**CSIS 2270:**

**Slide 01: Introduction to Hardware Additional Information**

**PC Hardware Components:**

* I/O devices: external the case.
* Processing & storage devices: internal to the case.
* Central Processing Unit (CPU)
  + Processor, microprocessor
  + Reads input, processes data, writes data to storage.

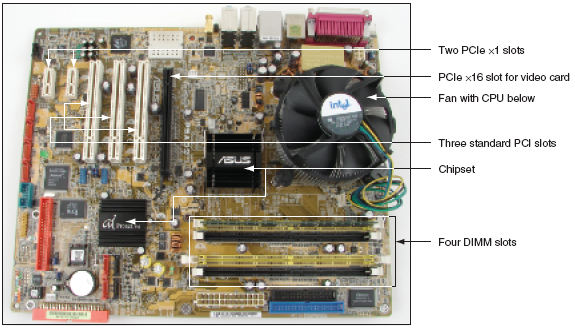
**Hardware Vs. Software:**

A hardware is every computer physical component, i.e.: monitor, motherboard, memory, mouse, keyboard…

A software is a program that executes a set of instruction. It uses the hardware for four basics functions: input, process, storage and output.

**Hardware Components:**

* **Motherboard:** 
  + Largest and most important circuit board.
  + Contains the CPU, expansion slots and other devices.
  + Processing, temporary storage, communication and power.
  + All devices communicate with the mother board.
  + Peripheral device links to motherboard via cable.

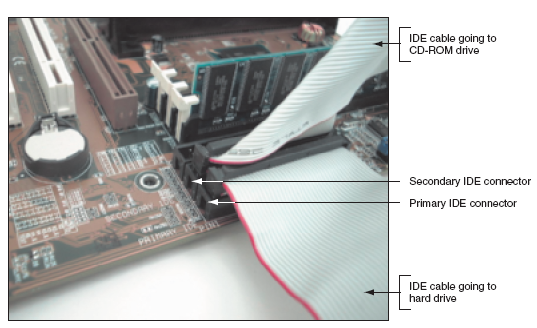


* **The Processor and the Chipset:**
  + CPU
    - Is inside the computer.
    - Performs most data processing.
  + Chipset
    - Group of two microchips controlling data flow.
* **Storage Devices:**
  + Primary storage (main memory)
    - Temporary (volatile) storage used by processor.
    - High speed data access speed.
    - RAM (Random Access Memory).
    - Located on motherboard, adapter cards.
    - Video memory: embedded on video card.
    - Dual line memory module (DIMM)

**A model of a building

Description automatically generated with low confidence**

* + Secondary storage (permanent storage/non-volatile)
    - Enables data to persist after machine turned off.
    - Higher capacity but slower access speed.
    - Examples: hard drive, CD, DVD and USB.
    - Remote storage locations containing data and instructions.
    - Permanent (nonvolatile).
    - Hard drives.
    - Magnetic hard drives (Use Integrated Drive Electronics).
    - Flash memory (Solid State Drive - SSD).
    - ROM (Read-Only Memory).
    - USB Flash drives.
    - Parallel and serial ATA standards enable secondary storage enables devices to interface with the motherboard.

****

* **Motherboard Components used For Communication Among Devices:**
  + Traces
    - Fine lines on top and bottom of the motherboard’s surface.
  + Bus
    - System of pathways.
  + Data bus
    - Carries the data.
  + Buses for expansion slots:
    - PCI (Peripheral Component Interconnect).
    - AGP (Accelerated Graphics Port).
  + System clock
* **Expansion Cards:**
  + Cards that connect the CPU to an external device: video, phone lines, network cable, sound.
* **Instructions Stored on the Motherboard and Other Boards:**
  + BIOS
    - Data and instructions stored on the ROM chips.
    - ROM chips are types of firmware.
  + ROM BIOS
    - System BIOS: manage simple devices.
    - Startup BIOS: starts the computer.
    - CMOS setup: changes motherboard settings.
  + CMOS RAM: includes date, time and port configurations.
  + Flash ROM: ROM chips that can be overwritten.
  + Computer Bus:
    - system of communication pathways, protocols.
  + ROM BIOS:
    - helps starts the PCs; manages simple devices; change some motherboard settings.

**Slide 02: Network and the OSI Model**

**Benefits of Networks:**

* Resource sharing.
* Reduced Cost and Easier Installation of Software.
* Improved Communications.
* More Workspace Flexibility.
* Reduced Cost of Peripherals.

**Requirements of a Network:**

* At least two computers.
* A transmission medium.
* A communication agreement (Protocol).

**Classifying Networks:**

* Local Area Networks – LANs
  + High-speed: ~100Mbps to 10Gbps.
  + Single physical location.
  + All nodes located within a small geographical area.
  + Wi-Fi and Ethernet usually.
  + Home, Airport, Campus, School.
* Wide Area Network – WAN
  + Network that uses telecommunications network to interconnect sites that are geographically distributed throughout a region, country, or the world.
  + Multiprotocol Label Switching (MPLS), Frame Relay, Integrated Services Digital Network (ISDN).

**Functions & Terms:**

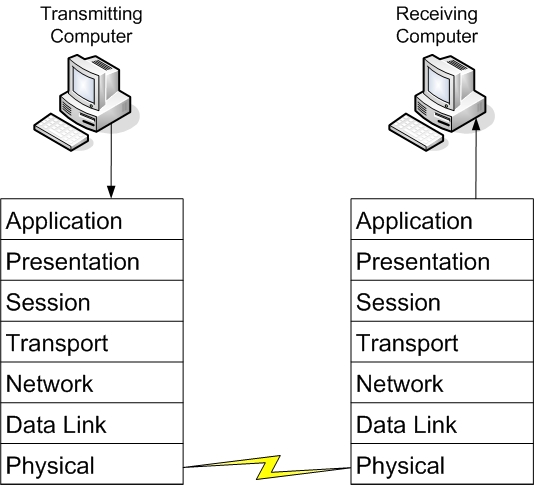
* **Hosts:** computer accessible over a network. It can be a client, a server or any other kind of computer.
* **Router:** networking device that forward packets between computer networks. It directs the traffic of packets over the internet.
* **Application:** software or program that runs on your computer.
* **Protocols:** Established set of rules that determines how data is transmitted between different devices in the same network.

**Organizing Networks with Layers:**

* Layer: is an abstraction of an interface that implements a service via its own internal layer actions or relying on services provided by a layer below.
* Deals with complex systems.
* Modularization eases maintenance.
* Simpler to update the system.

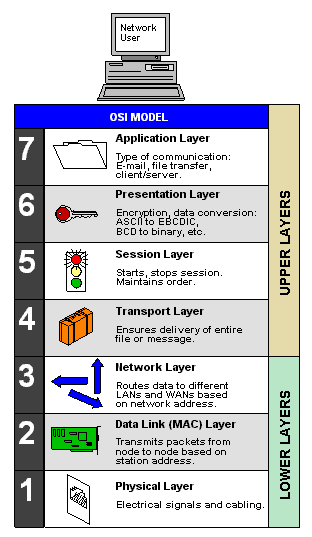
**Open System Interconnection (OSI):**

* The Open System Interconnection (OSI) reference model is used to define how the data communication occurs on computer networks.
  + Develop in 1984.
* This model is divided into layers, each of which provides services to the layer above.
* These layers are associated with protocols and devices.



**The Model:**

1. Physical Layer: (Units of measurement **BITS**)
   1. Electrical signals.
   2. Mechanical connections.
   3. Includes but it is not limited to cables (e.g. UTP, fiber), connectors (RJ45), patch panels, and network interface cards (NIC).
   4. Topologies: Analog versus digital encoding, bit synchronization, baseband versus broadband, multiplexing, etc.
   5. Baseband: every computer on the LAN shares the same channel or frequency to transmit data.
   6. Broadband: multiple channels that can be utilized by the communications system
2. Data Link (Mac) Layer: (Units of measurement **FRAMES**)
   1. Transmits packets from node to node based on station address.
   2. Usually implemented on network interface cards and network devices such as switches.
   3. Data transfer between neighboring network elements:
      1. Ethernet 802.11 (WIFI)
      2. The layer decides how transfer is accomplished over the physical layer.
      3. It provides the Media Access Control (MAC) service.
      4. Decide which device is allowed to transmit at a given moment, e.g. CSMA/CD (Carrier Sense Multiple Access with Collision Detection) for Ethernet.
      5. Provides error checking service and flow control for transmission over the physical layer.
      6. To transmit data to a neighboring device, it does so through the use of physical addresses. (address burned into the ROM of the NIC)
      7. Every network adapter must have a unique Media Access Control (MAC) address.
   4. Media Access Control Address:
      1. The MAC for LAN is 6 bytes in length.
      2. The number is exhibited in 12 hexadecimal codes
      3. The first 6 hexadecimal codes are used to indicate the vendor of the network interface, also called the Organizationally Unique Identifier (OUI)
      4. The last 6 hexadecimal values ate unique numbers assigned by the vendor.
   5. Switches:
      1. A layer 2 switch is one of the most common type of switch used on a LAN. It will be used to connect all devices within a network.
      2. These switches use the MAC address of each host computers network adapter when deciding where to direct frames of data.
      3. Every port on the switch is mapped to the MAC address(es) of the computer(s) that physically connects to it.
3. Network Layer: (Units of measurement **PACKETS**)
   1. Routers data to different LANs and WANs based on network address.
   2. This layer is dedicated to routing data from the source to destination between different networks.
   3. Devices that exist on the network layer are routers.
      1. Routers provide connection between networks.
      2. Routing protocols are used to determine the best path from source to destination: RIP, OSPF, BGP.
   4. Protocols used for this layer include IP and IPX.
   5. This layer receives the logical addressing of hosts. The address chances to the network that the device is presently connected to.
   6. Switches:
      1. Devices on layer 3 are also known as routers; however, recent technology has implemented the routers used for intranet in a similar way as layer 2 switch, and those routers are referred to as layer 3 switch.
      2. Layer 3 switch determines paths for data using logical addressing (IP addresses) instead of physical addressing (MAC).
      3. Layer 3 switches forward packets, whereas layer 2 switches forward frames.
4. Transport Layer: (Units of measurement **SEGMENTS** or **MESSAGES**)
   1. Ensures delivery of entire file or message.
   2. Concerns with the end-to-end (host-to-host) data transmission.
      1. Transmits messages between hosts through logical addressing (IP address).
      2. Shields the upper layers from transport implementation details.
   3. The protocols provide services such as break up messages and send them through the subnet.
      1. Handles end-to-end flow control, error checking and recovery.
      2. When reliable service is provided, the protocols will ensure correct reassembly at the receiving end, making sure there are no duplicates or lost messages.
      3. TCP and UDP
         1. Two main transport protocols on Internet ate the **Transmission Control Protocol (TCP)**, which is a connection-oriented protocol providing reliable service, and the **User Datagram Protocol (UDP)**, which is connectionless.
         2. TCP example: web browser.
         3. UDP example: video streaming.
5. Session layer: (Units of measurement **DATA**)
   1. Starts, stop sessions. Maintains order.
   2. i.e., log on and log off.
6. Presentation Layer: (Units of measurement **DATA**)
   1. Encryption, data conversion: ASCII to EBCDIC, BCD to binary and etc.
   2. Translates the data format from sender to receiver that may be used.
   3. Includes data conversion, data compression and file encryption.
      1. ACSII and EBCDIC (text).
      2. Jpeg, Gif and TIFF (image).
      3. Mpeg and QuickTime (sound/video).
7. Application Layer: (Units of measurement **DATA**)
   1. Type of communication:
      1. Email.
      2. File transfer.
      3. Client/Server.



* 1. Provides network services to user applications and is where message begins.
  2. End-user protocols such as FTP, SMTP, HTTP, Telnet, and RAS work at this layer.
  3. This layer is not the application itself, but the protocols that are initiated by this layer.

Table

Description automatically generated

**Communications Subnetwork:**

* Layer 1 through 3 of OSI model form the basis of the communication **subnetwork**.
  + Data are sent through neighboring devices (node-to-node)
* Regardless of what type of data transmission occurs in a computer network, the communication subnetwork will be employed.

**Connection Oriented Communications:**

* Connection-oriented (also known as CO mode) communications require that both end devices involved in the communication establish an end-to-end logical connection before data can be sent between the two.
* These connection-oriented systems are often considered reliable network services.
* If an individual packet is not delivered in a timely manner, it is resent.
  + These connection-oriented systems are often considered reliable network services.
  + If an individual packet s not delivered in a timely manner, it is resent.
    - i.e., Sending device needs to buffer up any data sent until an acknowledgement is received from the receiving device.
* TCP: port numbers are used to identify the applications on the computer.



**Connectionless Communications:**

* In connectionless communications (CL mode), no end-to-end connection is necessary before data is sent.
* Every packet that is sent has the destination address located in its header.
* This is sufficient to move independent packets, such as in the previously mentioned streaming media.
* But if a packet is lost, it will not be resent.

**Ports:**

A screenshot of a computer

Description automatically generated with low confidence

* Ports acts as logical communications endpoints for computers.
* There are a total of 65,536 ports. [0 – 65,535].
* They are defined by the Internet Assigned Numbers Authority or IANA and divided into categories.

Graphical user interface, application, Word

Description automatically generated

* Inbound ports:
  + Used by servers to accept incoming service requests.
* Outbound ports:
  + Used by client computers and are assigned dynamically by the operating system.

Graphical user interface, application, table

Description automatically generated

**TCP Model:**

* The TCP/IP (or TCP) model is similar to the OSI model.
* Most widely used nowadays.
* It is often used by software manufacturers who are not as concerned with how information is sent over physical media, or how data link is actually made.
* The model is composed of four layers.
* **Layer 01:** Data link layer (also simply known as the link or network access layer).
* **Layer 02:** Network layer (also simply known as the internet layer).
* **Layer 03:** Transport layer.
* **Layer 04:** Application layer.
  + The OSI physical layer is skipped altogether, and the application layer comprises the OSI application, presentation, and session layers.

Table

Description automatically generated

Diagram

Description automatically generated

**Slide 02: Understanding Local Area Networking**

**Protocol and Topology**

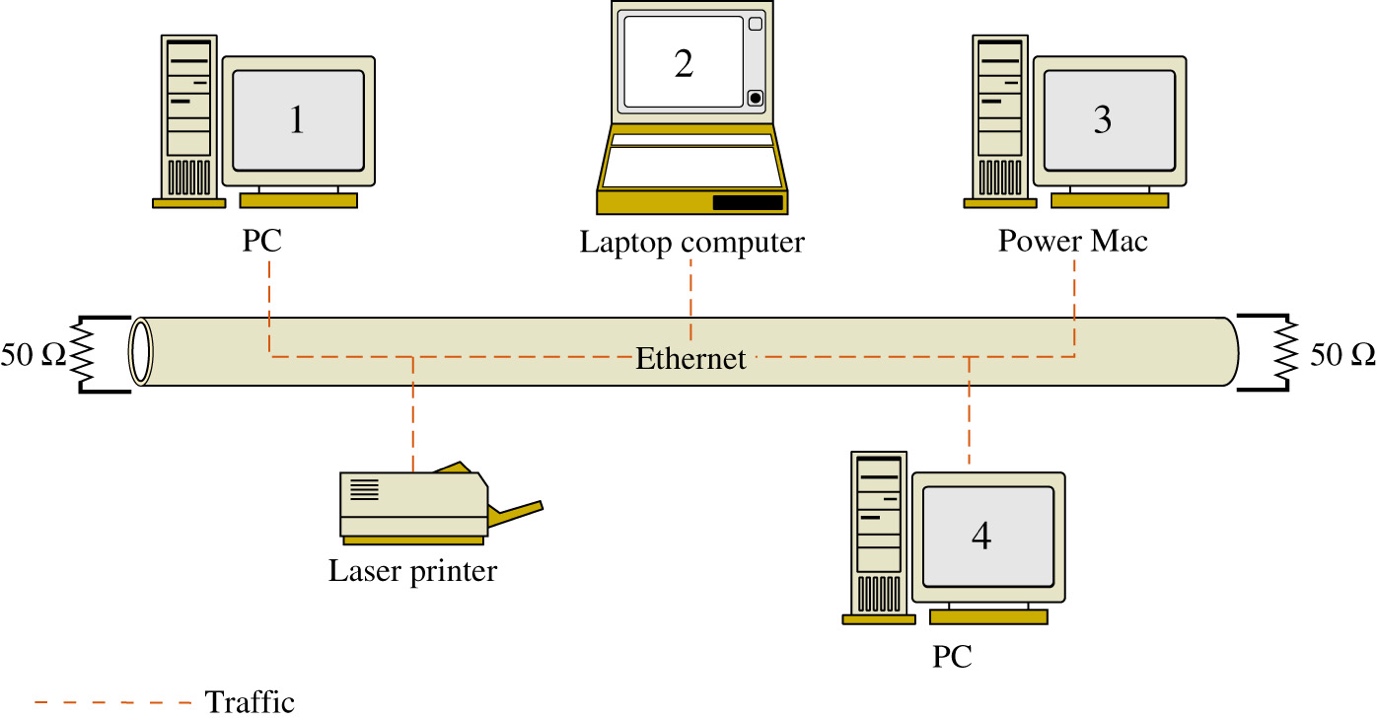
* Local area networks are defined in terms of the protocol and the topology used for accessing the network.
* The networking protocol is the set of rules established for the users to gain control of the network to exchange information.
* The topology is the network architecture used to interconnect the networking equipment.
  + It defines the physical connections of hosts in a computer network.

**Network Topology**

* There are several types of physical topologies including:
  + Bus
  + Ring
  + Star
  + Mesh
  + Tree

**Bus Topology**

* Network data traffic is carried over a common data link.

****

* Advantages:
  + Easy to implement and design.
  + Requires less cable than other topologies.
  + Inexpensive
* Disadvantages:
  + If the cable is broken at any point, the entire network is down.
  + Terminators are required at both ends.
  + Locating breaks is difficult.
  + Limits on cable length and number of nodes.
  + Performance degradation occurs under traffic load.
  + Introducing or connecting new devices takes the network down.

**Ring Topology**

Network data traffic is carried over a common data link.

* In a LAN environment, each computer is connected to the network using a closed loop.
* Packets move in the same direction.
* Used by Token Ring and FDDI.

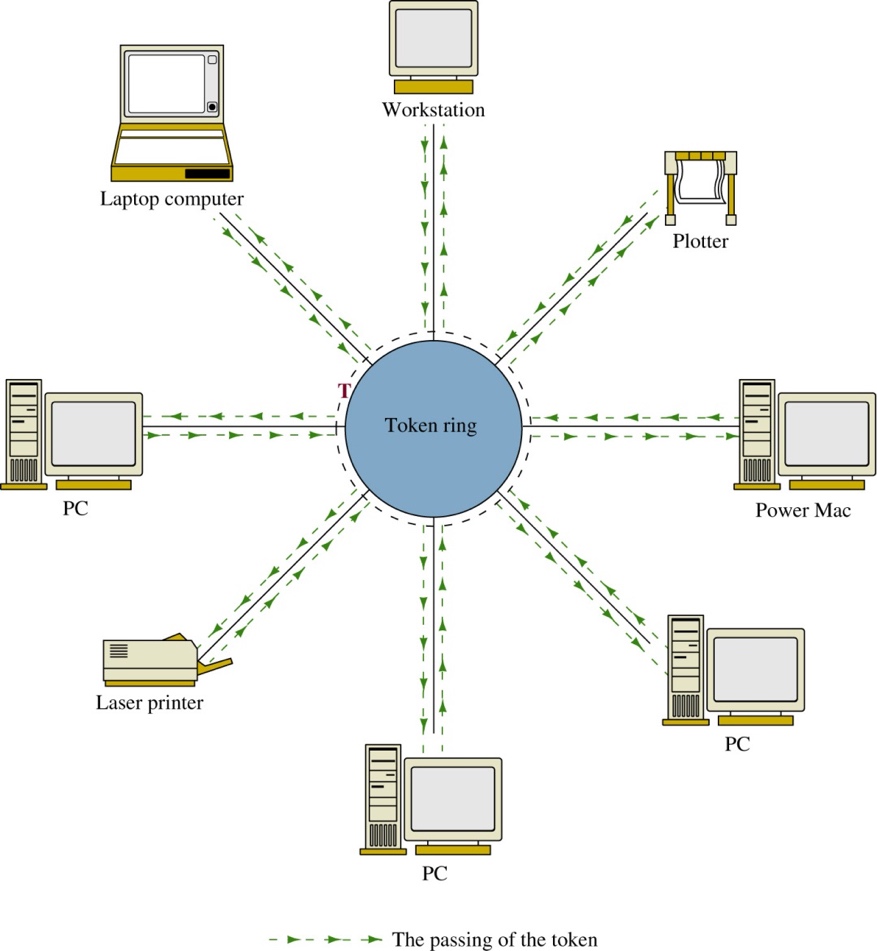
Diagram

Description automatically generated

* Advantages:
  + Performs better than bus under load.
  + Prevents collisions
  + Can be larger than a bus.
* Disadvantages:
  + Any break brings the entire network down.
  + Locating a break is difficult.
  + Introducing or connecting new devices takes the network down.

**Token Ring (IEEE 802.5)**

* A Token Ring network sends data logically in a ring fashion, meaning that a token goes to each computer, one at a time, and continues on in cycles.
* Token Ring computers are connected in a star fashion physically.



* Namely, all computer in a token ring network is connected to a central connecting device known as a Multistation Access Unit (MAU or MSAU)
* Advantages:
  + Deterministic – meaning that the networking devices gain control over the network within a fixed time interval.
  + Note: a physical star implements logical ring inside the central device’s electronics.

**Star Topology**

* Most widely used topology nowadays.
* Each computer is individually wired to a central connecting device (hub, switch or SOHO router) with twisted-pair cabling.
  + The networking devices do not share data connections to/from the central or switch.
* A hub broadcasts all data traffic to all networking devices connected to its data ports.

Diagram

Description automatically generated

* Advantages:
  + Better performance than bus or ring.
  + If a cable is broken, only the device connected to it is affected.
  + Can support larger numbers than the bus.
  + Easy to troubleshoot.
  + No network disruption when adding or removing devices.
* Disadvantages:
  + Single point of failure at the hub or switch.
  + Performance dependent on central device.
  + Size limited by connections on the hub or switch.

**Star Implementation**

Diagram

Description automatically generated

**Mesh Topology**

* Every computer connects to every other computer.
* No central connecting device is needed.
* Redundant data traffic paths.

Diagram

Description automatically generated

* Advantages:
  + Best of fault tolerance.
  + No disruption when adding or removing devices.
* Disadvantages:
  + Expensive to implement.
  + High maintenance cost.
  + Limitation on number of devices in each mesh.

**Local Area Network (LAN)**

* A local area network (LAN) is a group of devices that are confined to a small geographic area, usually one building.
* LAN requires computers with network adapters, central connecting devices, and some type of medium to tie it all together, be it cable or wireless connections.
* Networks are used to exchange data.

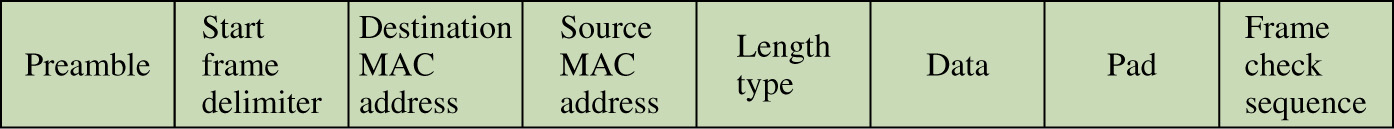
**Ethernet (802.3)**

* Ethernet is a set of rules that govern the transmission of data between network adapters hubs, switches, and other devices.
  + All network adapters and central connecting devices must be compatible with Ethernet in order to communicate with each other.
* Ethernet is the facto standard and has the largest share of networks in place today.
* Ethernet is standardized by the Institute of Electrical and Electronics Engineers (IEEE) as 802.3.
* It specifies the Medium Access Control Protocol – CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
* All stations ready to transmit will sense the carrier before transmission.
* If the carrier is idle, i.e., the station believes that no other is transmitting, it will start its transmission.
* The station will keep sensing the carrier while transmitting. If collision is detected, it will stop its transmission immediately.

**Frames**

* Computers on the Ethernet networks communicate by sending Ethernet frames.
* A frame is a group of bytes packaged by a network adapter of transmission across the network.
* These frames are created and reside on layer 2 of the OSI model.
* By default, computer on Ethernet networks all share a single channel. Because of this, only one computer can transmit at a time.
  + New networks with more advanced switches transcend this limitation.

**The Ethernet Frame**



1. **Preamble:** is an alternating pattern of 1’s and 0’s used for synchronization.
2. **Start frame delimiter:** a binary 8-bit sequence of 0’s and 1’s that indicates the start of the frame (10101011)
3. **Destination Mac Address:** each computer has an Ethernet network interface card (NIC) that has a unique media access control (MAC) address associated with it. The MAC address is 6bytes (12 hex characters) in length.
4. **Length/Type:** an indication of the number of bytes in the data field if this value is less than 1500. If this number is greater than 1500, it indicates the type of data format, for example IP or IPX.
5. **Data:** This is the data being transferred from the source to the destination and destination to the source.
6. **Pad:** A field is used to bring the total number of bytes up to the minimum of 64 if the data field is less than 64bytes.
7. **Frame check sequence:** A 4-byte CRC (Cyclic redundancy check) value used for error detection. The CRC is performed on the characters from the destination MAC address through the Pad fields. If an error is detected, the receiver will discard the frame.

Table

Description automatically generated

**Hub**

* A hub is the most basic of central connecting devices.
* It connects each of networked computers, known as hosts, to one another by the way of copper-based cables.
* Any host that sends data must first send data to the hub, where it is amplified and broadcast to the rest of the network.
* When two more stations transmit at the same time, their data frames will collide.

**Bridge**

* A bridge is used in computer network to interconnect two LAN segments.
  + A Segment is a section of a network separated by bridges, switches, and routers.
  + Computers on a LAN segment are interconnected using a centralized device such as a hub.
* Bridge is usually used to interconnect two LANs running the same type of protocol (e.g., Ethernet) and is called a **transparent bridge**.
* Bridges are also used to interconnect two LANs that are operating two different networking protocols. For example, LAN A could be an Ethernet LAN and LAN B could be a Token Ring.
* Bridge is a layer 2 device, i.e., it uses the MAC address information to make decisions regarding forwarding data packets.
* Only the data that needs to be sent to across the bridge to the adjacent network segment is forwarded.
* E.g., LAN A connects to port 1 of the bridge and LAN B connects to port 2 on the bridge. This creates two segments.

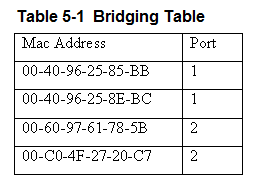
Diagram

Description automatically generated

* The bridges use the MAC addresses to build a bridging table of MAC addresses and port locations for hosts connected to the bridge ports.
* The source MAC address is stored into the **bridge table** as soon as a host transmits a data packet on the LAN.
* An **association** indicates that the destination MAC address is connected to one of the ports on the bridge.
* A bridge only forwards data packets when there is an **association** – used to isolate data traffic in each segment.

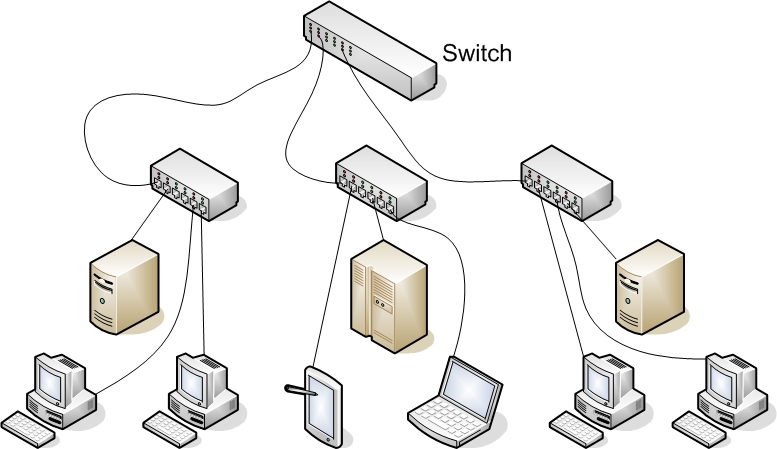
**Bridge Table – Expiration Counter**

* The MAC address entries stored in a bridge table are temporary. Each MAC address entry to the bridge table remains active as long as there is periodic data traffic activity from that host on its port.
* However, an entry into the table is deleted if the port becomes inactive. In other words, the entries stored into the table will have a limited lifetime.
* An expiration timer will commence once the MAC address is entered into the bridge table. The lifetime for the entry is renewed by new data traffic by the computer and the MAC address is reentered.
* Note: Hubs and bridges ae in general replaced by switches nowadays.



**Switch**

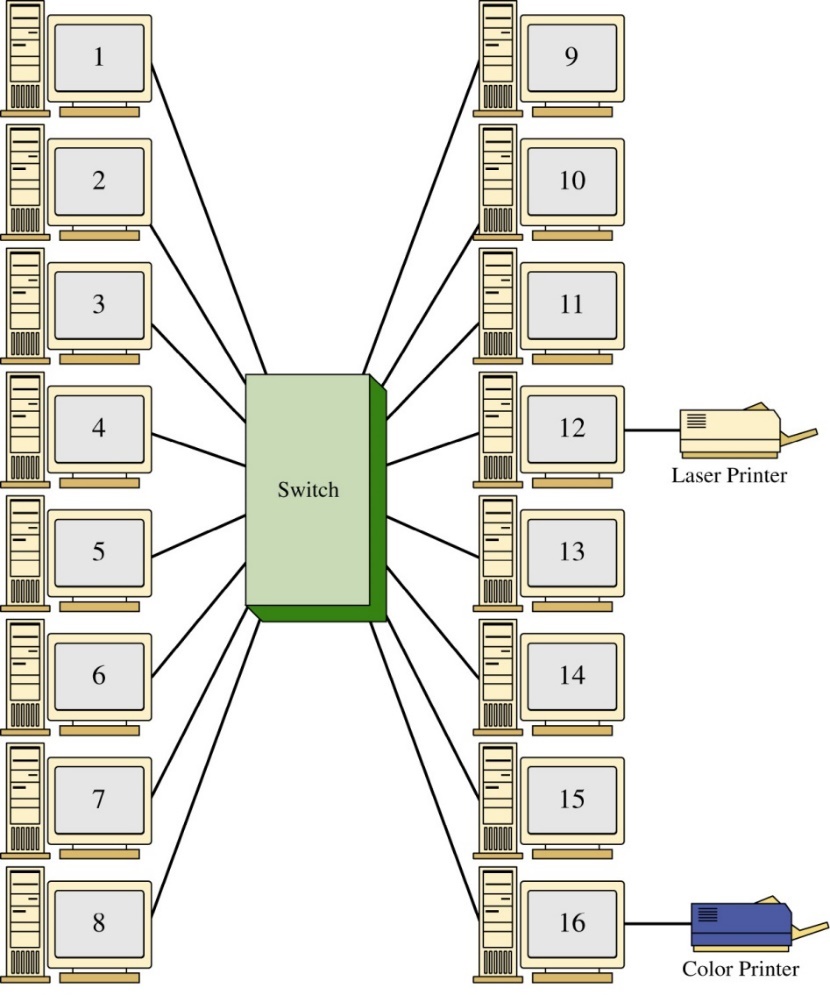
* The layer 2 switch is the most common type of central connecting device used on a LAN.
  + An improved network technology that minimizes data collisions and maximizing the use of LAN’s bandwidth.
  + Connect all devices on the same LAN segment
  + Use the MAC addresses of each host computer’s network adapter when deciding where to direct frames of data.
  + Every port on the switch is mapped to the MAC address(es) of the computer(s) that physically connects to it.
    - Operates in a similar way as bridges.



* The switch monitors data traffic on its ports and extracts the MAC address from the headers of Ethernet packets in the same way the bridge does to build a table of MAC addresses for the devices connects to its ports.
  + This information is stored in CAM – Content Addressable Memory.
* The switch has multiple ports similar to the hub and can switch in a data connection from any port to any other port similar to the bridge.
  + This is why the switch is sometimes called a multiport bridge. The switch minimizes traffic congestion and isolates data traffic in the LAN.
* The use of the switch enables simultaneous direct data connections for multiple pairs of hosts connected to the network.
  + Each switch connection provides a link with minimal collisions and therefore maximum use of the LAN’s bandwidth.

**CAM – Content Addressable Memory**

* The extracted MAC addresses are then used by the switch to map a direct communication between two network devices connected to its ports.
* The MAC address and port information remain in CAM as long as the device connected to the switch remains active.
* A timestamp establishes the time when the mapping of the MAC address to a switch port is established.
* Switches limit the amount of time address and port information are stored in CAM. This is called **aging time**.



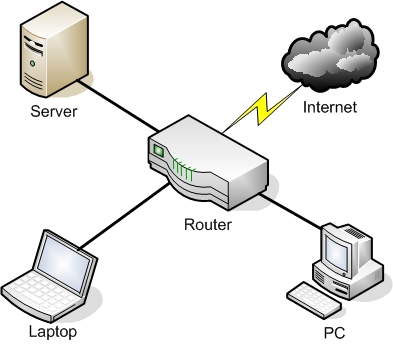
* Each host has a direct connection to the switch.
  + When a link is established between the two hosts, their link is isolated from any other data traffic.
* However, the exception to this is the **broadcast** or **multicast** messages are sent in the LAN.
  + The message is sent to all devices connected to the LAN
  + In a broadcast domain, any network broadcast sent over the network will be seen by all devices in the same network.
  + Broadcasts within a LAN will be passed by switches.
* Benefits:
  + Less network congestion.
  + Faster data transfers.
  + Excellent manageability.
  + Data traffic within a LAN is isolated. (main benefit)
    - The name for this is isolating the collision domains where the data traffic from one part of the network is isolated from the other networking devices.
    - A direct benefit is there will be an increase in the data transfer speed and throughput. (the LAN bandwidth is not being shared and the chances of data collision is minimized)
    - LAN will exhibit faster data transfer.
    - LAN will exhibit reduced latency. (data packets arrive at their destination quicky)

**Router**

* Router is used to interconnect computer networks.
  + Forward packets based on the destination network address.
* The router is a layer 3 device in the OSI model, which means the outer uses the network address (layer 3 addressing such as IP address) to make decisions regarding forwarding the data packets.
* The network address is also called a logical address rather than a physical address such as the MAC address.
  + The logical address describes the IP address location of the network and the address location of the host in the network.
* Route data packets entering or exiting the LAN
  + Differs from the layer 2 switch which use the Ethernet address for making decisions regarding forwarding data packets and only know how to forward data to hosts physically connected to their ports.
* Used to interconnect LANs (subnets) in a campus network.
* Interconnect networks around the country and the world.

**SOHO/ Home Router**

* A SOHO router combines the functions of a switch and a router
  + It also has a link to the Internet, thereby allowing the hosts to send data to and receive data from computers on the Internet.
* This communications link between the router and the Internet is where the LAN ends.



**Network Adapter and RJ45 Patch Cable**

* A network adapter, also known as a network interface card (NIC), is the device that enables you to send and receive data to and from your computer.
* An adapter can connect to the network by cable (wired) or by air (wireless).
* RJ45 port (or an 8P8C) is the most common type of network adapter port, allowing the adapter to connect to most of today’s wired networks.

**Serial Data Transfer**

* Generally, when data is transferred on a LAN, it is sent in a serial fashion over twisted-pair cabling.
* Serial Data Transfer means the transfer of one bit at a time – in other words, transfer in a single bit stream.

**Data Transfer Rate**

* Also known as bit rate, defines the maximum bits per second (bps) that can be transmitted over a network.
* The value is rated in bits, and it is signified with a lowercase b (i.e., 10 Mbps)
* Lower case b differentiates from data stored in the HD. Which uses an upper-case B, that stands for bytes, instead of bits.

**Types of Transfer**

* **Broadcast** has data sent to every host on the network.
* **Unicast** has data sent to one host only.
* **Multicast** has data sent to everyone in a group.
* **Anycast** has data sent to any one of the members in a group.

**IP Address**

* Today, every computer and many other devices have such an address.
* Allows each computer to send and receive information back and forth in an orderly and efficient manner.
* It is a logical address that identifies a computer network and the network it lives on.
* Every IP address is broken down into two pieces: the network portion and the host portion. For example: 192.168.10.101 before the number 101, the address identifies the network your computer is a member, and the number 101, differentiate your computer form others inside that network.

**Subnet masks**

* The subnet mask is a group of four numbers that identifies the network portion of an IP address
* The 255 identifies the network portion and the 1 identify the host portion.

Graphical user interface, text, application, Word

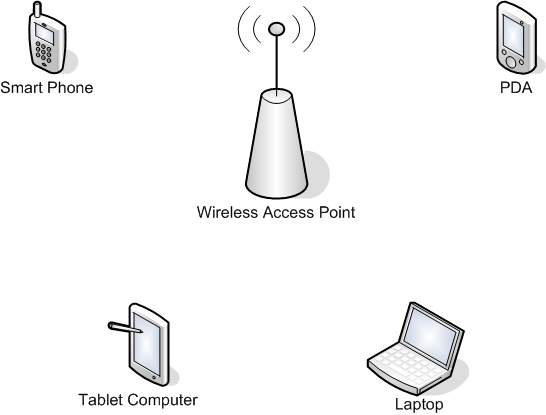
Description automatically generated

**Host**

* IP addresses are usually applied to your network adapter, but they can also be applied to other devices like routers, and so on.
* The fact that a device or computer has an IP address is what makes it a host.

**Wireless Local Area Network (WLAN)**

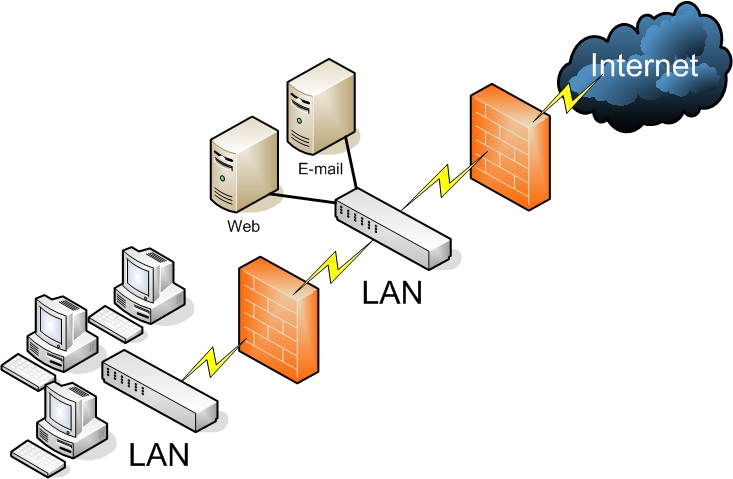
* Has the ability to roam.
* Wireless Access Point (WAP) acts as the central connecting device for the network.
* Wireless network adapters.

****

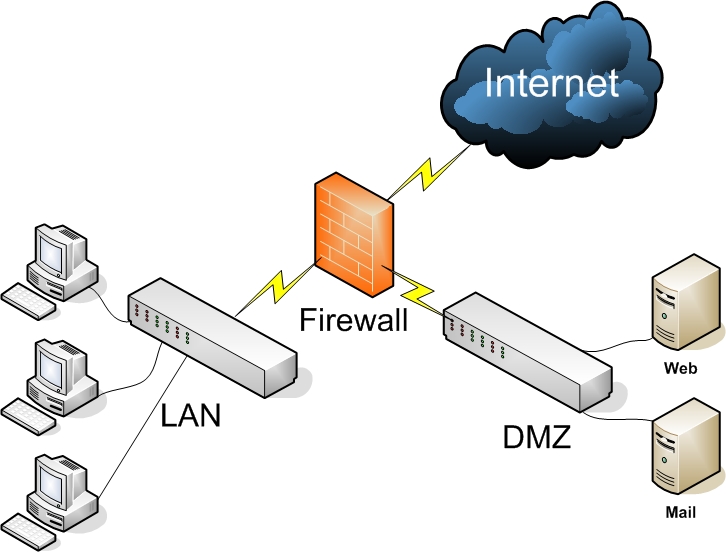
**Perimeter Network:**

* Also known as Demilitarized Zone (DMZ) is a small network that is set up separately from a company’s private LAN and the Internet.
* It is called a perimeter network because it is usually on the edge of the LAN, but DMZ has become much more popular term.

**Back-to-Back Configuration**

****

**3-Leg Perimeter Configuration**

****

**Slide 03: Understanding Wired and Wireless networks**

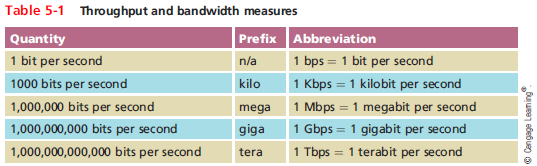
**Throughput**

* Amount of data transmitted during a given time period.
* Also called payload rate or effective data rate.
* Expressed as bits transmitted per second.

**Bandwidth**

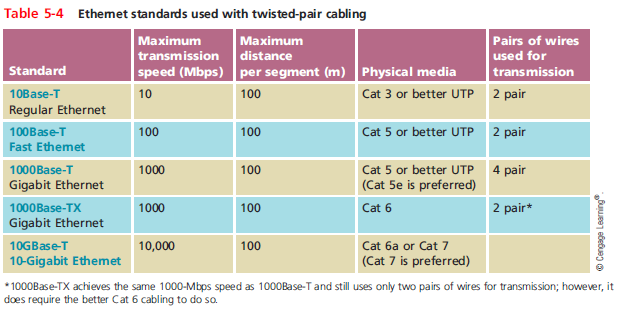
* Difference between highest and lowest frequencies medium can transmit.
* Range of frequencies.

Both are commonly expressed as bits transmitted per second, called bit rate.



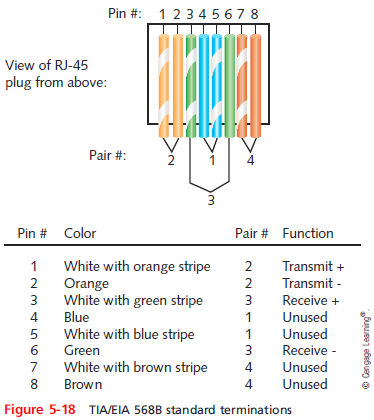
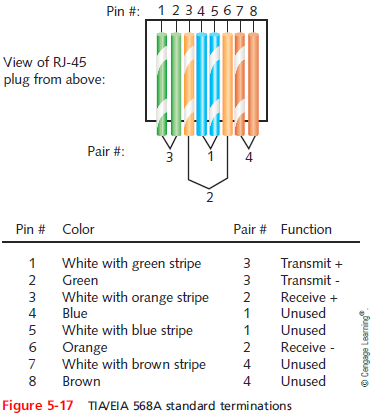
**Methods of Transmission**

* **Simplex:** signals may travel in only one direction (unidirectional, one-way)
* **Half-duplex:** signal may travel in both direction over a medium but in only one direction at a time.
* **Full-duplex:** signals may travel on both directions over a medium simultaneously (duplex) – Modern NICs use full-duplex by default.
* **Twisted-pair Cable TIA/EIA 568:** 
  + wired networks are still the most common type of physical connection that computers make.
  + Most commonly used cable in LANs.
  + Single twisted pair has eight wires: they are cooper conductors that transmit electric signals.
  + Eight wires grouped by four pairs: blue, orange, green and brown.
  + Twisted among themselves and together.
  + Twisting the cable is an attempt to reduce the crosstalk interference.
    - More pair twist per foot implies in more resistance to crosstalk, higher-quality and more expensive. However, high twist ratio can result in greater attenuation of the signal.
    - Trade-off between minimizing crosstalk and reducing signal attenuation.
  + Categories: 3,5, 5e, 6, 6a, and 7.
  + Category 5e or higher is used in modern LANs.
* **Shielded Twisted pair (STP):**
  + Individually insulated.
  + Surrounded by metallic substance shielding (foii).
  + Barrier for external electromagnetic forces.
  + Contain electrical energy of signals inside.
  + The shield must be grounded.
  + Expensive.
* **Unshielded Twisted pair (UTP):**
  + One or more insulated cable.
  + Plastic sheath.
  + No additional shielding.
  + Less expensive, however less noise resistance.
* **STP Vs. UTP:**
  + Throughput – STP and UTP transmit the same rate.
  + Cost – STP and UDP varies in cost (UTP is usually less expensive).
  + Connector – STP and UTP uses the RJ-45.
  + Noise immunity – STP is more noise resistance.
  + Size and scalability – maximum segment length for both: 100 meters.



**Cable Pinouts**

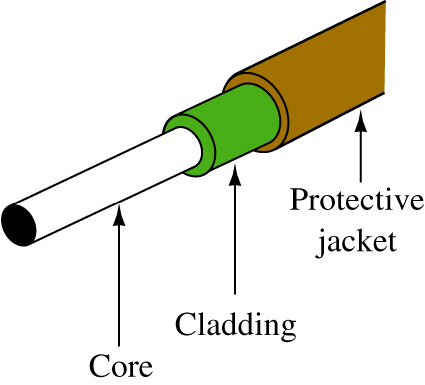
* Proper cable termination is a requirement for two nodes on a network to communicate.
* TIA/EIA specifies two methods of inserting wires into RJ-45 plugs.
  + TIA/EIA 568A
  + TIA/EIA 568B
* No functional difference between the two standards.



* Straight-through cable – terminate RJ-45 at both ends identically.
* Crossover cable – transmit and receive wires on one end reversed.
* Roller cable – all wires are reversed, the terminations are mirror image of each other, they are also called **console cables** and are used to connect a computer to the console port of a router/switch.

**Fiber-Optic Cable**

* The core portion is made of the glass fiber strand at the center that carries the transmitted light.
* Cladding:
  + Layer of glass or plastic surrounding fibers.
  + Different density from glass or plastic strands.
  + Reflects light back to core.
  + Allows fiber to bend.
* Data transmission:
  + Pulsing light sent from laser or light-emitting diode (LED) through central fibers.



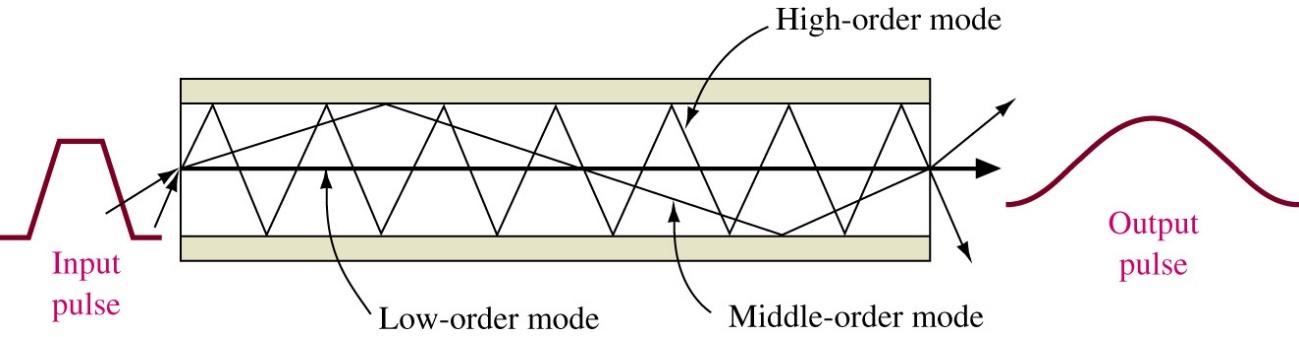
* Benefits over copper cabling:
  + Extremely high throughput.
  + Very high noise resistance.
  + Excellent security.
  + Able to carry signals for longer distances.
  + Industry standard for high-speed networking.
* Drawbacks:
  + More expensive than twisted pair cable.
  + Requires special equipment to splice.
* Throughput – reliable until rates of 100 gigabits per second per channel.
* Cost – most expensive transmission medium.
* Noise immunity – Unaffected by EMI.
* Size and scalability – segment vary from 150 to 40,000 meters depending on the light’s wavelength and type of cable.

**Single Mode Fiber (SMF)**

* Consists of narrow core (8-10 microns in diameter)
  + Laser-generated light travels over one path (little reflection).
  + Light doesn’t disperse as signals travels.
* Can carry signals for many miles before repeating is required.
* Rarely used for shorter connections due to cost.
* The internet backbone depends on SMF.

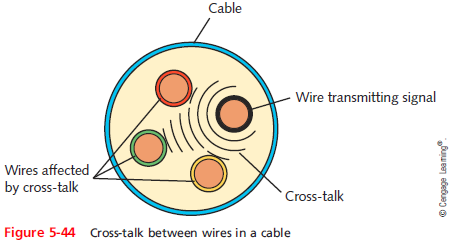
**Multimode Fiber (MMF)**

* Contains a core with a larger diameter than single mode fiber (50 – 62.5 microns).
* Laser and LED generated light pulses travel at different angles.
* Greater attenuation than single-mode fiber.
* Common uses:
  + Cables connecting router to a switch.
  + Cables connecting server on network backbone.



**Transmission Flaws**

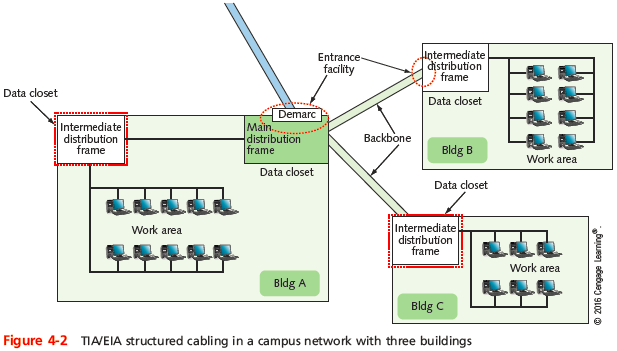
* Noise is any undesirable influence degrading or distorting signal.
* Types of noises:
  + EMI (Electromagnetic Interference): i.e., radio frequency interference.
* Crosstalk:
  + Signal on one wire infringes on adjacent wire signal.
  + Alien crosstalk occurs between two cables.
  + Near end crosstalk (NEXT) occurs near source.
  + Far end crosstalk (FEXT) occurs at the far end.



* Attenuation is the loss of signal’s strength as it travels away from source
* Two ways analog and digital signals are boosted:
  + Amplifier – increases the voltage, or strength, of signals.
    - Can also boot the noise that has accumulated in the signal.
  + Repeater – regenerates a digital signal in its original form.
    - Without noise previously accumulated.
* Latency
  + Delay between signal transmission and receipt
  + May cause network transmission errors.
  + Possible causes vary from the length of the cable to the connectivity devices such as routers and switches.
* Round Trip Time (RTT) is the time a packet takes to go from a sender to a receiver, them back from the receiver to sender.

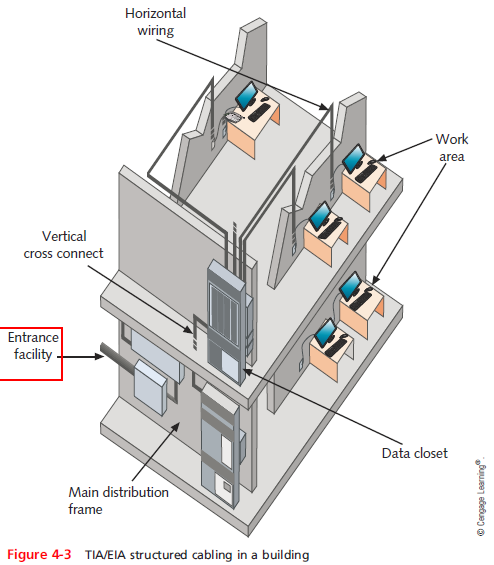
**Structured Cabling – Network Equipment in Commercial Buildings**

* TIA/EIA’s joint 568 Commercial Building Wiring Standard.
  + Structured cabling
  + Describers the best way to install networking media to maximize a performance and minimize upkeep.
  + Apply no matter what type of media, transmission technology, or networking speeds are involved.
  + Based on hierarchical design and assumes a network is based on the start topology.



**Structured Cabling System**

* There are six subsystems
  + Entrance facilities: the point where the external cabling interconnect with the internal building cabling in the equipment room (ER) [also known as the building entrance]
  + Equipment room (ER): a room set aside for complex electronic equipment such as network servers and telephone equipment.
  + Telecommunications closet (TC): the location for cabling termination points. The connection of the horizontal cabling to the backbone wiring is made at this point.
  + Backbone wiring: cabling interconnects telecommunications closets in the same building and between buildings.
  + Horizontal wiring: cabling extends out from the telecommunications closet into the LAN work area. Typically, it is structured in a star configuration running to ach TCO or telecommunications outlet, which is the wall plate where the twisted-pair cable terminates in the room.
  + Work area: the location of the computers and printers patch cables, jacks, etc.
  + MDF (Main Distribution Frame): the central telecommunications connect point for a campus or building. Usually connects two or more buildings.
  + IDF (Intermediate distribution frame): a building’s connection point to the campus backbone. [there is at list one per floor]



Diagram

Description automatically generated

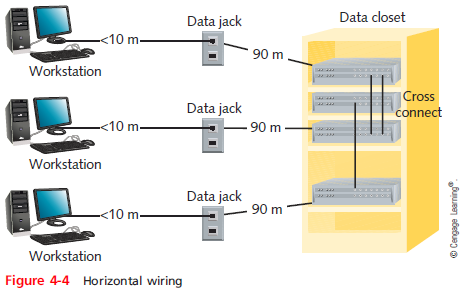
**The Campus Network Hierarchical Topology**

Diagram

Description automatically generated

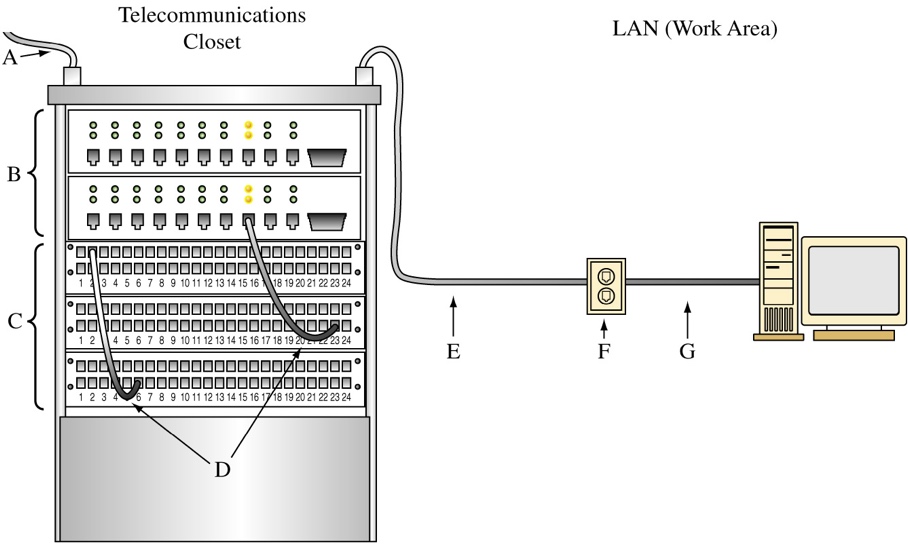
* The MC (main cross-connect) usually connects two or more buildings and it is typically the central telecommunications connection point for a campus or building. It is also called the Main Distribution Frame (MDF) or Main Equipment Room.

**Network Equipment in Commercial Buildings**

****

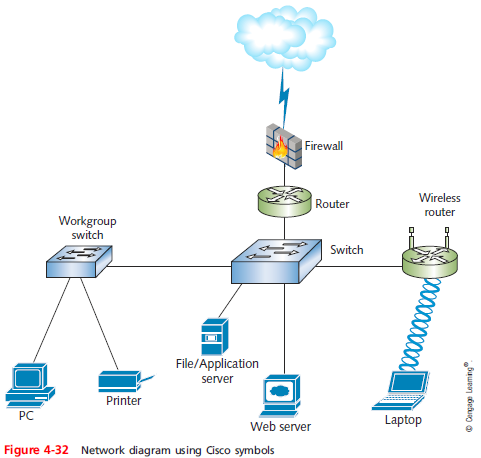
**Horizontal Cabling**

* Basic Components
  1. Backbone cabling interconnecting between closets
  2. Switch
  3. Patch panel
  4. Patch cables
  5. Cabling to the LAN
  6. Wall plate
  7. Patch cable connecting the computer to the wall plate

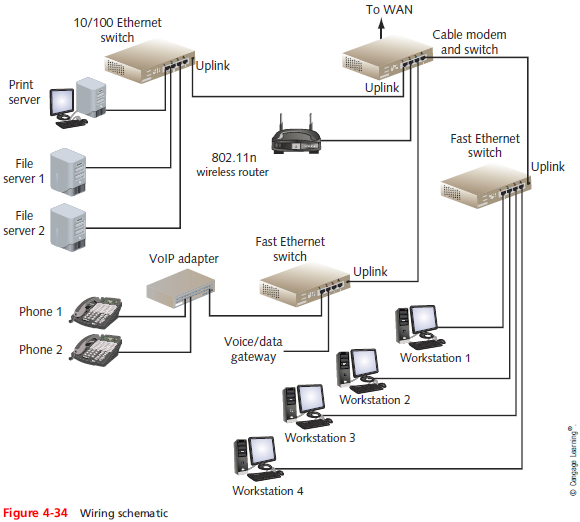


**Building and Maintaining Network Documentation**

* Having up-to-date and detailed documentation of our network is essential to good troubleshooting.
* Network diagrams – graphical representations of a network’s devices and connections.
  + May show physical layout, logical topology, IP addresses reserves, names of major network devices, and types of transmission media.
* Network mapping – the process of discovering and identifying the devices on a network.
* To adequately manage a network, record the following:
  + Network diagrams
  + Physical topology
  + Access methods
  + Protocols
  + Devices
  + Operating systems
  + Applications
  + Configurations



* Network diagrams provides broad snapshots of a network’s physical or logical topology.
  + Useful for planning where to insert a new switch or determining how a particular router, gateway, or firewall interact.
* Wiring schematic – a graphical representation of a network’s wired infrastructure.
  + In detailed form, it shows every wire necessary to interconnect network devices.

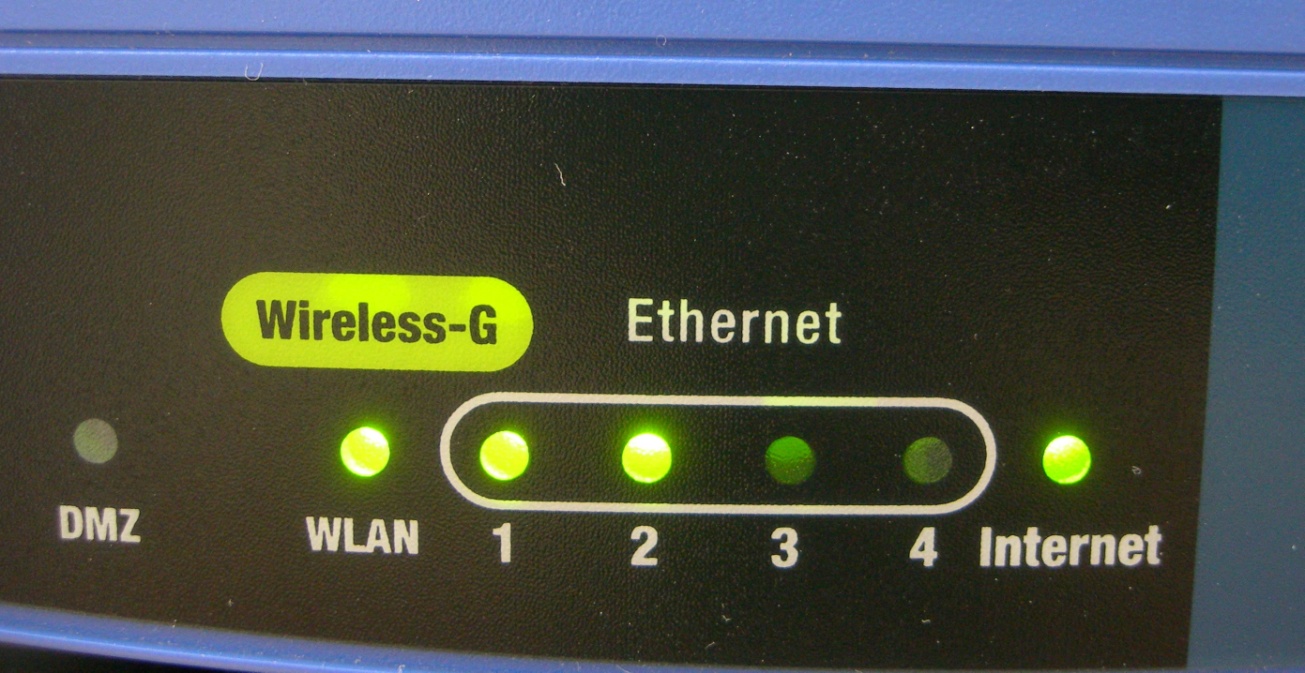


**Wireless Networks**

* Wireless devices might allow for central connectivity of client computers and handheld devices.
* They might offer an extension of connectivity to a pre-existing wireless network and could be used to connect entire local area networks to the internet.
* In addition, some wireless devices can be connected directly to each other in a point-to-point fashion, known as **ad-hoc** mode.

**Wireless Access Point (WAP)**

* By far, the most well-known wireless device is the wireless access point (WAP).
* Device is quite often also acting as a router, firewall, and IP proxy.



**Wireless Network Adapters**

* Wireless network adapters allow for connectivity between a desktop computer or laptop and the wireless access point.
* They come in many shapes and sizes, including USB, PC Card, ExpressCard, and of course, as an internal PCI pr PCI express adapter for a personal computer.

**Wireless LAN (WLAN)**

* Wireless LAN or WLAN is a network composed of at least one WAP and at least one computer or handheld device that can connect to the WAP.
* In order to ensure compatibility, the WAP and other wireless devices must all use the same IEEE 802.11 WLAN standard.
  + 802.11a: 5.0GHz up to 54Mbps
  + 802.11b: 2.4GHz up to 11Mbps
  + 802.11g: 2.4GHz up to 54Mbps
  + 802.11n: 2.4 and 5.0GHz, (MIMO) up to 600Mbps depending on the number of antennas.
  + 802.11ac: 5.0GHz up to 1300Mbps, Multi-user (MIMO).

**Wireless Encryption Options**

Table

Description automatically generated with medium confidence

* WPA and WPA2 both support:
  + Personal mode (uses pre-shared key)
  + Enterprise mode (uses 802.1x server for authentication)



* There are several different ways to connect to a wireless network.
  + Infrastructure mode – it occurs when wireless clients connect to a wireless access point.
  + Ad-hoc mode – all of the clients communicate directly witch each other.

**Service Set Identifier (SSI)**

* When utilizing infrastructure mode, the base unit (normally a WAP) will be configured with a service set identifier
* This then becomes the name of the wireless network, and it is broadcast over the airwaves.
* Thus, when clients want to connect to the WAP, they can identify it by the SSID.
  + Disabling SID broadcast doesn’t enhance security
  + Disabling SSID broadcast does not truly hide the SSID

**Slide 04: Internet Protocol Addressing and Subnetting**

**IPv4**

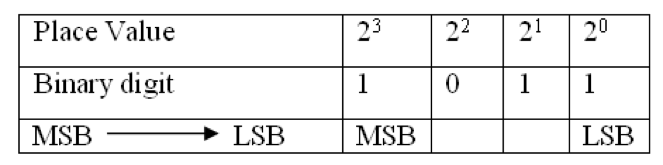
* As a network administrator, you will use the Transmission Control Protocol / Internet Protocol (TCP/IP) communications protocol suite most often.
* Internet Protocol version 4 or IPv4 is the most frequently used communications protocol. IP resides on the network layer of the OSI model.

**IP Addresses**

* IP addresses consist of four numbers, each being a 8-bit word, with a value between 0 and 255.
* An IP address is formed by a Network ID and a Host ID.
* A subnet mask is used to identify the number of bit used for the network ID.
* To connect to the internet, you will also need a gateway address and DNS server address.
  + Here, gateway refer to the router that a device is connected to

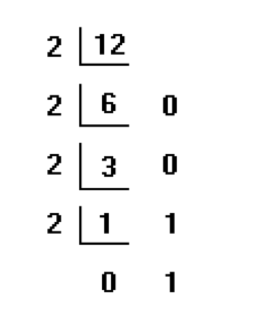
**Binary-Decimal Conversion**

* Binary numbers are represented by 0 or 1 in base 2 format.
* The value starts at with the LSB (Least Significant Bit) position.



**Algorithm to convert Decimal to Binary**

1. Divide the decimal number by 2, record the remainder of 0 or 1 and write the quotient or result of the division by 2.
2. Divide the quotient by 2 and record the remainder of 0 or 1. Write the quotient and repeat this step until the quotient is 0.
3. Write the remainder numbers (0’s and 1’s) in reverse order to obtain the binary equivalent value.



**Hexadecimal Numbers**

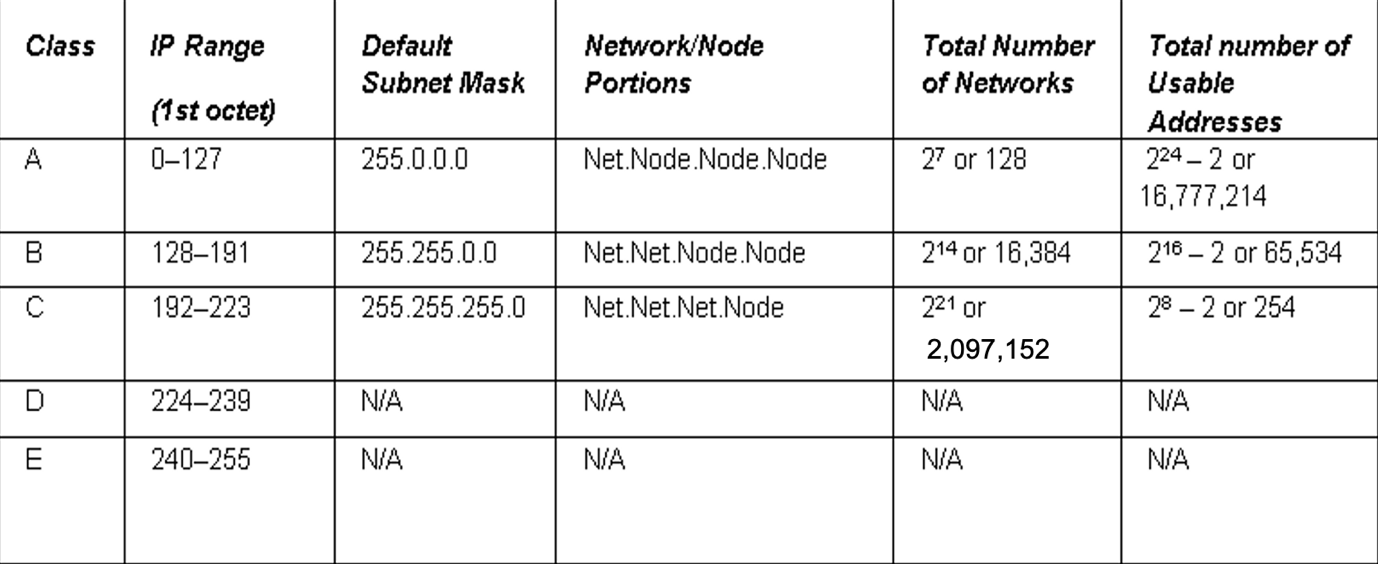
* Numbers are represented by 0 - 9 and A - F in base 16 format.
* It takes 4 binary number to represent a hexadecimal number.

Table

Description automatically generated

**Classful Network Architecture**

* The IPv4 classification system is known as the classful network architecture and is broken down into five classes, three of which are commonly used by hosts on networks – Class A, B, and C.
* The term node is synonymous with “host”.
* If an IP address is Class A, the first octet is considered to be the network portion.



**Loopback Testing**

* The range for class A is 0 – 127.
* The 127 network number isn’t used by hosts as a logical IP address. Instead, this network is used for loopback IP addresses, which allow for testing.

**Usable Addresses**

* Usable addresses are always going to be two less than the mathematical amount.
* The first and last addresses can’t be used.
  + The 0 (in binary) for the host bits defines the entire network.
    - 172.24.0.0 (Class B)
  + The 1 (in binary) defines the known as the broadcast address.
    - 172.24.255.255 (Broadcast a msg in the network 172.24.0.0)

**Class D and E**

* Classes D and E are not used by regular hosts.
  + Class D is used for what is known as multicasting.
  + Transmitting data to multiple computers belonging to a multicast group.
* Class E was reserved for future use, but this has given way to IPv6 instead.

**Public and Private Addresses**

* IPv4 addresses are further classified as either public or private. **Public IP addresses are ones that are exposed to the internet.**
  + Any computer can communicate with them.
* **Private IP addresses are hidden from the internet and any other networks.**
  + They are usually behind an IP proxy or firewall device.
  + Intended to be used on internal networks called intranets or home networks.
  + These are called non-routable IP address.

**Private IP Addresses and NAT**

Class A – 10.0.0.0 to 10.255.255.255

Class B – 172.16.0.0 to 172.31.255.255

Class C – 192.168.0.0 to 192.168.255.255

These addresses type must be translated by a **Network Address Translation (NAT)** process on a server or router to public IP addresses for internet access.

**APIPA**

* APIPA is an acronym for **Automatic Private IP Addressing**.
* It uses a single class B network number: 169.254.0.0.
  + IP address range is 169.254.0.1 through 169.254.255.254.
* If a windows client cannot get an IP address from a DHCP server and has not been configured statically, it will auto-assign a number on this network.

**Static and Dynamic Addresses**

* Static IP address are addresses that are manually assigned to a host.
* Dynamic IP addresses are more common than static IP addresses, whereas they automatically obtain an IP address (and other IP information) from a DHCP Server (Dynamic Host Configuration Protocol).