1. Introduction to Computer Network for Non-Techies
   1. Basic Networking rules
      1. Communication Protocols
         1. TCPIP
         2. TCP (Data must be delivered uncorrupted)
         3. UDP (Data can be delivered corrupted)
      2. Data must be delivered uncorrupted.
      3. Must be capable of determining the origin and destination of a piece of information. [IP, Mac Address]
   2. Types of Computer Networks
      1. Architecture
         1. Client Server
            1. Composed of clients and servers.
            2. Servers provide resources.
            3. Clients receive resources.
            4. Servers provided centralized control over network resources [files, printers]
            5. Advantages

Centralized user, security, and access to simplify network administration.

More powerful server = more efficient access to network resources; scales up more efficiently

Single password to access all resources.

* + - * 1. Disadvantages

Server failures renders an unusable or loss of resources.

Complex, specific purpose server require expert staff [Dedicated cost]

Dedicated hardware and specialized software add to the cost of ownership.

* + - 1. Peer to Peer
         1. No dedicated servers.
         2. Share resources as it needs.
         3. No centralized control over shared resources.
         4. All computers on the network can be a client or a server
         5. Advantages

Easy to install and configure

Does not depend on dedicated server

Individual users control the resources

Inexpensive to operate

No dedicated administrators

* + - * 1. Disadvantages

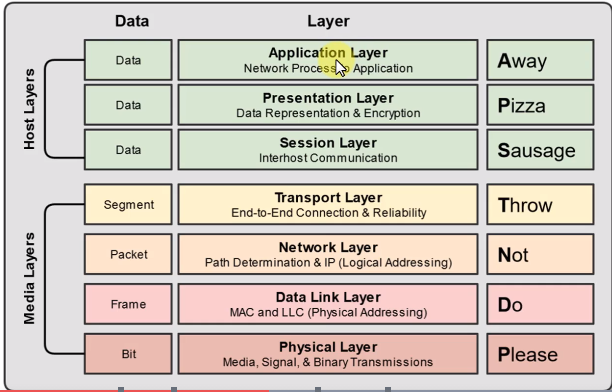
Network security

Users may be forced to use a variation of shared password for different resources.

Each machine must be backed up individually to protect all shared data.

No centralized organizational scheme to locate or control access to data.

* + 1. Size
       1. Local Area Network (LAN)
          1. Network within a small geographical area such as a single room or building.
       2. Campus Area Network (CAN)
          1. Network of multiple interconnected LAN in a limited geographical area such as Campus or corporation
       3. Metropolitan Area Network (MAN)
          1. Network that interconnects users with computer resources in a city
       4. Wide Area Network (WAN)
          1. Network that extends over a large geographical distance, typically over multiple cities, and countries.
  1. Why build a network?
     1. Efficient modes of communication
     2. Cost savings
     3. Backup and recovery of data
     4. Encourages the use of policies and procedures.
  2. Computer network protocols
     1. Physical Protocols
        1. Wiring, connections and signals
     2. Logical Protocols
        1. Software controlling, how and when data is sent and received to computers supporting physical protocols.
  3. OSI model
     1. Open systems interconnection reference model
        1. Conceptual framework shows how data moves in a network.
        2. Created to give a guide how network operate.
     2. Model stack
        1. Upper layers (host layers)
           1. Handled by host computer with application-specific functions
        2. Lower layers (Media layers)
           1. Provide network-specific function



Layer 7 Application Layer

Users communicate with computer

Acts an interface between an application and end-user protocols

Applications don’t reside in the application layer protocol, it interfaces with the application-lyaer protocol

Layer 6 Presentation Layer

Ensures that data transferred from one system’s application layer can be read by the application layer of another

Provide character code conversion, data compression, and data encryption

Layer 5 Session Layer

Responsible for setting up, managing, then tearing down sessions between network devices

Ensures data from different application sessions are kept separate

Coordinates communication between systems

Start, stop, restart

Layer 4 Transport layer

Ensures data is delivered error-free and in sequence

Segments data and reassemble correctly

Can be connection-oriented or connectionless

Considered the ‘Post Office’ Layer

TCP (Transmission Control Protocol) – Connection oriented and error free delivery

UDP (user Datagram Protocol) – Connectionless and not always error free

Layer 3 Network layer

Routing layer

Provides logical addressing and routing services

Places 2 addresses in the packet

Source and Destination IP

Layer 2 Data Link layer

Provide physical transmission of data

Ensures that messages are delivered to the proper device on a LAN using MAC addresses

Translates messages from the network layer into bits for the physical layer

The “switching” layer

Layer 1 Physical layer

Define the physical and electrical medium for network communications

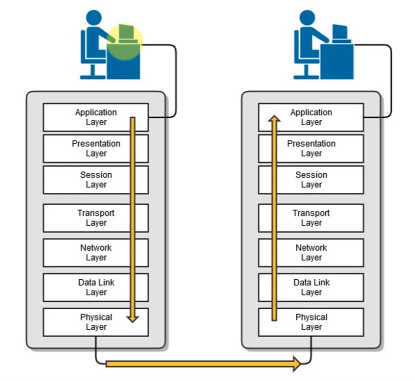
Send bits and receive bits

Network cabling, jacks, patch, panels

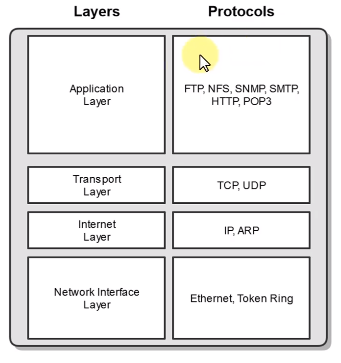
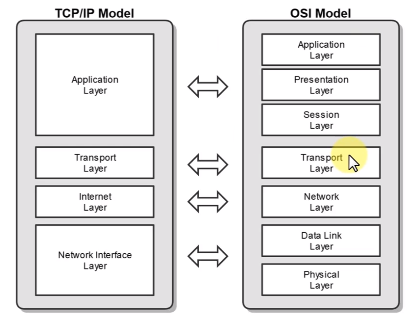
Encoding signal types

Ethernet IEEE 802.3 Standard

* + - * 1. Interaction example



* 1. TCP/IP Model
     1. Suite protocol which the internet was built.
     2. Standard for computer networking,
     3. Based on 4-layer model similar to the OSI model.



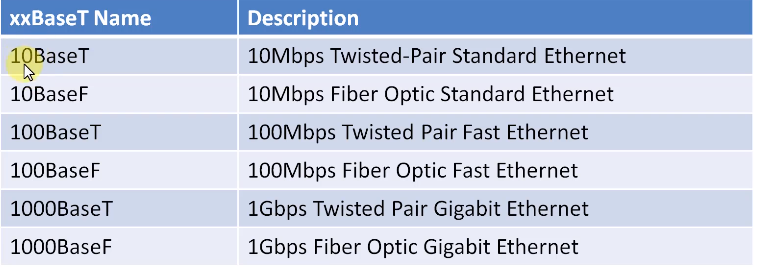
* + 1. Commonly called the internet protocol
    2. TCP/IP Protocols
  1. Media Access Control (MAC)
     1. Physical address of the network adapter card
        1. OSI later 2 (Data Link) Layer Address
        2. TCP/IP Layer 1 (Network Interface) Layer Address
     2. Six bytes (48 Bits), hexadecimal
        1. First 3 bytes (24 bits) are assigned by the IEEE to the manufacturer.
           1. OUI assigned by IEEE – Organizationally Unique Identifier
        2. Last 3 bytes (24 bytes) are usually assigned sequentially.
           1. Allow for uniqueness.
        3. 00:21:70:6f:06:f2
  2. IPv4 (Internet Protocol Version 4)
     1. OSI Layer 3 (Network) Address
     2. Dotted Decimal Format Mask Binary Format.
     3. 4 bytes = 32 bits = 4 octet
  3. IP vs MAC

|  |  |
| --- | --- |
| IP | MAC |
| Network address | Data Link addresses |
| Logical Addresses | Physical Addresses |
| Changeable | Physically burned on NIC |
| Dotted Decimal Notation | hexadecimal |

* 1. Duplex Communication

|  |  |
| --- | --- |
| Half Duplex | Full Duplex |
| Send and receive not at the same time | Can send and receive data simultaneously |

* 1. Ethernet
     1. Standard communication protocol for building a local area network
        1. Speeds, cabling, connectors, equipment
        2. Physical and data link layers of LAN
     2. Controls how data is transmitted over LAN
     3. Supports network built with thin and thick coaxial, twisted-pair, and fire-optic cabling
     4. Uses CSMA/CD access methodology
     5. Uses “xx Base T” naming convention
        1. Xx: Speed
        2. Base: Baseband communication (Single frequency)
        3. Type of Cable



1. Network Topologies
   1. Physical
      1. Physical design of network including the network devices, locations, and cables similar to building blueprint.
   2. Logical
      1. Define how data moves throughout the network. [csma/CA, csma/cd, ethernet]
2. Common physical topology
   1. Importance
      1. Useful in planning a network.
      2. Shows the network on a “map”.
      3. Assists in understanding signal flow.
   2. Bus Topology
      1. All devices are connected to a single network cable.
      2. Terminators are required for both end of the cable.
      3. Single break in cable will take down the network.
   3. Ring Topology
      1. All devices are connected in a circular fashion.
      2. Each computer ins connected to 2 other computer.
      3. Data travels from node to node with each computer handling data, either unidirectional or bidirectional.
   4. Star topology
      1. All devices are connected to a central device.
      2. Popular and used in large and small networks.
      3. Central device is a single point of failure.
   5. Mesh topology
      1. Each device is connected to every other device by separate cabling.
      2. Highly redundant and fault-tolerance
      3. Used in wide area networks (WANs)
      4. Expensive to install.
3. Network Interface Cards (NIC)
   1. It provides the physical and electrical, light or radio frequency connection to the network media.
   2. Can be an expansion card, USB devices or built directly into the motherboard.
4. Hubs
   1. Used to connect devices together within a network
   2. Used in early networks; replace by **switches**
   3. Multiport repeater (floods other device with data)
   4. Less efficient that a switch
5. Switches
   1. Similar to a hub, it connect devices
   2. Intelligence network device
   3. Memorise MAC address of each deuce and connect it via MAC address Table
   4. Breaks up collision domain
   5. Pays attention to Source and Destination Mac Addresses during communication process
6. Hubs VS Switches

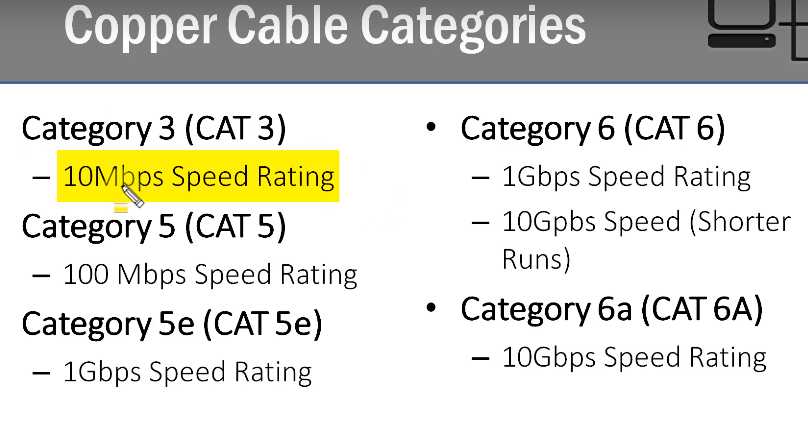
|  |  |
| --- | --- |
| Hubs | Switches |
| Dumb device, Floods all ports, inefficient | Intelligent device, learns port by MAC address, delivers to specified ports, efficient |
| OSI Layer 1 device | OSI layer 2 |
| Decease throughput, frequent collisions | Increased throughput, less frequent throughput |
| Less secure | More secure |

1. Wireless Access Points
   1. Not a wireless router; it is a bridge that extends the wireless network
   2. Allow mobile users to connect to a wired network wirelessly
   3. Effective bandwidth & Encryption (WEP, WPA, WPA2) (IEEE 802.11 Standard)
2. Routers
   1. Connect different networks together
   2. Routes traffic between networks using IP address
   3. Use intelligent decisions to find the best way to get a packet of information from one network to anther
   4. OSI layer 3 Device
      1. L3 – Router
      2. L2 – Switch
      3. L1 – Hub
3. Firewalls
   1. Protect LAN from Malicious Activity
   2. Prevents unwanted network traffic on different networks from accessing the network
   3. Controls the flow of information in and out of the network
4. DHCP Servers
   1. Dynamic Host configuration Protocol Server
   2. Auto assign IIP address to hosts
   3. Make administering a network easier
   4. Alternative to static IP address
5. All-in-one SOHO devices
   1. Small office home office device
6. Type of Cabling
   1. Coaxial
   2. Twisted Pair
      1. Twisted-pair copper cabling
         1. 4 twisted par of wires with rj-45 connector
         2. Balanced pair operation
            1. + & - signals
            2. Equal and opposite signal
         3. Why are they twisted?
            1. Help reduce interference.

Crosstalk

Noise

* + - 1. Security concerns
         1. Signal emanations
      2. 100m max distance
         1. Signal attenuation
    1. Unshielded Twisted pair (UTP)
    2. Shielded Twisted Pair (STP)
    3. Electromagnetic Interference
    4. Roles of Twists
       1. Reduce crosstalk
       2. Increases signals
       3. Supports faster speeds
    5. Copper cable
       1. speed



* + - 1. Wiring standards
         1. 568A & 568B
         2. Why are standard important?

Lower cost

Increase interoperability

Easier maintenance

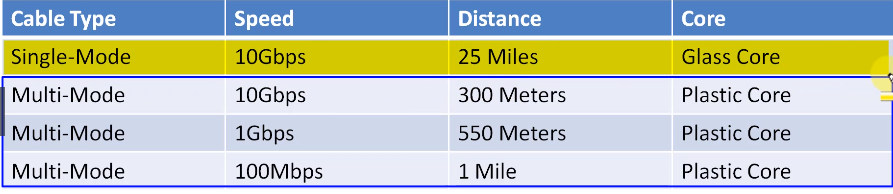
* + - 1. Type of cable
         1. Straight through

Connect unlike devices

* + - * 1. Crossover

Connect similar devices

* 1. Fiber Optic
     1. Glass or plastic fiber that carries light
        1. High bandwidth
        2. Long distance
        3. Immune to EMI
        4. Doesn’t emanate signals
     2. 2 types
        1. Multi-mode Fiber
           1. Shorter distances up to 1 mile
        2. Single-mode Fiber
           1. More expensive
           2. Longer distances (up to 25 miles)
     3. Why use fiber?
        1. More expensive but higher performance
        2. Immune to EMI and signal emanations
        3. Lower signal attenuation
        4. More reliable and secure
        5. Decreasing cost due to higher rate of adoption



* 1. Cable selection criteria
     1. Cost constraint
     2. Transmission speed requirement
     3. Distance requirement
     4. Noise and Interference immunity