5️⃣

Chapter 5 Networking Concepts

Class	CompTIA A+
Created	@November 24, 2021 11:45 AM
Date	Monday
Importance	☐
Materials	
Packet Tracer	
Reviewed	☑
Study Schedule (Class notes)	
Type	Lecture

Network Components and Types

Types of networks

1. Host devices

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

2. Intermediary devices

   Computer networks contain many devices that exist in between the host devices. These intermediary devices ensure that data flows from one host device to another host device.

   The most common devices:

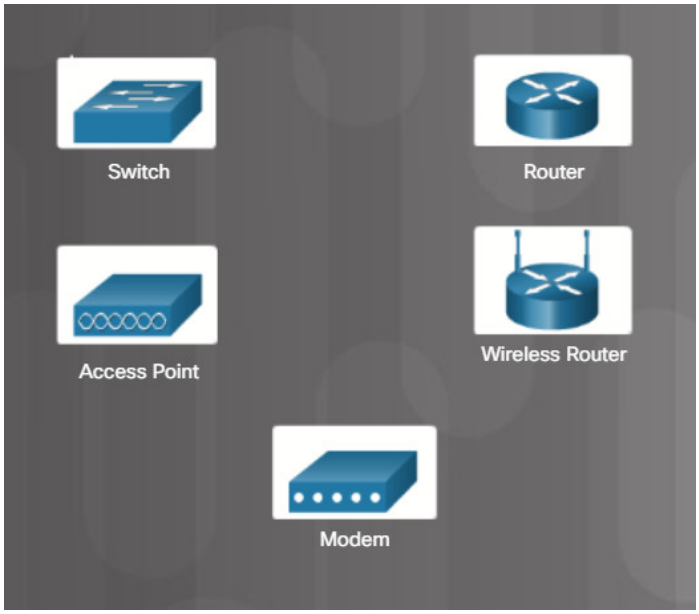
   a. **Switch**: connects multiple devices to the network

   b. **Router**: forwards traffic between networks

c. **Wireless router**: connects multiple wireless devices to the network and may include a switch to connect wired hosts

d. **Access point (AP)**: connects to a wireless router and is used to extend the reach of a wireless network

e. **Modem**: connects a home or small office to the Internet



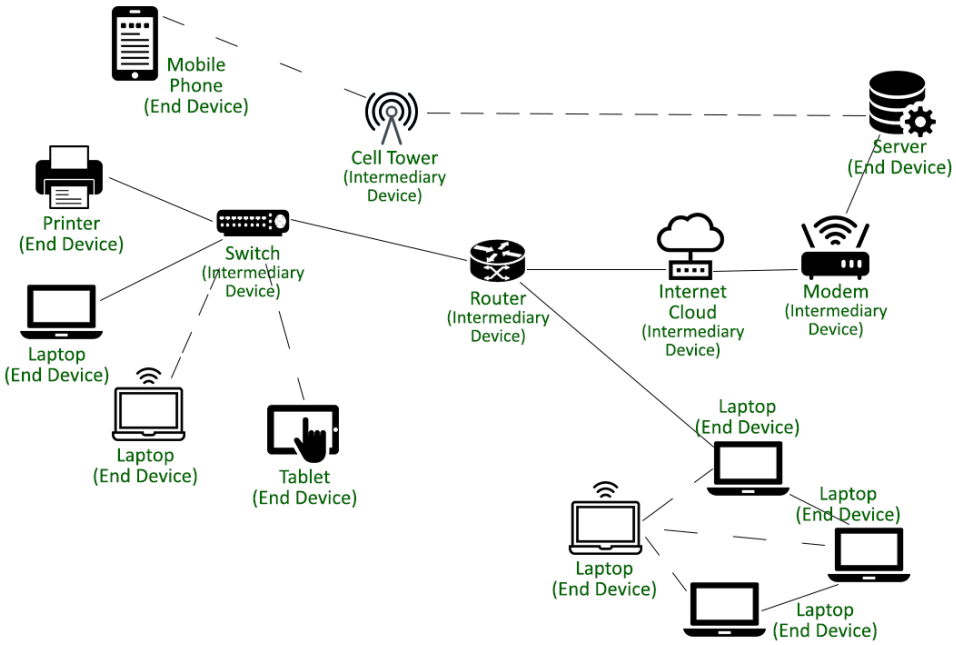
3. **Network media**

a. LAN media

b. WAN media

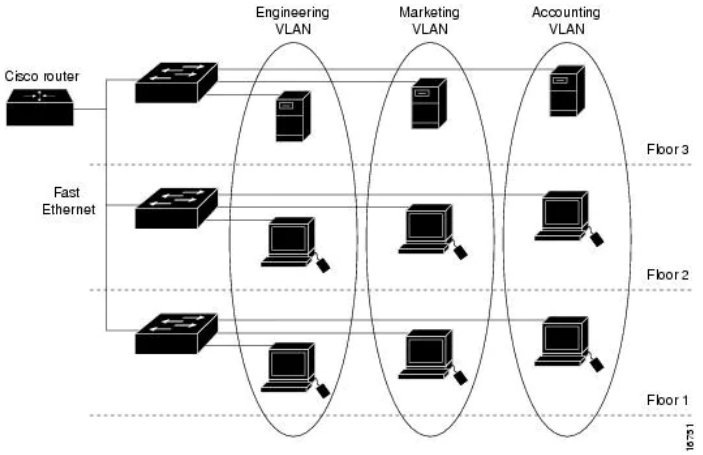
c. Wireless media

d. Network



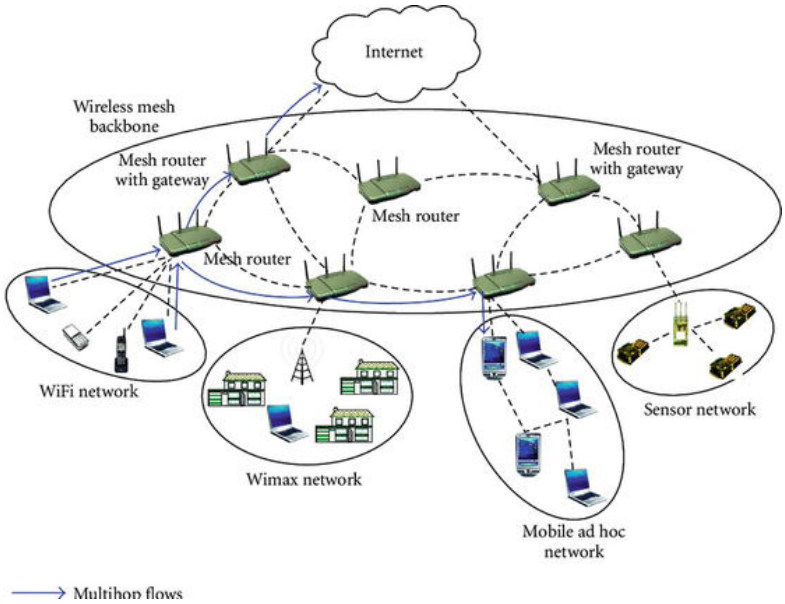
Network topologies and description

- A **personal area network (PAN)** is a network that connects devices, such as mice, keyboard, printers, smartphones, and tablets within the range of an individual person. They are mostly connected via Bluetooth.
- A **local area network (LAN)** is defined as a network that connects devices using wire cables in a small geographical area. The distinguishing characteristics for LANs today is that they are typically owned by an individual.
- **Virtual LANs (VLANs)** allow an administrator to segment the ports on a single switch as if it were multiple switches.

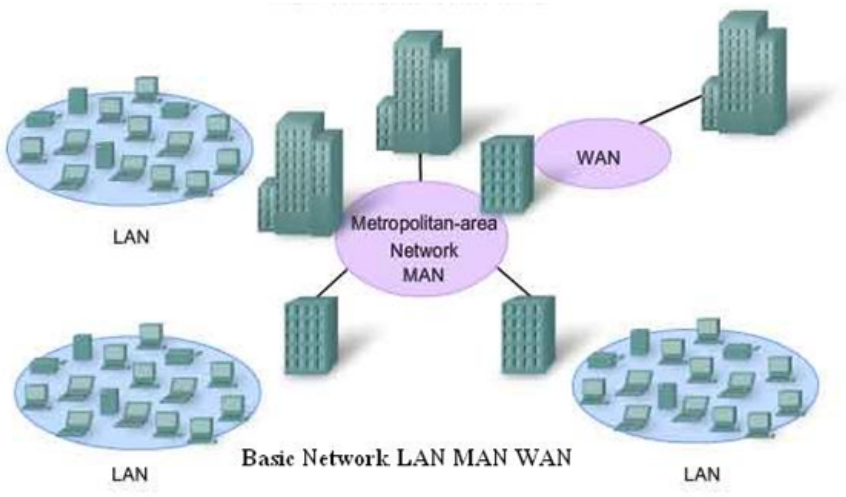


- A **wireless LAN (WLAN)** is similar to a LAN but wirelessly connects users and devices in a small geographical area instead of using a wired connection.

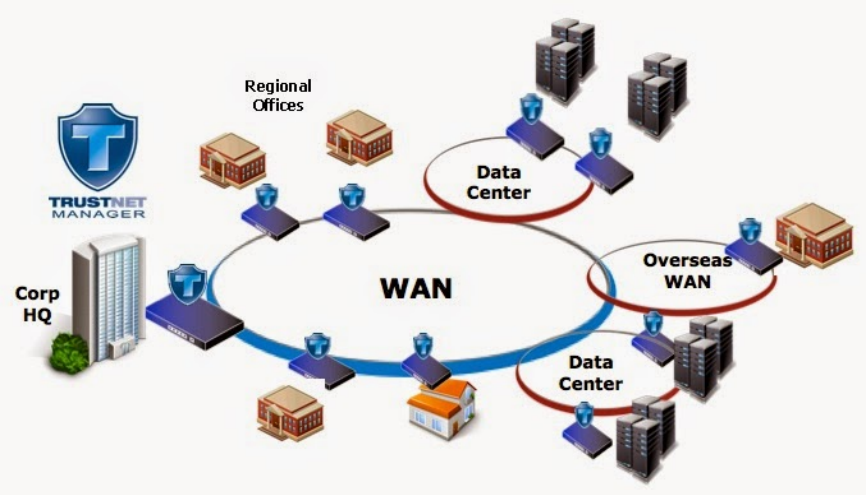
- A **wireless mesh network (WMN)** uses multiple access points to extend the WLAN.



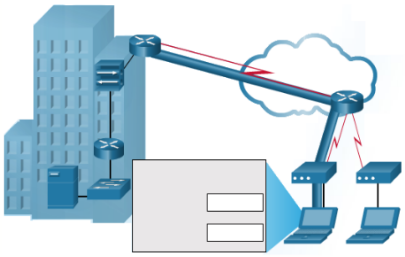
- A **metropolitan area network (MAN)** is a network that spans across a large campus or a city.



- A **wide area network (WAN)** connects multiple networks that are in geographically separated locations.



- A **virtual private network (VPN)** is used to securely connect to another network over an insecure network. The most common type of VPN is used by teleworkers to access a corporate private network.



Internet connection type

Broadband technologies

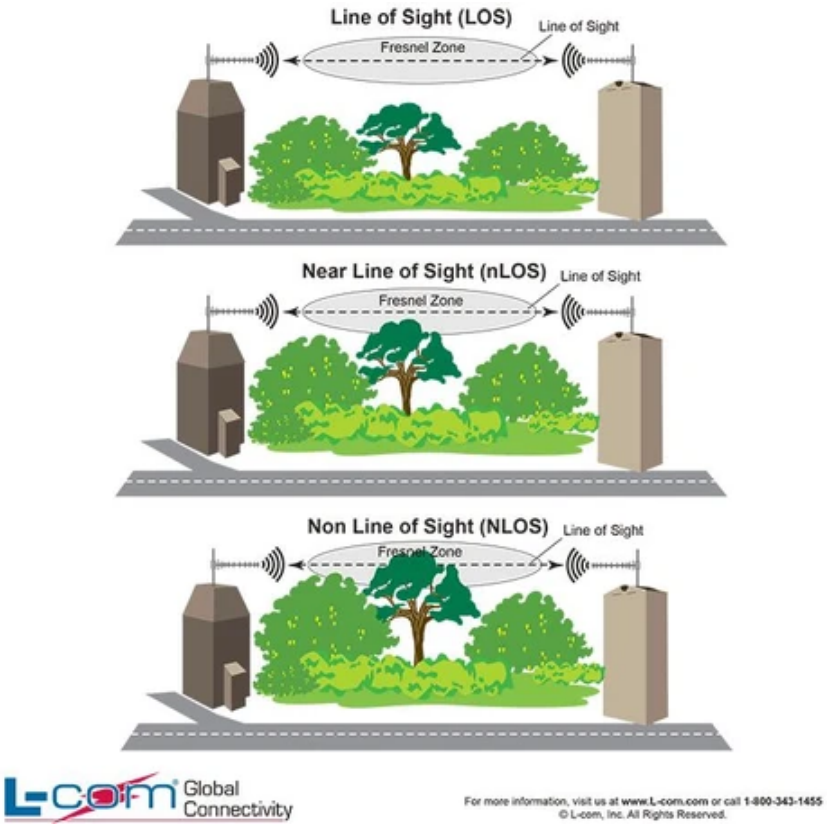
- Analog telephone internet access can transmit data over standard voice telephone lines. It uses an analog modem to place a telephone call to another modem at a remote site.
- Integrated serviced digital network (ISDN) uses multiple channels and can carry different types of services. ISDN is a standard that uses multiple channels to send voice, video, and data over normal telephone wires.
- Broadband uses different frequencies to send multiple signals over the same medium. Some common broadband network connections include cable, digital subscriber line (DSL), ISDN, satellite, and cellular.

DSL, Cable, and Fiber

- **DSL is an always-on service,** which means that there is no need to dial up each time you connect to the internet.
- Cable connection doesn't use telephone lines.
- Fiber optic cables are made of glass or plastic and use light to transmit data. It has a very high bandwidth, which enables them to carry large amounts of data. Fiber is used in backbone networks, large enterprise environments and large data centers.

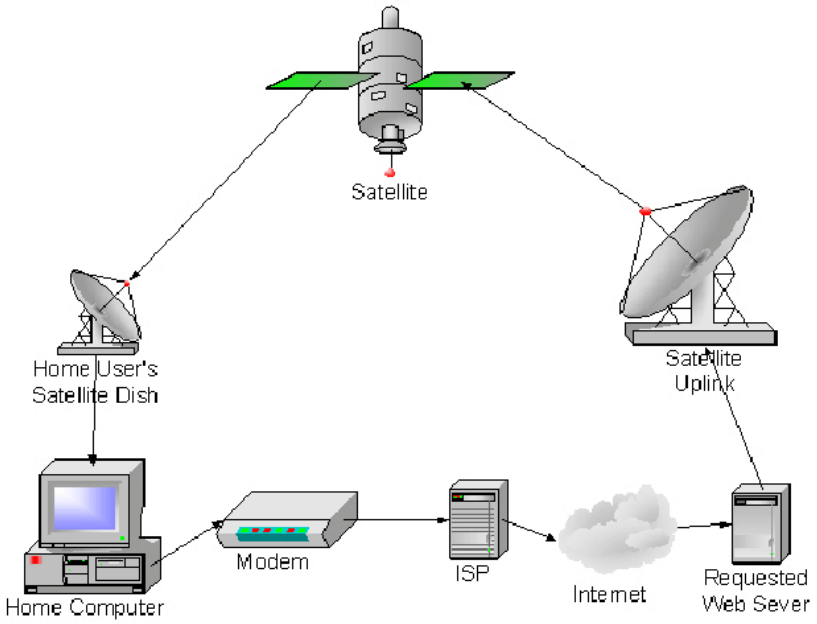
Line of sight wireless internet service

Line of sight wireless internet service is an always-on service that uses radio signals for transmitting internet access.



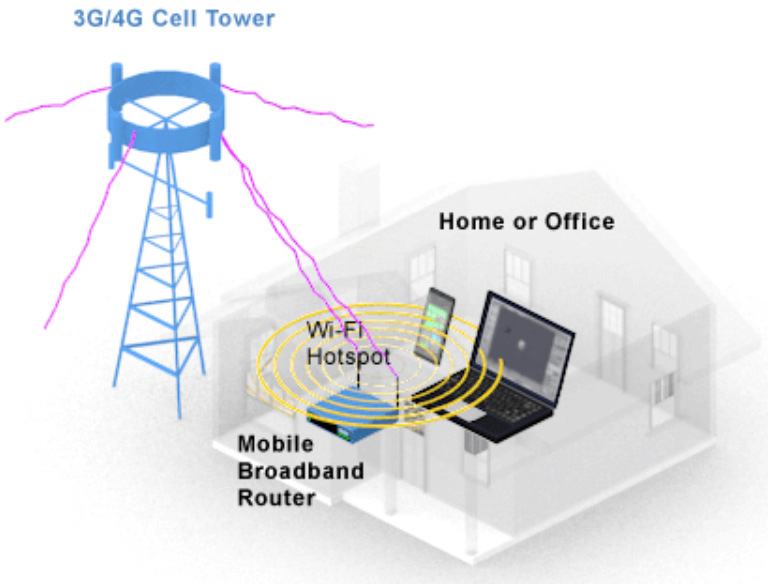
Satellite

Broadband satellite is an alternative for customers who cannot get cable or DSL connections. It doesn't require a phone line or cable, but uses a satellite dish for two-way communication.



Cellular

Cell phone technology relies on cell towers distributed throughout the user's coverage area to provide seamless access to cell phone services and the internet.



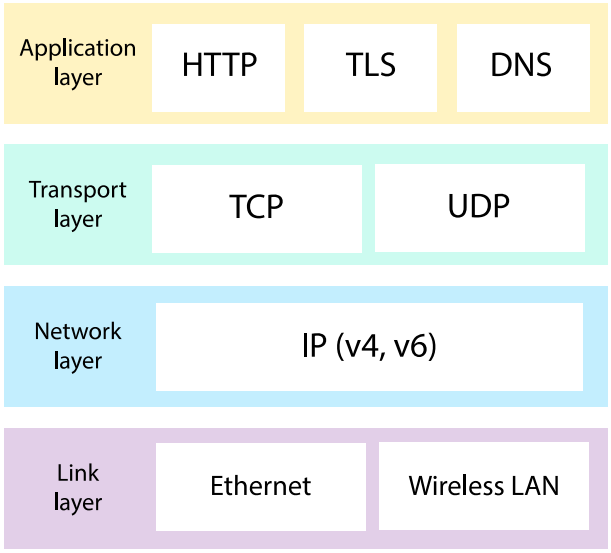
Mobile hotspot and tethering

It can be made using Wi-Fi, Bluetooth, or by using a USB cable.

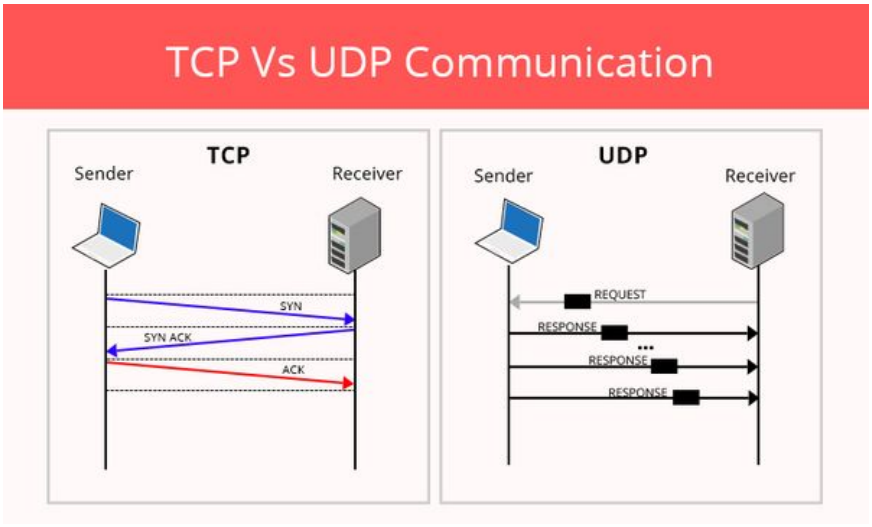
Networking protocols, standards, and services

Transport layer protocols

Network access —> Internet —> Transport —> Application



- TCP: **Reliably**, with guaranteed delivery, and data assembled in proper order
  - TCP adds some "overhead", which means there will be some additional **delay**.
  - SMTP/POP Email
  - HTTP web
- UDP: As **quick** as possible, with some tolerance for **loss of data**
  - real-time video
  - IP telephony



The TCP/IP Model

- The TCP/IP model consists of layers that **perform functions necessary to prepare data for transmission over a network.**
- TCP/IP stands for two important protocols in the model:
  - Transmission Control Protocol (***TCP***) is responsible for tracking all the network connections between a user's device and multiple destinations
  - Internet Protocol (***IP***) is responsible for adding addressing so that data can be routed to the intended destination.
- The two protocols that operate at the **transport layer are TCP and User Datagram Protocol (UDP).**

TCP

TCP transport is analogous to sending packages that are tracked from source to destination.

Three operations of reliability:

- Numbering and tracking data segments transmitted to a specific device from a specific application
- Acknowledging receiving data
- Retransmitting any unacknowledged data after a certain period of time

UDP

UDP is similar to placing regular, non-registered, letter in the mail. **UDP provides the basic functions for delivering data segments between the appropriate applications, with very little overhead and data checking.**

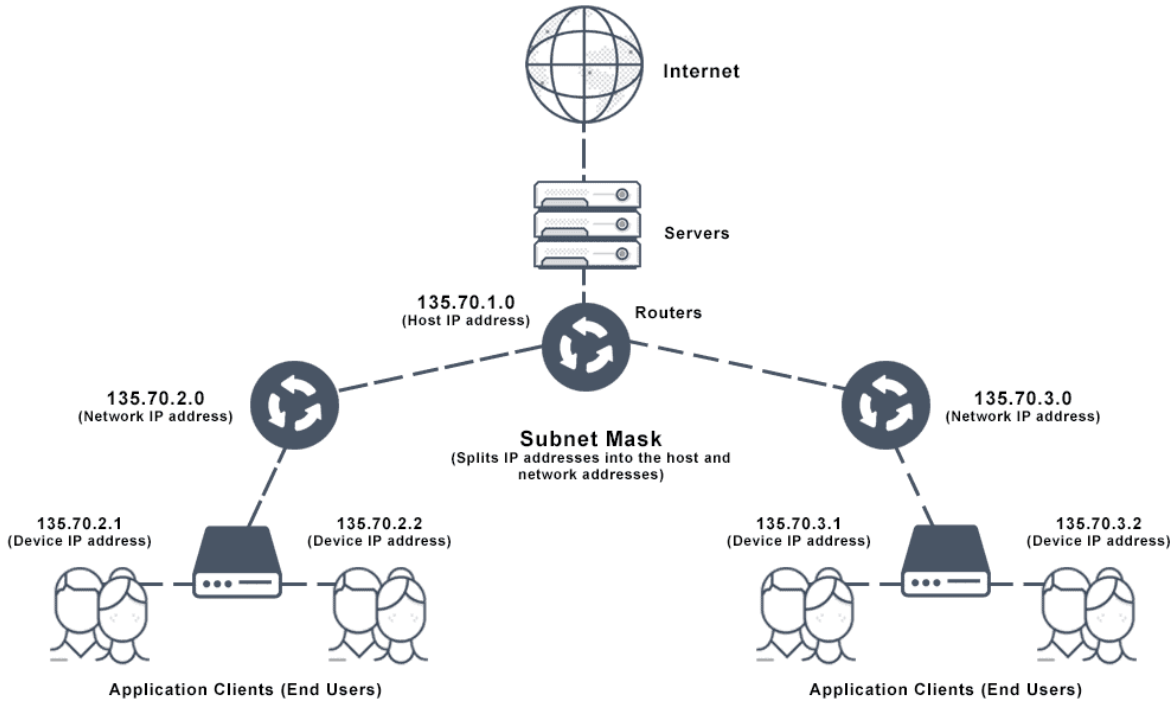
IP addresses

IP address classes

IP address	Subnet mask			
Class A	255.0.0.0	1-126	N.H.H.H	2^24 IP addresses
Class B	255.255.0.0	128-191	N.N.H.H	2^16 IP addresses
Class C	255.255.255.0	192-223	N.N.N.H	2^8 IP addresses

- 127 is reserved for the loopback or localhost (testing use)
- 255.255.255.255 is the broadcast network.
- A subnet mask or subnet is a logical subdivision of an IP network. **It splits the IP address into the host and network addresses**, thereby defining which part of the IP address

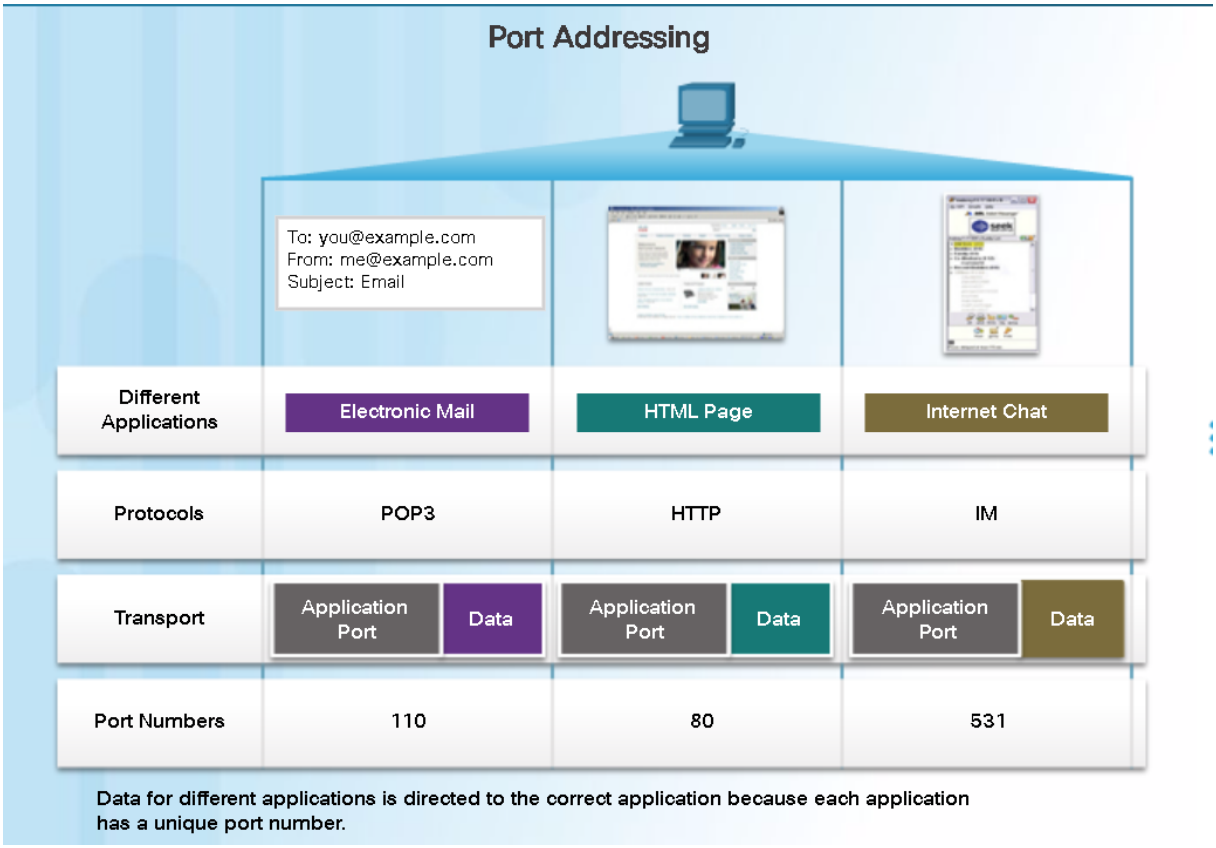
belongs to the device and which part belongs to the network.



- IPv4 address has 32 bits
- IP address contains network address and host address. 255.0.0.0: 255 is the network address and 0.0.0 is the host address.

Application Port Numbers

Every network application is identified by the transport protocol using a **well known** port number



Port addressing

Classify application port numbers

TCP and UDP use a source and destination port number to keep track of application conversations. The source port number is associated with the originating application on the local device. The destination port number is associated with the destination application on the remote device. These are not physical ports. They are numbers that are used by TCP and UDP to identify the applications that should handle the data.

Wireless Protocols

WLAN protocols

Bluetooth, NFC, and RFID

A Bluetooth device can connect up to seven other Bluetooth devices.

RFID uses the frequencies within the 125 MHz to 960 MHz range to uniquely identify items.

NFC uses frequency 13.56 MHz and is a subset of the RFID standards.

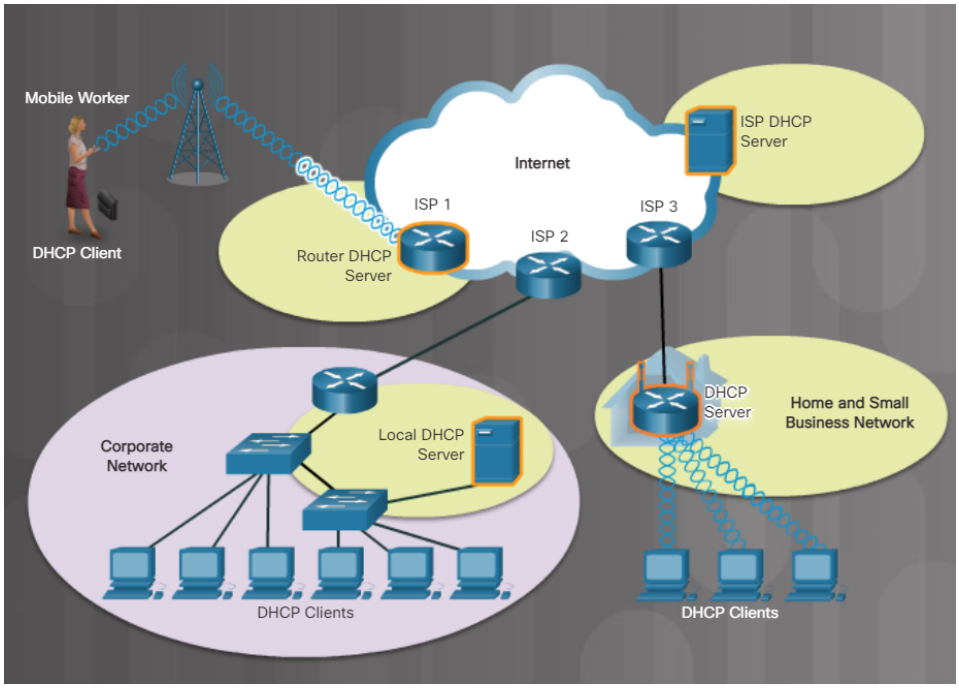
Network Services

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

- File client stores corporate and user files in a central location. The client devices access these files with client software.
- Web client runs web service software and clients use their browser software to access web pages on the server.
- Email server runs email server software and clients use their mail client software to access email on the server.

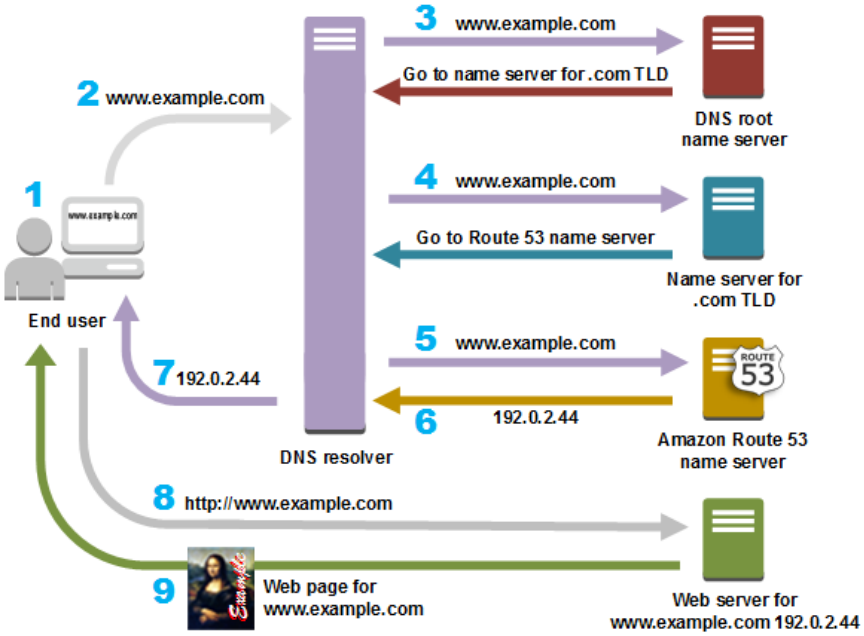
▼ DHCP Server

Dynamic Host Configuration Protocol (DHCP) is the service used by ISPs, network administrators, and wireless routers to automatically assign IP addressing information to hosts.



▼ DNS Server

DNS is the method computers use to **translate domain names into IP addresses**.



▼ Print Server

Print servers enable multiple computer users to access a single printer.

▼ File Server

The File Transfer Protocol (FTP) provides the ability to transfer files between a client and a server. FTP has many security weaknesses.

- File Transfer Protocol Secure (FTPS) is request the file transfer session be encrypted.
- SSH File Transfer Protocol (SFTP) is an extension to secure shell (SSH) protocol
- Secure Copy (SCP) uses SSH to secure file transfers.

▼ Web Server

The host accesses the web resources using the Hypertext Transfer Protocol (HTTP) or the secure HTTP (HTTPS).

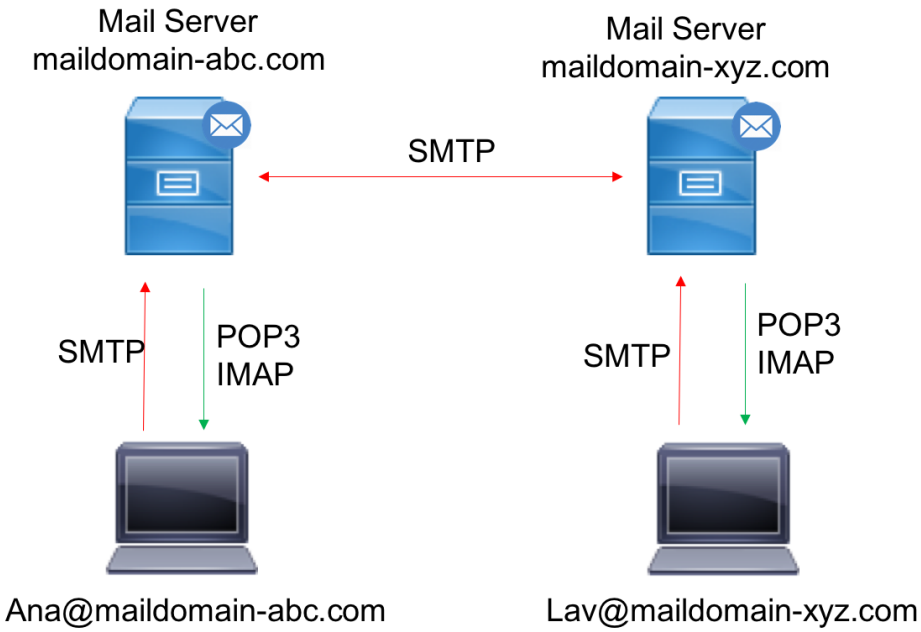
HTTP is a set of rules for exchanging text, graphic images, sound and video on the World Wide Web. It **operates on port 80**.

HTTPS adds encryption and authentication services using Secure Sockets Layer (SSL) protocol or the newer **Transport Layer Security (TLS)** protocol. It **operates on port 443**.

▼ Mail Server

Email is a store-and-forward method of sending, storing, and retrieving electronic messages across a network. Email messages are stored in databases on mail servers.

- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP), **POP3 operates on port 110.**
- Internet Message Access Protocol (IMAP)

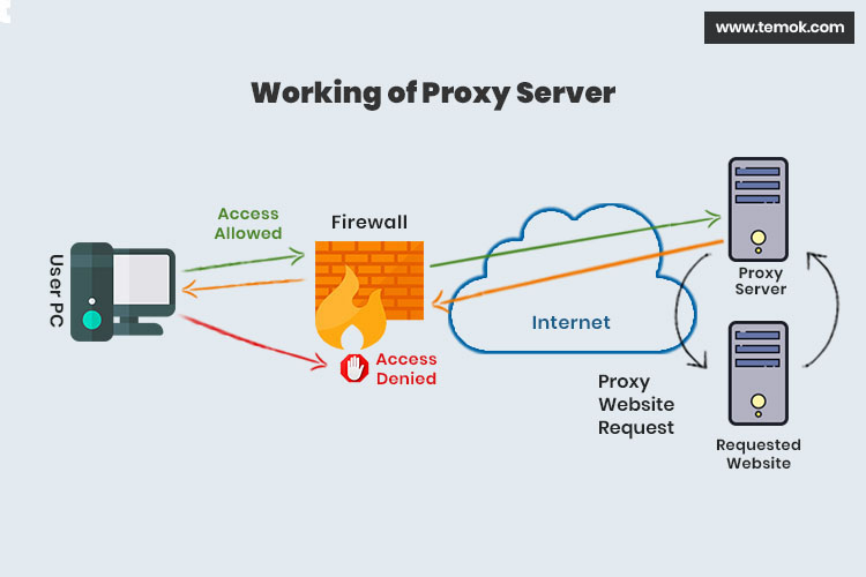


▼ Proxy Server

Proxy server have the authority to act as another computer.

A popular use for proxy servers is to act as storage or cache for web pates that are frequently accessed by devices on the internet network.

A proxy server can effectively hide the IP addresses of internal hosts because all requests going out to the internet are sources from the proxy server's IP address.



▼ Authentication Server

Access to network devices is typically controlled through authentication, authorization, and accounting services (AAA).

AAA is a way to control who is permitted to access a network (authentication), what they can do while they are there (authorize), and track what actions they perform while accessing the network (accounting).

▼ Syslog Server

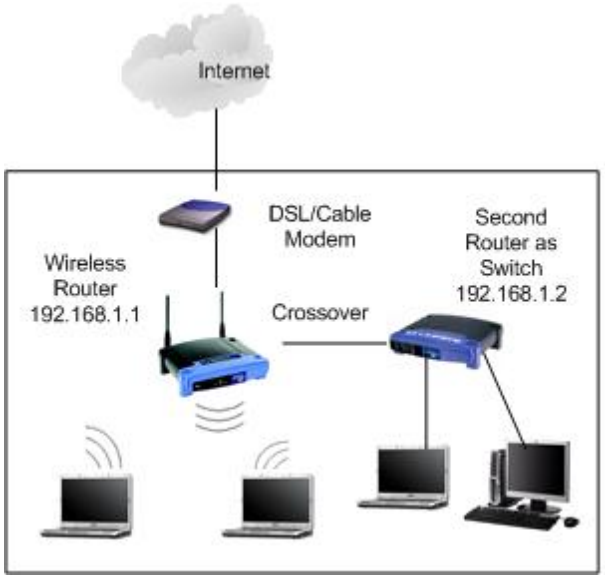
The syslog protocol allows networking devices to send their system messages across the network to syslog servers.

Network devices

- **Switches** connect devices on the same network
- **Switches** examine the Ethernet MAC addresses to determine which port to forward the data
- **Routers** forward data between different networks.
- **Routers** examine the IP address to determine which interface to forward the data.

Routers can have all the functionality of a switch or a wireless AP.

Routers connect network and switches use MAC addresses to forward traffic within a single network.



Network Interface Card (NIC)

A NIC provides the physical connection to the network at the PC or other end device.

- Ethernet NIC
- Wireless NIC
- USB NIC

Repeaters, Bridges, and Hubs - legacy

- **Repeater is regenerating weak signals.** It is also called extenders because it extends the distance a signal can travel.
- **Hub receive data on one port and then send it out to all other ports.**
- **Bridge were introduced to divide LANs into segments.** Bridges keep a record of all the devices on each segment.

Switches

A **switch microsegments a LAN**. Micro segmenting means that switches filter and segment network traffic by sending data only to the device to which it is sent.

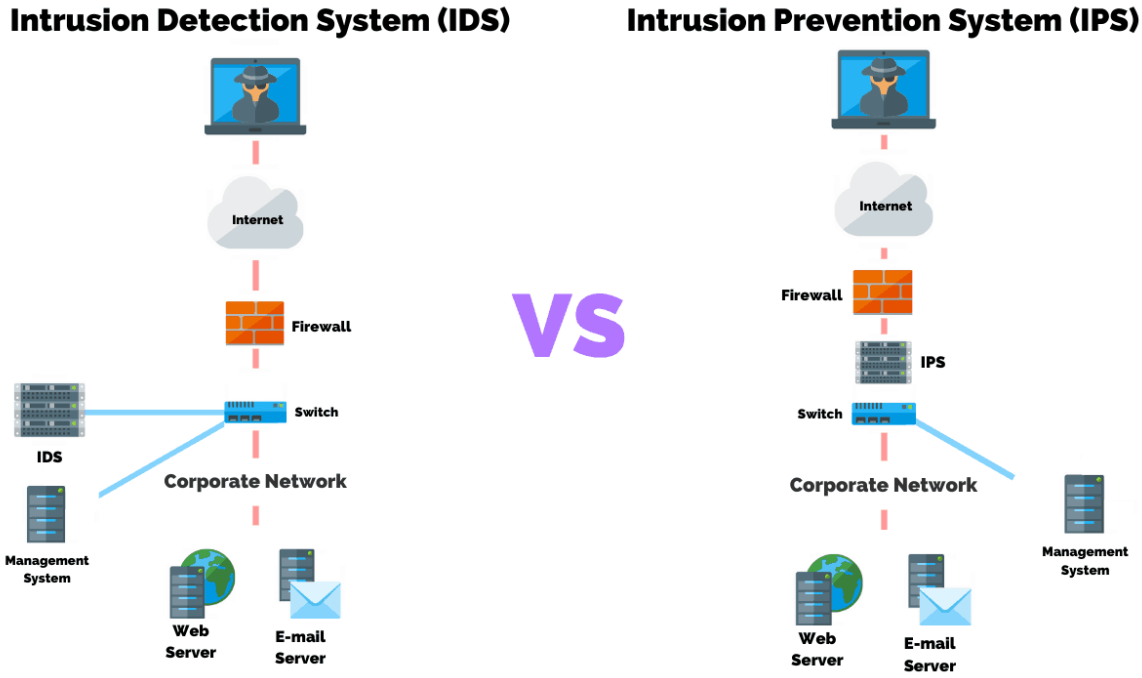
Wireless Access Points

APs provide network access to wireless devices.

Security Devices

A firewall is a network security device or software within a device that monitors and controls incoming and outgoing network traffic based on a predetermined set of security rules.

Firewalls protect data and equipment on a network from unauthorized access. A firewall resides between two or more networks.



▼ Intrusion Detection System (IDS)

It passively monitor traffic on the network.

Stand-alone IDS systems have largely disappeared in favor of IPS.

▼ Intrusion Prevention System (IPS)

An IPS builds upon IDS technology.

An IPS device is implemented in inline mode. This means that all inbound and outbound traffic must flow through it for processing.

▼ UTMs

Unified Threat Management (UTM) is a generic name for an all-in-one security appliance. UTMs include all the functionality of an IDS/IPS as well as stateful firewall services. Stateful firewalls provide stateful packet filtering by using connection information maintained in a state table. A stateful firewall tracks each connection by logging the source and destination addresses.

▼ Endpoint management server

An endpoint management server is typically responsible for monitoring all the end devices in your network including desktops, laptops, servers, tablets, and any device connected to your network. It can restrict an end device's connection to the network if the device does not meet certain predetermined requirements.

Network cables

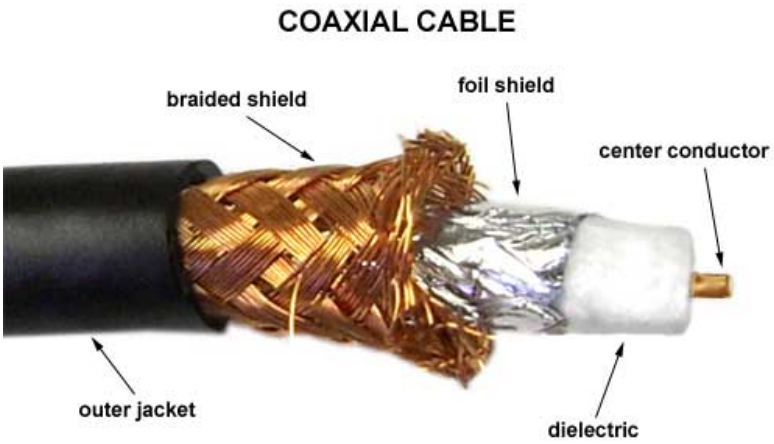
Network tools

- Wire cutters are used to cut wires.
- Wire strippers are used to remove the insulation from wire so that it can be twisted to other wires or crimped to connectors to make a cable.
- Crimper is used to attach connectors to wires.
- Punch down tool is used to terminate wire into termination blocks
- Multimeter is a device that can take many types of measurements. It measures AC/DC voltage, electric current, and other electrical characteristics.
- Cable tester is used to check for wiring shorts.
- Loopback adapter tests the basic functionality of computer ports.
- Tone generator and probe is a two-part tool used to race the remote end of a cable for testing and troubleshooting.
- Wi-Fi analyzer is mobile tool for auditing and troubleshooting wireless networks.

Copper cables and connectors

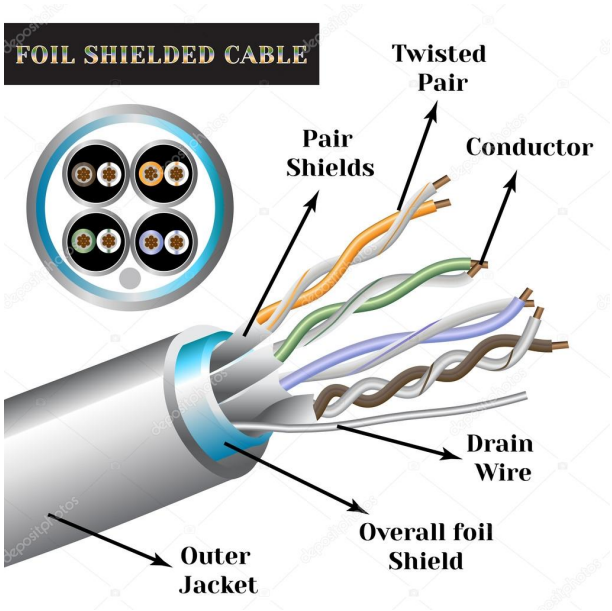
Coaxial cables

- It is usually constructed of either copper or aluminum. It's used by both cable television companies and satellite communication systems.
    - BNC
    - N type
    - F type

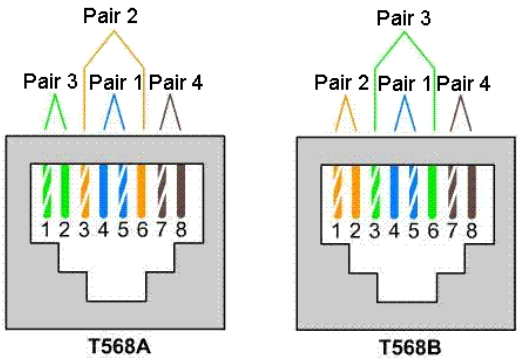


Twisted-pair cables

- It is a type of copper cabling used for telephone communications and most Ethernet network. The pair is twisted to provide protection against crosstalk, which is the noise generated by adjacent pairs of wires in the cable.



- Twisted-pair wire schemes



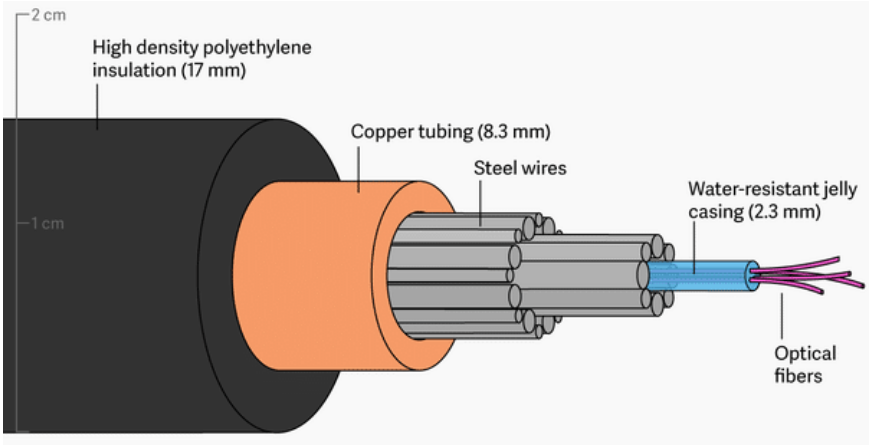
Build and test a network cable

1. Cut the cable to length
2. Strip the cable to expose
3. Untwist the wire pairs are remove the string and separator if necessary
4. Organize the wire ends in the correct color code and trim the wires to length
5. Place the wire ends into the RJ-45 connector
6. Ensure the wire ends reach the end of the RJ-45 connector
7. Crimp the RJ-45 connector to the cable
8. Test the cable for continuity

Fiber cables and connectors

Fiber-optic cables

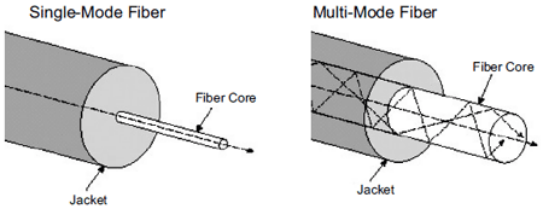
- It is composed of two kinds of glass (core and cladding) and a protective outer shield (jacket).

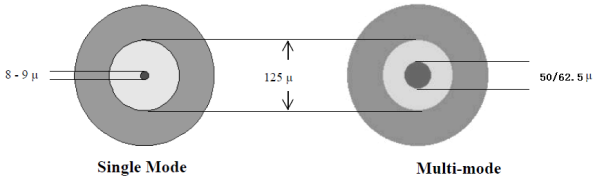


Types of fiber media

- Single-mode fiber (SMF) consists of a very small core and uses laser technology to send a single ray of light.

- Multimode fiber (MMF) consists of a larger core and uses LED emitters to send light pulses.





Fiber optic connectors

An optical fiber connector terminates the end of an optical fiber.