



Ch 1: Introduction to Networks

Ch 2: Configuring a Network Operating System



Computer Networks Course

BY

Dr. Essam Halim Houssein

Cisco | Networking Academy®
Mind Wide Open™

Computer Networks Course

A. List of References:

Essential Reference: Cisco System, CCNA V5 (Model 1 & 2) [CCENT Certification] .

Course Coordinator: Dr. Essam H. Houssein

Signature :(*Dr. Essam Halim*)

Computer Networks Course

Weighting of Assessments:

<i>Final-Term Examination</i>	(65 Degree)	65%
<i>Mid-Term Examination</i>	(10 Degree)	10%
<i>Practical and Oral Examination</i>	(<i>Project</i> 20 Degree)	20%
<i>Other types of assessment</i>	(<i>Assignments</i> 5 Degree)	5 %
		100 %

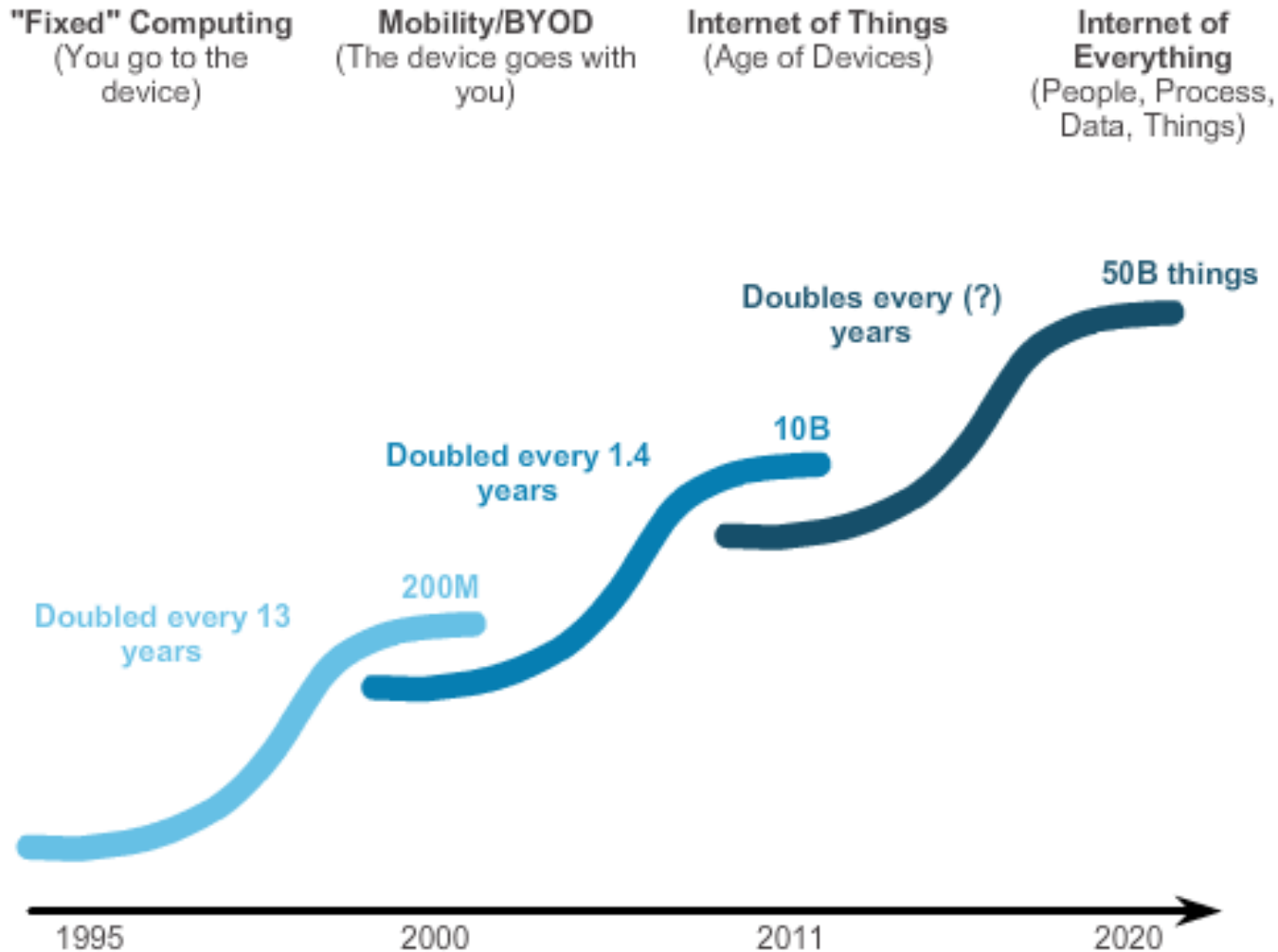
As the course title states, the focus of this course is on learning the fundamentals of networking. In this course, you will learn both the practical and conceptual skills that build the foundation for understanding basic networking.

You will do the following:

Network communication and introduced to the two major models used to plan and implement networks: OSI and TCP/IP gain an understanding of the "layered" approach to networks examine the OSI and TCP/IP layers in detail to **understand their functions and services become familiar with the various network devices and network addressing schemes discover the types of media used to carry data across the network.** *By the end of this course, you will be* able to build simple LANs, perform basic configurations for routers and switches, and implement IP addressing schemes.

Chapter 1: Exploring the Network

Imagine a world without the Internet.



The **IoE** is bringing together people, process, data, and things to make networked connections more relevant and valuable

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

Some forms of communication include:

Instant Messaging (IM) / Texting – IM and texting both enable instant real-time communication between two or more people.

Social Media – Social media consists of interactive websites

Collaboration Tools - Collaboration tools give people the opportunity to work together on shared documents.

Weblogs (blogs) - Weblogs are web pages that are easy to update and edit.

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.

Podcasting - Podcasting is an audio-based medium that originally enabled people to record audio and convert it for use.

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.

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

How do you play on the Internet?

Providing Resources in a Network

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.

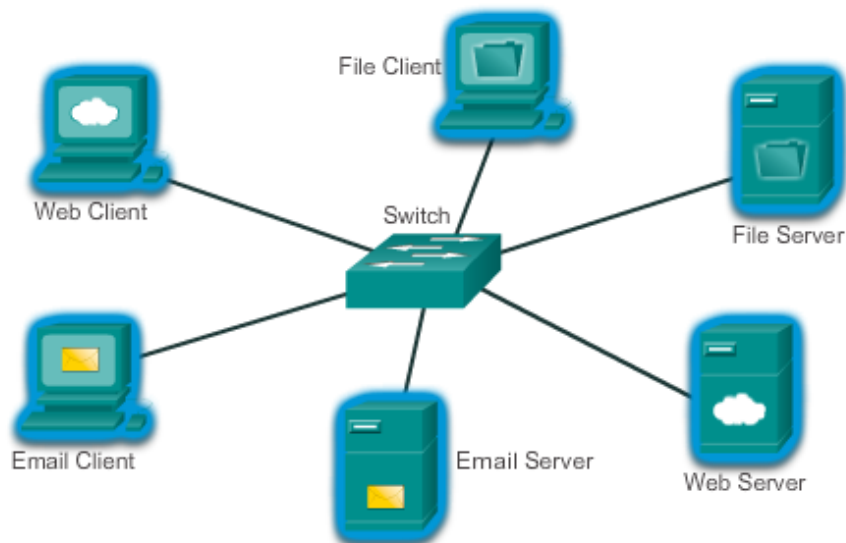
In businesses and large organizations, networks can be used on an even broader scale to allow employees to provide consolidation, storage, and access to information on network servers.

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

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.

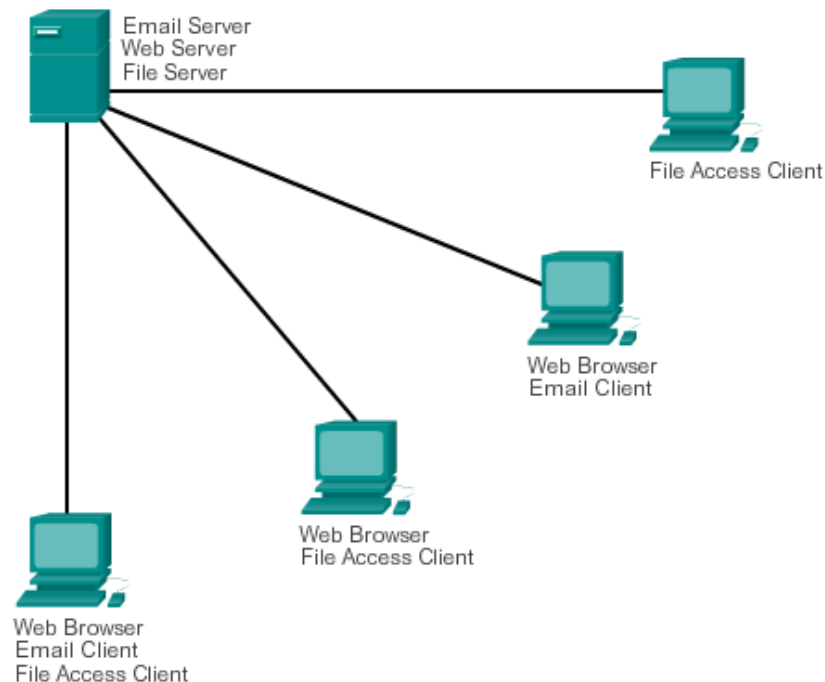
Clients are computer hosts that have software installed that enable them **to request and display the information** obtained from the server. An example of client software is a web browser, like Internet Explorer.



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.



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**.

Components of a Network

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

The network infrastructure contains **three** categories of **network components**:

1. **Devices**
2. **Media**
3. **Services**

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:

1. Computers (work stations, laptops, file servers, web servers).
2. Network printers.
3. VoIP phones.
4. TelePresence endpoint.
5. Security cameras.
6. Mobile handheld devices (such as smartphones, tablets, etc).

A host device is either the source or destination of a message transmitted over the network...

Intermediary (network) devices interconnect end devices. These devices provide connectivity and work behind the scenes to ensure that data flows across the network. Network devices connect the individual hosts to the network and can connect multiple individual networks to form an internetwork.

Examples of intermediary network devices are:

1. **Network Access (switches and wireless access points).**
2. **Internetworking (routers).**
3. **Security (firewalls).**

Processes running on the network devices perform these functions:

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

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

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

1. **Metallic wires within cables.**
2. **Glass or plastic fibers (fiber optic cable).**
3. **Wireless transmission.**

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:**

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

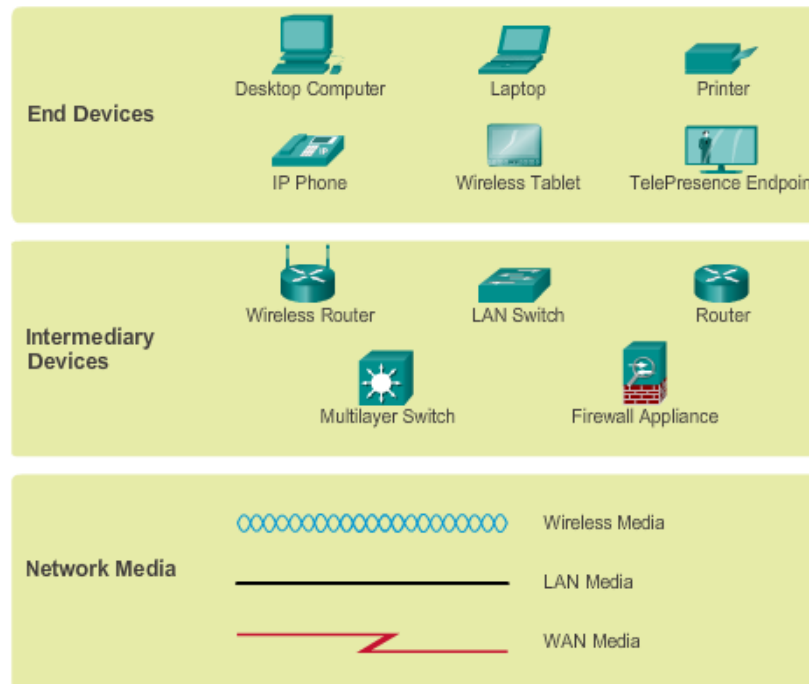
In addition to these representations, specialized terminology is used when discussing how each of these devices and media connect to each other. Important terms to remember are:

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.

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**.



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 network devices, configured ports, and cable installation.

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

LANs, WANs, and the Internet

Network infrastructures can vary greatly in terms of:

- ❑ Size of the area covered, Number of users, Number and types of services

The two most common types of network infrastructures:

Local Area Network (LAN) - A network infrastructure that provides access to users and end devices in a small geographical area.

Wide Area Network (WAN) - A network infrastructure that provides access to other networks over a wide geographical area.

Other types of networks include:

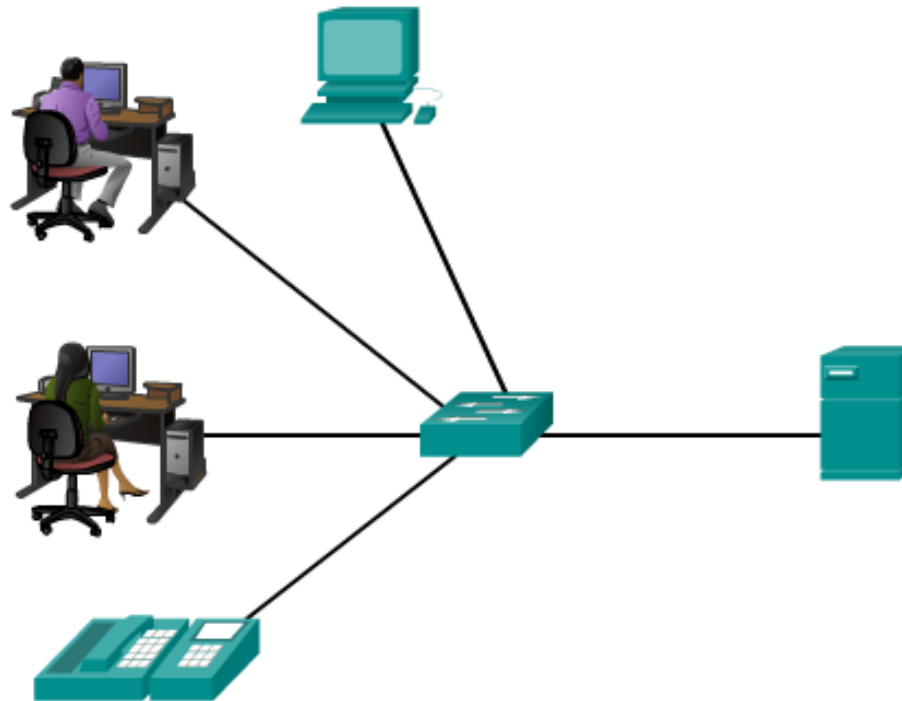
Metropolitan Area Network (MAN) - A network infrastructure that spans a physical area larger than a LAN but smaller than a WAN (e.g., a city).

Wireless LAN (WLAN) - Similar to a LAN but wirelessly.

Storage Area Network (SAN) - A network infrastructure designed to support file servers and provide data storage, retrieval, and replication.

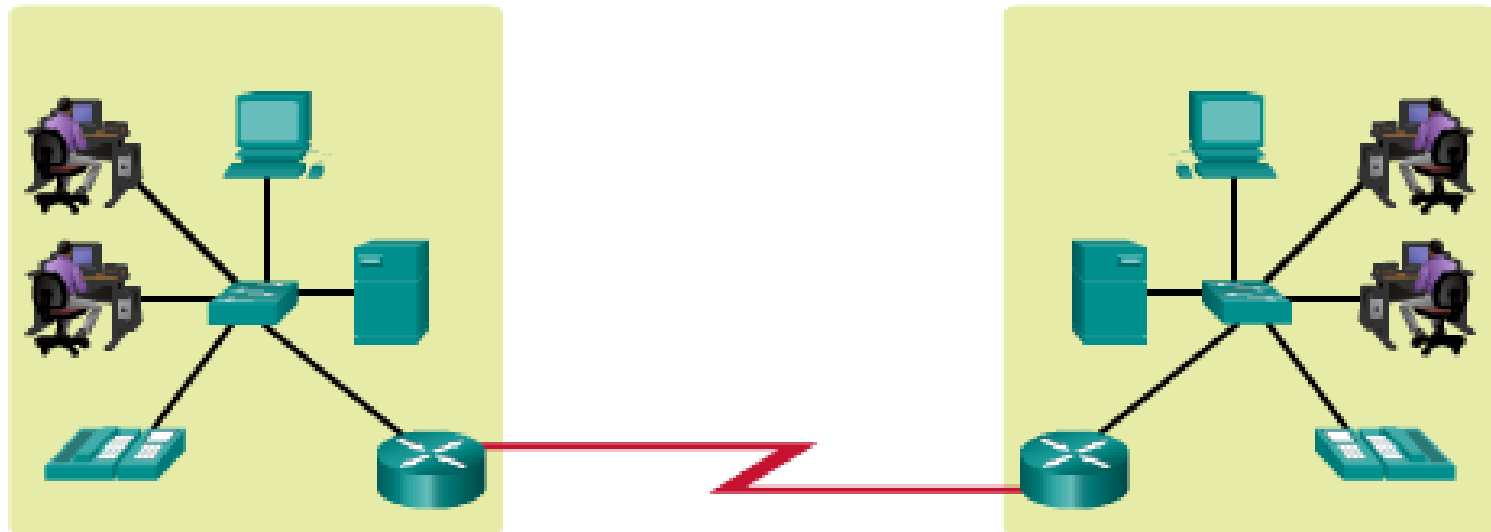
Local Area Networks (LANs) - Specific features of LANs include:

1. LANs interconnect end devices in a limited area.
2. A LAN is usually administered by a single organization or individual.
3. LANs provide high speed bandwidth to internal end devices and network devices.

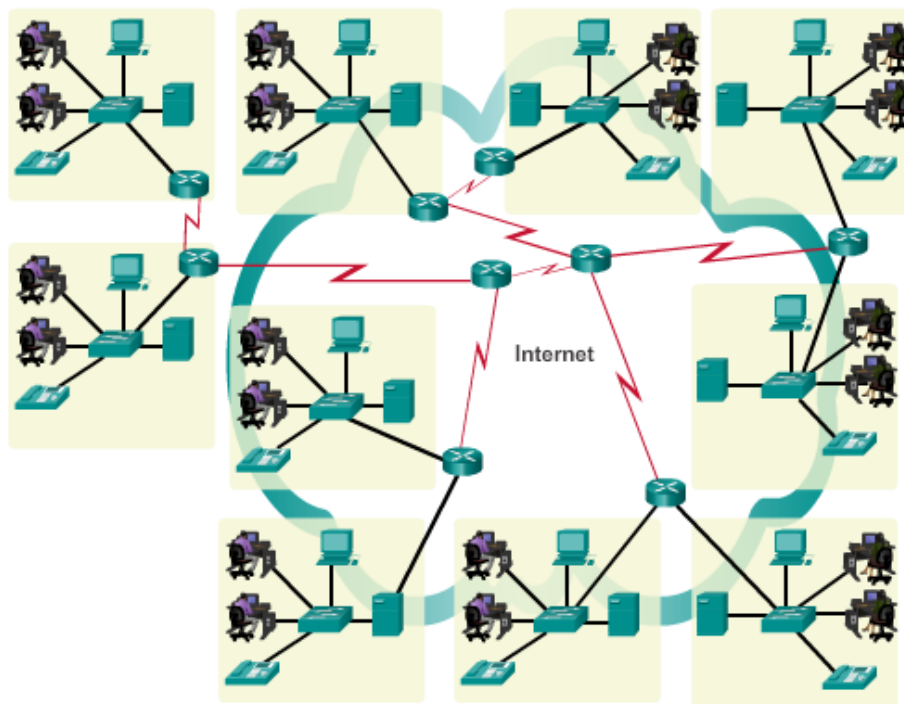


Wide Area Networks (WANs) are typically managed by service providers (SP) or Internet Service Providers (ISP). **Specific features of WANs include:**

1. WANs interconnect LANs over wide geographical areas.
2. WANs are usually administered by multiple service providers.
3. WANs typically provide slower speed links between LANs.



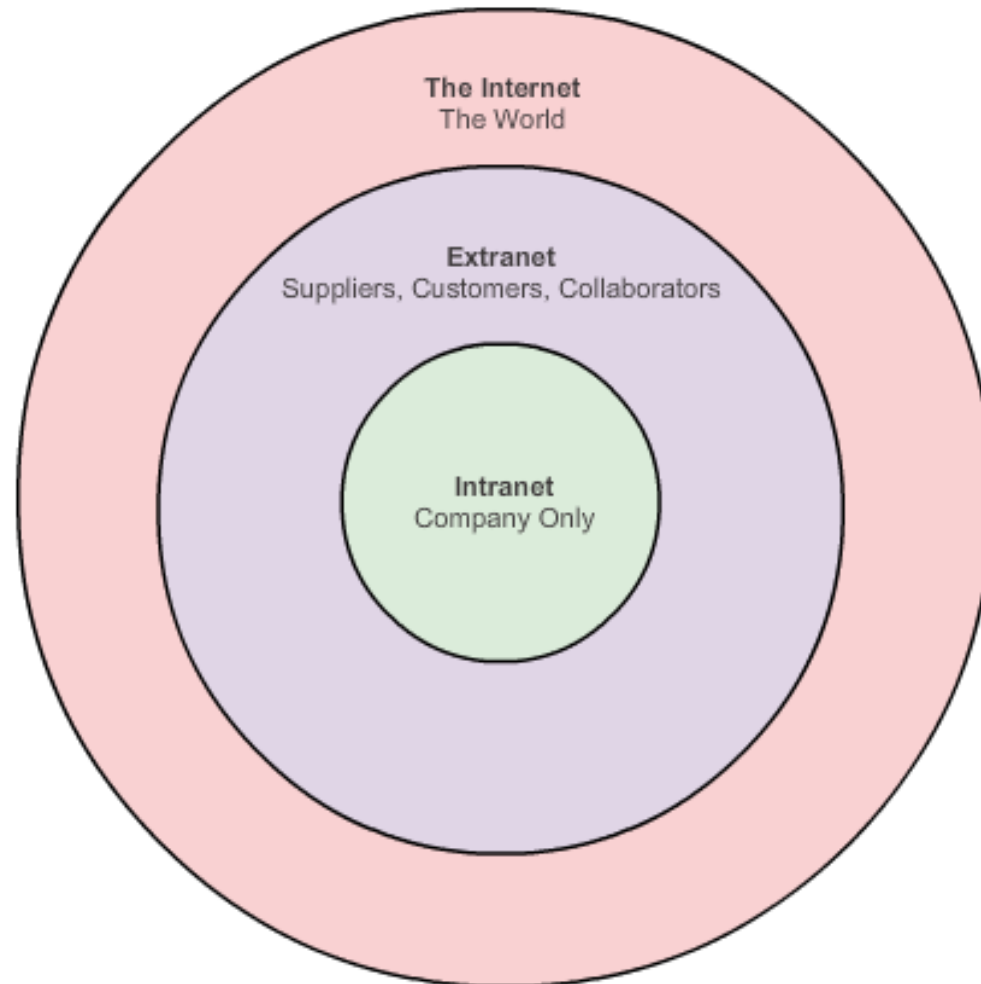
Internet is a worldwide collection of interconnected networks (internetworks or internet for short), cooperating with each other to exchange information using common standards. Through telephone wires, fiber optic cables, wireless transmissions, and satellite links, Internet users can exchange information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



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

☐ **Intranet**

☐ **Extranet**



Connecting to the Internet

Cable - Typically offered by cable television service providers, the Internet data signal is carried on the same coaxial cable that delivers cable television.

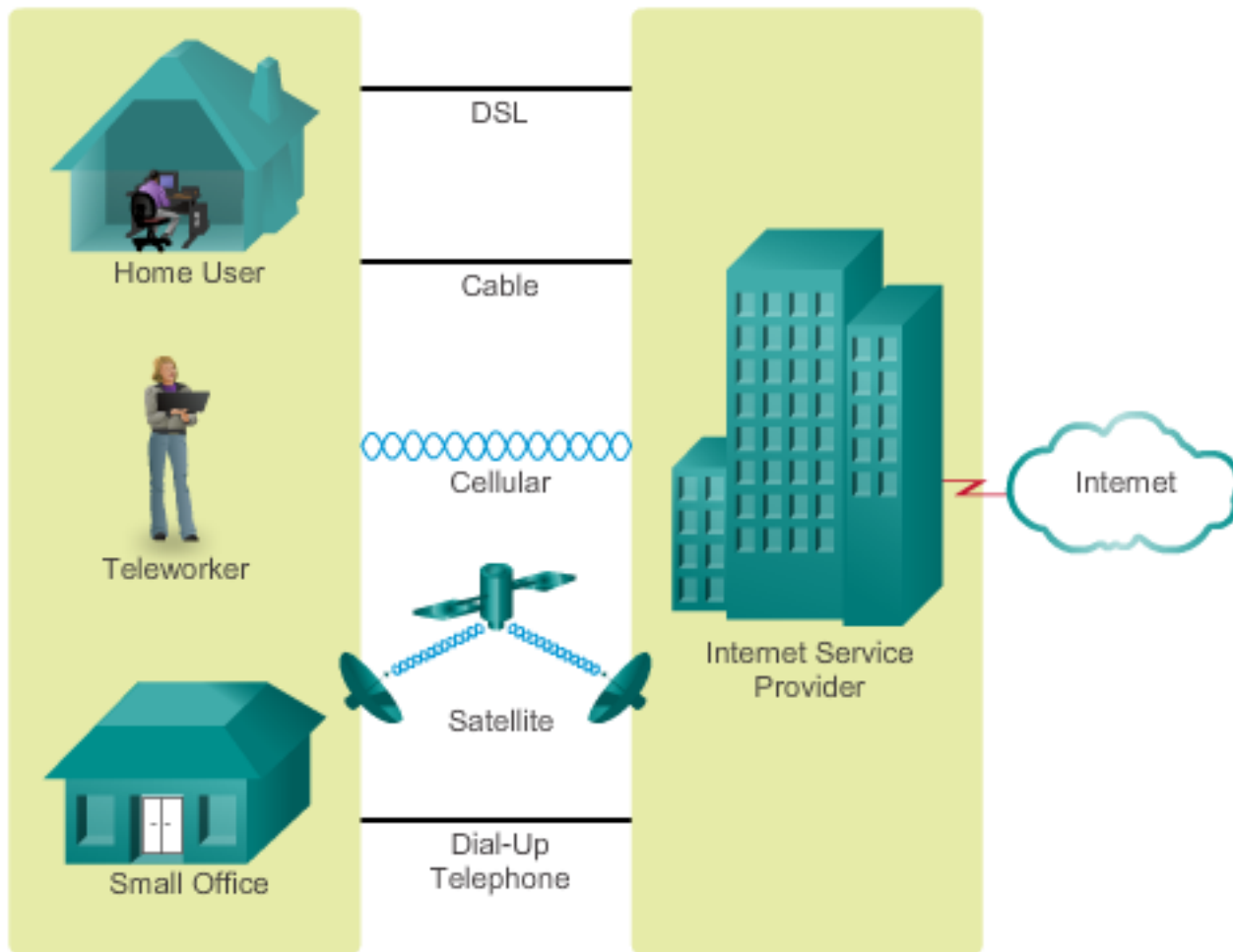
DSL - Provides a high bandwidth, always on, connection to the Internet. It requires a special high-speed modem that separates the DSL signal from the telephone signal and provides an Ethernet connection to a host computer or LAN. DSL runs over a telephone line, with the line split into three channels.

Cellular - Cellular Internet access uses a cell phone network to connect.

Satellite - Satellite service is a good option for homes or offices that do not have access to DSL or cable.

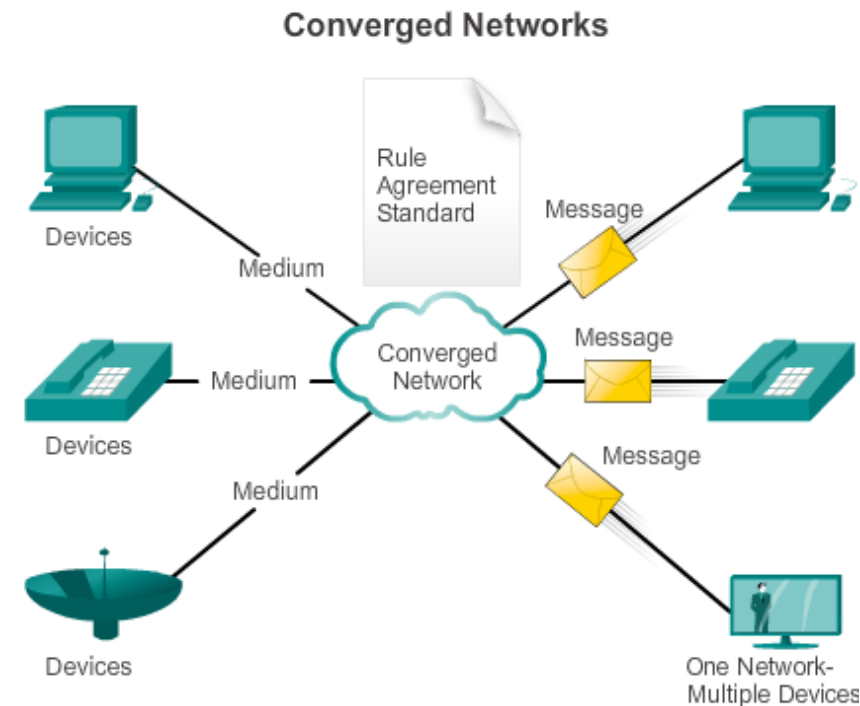
Dial-up Telephone - An inexpensive option that uses any phone line and a modem. To connect to the ISP, a user calls the ISP access phone number.

Connection Options



Converged Networks

Converged networks are capable of delivering voice, video streams, text, and graphics between many different types of devices over the same communication channel and network structure, as shown in Figure.



Converged data networks carry multiple services on one network.

There are **four basic characteristics** that the underlying architectures need to address in order to meet user expectations (**Reliable Network**):

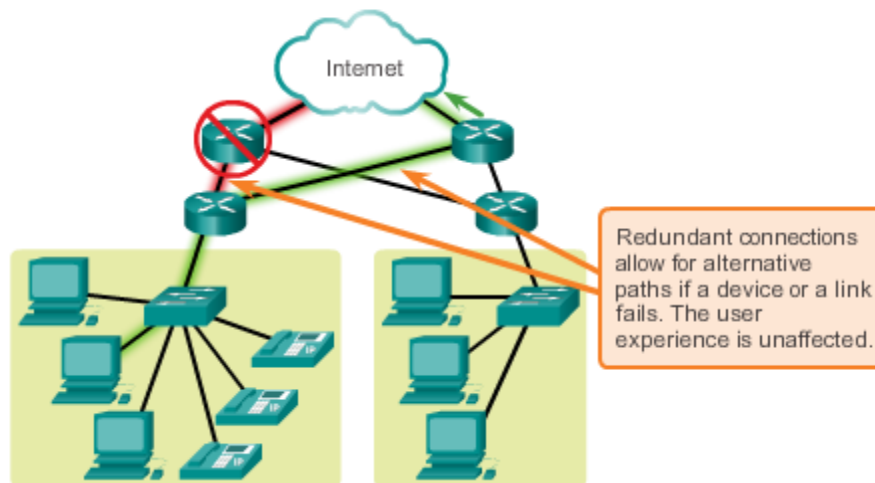
1-Fault Tolerance

2-Scalability

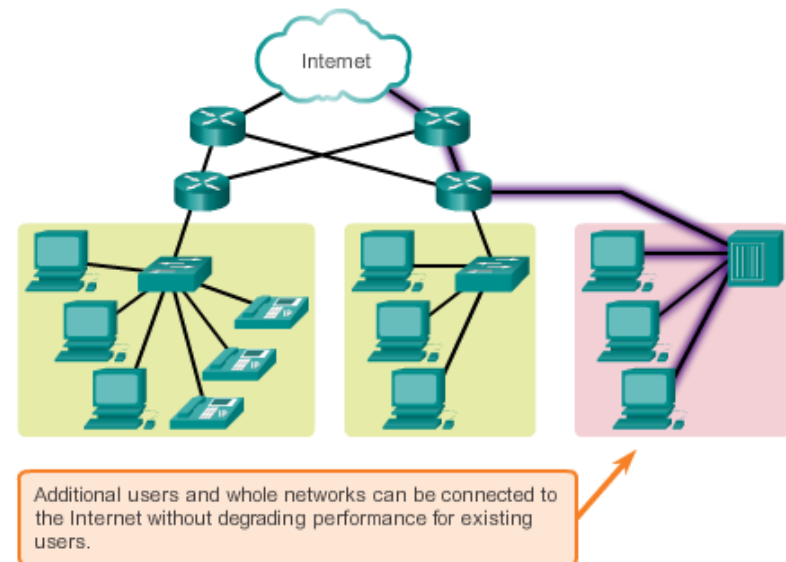
3-Quality of Service (QoS)

4-Security

Fault Tolerance

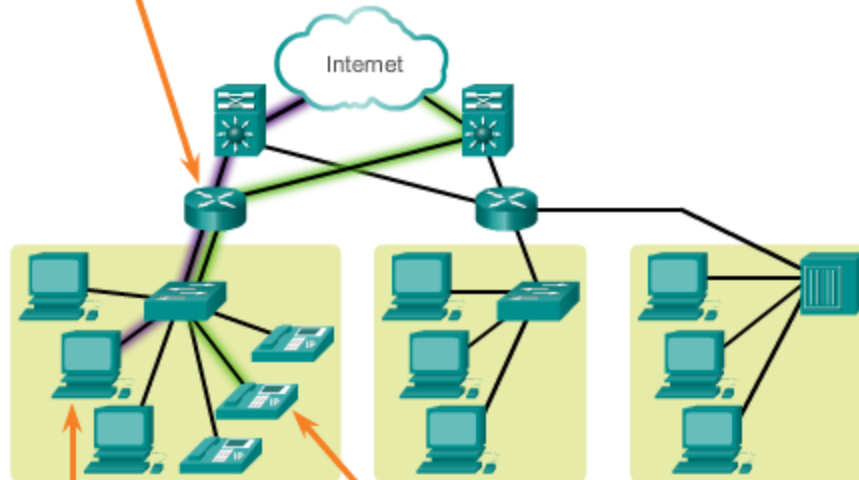


Scalability



Quality of Service (QoS)

Quality of Service, managed by the router, ensures that priorities are matched with the type of communication and its importance to the organization.

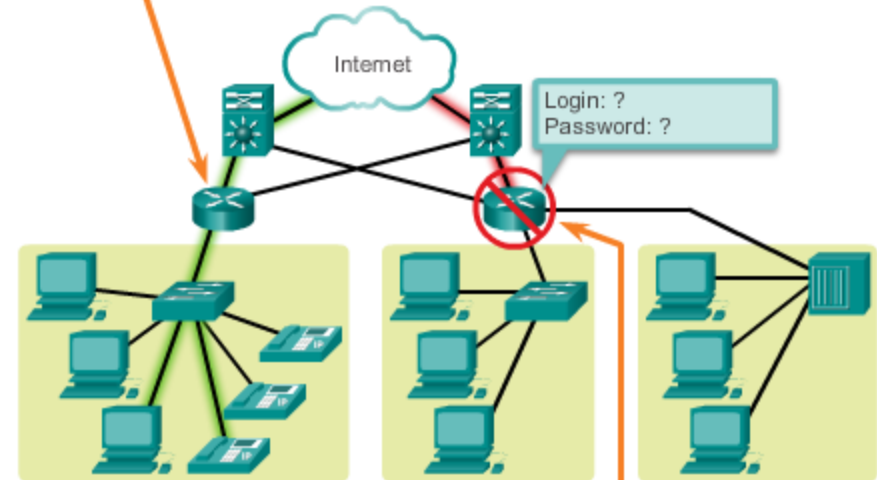


Web pages can usually receive a lower priority.

Streaming media will need priority to maintain a smooth, uninterrupted user experience.

Security

Administrators can protect the network with software and hardware security and by preventing physical access to network devices.

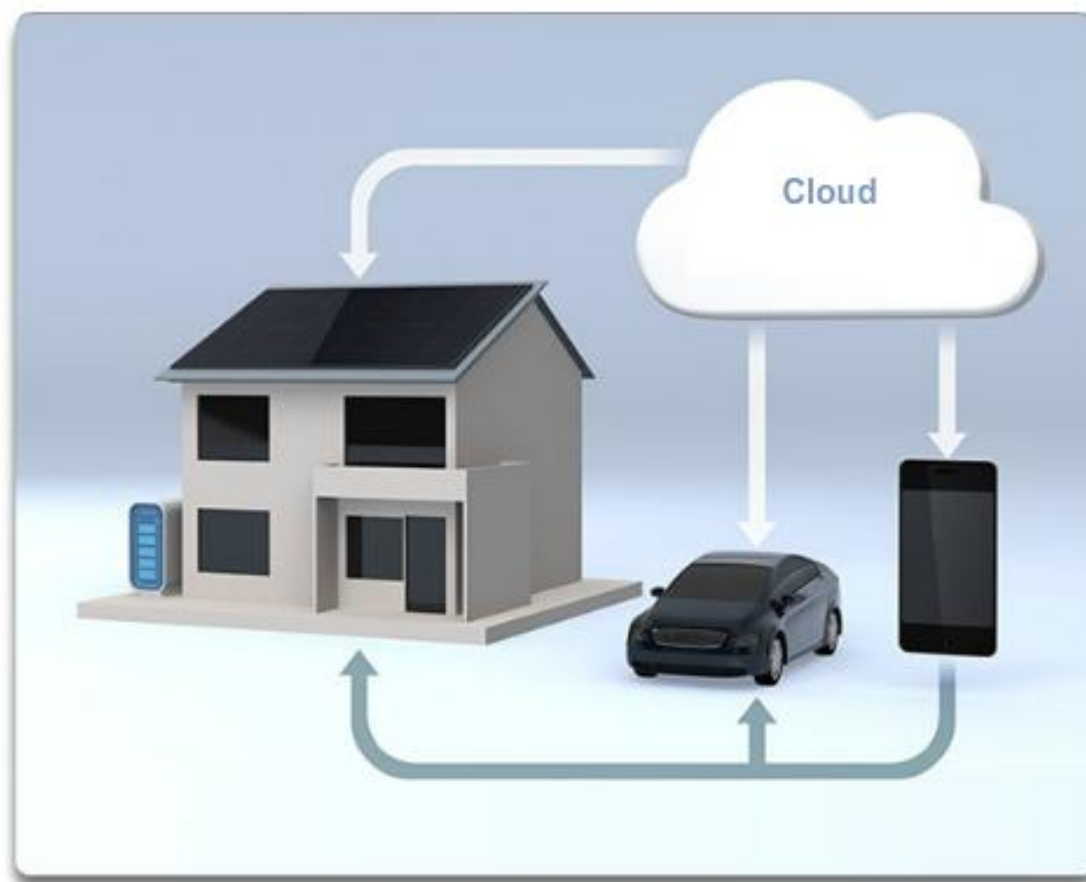


Security measures protect the network from unauthorized access.

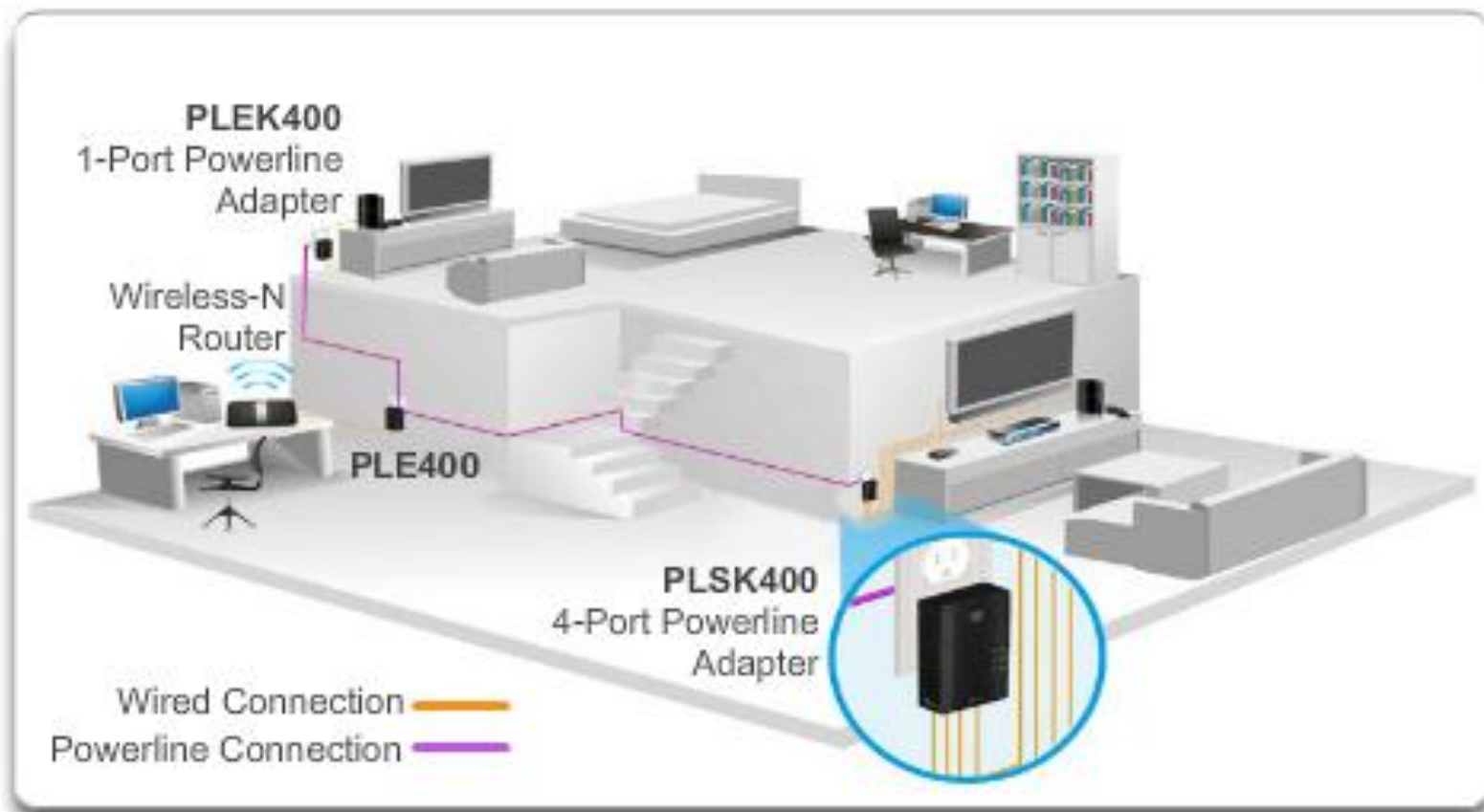
Circuit-Switched Connection-Oriented Networks and Packet-Switched Networks?

Networking Technologies for the Home

Smart Home Technology



Powerline Networking



Network Security

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.

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.

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.

Summary

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

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

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

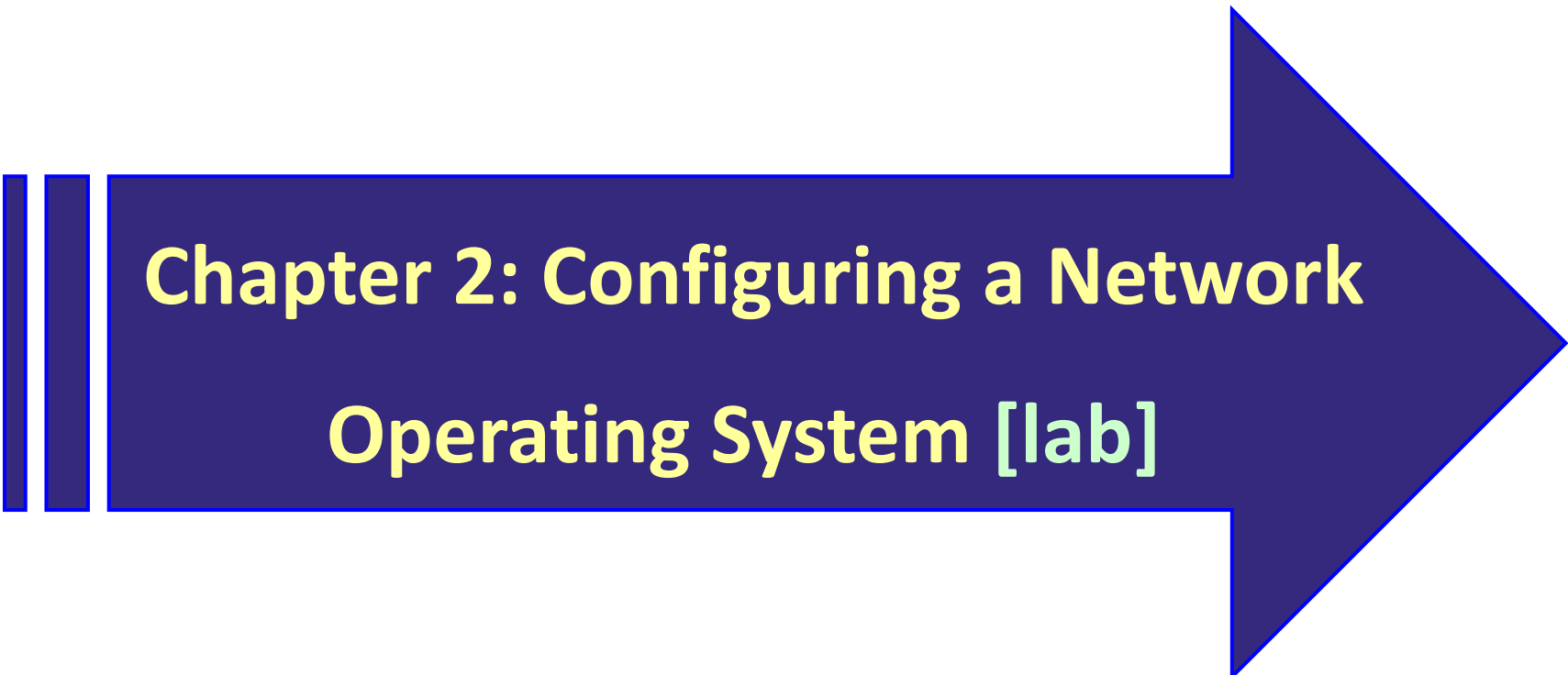
The network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which communication can occur. It is made up of network components including end devices, intermediate device, and network media.

Summary

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

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

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

A large blue arrow pointing to the right, which serves as a background for the chapter title. To the left of the arrow's tail are two vertical blue bars of different heights.

Chapter 2: Configuring a Network Operating System [lab]

All of these end devices are usually connected to a home router. Home routers are actually four devices in one:

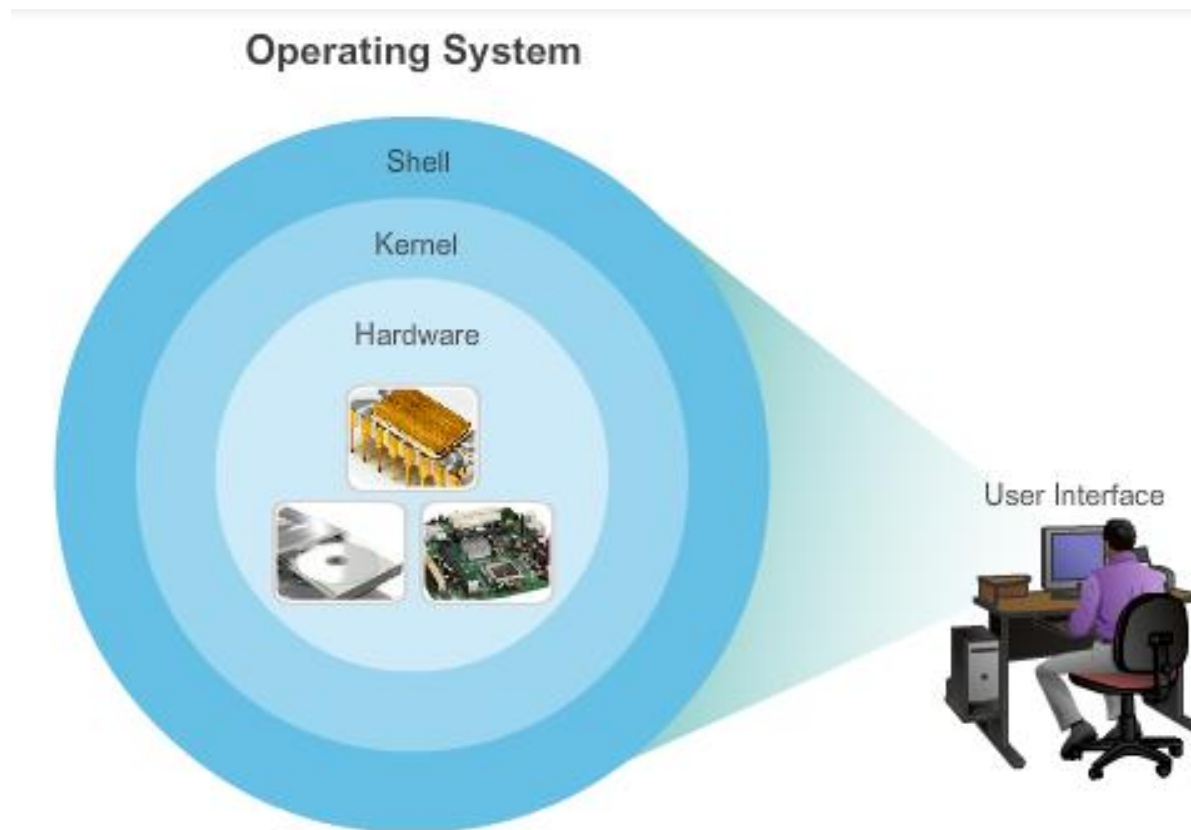
Router - Forwards data packets to and receives data packets from the Internet.

Switch - Connects end devices using network cables.

Wireless access point - Consists of a radio transmitter capable of connecting end devices wirelessly.

Firewall appliance - Secures outgoing traffic and restricts incoming traffic.

All end devices and network devices connected to the Internet require an operating system (OS) to help them perform their function.



The **IOS** file itself is several megabytes in size and is stored in a semi-permanent memory area called **flash**, compact flash card and **non-volatile** storage.

In many Cisco devices, the IOS is copied from **flash into random access memory (RAM)** when the device is powered on. RAM is considered **volatile** memory because data is lost during a power cycle.

There are several ways to access the CLI environment. The most common methods are:

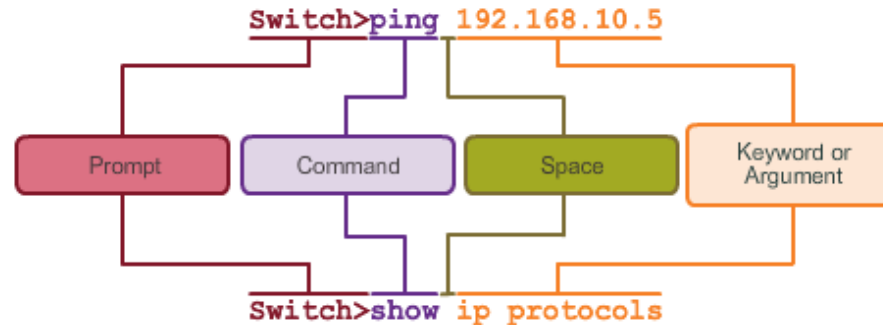
1. **Console.**
2. **Telnet or SSH.**
3. **AUX port.**

Navigating the IOS

After a network technician is connected to a device, it is possible to configure it. **The network technician must navigate through various modes of the IOS.** The **Cisco IOS modes** are quite similar for switches and routers. The CLI uses a hierarchical structure for the modes.

1. **User executive (User EXEC) mode.**
2. **Privileged executive (Privileged EXEC) mode.**
3. **Global configuration mode.**
4. **Other specific configuration modes.**

Basic IOS Command Structure



The IOS has several forms of help available:

Context-Sensitive Help.

Command Syntax Check (Ambiguous, Incomplete and Incorrect).

Hot Keys and Shortcuts.

Show command – Hostnames - Limiting Access to Device Configurations -
 Saving Configurations - Ports and Addresses - Addressing Devices -
 Verifying Connectivity ??????

