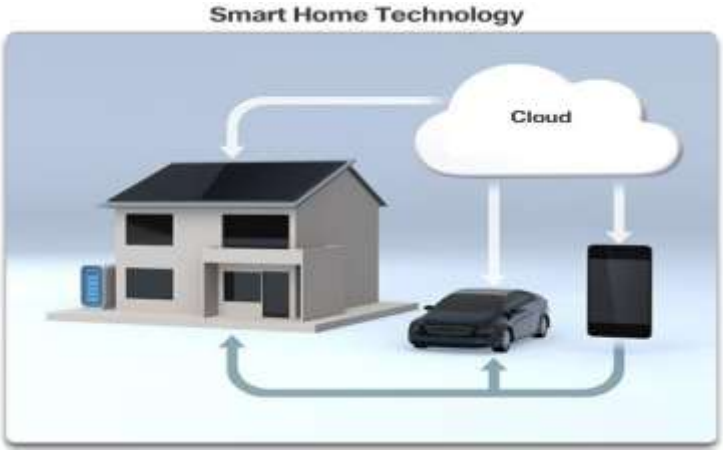
- **Agility and rapid deployment** - IT department can focus on delivering the tools to mine, analyze, and share the information and knowledge from databases, files, and people.
- **Reduced cost of infrastructure** - Technology is moved from on-site to a cloud provider, eliminating the cost of hardware 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.



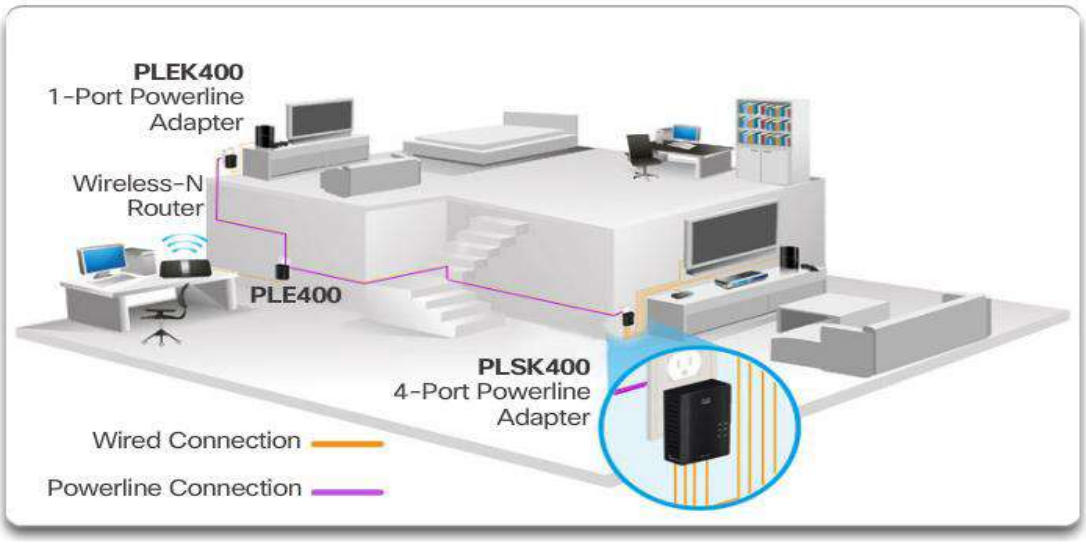
1.4.2.1 Technology Trends in the Home

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.



1.4.2.2 Powerline Networking

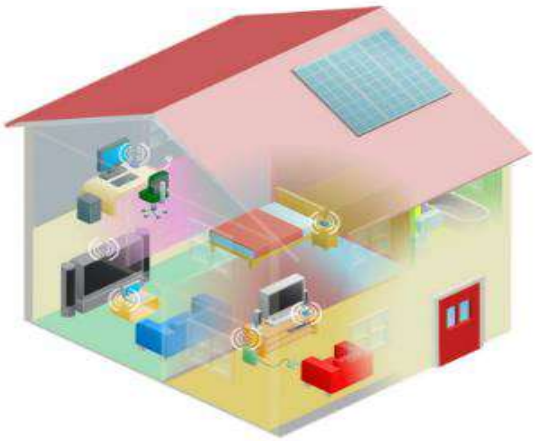
Powerline networking is an emerging trend for home networking that uses existing electrical wiring to connect devices. The concept of "no new wires" means the ability to connect a device to the network wherever there is an electrical outlet. This saves the cost of installing data cables and without any 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.



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.



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.

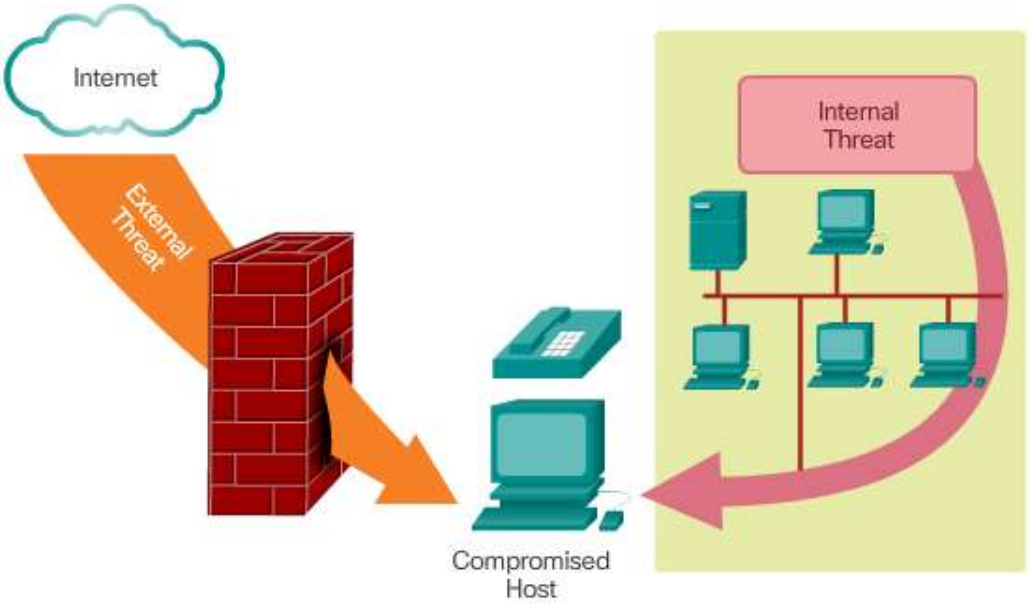
- **Spyware and adware** - software installed on a user device that secretly collects information about the user.

- **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.



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.