CHAPTER 1: EXPLORING THE NETWORK

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.

GLOBALLY CONNECTED

Networking Today

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.

Networks have changed the way we learn. 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.

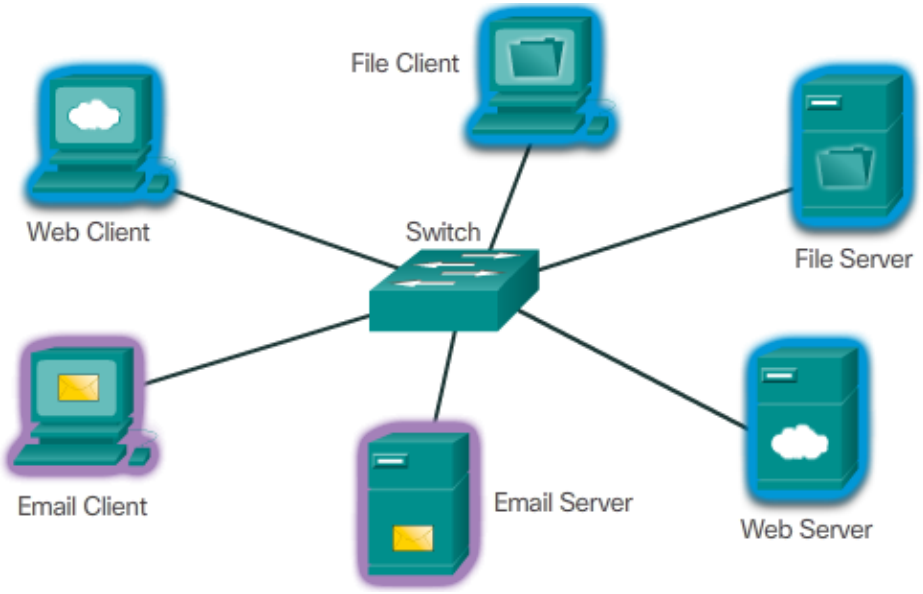
Networks have changed the way we communicate. The globalization of the Internet has ushered in new forms of communication that empower individuals to create information that can be accessed by a global audience. Some forms of communication include: texting, social media, collaboration tools, blogs, wikis, podcasting, and Peer-to-Peer (P2P) File Sharing.

Networks have changed 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.

Networks have changed the way we play. 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.

Networks come in all sizes. They can range from simple networks consisting of two computers to networks connecting millions of devices. **Small home networks** connect a few computers to each other and the Internet. The **Small Office/Home Office** or **SOHO** network enables computers within a home office or a remote office to connect to a corporate network or access centralized, shared resources. **Medium to large networks**, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected computers. The **Internet** is a network of networks that connects hundreds of millions of computers world-wide.

Providing Resources in a Network



All computers connected to a network that participate directly in network communication are classified as hosts. **Hosts** are also called end devices.

Servers are computers with software that enable them to provide information, like email or web pages, to other end devices on the network. Each service requires separate server software.

Clients are computers with software installed that enable them to request and display the information obtained from the server.

In small businesses and homes, many computers function as the servers and clients on the network. This type of network is called a **peer-to-peer network**.

The advantages of peer-to-peer networking:

- Easy to set up
- Less complexity
- Lower cost since network devices and dedicated servers may not be required
- Can be used for simple tasks such as transferring files and sharing printers

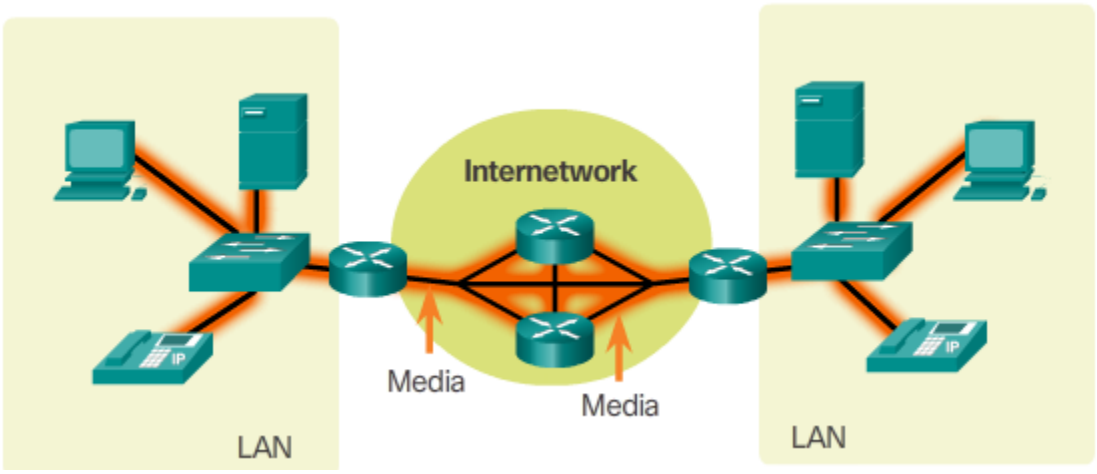
The disadvantages of peer-to-peer networking:

- No centralized administration
- Not as secure
- Not scalable
- All devices may act as both clients and servers which can slow their performance

LANS, WANS AND THE INTERNET

Network Components

The network infrastructure contains three categories of network components: Devices, Media and Services.



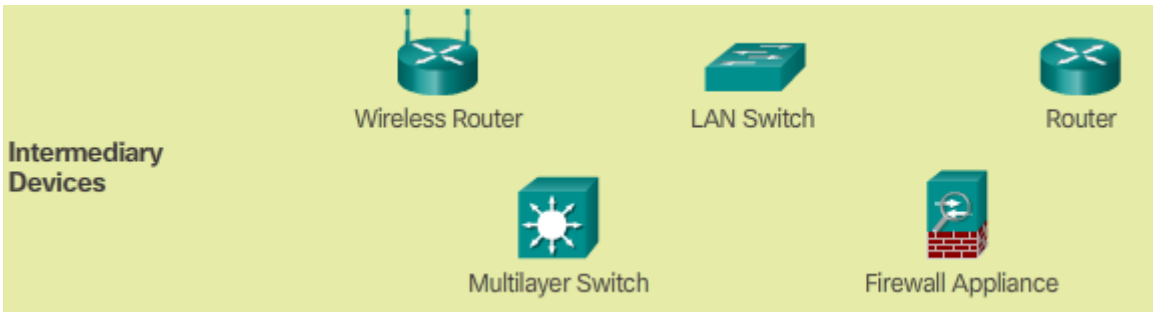
Devices and media are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices.

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.

The network devices that people are most familiar with are called **end devices**.

An **end device** is either the source or destination of a message transmitted over the network. To distinguish one end device from another, each end device on a network is identified by an address. When an end device initiates communication, it uses the address of the destination end device to specify where the message should be sent.

Intermediary devices connect the individual end devices to the network and can connect multiple individual networks to form an internetwork.

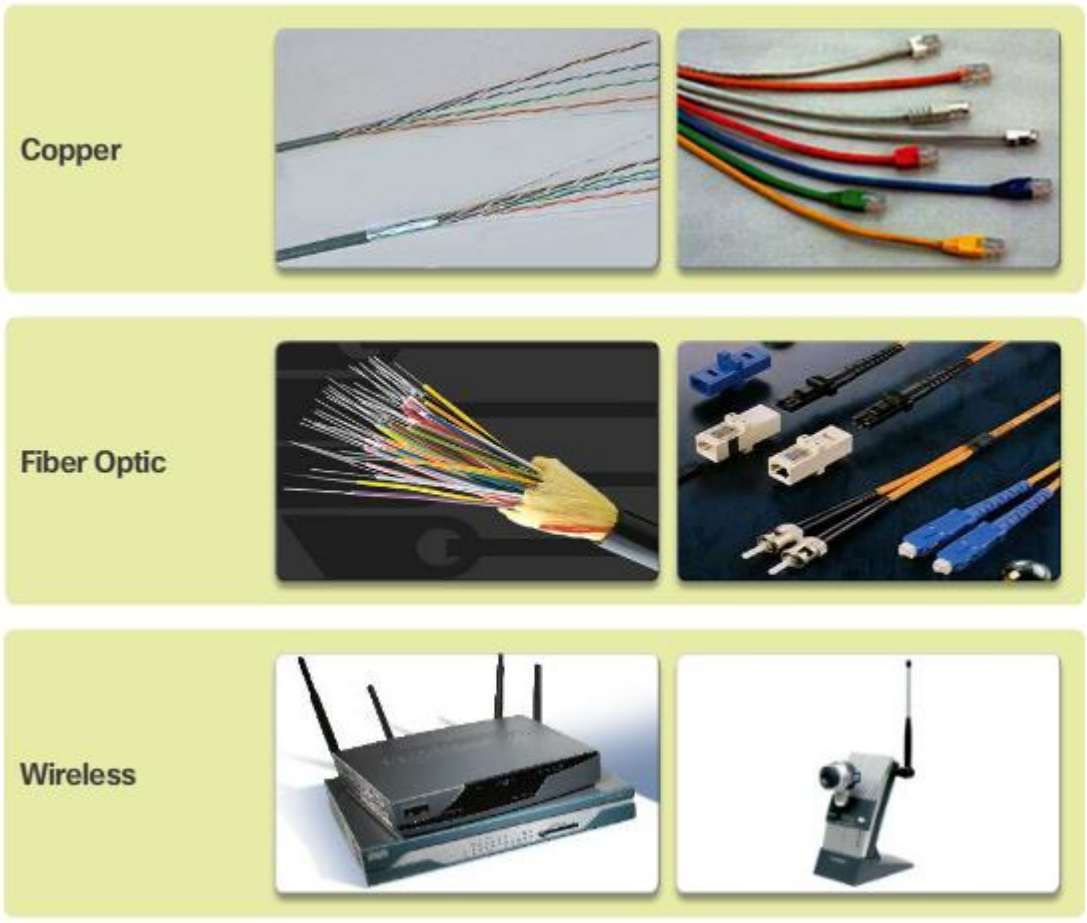


Intermediary devices use the destination end device address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network.

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

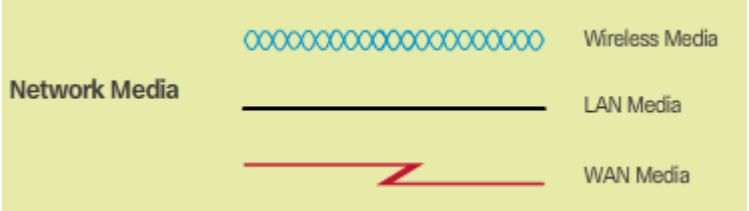
Communication across a network is carried on a **medium**. The **medium** provides the channel over which the message travels from source to destination.



Modern networks primarily use three types of media to interconnect devices and to provide the pathway over which data can be transmitted.

- **Metallic wires within cables** - data is encoded into electrical impulses
- **Glass or plastic fibers (fiber optic cable)** - data is encoded as pulses of light
- **Wireless transmission** - data is encoded using wavelengths from the electromagnetic spectrum

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 in a large network are connected. This type of "picture" of a network is known as a **topology diagram**.



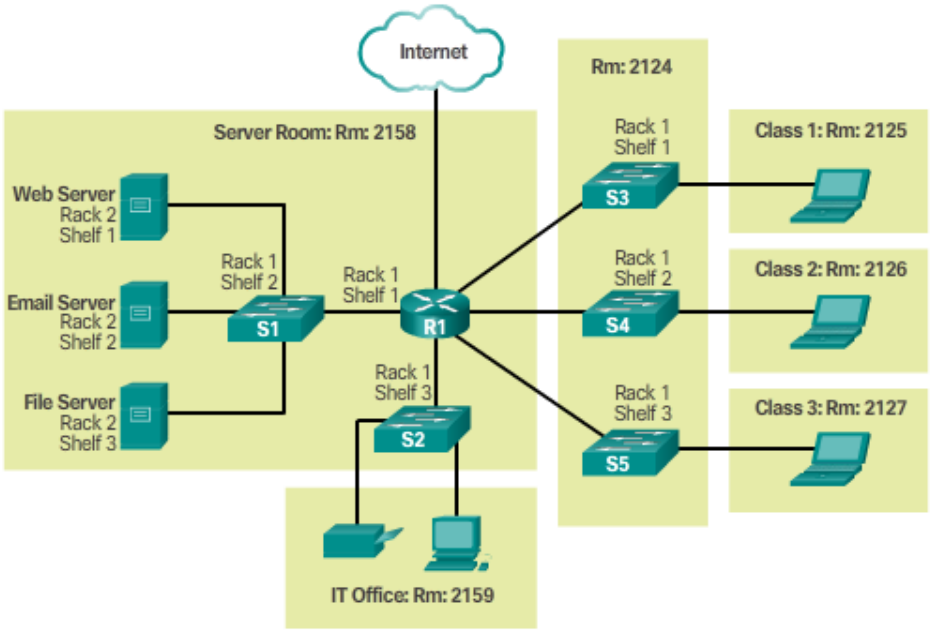
In addition to these representations, specialized terminology is used when discussing how each of these devices and media connect to each other. Important terms to remember are:

- **Network Interface Card** - A NIC, or LAN adapter, provides the physical connection to the network at the PC or other end device.
- **Physical Port** - A connector or outlet on a networking device where the media is connected to an end device or another networking device.
- **Interface** - Specialized ports on a networking device that connect to individual networks.

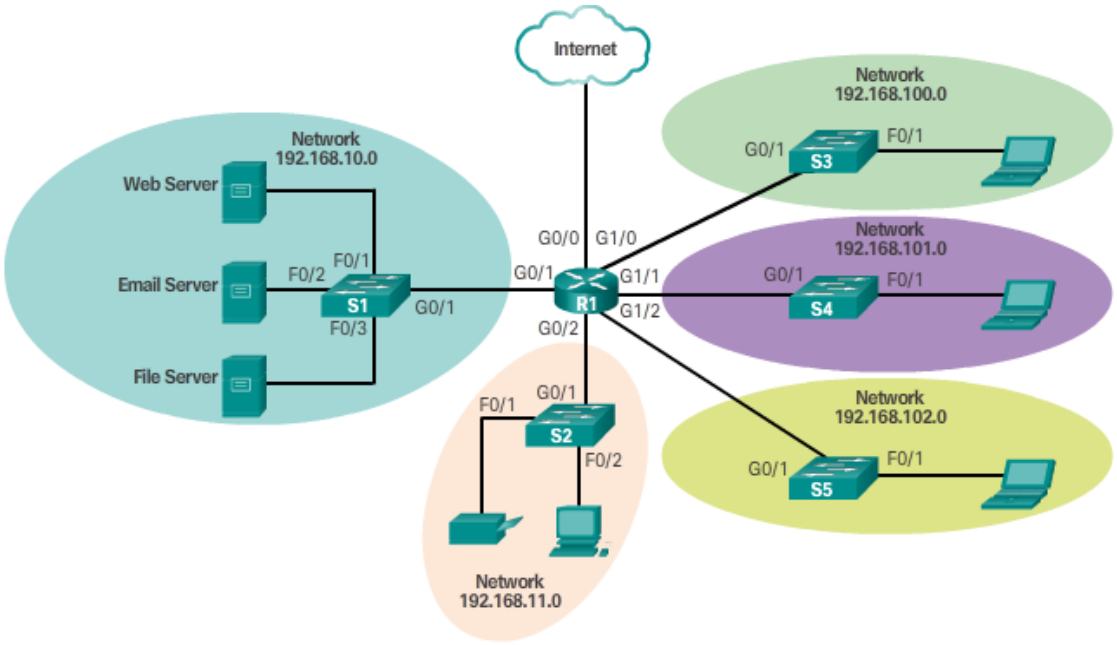
Topology diagrams are mandatory for anyone working with a network. They provide a visual map of how the network is connected.

There are two types of topology diagrams:

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



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



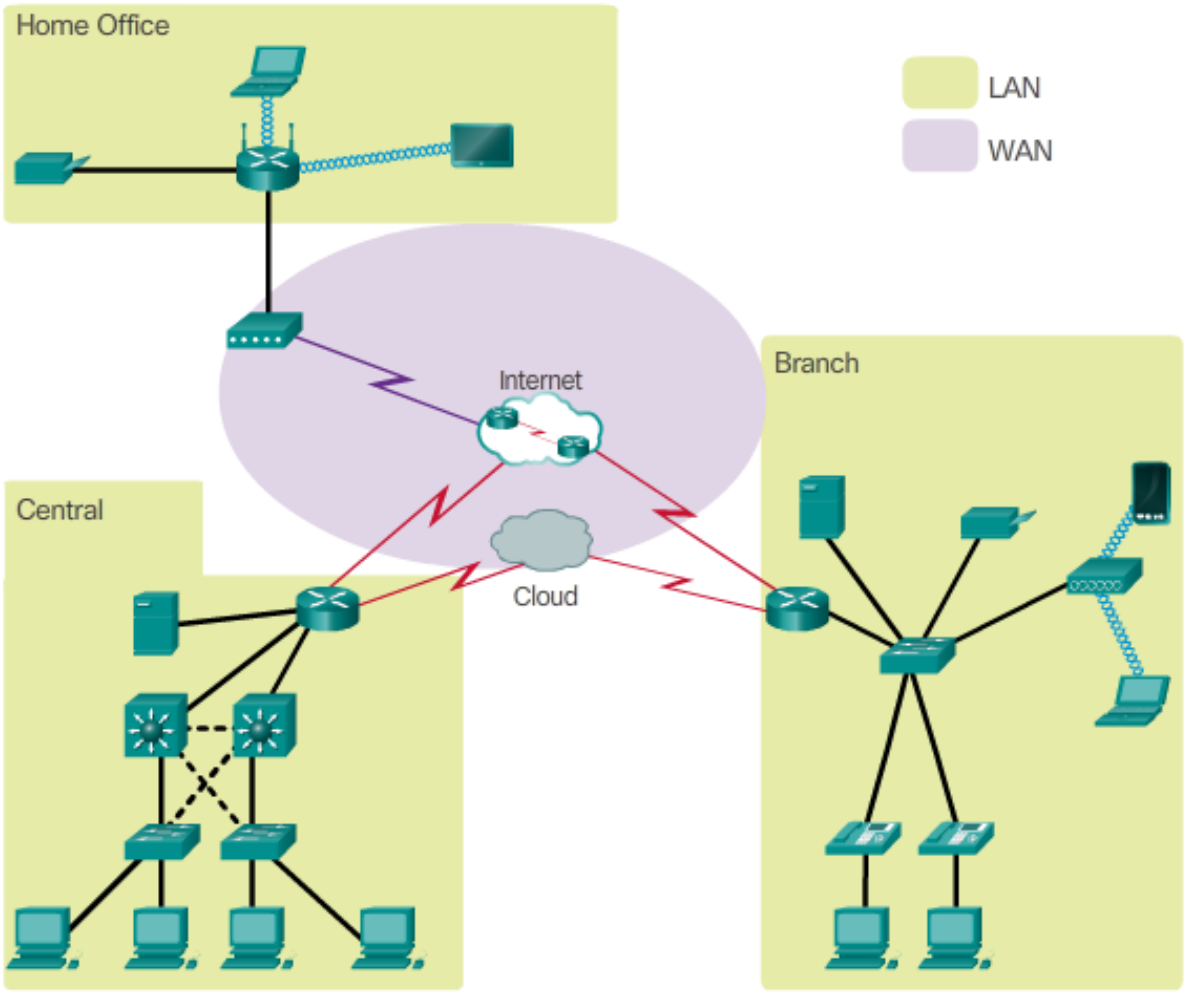
LANs and WANs

Network infrastructures can vary greatly in terms of:

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

The two most common types of network infrastructures are:

- **Local Area Network (LAN)** - A network infrastructure that spans a small geographical area. Specific features of LANs include:
    - Interconnect end devices in a limited area such as a home, school, office building, or campus.
    - Is usually administered by a single organization or individual.
    - Provide high speed bandwidth to internal end devices and intermediary devices.
- **Wide Area Network (WAN)** - 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:
    - Interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
    - Usually administered by multiple service providers.
    - Typically provide slower speed links between LANs.

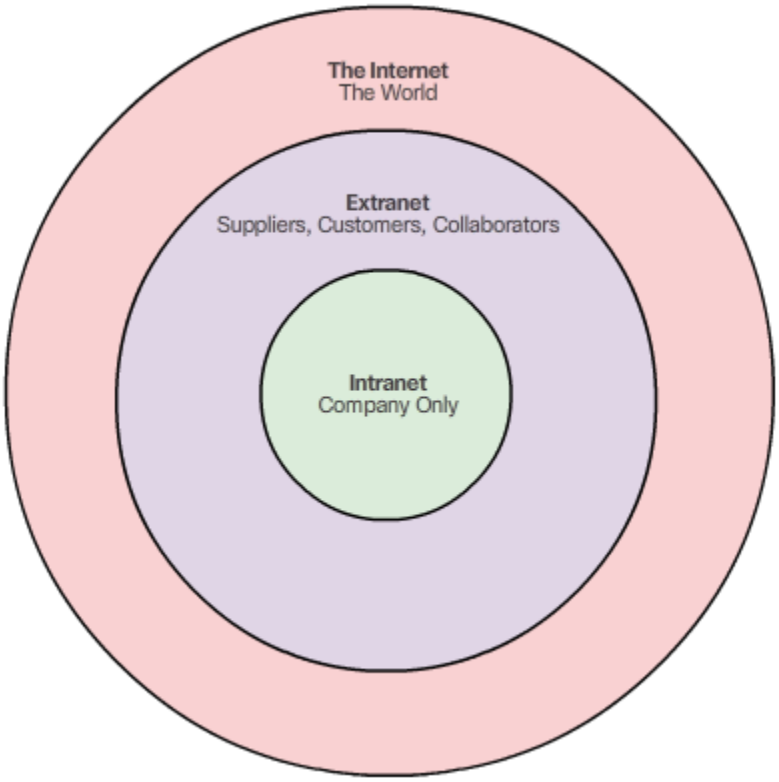


The Internet, Intranets, and Extranets

The **Internet** is a worldwide collection of interconnected networks. The Internet is not owned by any individual or group. 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.

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

- **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.
- **Extranet** - An organization may use an extranet to provide secure and safe access to individuals who work for a different organization, but require access to the organization's data. Examples of extranets include:
    - A company that is providing access to outside suppliers and contractors.
    - A hospital that is providing a booking system to doctors so they can make appointments for their patients.
    - A local office of education that is providing budget and personnel information to the schools in its district.



Internet Connections

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. Organizations typically require access to other corporate sites and the Internet.

Common connection options for small office and home office users are:

- **Cable** - Typically offered by cable television service providers, the Internet data signal is carried on the same cable that delivers cable television.
- **DSL** - Digital Subscriber Lines provide a high bandwidth, always on, connection to the Internet. DSL runs over a telephone line.
- **Cellular** - Cellular Internet access uses a cell phone network to connect. Wherever you can get a cellular signal, you can get cellular Internet access.

- **Satellite** - The availability of satellite Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all.
- **Dial-up Telephone** - An inexpensive option that uses any phone line and a modem. The low bandwidth provided by a dial-up modem connection is usually not sufficient.

Common connection options for businesses are:

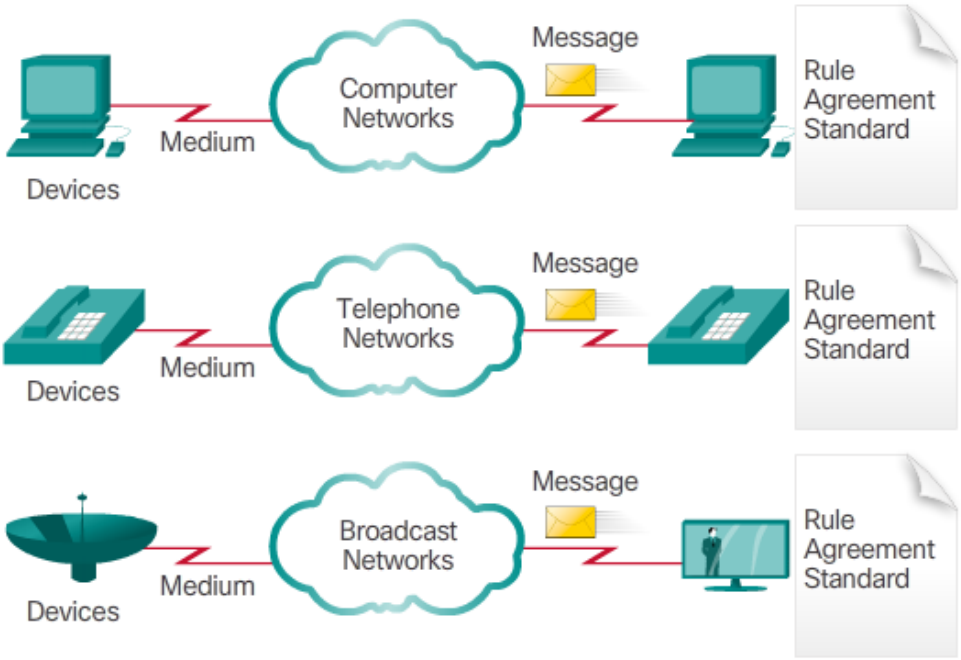
- **Dedicated Leased Line** - Leased lines are actually reserved circuits within the service provider's network that connect geographically separated offices for private voice and/or data networking. The circuits are typically rented at a monthly or yearly rate.
- **Ethernet WAN** - Ethernet WANs extend LAN access technology 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.

THE NETWORK AS A PLATFORM

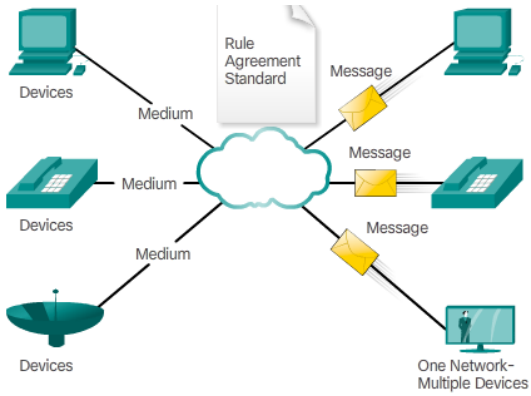
Converged Networks

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.



Multiple services are running on multiple 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

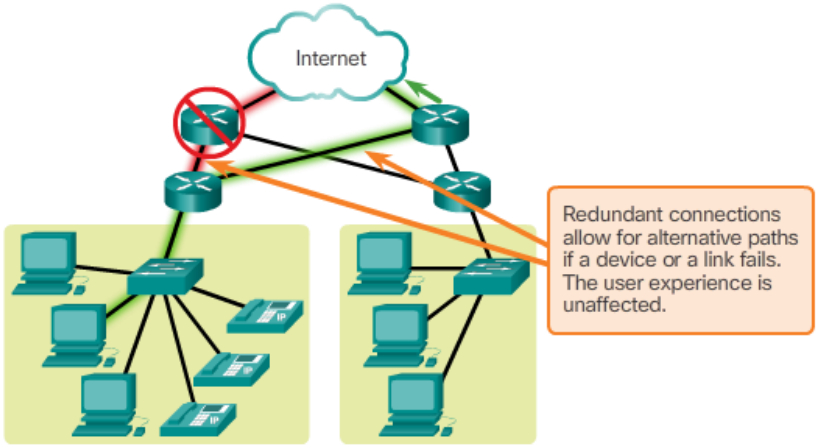


Converged data networks carry multiple services on one network.

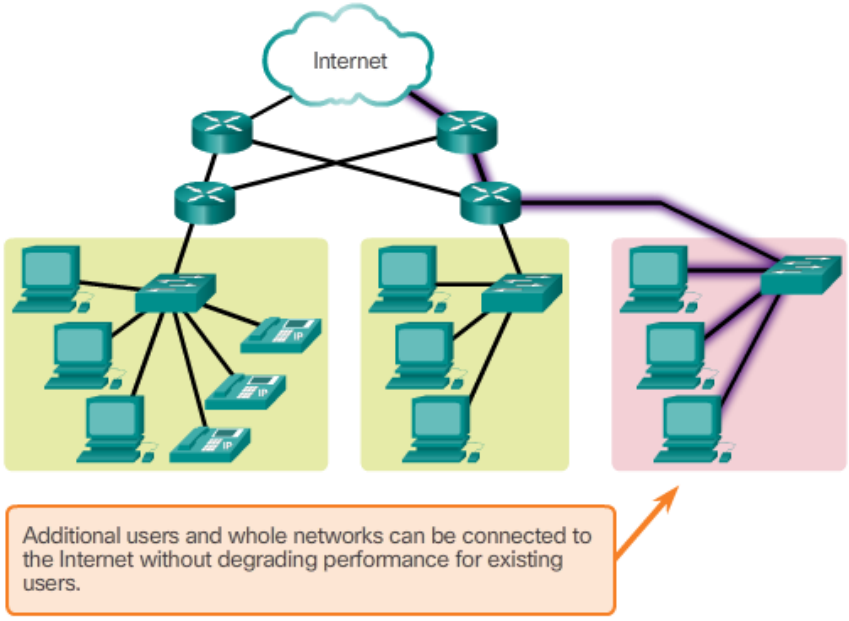
Reliable Network

The term **network architecture** refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move data 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:

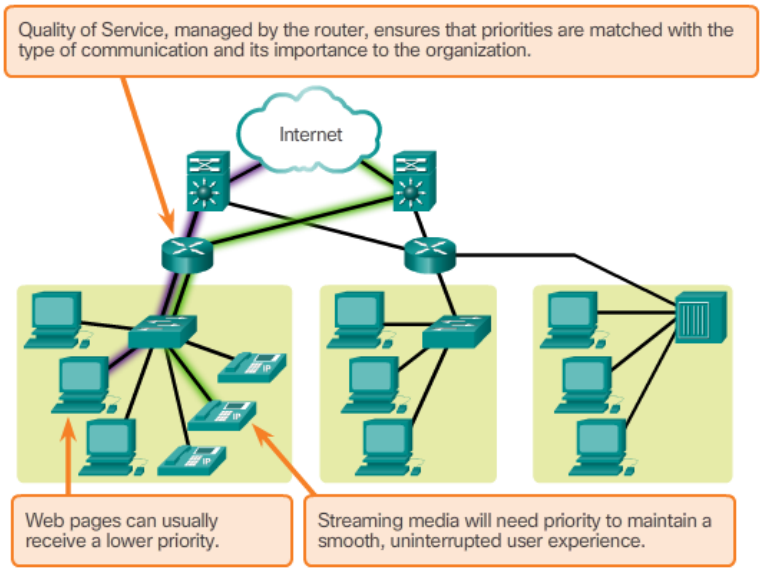
- **Fault Tolerance** - A fault tolerant network is one that limits the impact of a failure, so that the fewest number of devices are affected.



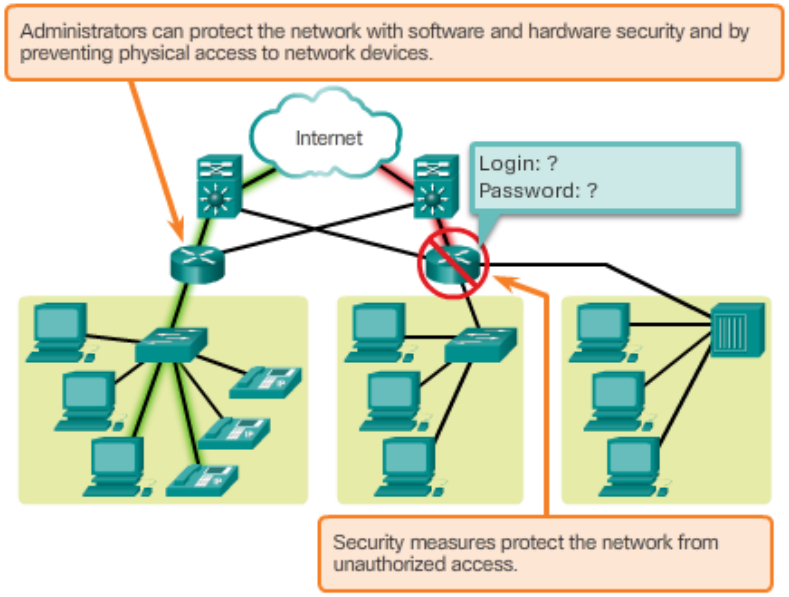
- **Scalability** - A scalable network can expand quickly to support new users and applications without impacting the performance of the service being delivered to existing users.



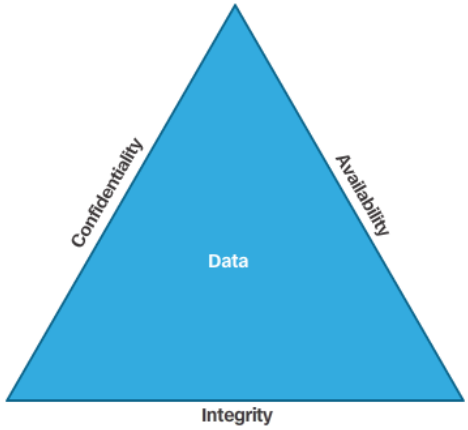
- **Quality of Service (QoS)** - QoS becomes a primary mechanism for managing congestion and ensuring reliable delivery of content to all users.



- **Security** - There are two types of network security concerns that must be addressed:
  - **Securing a network infrastructure** includes the physical securing of devices that provide network connectivity, and preventing unauthorized access to the management software that resides on them.



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



- **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.

THE CHANGING NETWORK ENVIRONMENT

Network Trends

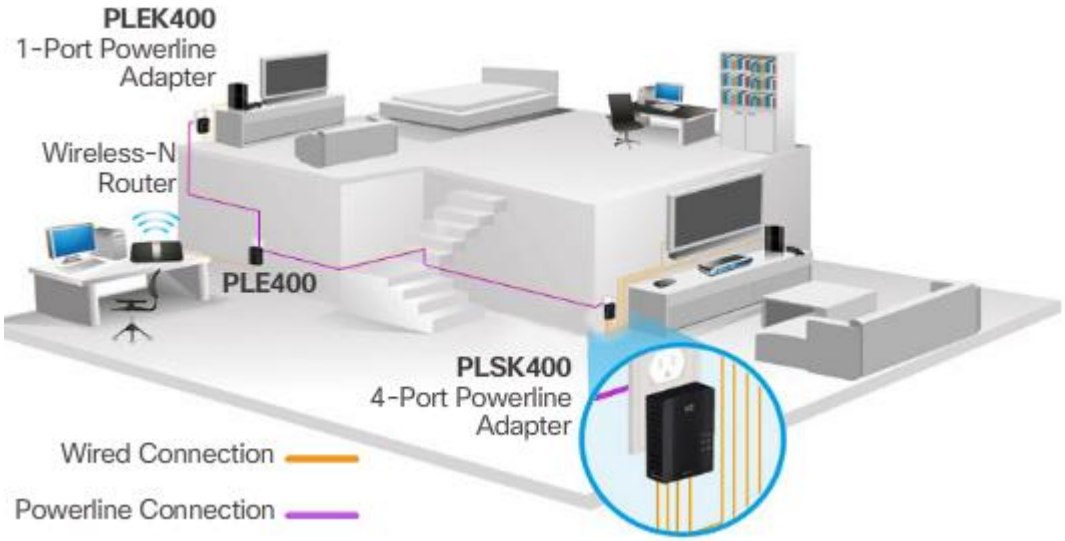
As new technologies and end user devices come to market, businesses and consumers must continue to adjust to this ever-changing environment. There are several new networking trends that will effect organizations and consumers. Some of the top trends include:

- **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.
- **Online Collaboration** - Collaboration is defined as "the act of working with another or others on a joint project." Collaboration tools, like Cisco WebEx shown in the figure, give employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives.
- **Video Communication** - 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.
- **Cloud Computing** - 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.

Network Technologies for 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.

Powerline networking is also 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.

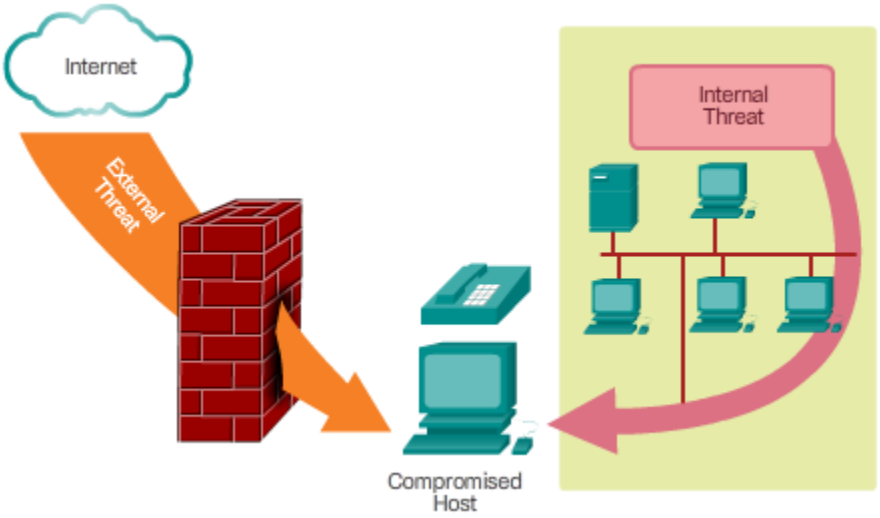


Connecting to the Internet is vital in smart home technology. DSL and cable are common technologies used to connect homes and small businesses to the Internet. However, wireless may be another option in many areas.

Wireless Internet Service Provider (WISP) 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.

Network Security

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 that is 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.



Threat vectors may be **external** or **internal**. 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

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 end 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** – These are used to protect end devices from becoming infected with malicious software.
- **Firewall filtering** – This is used to block unauthorized access to the network. This may include a host-based firewall system that is implemented to prevent unauthorized access to the end 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** – These are used to provide more advanced firewall capabilities that can filter large amounts of traffic with more granularity.
- **Access control lists (ACL)** – These are used to further filter access and traffic forwarding.
- Intrusion prevention systems (IPS) – These are used to identify fast-spreading threats, such as zero-day or zero-hour attacks.
- **Virtual private networks (VPN)** – These are used to provide secure access to remote workers.

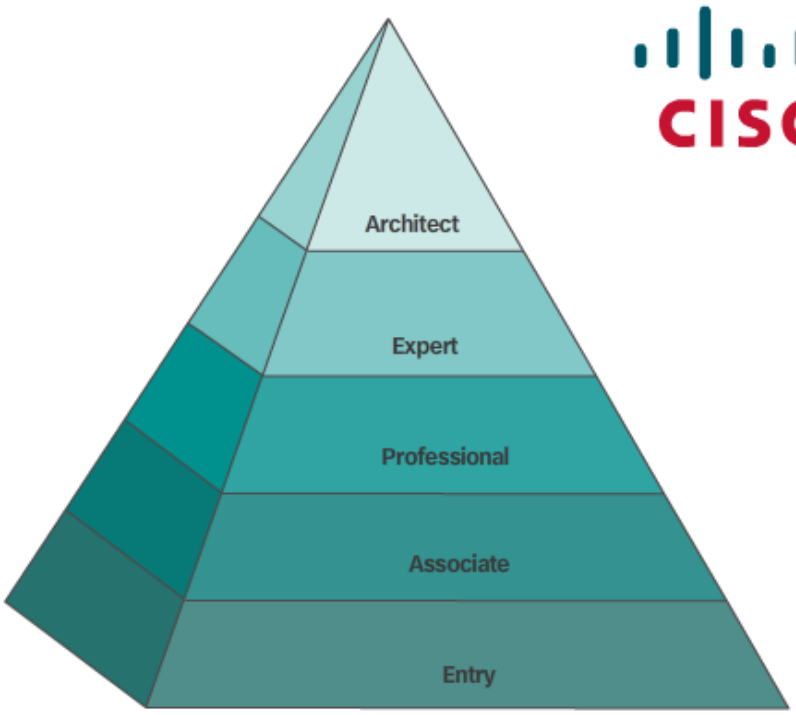
Network Architecture

The **network architecture** refers to the devices, connections, and products that are integrated to support the necessary technologies and applications. A well-planned network technology architecture helps ensure the connection of any device across any combination of networks. While ensuring connectivity, it also increases cost efficiency by integrating network security and management and improves business processes.

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

CCNA certification validates an individual's ability to install, configure, operate, and troubleshoot medium-size route and switched networks, including implementation and verification of connections to remote sites in a WAN. CCNA curriculum also includes basic mitigation of security threats, introduction to wireless networking concepts and terminology, and

performance-based skills. This CCNA curriculum includes the use of various protocols, such as: IP, Open Shortest Path First (OSPF), Serial Line Interface Protocol, Frame Relay, VLANs, Ethernet, access control lists (ACLs) and others.



SUMMARY

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

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

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

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

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

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

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