Elk Technologies
https://elktech.org
Scott Stephenson

Module 1: Networking Today

Introduction to Networks

Cisco | Networking Academy®
Mind Wide Open™

Module Objectives

- Module Title: Networking Today
- Module Objective: Explain the advances in modern technologies.

Topic Title	Topic Objective
1.1 Networks Affect our Lives	Explain how networks affect our daily lives.
1.2 Network Components	Explain how host and network devices are used.
1.3 Network Representations and Topologies	Explain network representations and how they are used in network topologies.
1.4 Common Types of Networks	Compare the characteristics of common types of networks.
1.5 Internet Connections	Explain how LANs and WANs interconnect to the internet.
1.6 Reliable Networks	Describe the four basic requirements of a reliable network.
1.7 Network Trends	Explain how trends such as BYOD, online collaboration, video, and cloud computing are changing the way we interact.
1.8 Network Security	Identify some basic security threats and solution for all networks.
1.9 The IT Professional	Explain employment opportunities in the networking field.

1.1 Networks Affect Our Lives

Networks Connect Us

- 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.
- Networks support the way we:
  - Learn
  - Communicate
  - Work
  - Play

No Boundaries

- Advancements in networking technologies are helping create a world without boundaries.
- The immediate nature of communications over the Internet encourages global communities.
- Cisco refers to the impact of the Internet and networks on people the “human network”.

Networks Support the Way We Communicate

- The globalization of the Internet has empowered individuals to create information that can be accessed globally.
- Forms of communication:
  - **Texting** – the act of sending text and other visual/audio information from one cell phone to another.
  - **Podcast** – an audio-based medium that allows people to deliver their recordings to a wide audience.
  - **Social Media** – interactive websites where people create and share user-generated content with friends and family.
  - **Wiki** – web pages that groups of people can edit and view together.
  - **Instant Messaging** – real-time communication between two or more people.
  - **Weblog** (blog) – a discussion or informational site published on the web and consisting of discrete entries called posts.

1.2 Network Components

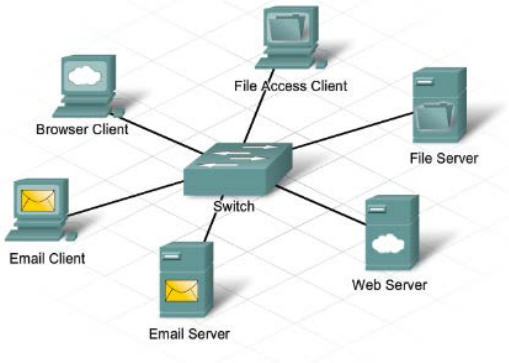
Host Roles

- Every computer on a network is called a host, node, client, or end device.
- Clients are computers that send requests to the servers to retrieve information:
  - Web page from a web server
  - Email from an email server
  - File from a file server

Server Type	Description
Email	Email server runs email server software. Clients use client software to access email.
Web	Web server runs web server software. Clients use browser software to access web pages.
File	File server stores corporate and user files. The client devices access these files.

Client/Server

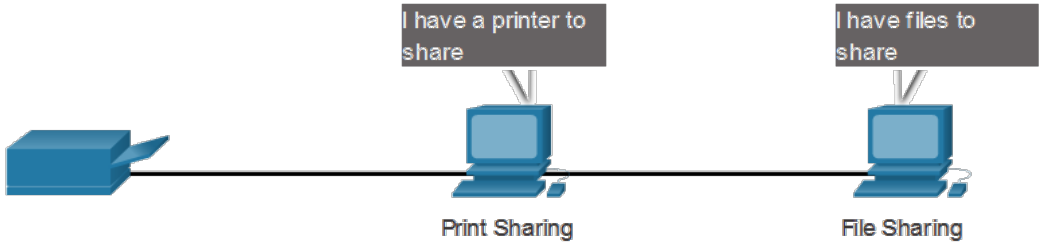
- Server software runs on dedicated computers.
- Servers are computers that provide information to end devices on the network.
- Servers provide information to other devices on the network.



- Advantages:
  - Can provide services simultaneously to one or many clients
  - Can run multiple types of software and services
  - Add security
- Disadvantages:
  - More Devices
  - More complex
  - Single point of failure

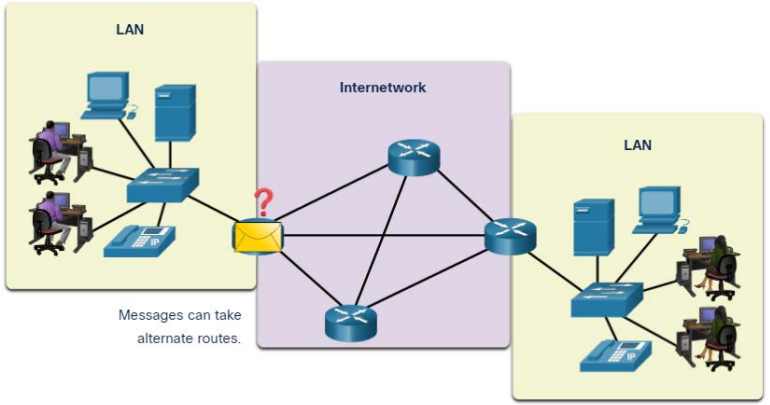
Peer-to-Peer

- It is possible to have a device be a client and a server in a **Peer-to-Peer** Network.
- This type of network design is only recommended for very small networks.
- No device is in control
- Advantages:
  - Easy to create/set up
  - Less cost to implement
  - Less complexity
  - Use for simple tasks (file transfer or printer sharing)
- Disadvantages:
  - Lacks centralized administration
  - Not as secure
  - Not scalable
  - Acting as both client and server can slow down performance



End Devices

- An end device is where a message originates from or where it is received.
- Data originates with an end device, flows through the network, and arrives at an end device.
- Functions of end devices on a network:
  - Either the source or destination of a message
  - Originate the data that flows through the network
  - The interface between humans and the communication network
- Examples of end devices:
  - 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)



Intermediary Network Devices

- Functions of intermediary devices on a network:
  - Provide connectivity – Ensure data flows across the network
  - Direct the path of the data
  - Connect the individual end devices/hosts to the network
  - Connect multiple individual networks to form an internetwork
  - They filter the flow of data based on security settings
- Examples of intermediary network devices:
  - Network Access Devices (switches, and wireless access points)
  - Internetworking Devices (routers)
  - Security Devices (firewalls)
- Management of data as it flows through a network is also the role of an intermediary device, including:
  - Regenerate and retransmit data signals.
  - Maintain information about what pathways exist in the network.
  - Notify other devices of errors and communication failures.

Network Components

- **Repeater** – (Layer 1) Extends the range of a signal by receiving then regenerating it and sending it out all other ports. Allows for collisions on the network segment

- **Hub** – (Layer 1) A multiport repeater or concentrator

- **Bridge** – (Layer 2) Has the intelligence to determine if an incoming frame is to be sent to a different segment, or dropped. Makes forwarding decisions based on the destination MAC address that is contained in the frame. A bridge has two ports

- **Switch** – (Layer 2) A multiport bridge. Has several ports and refers to a table of MAC addresses to determine which port to use to forward the frame

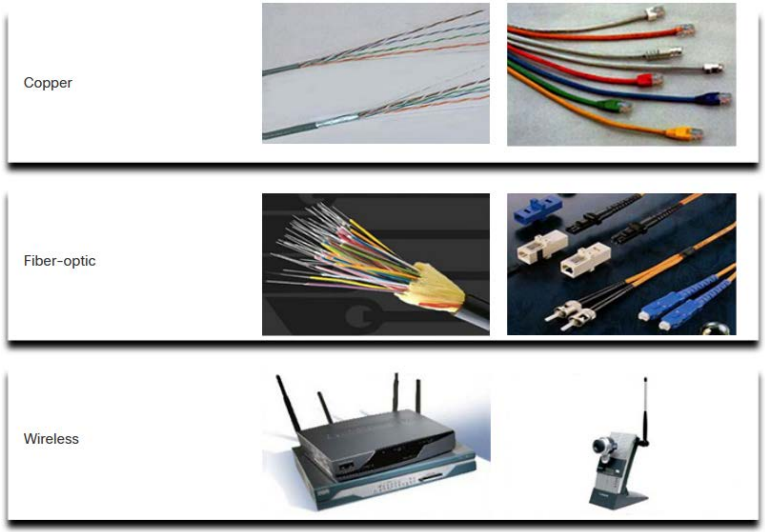
Network Components

- **Router** – (Layer 3) Connect networks to each other. They use IP addresses to forward packets to other networks. Performs the function of determining the path that messages should take through internetworks

- **Firewall** – (Layer 4) A software or hardware device that protects networks by blocks incoming packets. Makes intelligent decisions based on port numbers or protocols

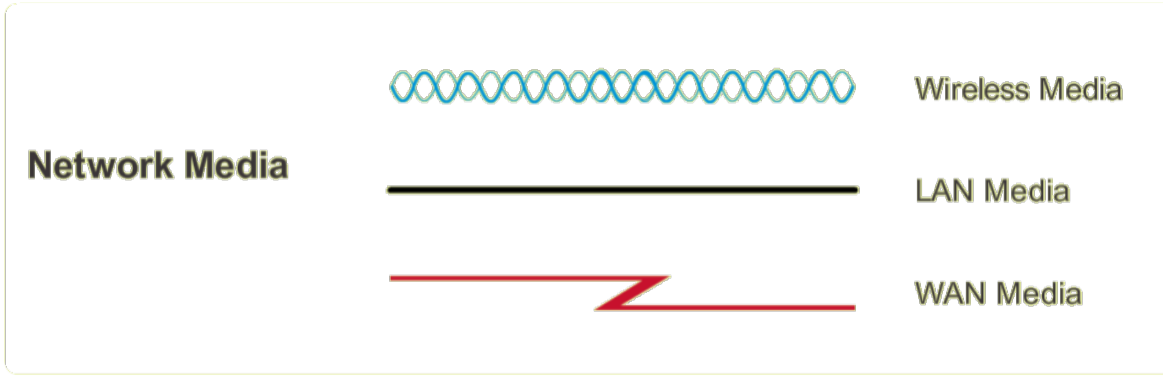
Network Media

- Provide the pathway for data transmission
- Interconnect devices
- Communication across a network is carried through a **medium** which allows a message to travel from source to destination:
  - **Metal wires within cables** (copper cable) – uses electrical impulses waves
  - **Glass or plastic fibers within cables** (fiber-optic cable) – uses pulses of light
  - **Wireless transmission** – uses modulation of specific frequencies of electromagnetic



Network Media

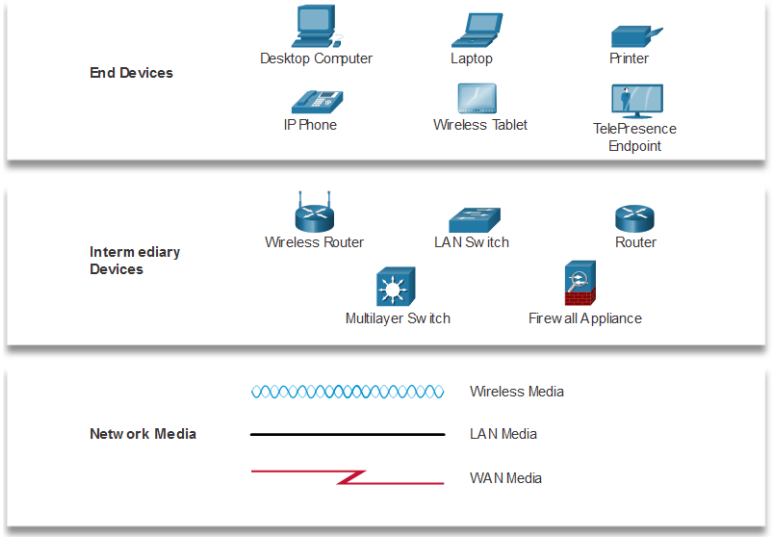
- Criteria to consider when choosing network media:
  - The maximum distance that the media can successfully carry a signal.
  - The environment in which the media will be installed.
  - The amount of data and at what speed must it be transmitted.
  - The cost of the media and installation.



1.3 Network Representations and Topologies

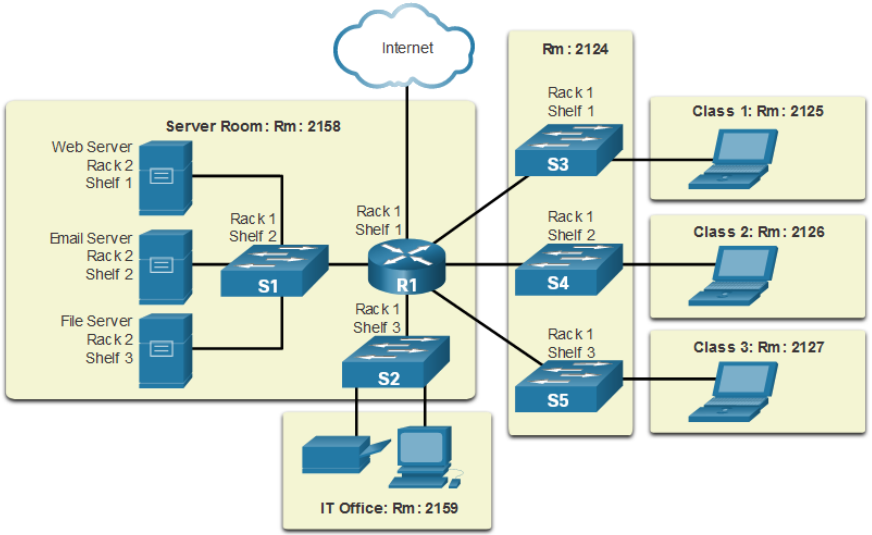
Network Representations

- **Network diagrams**, often called **topology diagrams**, use symbols to represent devices within the network.
- Important terms to know include:
  - Network Interface Card (NIC)
  - Physical Port
  - Interface
- Often, the terms port and interface are used interchangeably.

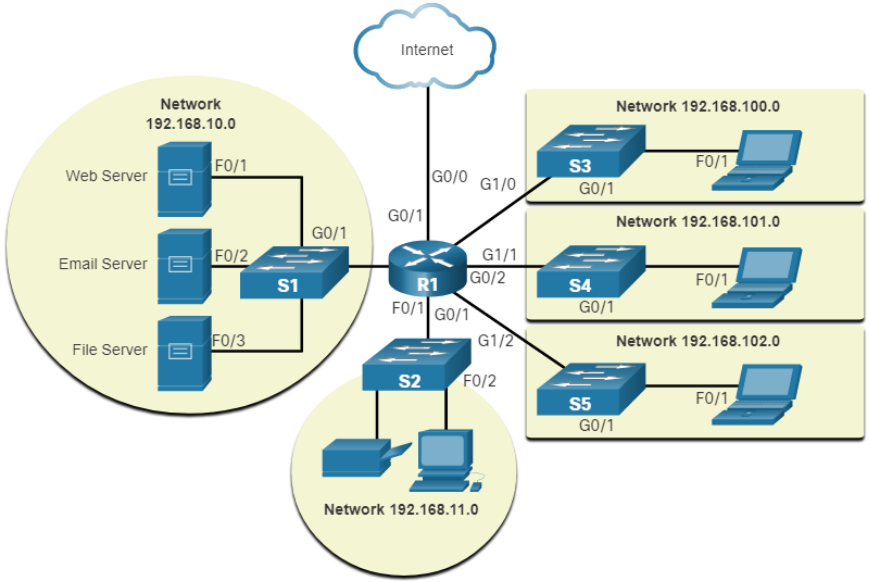


Topology Diagrams

Physical topology diagrams illustrate the physical location of intermediary devices and cable installation.



Logical topology diagrams illustrate devices, ports, and the IP addressing scheme of the network.



1.4 Common Types of Networks

Networks of Many Sizes

Small Home

SOHO

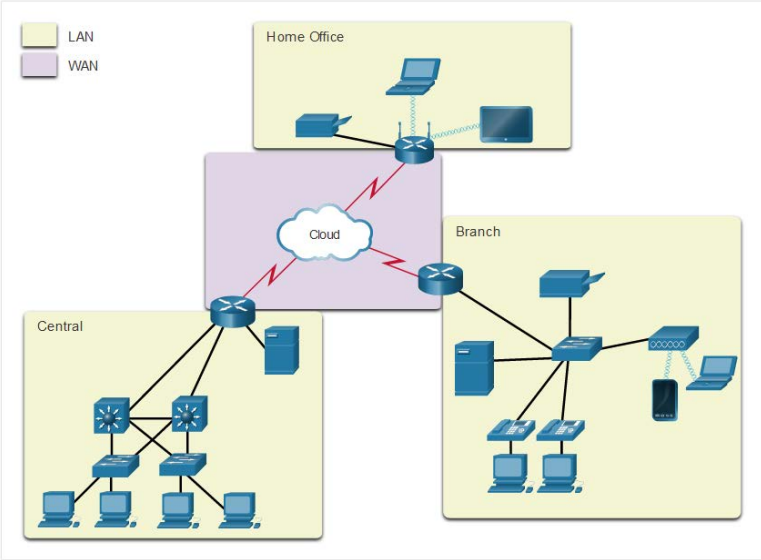
Medium/Large

World Wide

- **Small Home Networks** – connect a few computers to each other and the Internet.
- **Small Office/Home Office** (SOHO) – enables computer within a home or remote office to connect to a corporate network.
- **Medium to Large Networks** – many locations with hundreds or thousands of interconnected computers.
- **World Wide Networks** – connects hundreds of millions of computers world-wide – such as the internet.

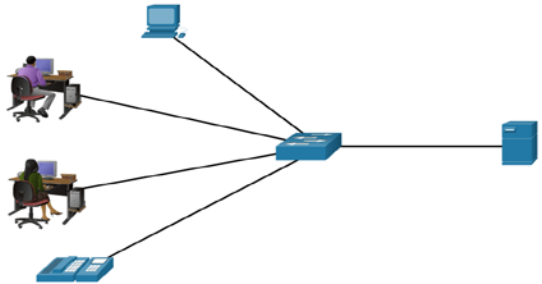
LANs and WANs

- Network infrastructures vary greatly in terms of:
  - Size of the area covered
  - Number of users connected
  - Number and types of services available
  - Area of responsibility
- Most common types of networks:
  - **Local Area Network (LAN)**
  - **Wide Area Network (WAN)**
  - **Wireless LAN (WLAN)**
- Other types of networks:
  - **Metropolitan Area Network** (MAN)
  - **Storage Area Network** (SAN)
  - **Network Area Storage** (NOS)
  - **Personal Area Networks** (PAN)



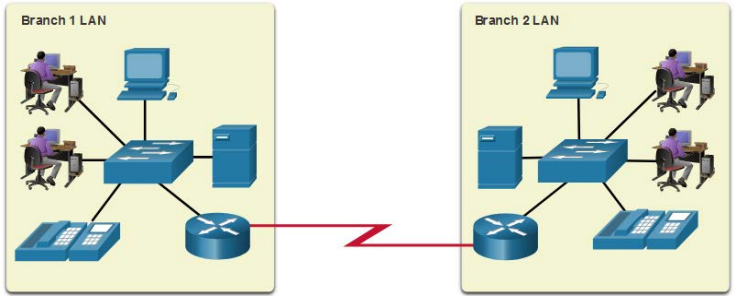
LANs and WANs

Local Area Network



- A network infrastructure that spans a small geographical area.
- Interconnect end devices in a limited area.
- Administered by a single organization or individual.
- Provide high-speed bandwidth to internal devices.

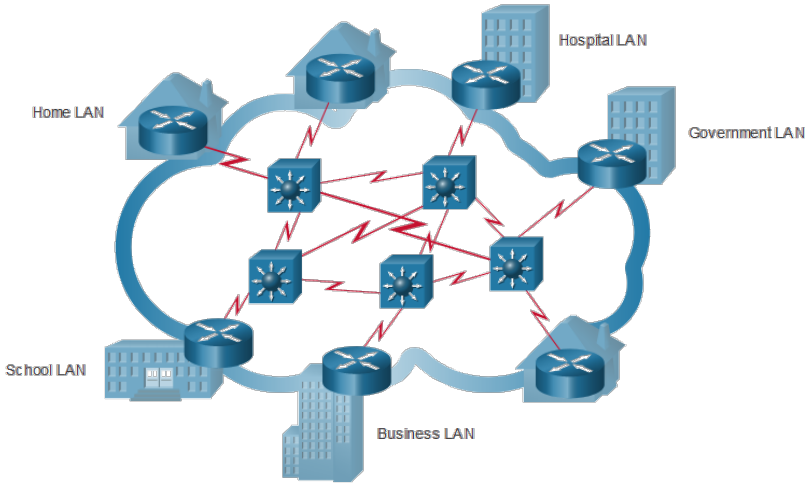
Wide Area Network



- A network infrastructure that spans a wide geographical area.
- Interconnect LANs over wide geographical areas.
- Typically administered by one or more service providers.
- Typically provide slower speed links between LANs.

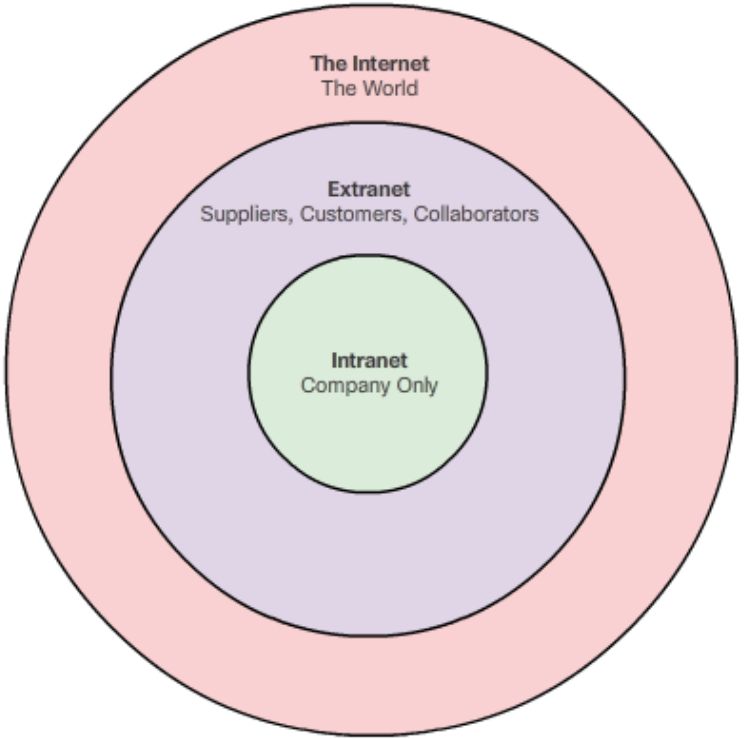
The Internet

- The internet is a worldwide collection of interconnected LANs and WANs.
- LANs are connected to each other using WANs.
- WANs may use copper wires, fiber optic cables, and wireless transmissions.
- The internet is not owned by any individual or group. The following groups were developed to help maintain structure on the internet:
  - IETF
  - ICANN
  - IAB



Intranets and Extranets

- The **Internet** is a public collection of all networks external from your network accessible by all.
- An organization might use an **Extranet** to provide secure access to their network for individuals who work for a different organization that need access to their data on their network.
- An **Intranet** is a private collection of LANs and WANs internal to an organization that is meant to be accessible only to the organizations members or others with authorization.



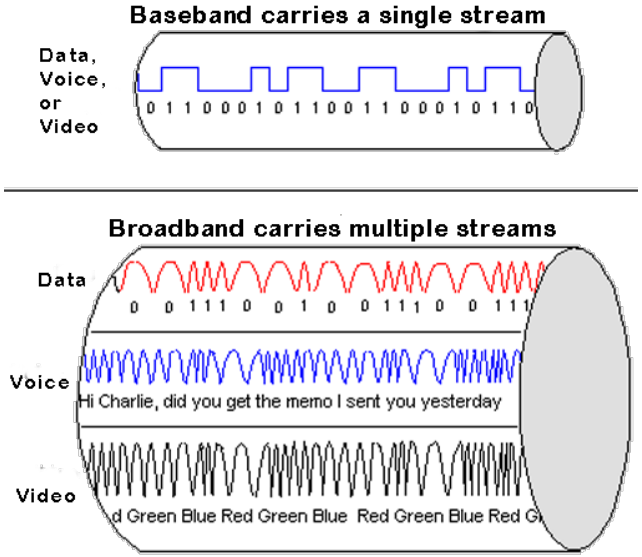
1.5 Internet Connections

Internet Access Technologies

- There are many ways to connect users and organizations to the internet:
  - Popular services for home users and small offices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.
  - Organizations need faster connections to support IP phones, video conferencing and data center storage.
  - Business-class interconnections are usually provided by service providers (SP) and may include: business DSL, leased lines, and Metro Ethernet.

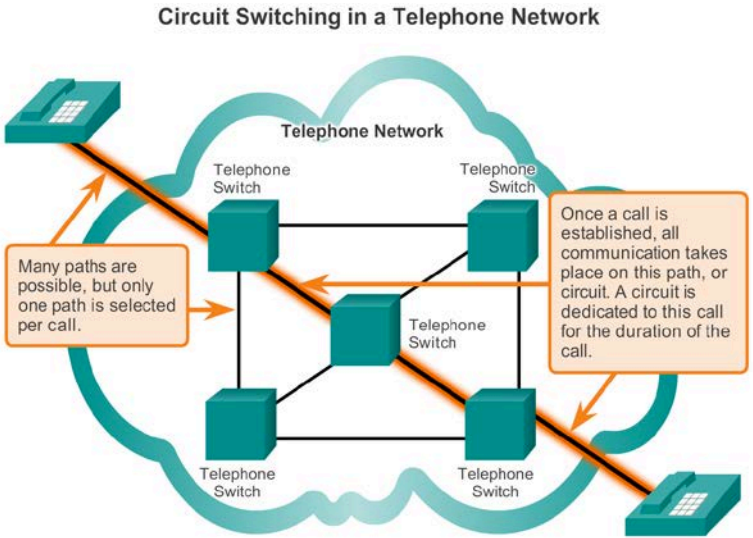
Internet Connections

- Internet Access Technologies
  - Internet Service Provider (ISP)
  - **Baseband** – Carries a single signal/data stream
  - **Broadband** – Carries multiple signals/data streams at once
    - Voice
    - Video
    - Data
    - Control



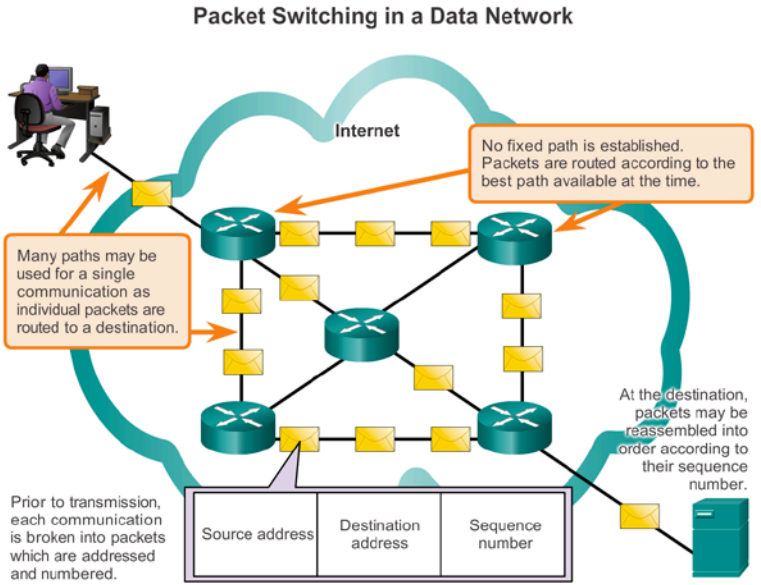
Circuit-Switched Networks

- A Plain Old Telephone System (POTS)
- A characteristic of circuit-switched networks is that if all circuits are busy, a new call cannot be placed
- There is a finite number of circuits. During peak periods, some calls may be denied
- The circuits stays active, even if no one is speaking
- No fault tolerance



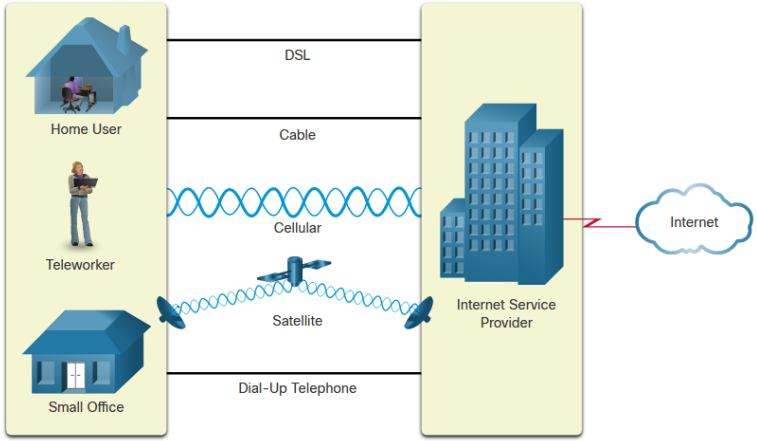
Packet-Switched Networks

- Always on and Always connected
- DSL and Cable
- The term congestion defines a state where the demand on the network resources exceeds the available capacity
- During peak periods, communications may be delayed, but not denied



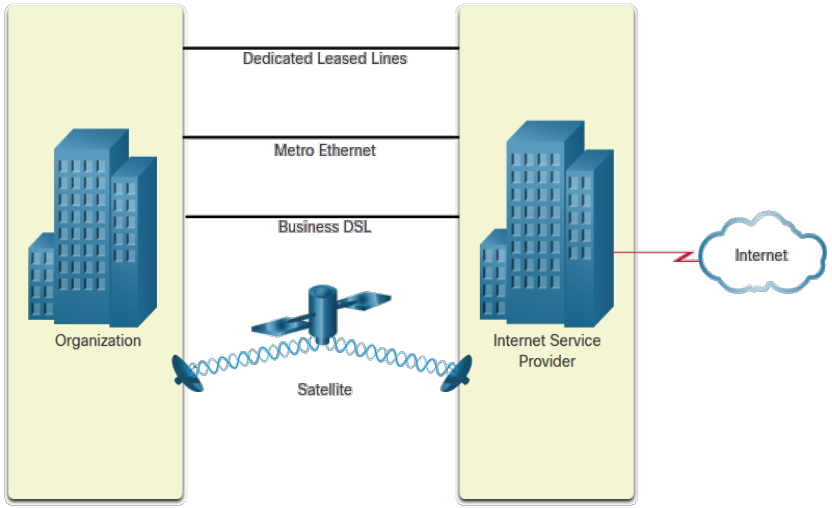
Home and Small Office Internet Connections

- Types of Internet:
  - **Cable** – (broadband) high bandwidth, always on, internet offered by cable television service providers.
  - **DSL** – (broadband) high bandwidth, always on, internet connection that runs over a telephone line.
  - **Dial-up** – (baseband) an inexpressive, low bandwidth option using a modem.
  - **Cellular** – uses a cell phone network to connect the to internet.
  - **Satellite** – major benefit to rural areas without Internet Service Providers.
  - **Wireless WANs** – mobile hotspot



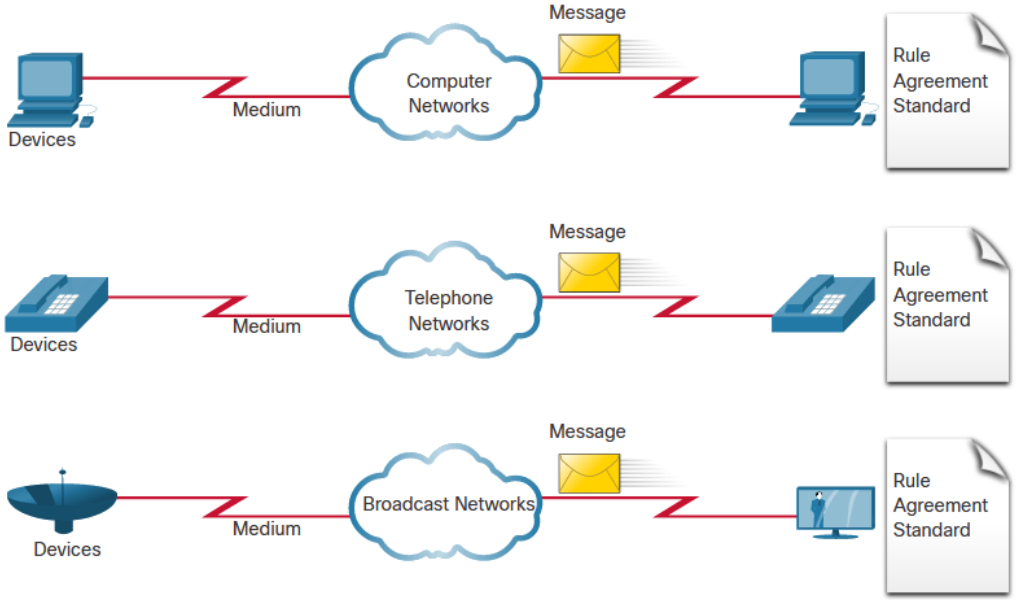
Businesses Internet Connections

- Corporate business connections may require:
  - higher bandwidth
  - dedicated connections
  - managed services



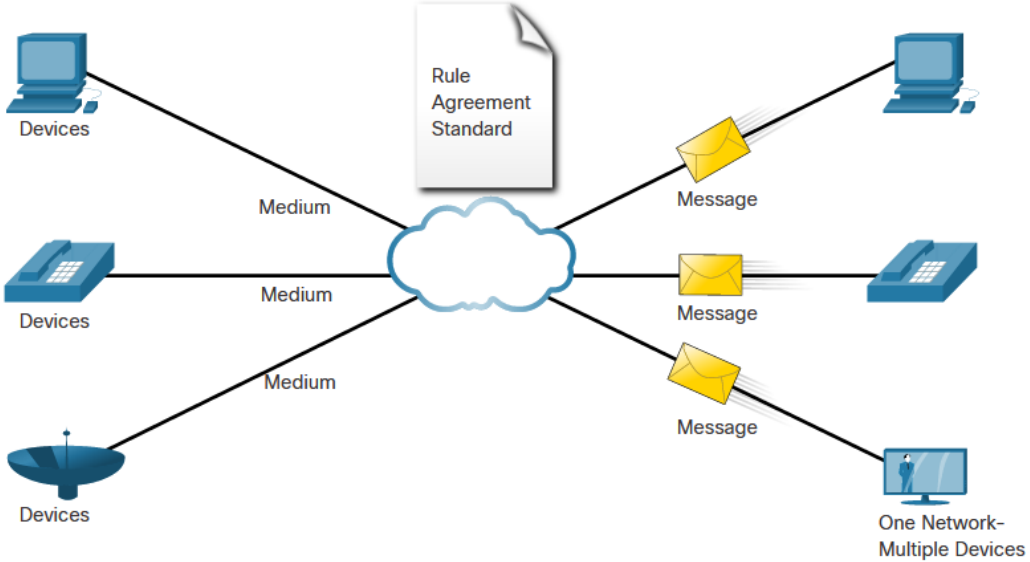
- **Dedicated Leased Line** – These are reserved circuits within the service provider's network that connect distant offices with private voice and/or data networking.
- **Ethernet WAN** – This extends LAN access technology into the WAN.
- **DSL –** Business DSL is available in various formats including Symmetric Digital Subscriber Lines (SDSL).
- **Satellite** – This can provide a connection when a wired solution is not available.

The Converging Network



- Before converged networks, an organization would have been separately cabled for telephone, video, and data. Each of these networks would use different technologies to carry the signal.
- Each of these technologies would use a different set of rules and standards.

The Converging Network

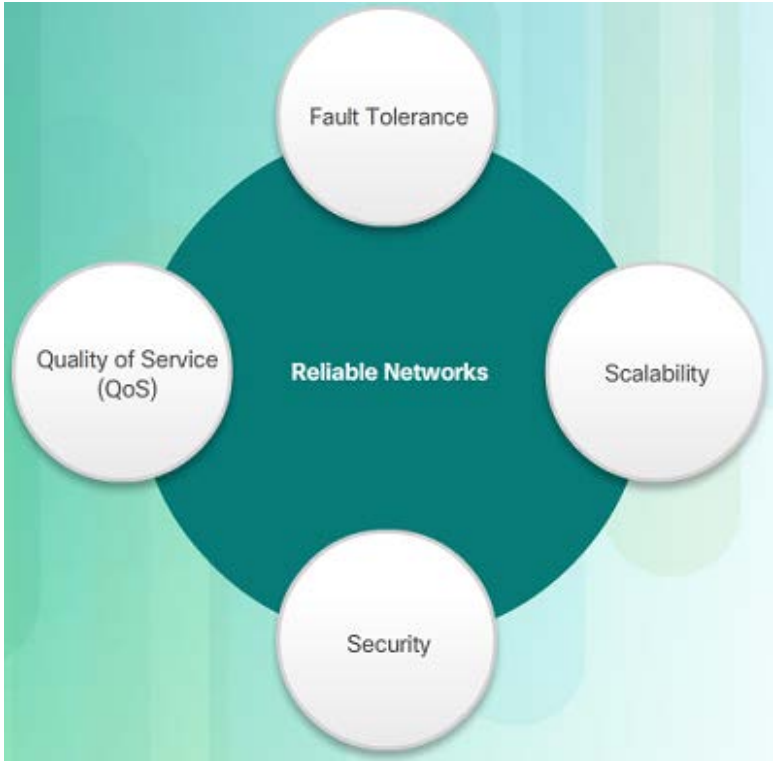


- Converged data networks carry multiple services on one link including:
  - data
  - voice
  - video
- Converged networks can deliver data, voice, and video over the same network infrastructure. The network infrastructure uses the same set of rules and standards.

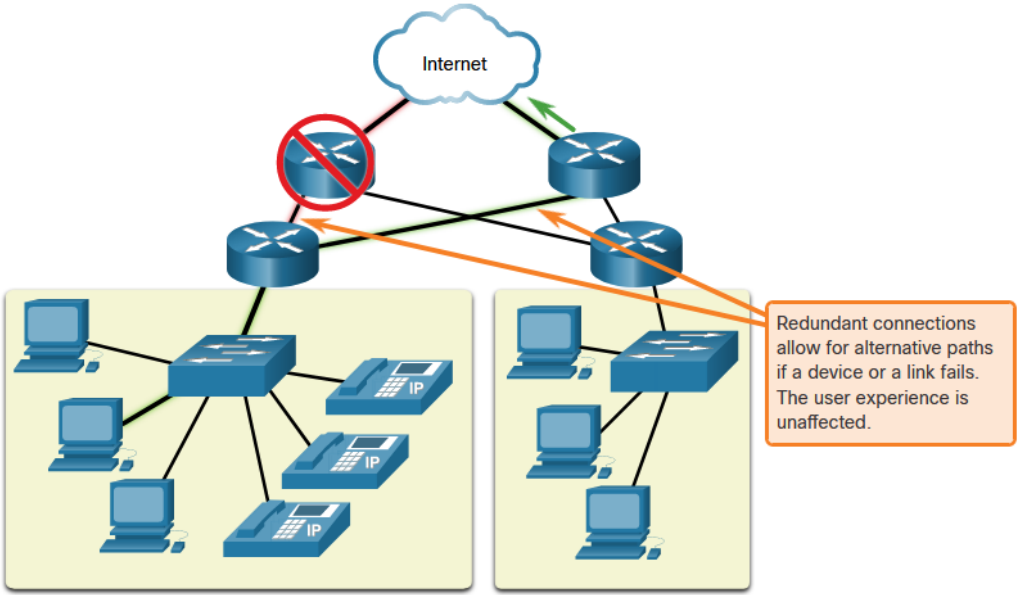
1.6 Reliable Networks

Network Architecture

- Network Architecture refers to the technologies that support the infrastructure that moves data across the network.
- There are four basic characteristics that the underlying architectures need to address to meet user expectations:
  - **Fault Tolerance** – Provide redundant links and devices.
  - **Scalability** – Expand the network without degrading the service for existing users.
  - **Quality of Service** (QoS) – Match the type of communication with a specific priority.
  - **Security** – Protect the network from unauthorized access.

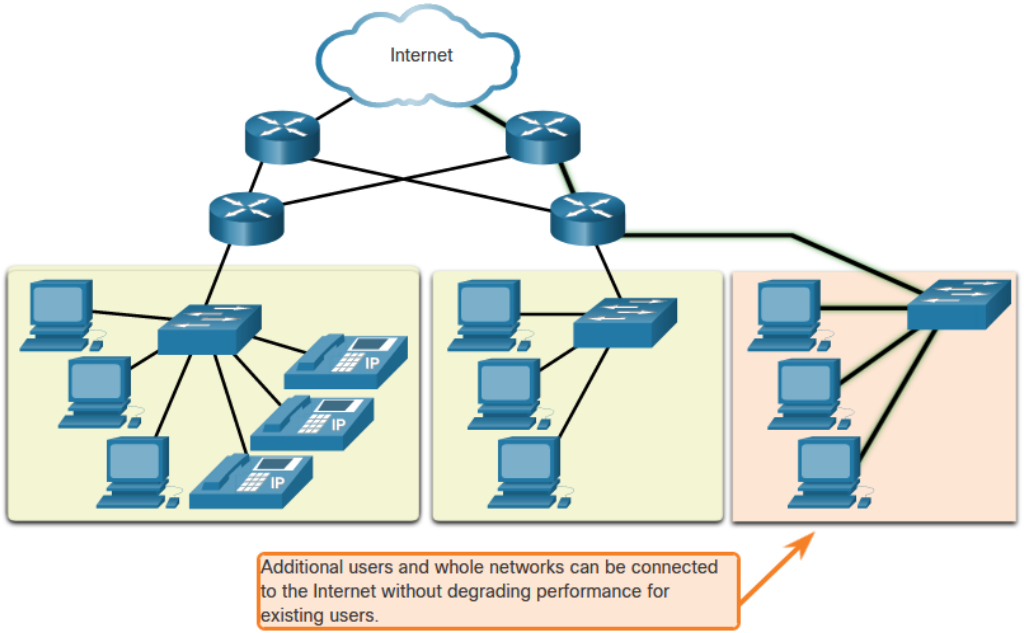


Fault Tolerance



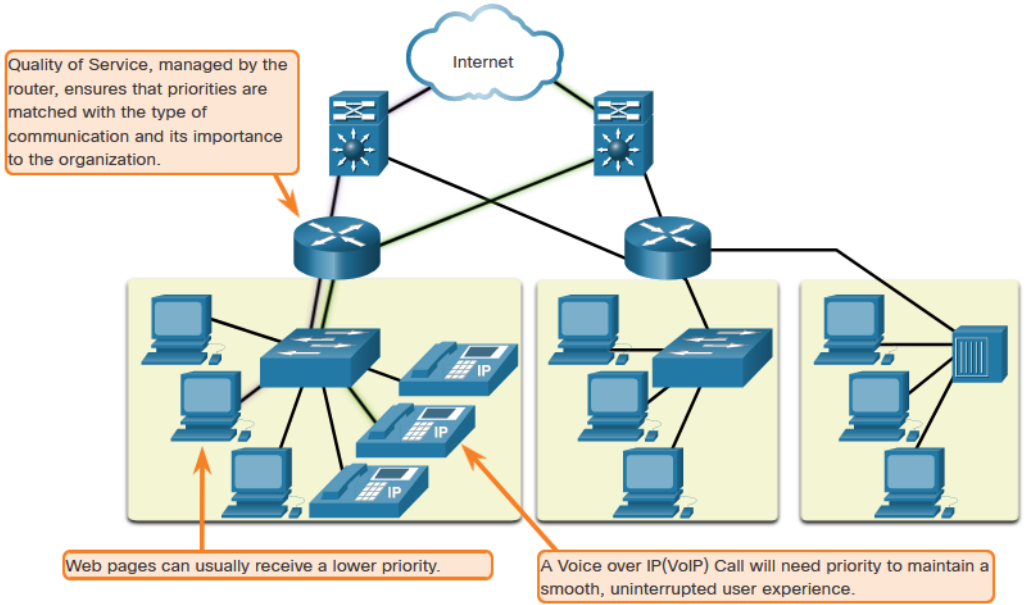
- A **fault tolerant** network limits the impact of a failure by limiting the number of affected devices. Multiple paths are required for fault tolerance.
- Reliable networks provide redundancy by implementing a packet switched network:
  - Packet switching splits traffic into packets that are routed over a network.
  - Each packet could theoretically take a different path to the destination.
- This is not possible with circuit-switched networks which establish dedicated circuits.

Scalability



- A **scalable** network can expand quickly and easily to support new users and applications without impacting the performance of services to existing users.
- Network designers follow accepted standards and protocols in order to make the networks scalable.

Quality of Service

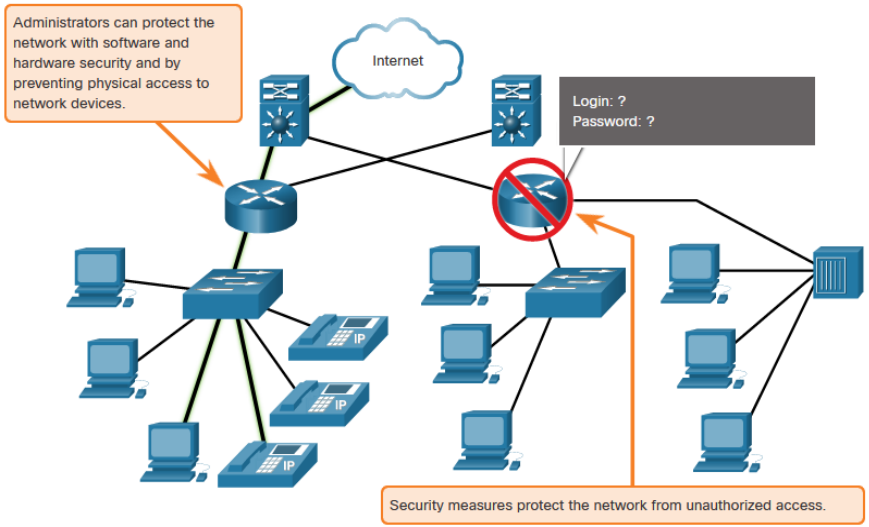


- Voice and live video transmissions require higher expectations for those services being delivered.
- Have you ever watched a live video with constant breaks and pauses? This is caused when there is a higher demand for bandwidth than available – and QoS isn't configured.
- **Quality of Service** (QoS) is the primary mechanism used to ensure reliable delivery of content for all users.
- With a QoS policy in place, the router can more easily manage the flow of data and voice traffic.

Quality of Service (QoS)

- Examples of priority decisions for an organization might include:
  - **Time-sensitive communication** - increase priority for services like telephony or video distribution/conferencing
  - **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
- The network provides predictable levels of service to different types of traffic

Network Security



- There are two main types of **network security** that must be addressed:
  - **Network infrastructure security**
    - Physical security of network devices
    - Preventing unauthorized access to the devices
  - **Information Security**
    - Protection of the information or data transmitted over the network

Network Security

- Goals of network security:
  - **Confidentiality** – Only the intended recipients can access and read the data (Requiring strong, complex passwords)
  - **Integrity** – The assurance that the information has not been altered during transmission
  - **Availability** – The assurance of timely and reliable access to data for authorized users
  - **Congestion** – a term that describes the state of a network when the demand on the network resources exceeds the available capacity.
  - **Bandwidth** – a measure of the data carrying capacity of the media.

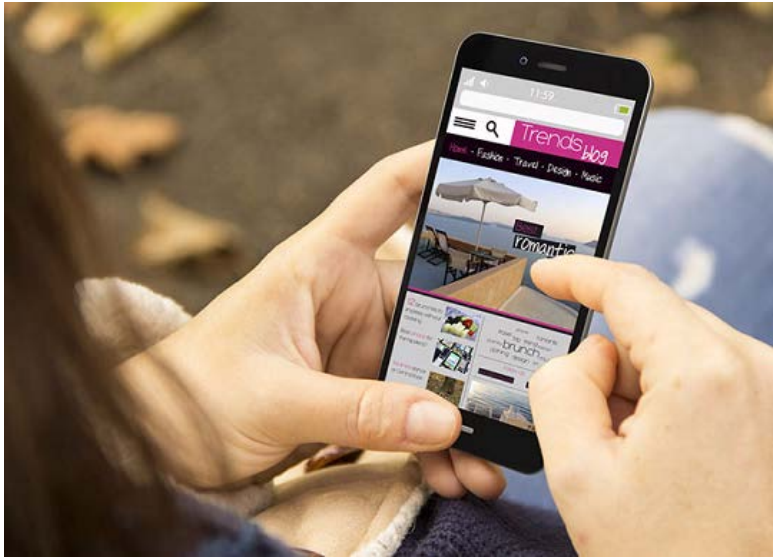
1.7 Network Trends

Recent Trends

- The role of the network must adjust and continually transform in order to be able to keep up with new technologies and end user devices as they constantly come to the market.
- Several new networking trends that effect organizations and consumers:
  - Bring Your Own Device (BYOD)
  - Online collaboration
  - Video communications
  - Cloud computing

Bring Your Own Device

- **Bring Your Own Device (BYOD)** allows users to use their own devices giving them more opportunities and greater flexibility.
- BYOD allows end users to have the freedom to use personal tools to access information and communicate using their:
  - Laptops
  - Netbooks
  - Tablets
  - Smartphones
  - E-readers
- BYOD means any device, with any ownership, used anywhere.



Online Collaboration

- Collaborate and work with others over the network on joint projects.
- Collaboration tools including Cisco WebEx (shown in the figure) gives users a way to instantly connect and interact.
- Collaboration is a very high priority for businesses and in education.
- Cisco Webex Teams is a multifunctional collaboration tool.
  - send instant messages
  - post images
  - post videos and links

Cloud Computing

- **Cloud computing** allows us to store personal files or backup our data on servers over the internet.
  - Applications can also be accessed using the Cloud.
  - Allows businesses to provide access to files anywhere, anytime, and on any device.

- Cloud computing is made possible by data centers.
  - Smaller companies that can't afford their own data centers, lease server and storage services from larger data center organizations in the Cloud.

Cloud Computing

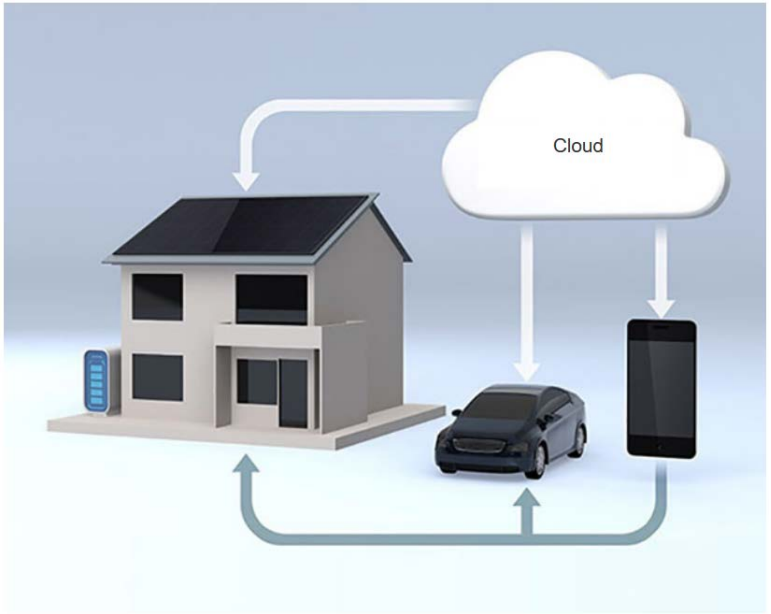
- Four types of Clouds:
  - **Public** Clouds
    - Available to the general public through a pay-per-use model or for free.
  - **Private** Clouds
    - Intended for a specific organization or entity such as the government.
  - **Hybrid** Clouds
    - Made up of two or more Cloud types – for example, part custom and part public.
    - Each part remains a distinctive object but both are connected using the same architecture.
  - **Custom** Clouds
    - Built to meet the needs of a specific industry, such as healthcare or media.
    - Can be private or public.

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

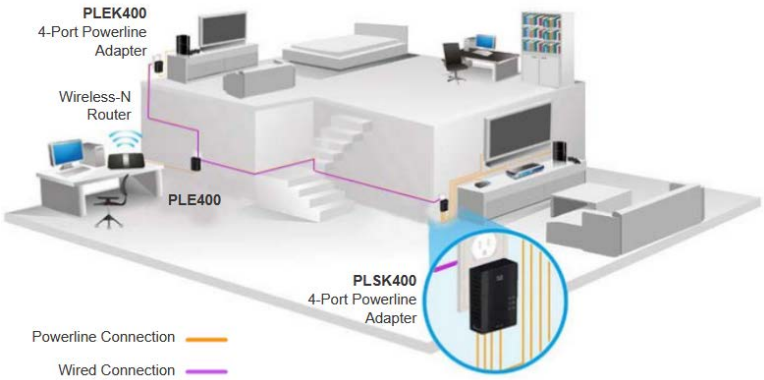
Technology Trends in the Home

- Smart home technology is a growing trend that allows technology to be integrated into every-day appliances which allows them to interconnect with other devices.
- Ovens might know what time to cook a meal for you by communicating with your calendar on what time you are scheduled to be home.
- Smart home technology is currently being developed for all rooms within a house.



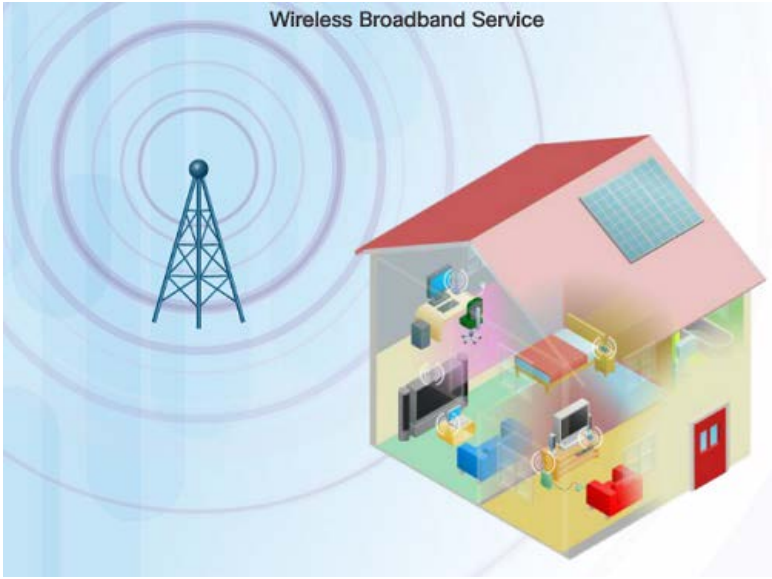
Powerline Networking

- **Powerline networking** can allow devices to connect to a LAN where data network cables or wireless communications are not a viable option.
- Using a standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet by sending data on certain frequencies.
- Powerline networking is especially useful when wireless access points cannot reach all the devices in the home.



Wireless Broadband

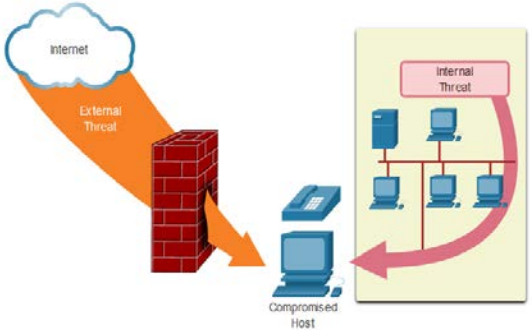
- In addition to DSL and cable, wireless is another option used to connect homes and small businesses to the internet.
  - More commonly found in rural environments, a Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to designated access points or hotspots.
  - Wireless broadband is another solution for the home and small businesses.
    - Uses the same cellular technology used by a smart phone.
    - An antenna is installed outside the house providing wireless or wired connectivity for devices in the home.



1.8 Network Security

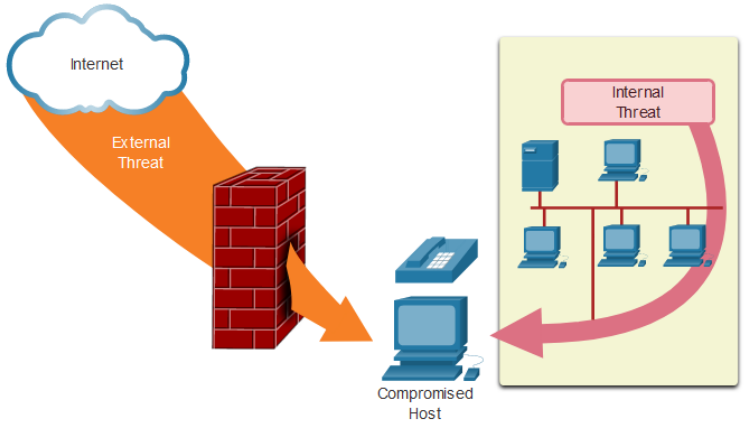
Security Threats

- Network security is an integral part of networking regardless of the size of the network.
- The network security that is implemented must take into account the environment while securing the data, but still allowing for quality of service that is expected of the network.
- Securing a network involves many protocols, technologies, devices, tools, and techniques in order to secure data and mitigate threats.
- Threat vectors might be external or internal.



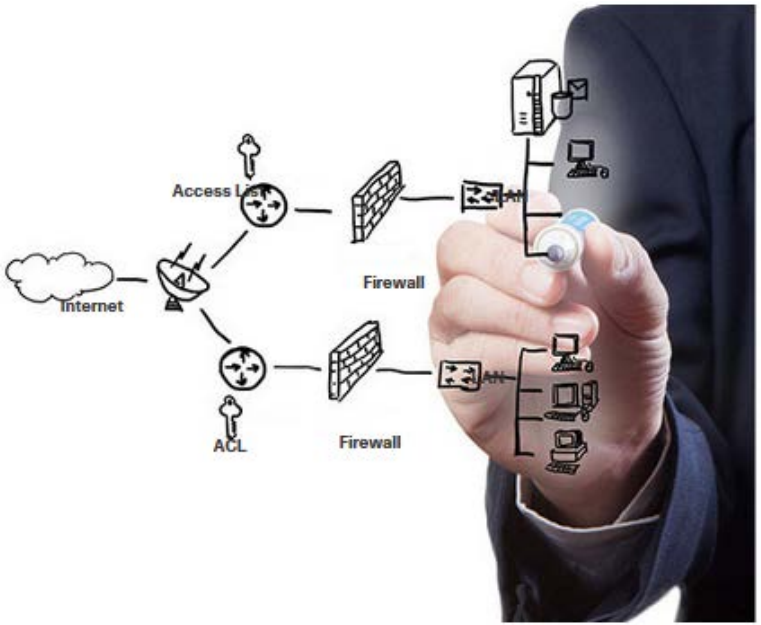
Security Threats

- **External Threats**:
  - Viruses, worms, and Trojan horses
  - Spyware and adware
  - Zero-day attacks
  - Threat Actor attacks
  - Denial of service attacks
  - Data interception and theft
  - Identity theft
- **Internal Threats**:
  - lost or stolen devices
  - accidental misuse by employees
  - malicious employees



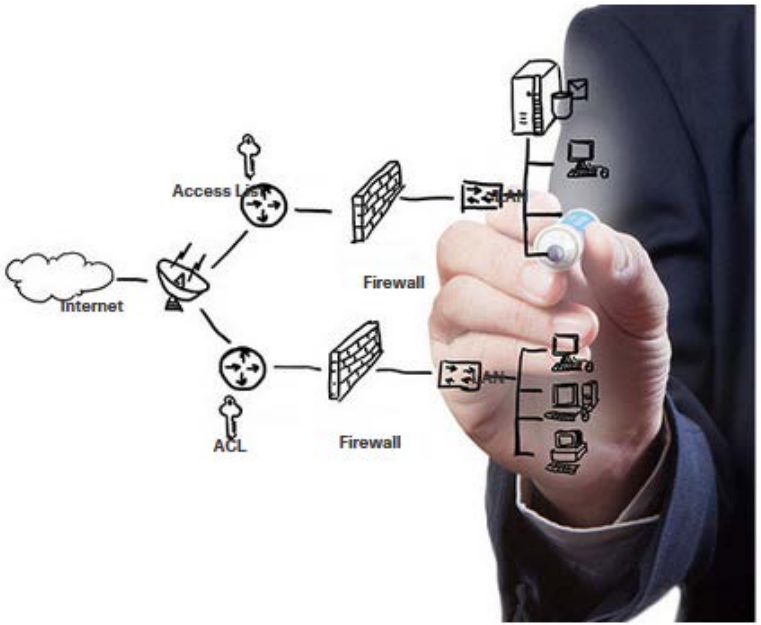
Security Solutions

- Security must be implemented in multiple layers using more than one security solution.
- Network security components for home or small office network:
  - **Antivirus** and **antispyware** software should be installed on end devices.
  - **Firewall** filtering used to block unauthorized access to the network.



Security Solutions

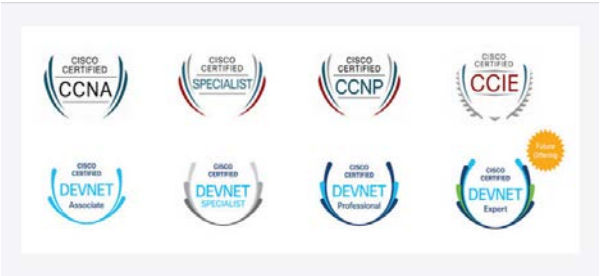
- Larger networks have additional security requirements:
  - **Dedicated firewall system**
  - **Access control lists** (ACL)
  - **Intrusion prevention systems** (IPS)
  - **Virtual private networks** (VPN)
- The study of network security starts with a clear understanding of the underlying switching and routing infrastructure.



1.9 The IT Professional

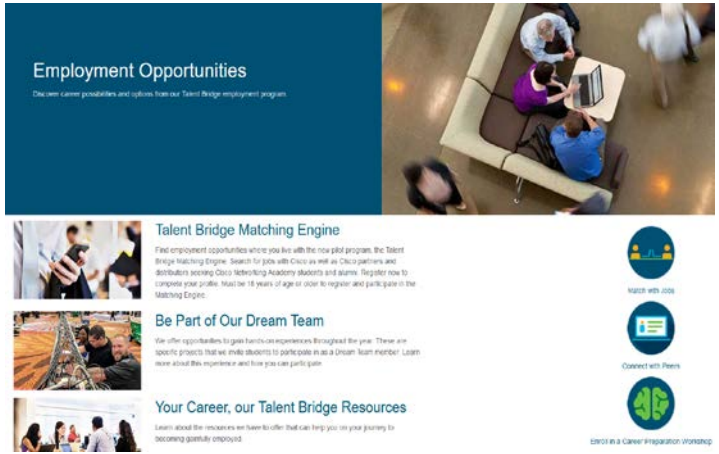
CCNA

- The Cisco Certified Network Associate (CCNA) certification:
  - demonstrates that you have a knowledge of foundational technologies
  - ensures you stay relevant with skills needed for the adoption of next-generation technologies.
- The new CCNA focus:
  - IP foundation and security topics
  - Wireless, virtualization, automation, and network programmability.
- New DevNet certifications at the associate, specialist and professional levels, to validate your software development skills.
- Specialist certification validate your skills in line with your job role and interests.



Networking Jobs

- At www.netacad.com you can click the Careers menu and then select Employment opportunities.
  - Find employment opportunities by using the Talent Bridge Matching Engine.
  - Search for jobs with Cisco, Cisco partners and distributors seeking Cisco Networking Academy students and alumni.



1.10 Module Practice and Quiz

What did I learn in this module?

- Through the use of networks, we are connected like never before.
- All computers that are connected to a network and participate directly in network communication are classified as hosts.
- Diagrams of networks often use symbols to represent the different devices and connections that make up a network.
- A diagram provides an easy way to understand how devices connect in a large network.
- The two types of network infrastructures are Local Area Networks (LANs), and Wide Area Networks (WANs).

What did I learn in this module?

- SOHO internet connections include cable, DSL, Cellular, Satellite, and Dial-up telephone.
- Business internet connections include Dedicated Leased Line, Metro Ethernet, Business DSL, and Satellite.
- Network architecture refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data across the network.
- There are four basic characteristics of network architecture: Fault Tolerance, Scalability, Quality of Service (QoS), and Security.

What did I learn in this module?

- Recent networking trends that affect organizations and consumers: Bring Your Own Device (BYOD), online collaboration, video communications, and cloud computing.
- There are several common external and internal threats to networks.
- Larger networks and corporate networks use antivirus, antispyware, and firewall filtering, but they also have other security requirements: Dedicated firewall systems, Access control lists (ACL), Intrusion prevention systems (IPS), and Virtual private networks (VPN)
- The Cisco Certified Network Associate (CCNA) certification demonstrates your knowledge of foundational technologies.

New Terms and Commands

- Peer-to-Peer File Sharing
- Small Office/Home Office or SOHO
- Medium to large network
- Server
- Client
- Peer-to-Peer network
- End device
- Intermediary device
- Medium
- Network Interface Card (NIC)
- Physical Port
- Interface
- Physical topology diagram
- Logical topology diagram
- Local Area Network (LAN)
- Wide Area Network (WAN)
- Internet
- Intranet
- Extranet
- Internet Service Provider (ISP)
- Converged networks
- Network architecture
- Fault tolerant network
- Packet-switched network
- Circuit-switched network
- Scalable network
- Quality of Service (QoS)
- Network bandwidth
- Bring Your Own Device (BYOD)
- Collaboration
- Cloud computing
- Private clouds
- Hybrid clouds
- Public clouds
- Custom clouds
- Data center
- Smart home technology
- Powerline networking
- Wireless Internet Service Provider (WISP)
- Network architecture


CISCO


Elk Technologies
https://elktech.org
Scott Stephenson