Chapter 1
Internetworking

Internetworking Basics

- Network segmentation – Breaking up a large network into multiple smaller networks
  - Common causes of LAN traffic congestion:
    - Too many hosts in a collision or broadcast domain
    - Broadcast storms
    - Too much multicast traffic
    - Low bandwidth
    - Adding hubs to your network
    - A bunch of ARP broadcasts

- Routers
  - Don't forward broadcast traffic (break up broadcast domains)
  - Filter network information based on layer 3 information

- How routers function in a network
  - Packet switching
  - Packet filtering
  - Internetwork communication
  - Path selection

- Switches
  - Break up collision domains (each cable connecting to a switch is considered a collision domain)
  - Can be used at layer 3 (layer 3 can be implemented on higher end switches)

- Hubs
  - Information goes on one port and comes out on all ports
  - Never use a hub unless you absolutely have to, they don't break up broadcast domains or collision domains, they just extent your network and cause more traffic than necessary

Internetworking Models

- OSI Reference Model (Created by ISO)
  - Describes how information from one computer is communicated to another

The Layered Approach

- Advantages of a reference model
  - Facilitates component development, design and troubleshooting by breaking up the overall process into smaller chunks
  - Allows multiple vendor development through standardization of network components
  - Encourages industry standards by defining what happens at each layer

  - Allows hardware from multiple vendors to communicate with one another
  - Prevents changes in one layer from affecting other layers to expedite development

The OSI Reference Model

- OSI model has seven layers, divided into three groups
  - Upper
    - Communicate with the user interface and application
      - (1) Application, Presentation and Session layers
  - Middle
    - Reliable communication and routing to a remote network
      - (1) Transport and Network layers
  - Lower
    - Communicate to the network
      - (1) Data Link and Physical layers

- Application (Layer 7)
  - Provides a user interface
- Presentation (Layer 6)
  - Presents data
  - Handles processing such as encryption
- Session (Layer 5)
  - Keeps different applications' data separate
- Transport (Layer 4)
  - Provides reliable or unreliable delivery
  - Performs error correction before retransmit
- Network (Layer 3)
  - Provides logical addressing (IP addresses) – Think routers and layer 3 switches
- Data Link (Layer 2)
  - Combines packets into bytes and bytes into frames
  - Provides access to media using MAC addresses – Think switches
  - Performs error detection (not correction)
- Physical (Layer 1)
  - Moves bits between devices
  - Specifies cables and their speed, pinouts, voltage, etc.

The Application Layer

- Marks the spot where users communicate to the computer and only comes to play when access to the network will be needed
- Works as the interface between the actual program and the next layer down
- Provides a way for the application to send information down the protocol stack

The Presentation Layer

- Presents data to the application layer

- Responsible for data translation and code formatting

The Session Layer

- Responsible for setting up, managing and dismantling sessions between hosts and keep data separate between multiple applications
- Dialog control
- Communication comes in three modes
    - Simplex
        - 1 way communication (sending something and not getting a reply)
    - Half-duplex
        - Two way communication, but takes place only one direction at a time (think a walkie-talkie)
    - Full-duplex
        - Two way communication where communication can be transmitted and received at the same time

The Transport Layer

- Breaks up and reassembles data
- Can establish a logical connection between hosts for communication
- TCP and UDP reside at this layer
    - TCP is reliable delivery with confirmation (a host sends the data and receives acknowledgment of the data being delivered)
    - UDP is unreliable (there is no confirmation that the information was received by the recipient, such as a cable box streaming a show)
- Establishes sessions and tears them down when they are done
- Can be connection-oriented or connectionless
    - Connection-Oriented Communication
        - 3 way handshake happens before hosts start communicating
            (1) Host sends a SYN request (synchronization)
            (2) Receiver sends a SYN/ACK back to the host establishing rules for communication and creates a bidirectional connection
            (3) Host sends an ACK back to the receiver with an agreement to the rules and the two hosts start communicating
- Flow Control
    - Ensures data integrity by allowing applications to request reliable data transport
    - Prevents a sending host from overflowing the buffer of the receiving host
        - Reliable data transport involves:
            (1) Delivered segments are acknowledged back from the receiver to the host
            (2) Segments not acknowledged are retransmitted
            (3) Destination host reassembles all segments in proper order before the information is moved up in the layered model
            (4) Data flow is maintained to avoid congestion, overloading or data loss
- Windowing

  - Controls how much information is transferred from one end to another before and acknowledgment is required to continue
    - If the window size is 3, the host sends segments 1, 2 and 3 and stops until it receives an acknowledgment, then continues with 4, 5 and 6
      1. Host sends 1, 2, 3, receiver sends ACK 4 requesting the next window of packets to come in, the host sends 4, 5, 6 and the receiver sends an ACK 7 basically saying it's ready for the next window of segments
      2. Data loss: Host sends segments 1,2,3 but segment 2 was lost in transit, so the receiver only has 1 and 3. The receiver sends an ACK 2 and the host retransmits segment 2, so the receiver now has 1, 2 and 3. The receiver will then send an ACK 4 to the host and the host transmits segments 4, 5 and 6.

<u>The Network Layer</u>

- Transports data between devices that aren't locally attached
- Router receives packet:
  - It looks at the destination IP address
  - If it isn't destined for the router, it looks up the IP address in a routing table which specifies the exit interface it should send the packet to
  - The packet it sent to the interface where it is framed and sent toward its destination
  - If the router can't find an entry for the IP address in the routing table, the packet is dropped
- Two types of packets used at the network layer:
  - Data packets
    - Used to transport user data through internetworks
      1. Protocols used for this: IPv4, IPv6
  - Route packets
    - Used to update routers with information about neighboring routers
      1. Protocols used for this: RIP, RIPv2, EIGRP and OSPF
- Router characteristics you should never forget:
  - Routers do not forward broadcast or multicast traffic by default
  - Routers use logical addresses in the network layer header to determine the next hop router to forward the packet to
  - Routers can use access lists created by admins for security to prevent certain traffic from exiting or entering a router
  - Routers can be configured to act as a layer 2 bridge
  - Routers provide connections between VLANS
  - Routers can provide QoS for specific network traffic

<u>The Data Link Layer</u>

- Provides for the physical transmission of data and handles error notification, network topology, and flow control
- Ensures data is transmitted to the proper device on a LAN using hardware addresses
- Translates messages from the network layer into bits for the physical layer to transmit
- Messages from the network layer are encapsulated into data frames at this layer

- While the network layer gets packets to the right network, the data link layer provides a way to take the data and sent it to the proper host on a LAN once the packet arrives at the correct network
- The frame is stripped at each hop and rebuilt with new information about the next hop
    - Router A receives a frame with the destination MAC address of itself and strips the data, looks at the destination address in the LLC portion of the frame and realizes it's not for a network locally attached to it
    - Router A looks up the destination IP address in its routing table and sees that Router B has a connection to the IP address
    - Router A frames the packet with a source MAC address being its own and the destination MAC address of Router B
- Data link layer has two sublayers:
    - Logical Link Control (Upper sublayer)
        - Identifies network layer protocols and encapsulates them
        - LLC headers tell the Data Link layer what to do with a packet once the frame is received
        - Makes it possible for multiple network protocols to coexist within a network and to be transported on the same network medium
    - Media Access Control (MAC) (Lower sublayer)
        - Defines how packets are placed on the media
        - Physical addressing
        - Logical topologies
        - Error notification (not correction), order of delivered frames and flow control can be used at this sublayer
        - Host receives a frame, looks in the LLC header to find out where the packet is destined
        - LLC can also provide flow control and sequencing
- Switches and Bridges at the data link layer
    - Layer 2 switching is considered hardware-based bridging
    - Switches contain filter tables that records what MAC addresses are connected to what interface
    - When a frame is sent, the hardware address is looked up in the table and forwarded only to the destination hardware address
    - If the hardware address is not in the table, the frame is sent out to everyone, in hopes of it receiving a reply, in which the reply will cause the table to be updated

The Physical Layer

- Sends and receives bits
- Bits are either a 1 or a 0
- Specifies the electrical, mechanical, procedural, and functional requirements for activating, maintaining, and deactivating a physical link between end systems
- DTE (Data Terminal Equipment) and DCE (Data Communication Equipment) is defined at this layer
    - DTE
        - Attached device
    - DCE
        - Located at the service provider
- Hubs at the physical layer
    - Hubs are repeaters

- Hubs don’t look at any information in frames and just forwards received frames out onto every port, causing a mess and congestion
- Mainly used to extend a network, but are worthless, so don’t use unless you absolutely have to

Chapter 2
Ethernet Networking and Data Encapsulation

- Collision Domain
    - A frame is sent out by a host and all hosts connected to the collision domain are forced to pay attention to it
    - The less, the better
    - Every connection on a switch/bridge is considered a collision domain
- Broadcast Domain
    - A frame is sent out to a broadcast domain when it's specified as a broadcast and only the specified segment receives the frame
    - Every connection on a router is considered a broadcast domain
    - Routers do not forward broadcasts by default

CSMA/CD

- Carrier Sense Multiple Access with Collision Detection
    - Helps devices share bandwidth evenly while preventing two devices from simultaneously transmitting data
    - When a host wants to transmit, it listens to see if anything is being transmitted, if not, it transmits what it needs to transmit
- When a collision occurs:
    - Jam signal informs all devices that a collision occurred
    - The collision invokes a random backoff algorithm
    - When the timer expires, all hosts have equal priority to transmit
    - If collisions keep occurring after 15 tries, the notes attempting to transmit will time out

Half- and Full-duplex Ethernet

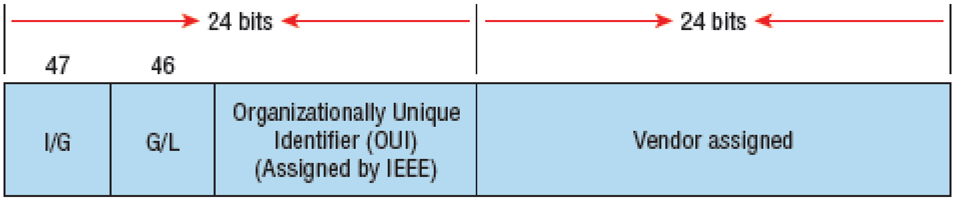
- IEEE 802.3 specification
    - Half Duplex
        - Uses CSMA/CD
        - Hubs can only operate in half duplex mode (anything connected to the hub will be configured to run in half duplex as well)
        - Uses only 1 wire pair to send and receive data, which in effect does not allow simultaneous sending and receiving
    - Full Duplex
        - Uses two wire pairs which allows simultaneous sending and receiving, preventing collisions
        - Point to point connection between the transmitting device and receiving device
        - Can be used in all connections with the exception of a hub and anything that connects directly to the hub

- Auto-detect mechanism
    - When a full duplex Ethernet port is turned on it connects to the remote end and negotiates with the other end of the link
        - It decides on speed, and then checks if it can run full duplex, and if it can't, it will default to half duplex
- Important points:
    - There are no collisions in full duplex
    - A dedicated switch port is required for each full-duplex node
    - The host NIC and the switch port must be capable of running in full duplex
    - If the autodetect mechanism fails, the duplex is set to half with a speed of 10 Mbps

Ethernet at the Data Link Layer

Ethernet Addressing

- MAC (Media Access Control)
    - Burned onto each Ethernet NIC
    - 48-bits long (6-bytes), written in hexadecimal format
        - Example: 00:0A:95:9D:68:16

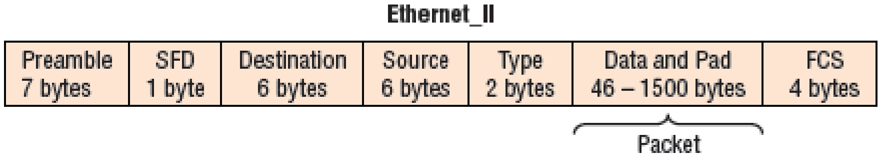


- The OUI (Organizationally Unique Identifier) is assigned by the IEEE to an organization
    - It's composed of 24 bits (3 bytes)
- In conjunction with the OUI, the vendor uniquely assigns it's own 24 bit identifier to each adapter
    - There is no guarantee that every single one of the adapters is unique
- I/G bit
    - Individual/Group bit
    - High order
    - When the value of the I/G is 0, we can assume that the address is the MAC address of a device and that it will appear in the source portion of the MAC header
    - When it's a 1, we can assume that the address represents either a broadcast or multicast address in Ethernet
- G/L bit
    - Global/Local bit
    - When this is a 0, it represents a globally administered address, as assigned by the IEEE
    - When this is a 1, it represents a locally governed and administered address

Ethernet Frames

- Data link layer is responsible for combining bits into bytes and bytes into frames

- Functions of Ethernet stations is to pass data frames between each other using a group of bits known as a MAC frame
    - This provides error detection, not correction
    - Example of an Ethernet frame:



Ethernet_II

Preamble 7 bytes	SFD 1 byte	Destination 6 bytes	Source 6 bytes	Type 2 bytes	Data and Pad 46 – 1500 bytes	FCS 4 bytes

Packet

- Details of the Ethernet Frame pictured above:
    - Preamble: An alternating pattern that allows the receiving device to lock in the incoming signal
    - Start Frame Delimiter (SFD)/Synch: The SFD is 10101011. The last pair of 1s allows the receiver to come into the alternating 1,0 pattern somewhere in the middle and still synch up to detect the beginning of the data
    - Destination: A 48-bit value using the LSB (Least Significant Bit) first. This is the MAC address destination. This is used to verify that a packet is for a particular node. If the destination is all 1s, it is a broadcast
    - Source: MAC address, 48-bits in length that identifies the source of the frame (who sent it)
    - Type: Identifies the network protocol
    - Data: This is the packet sent down to the Data Link Layer from the Network Layer. The size can vary from 46 to 1500 bytes
    - Frame Check Sequence (FCS): Stores the CRC (cyclic redundancy check) information. When the frame is received, the receiving node will run an algorithm against the frame and compare the answer to that in the FCS field. If it doesn't match, the node discards the frame

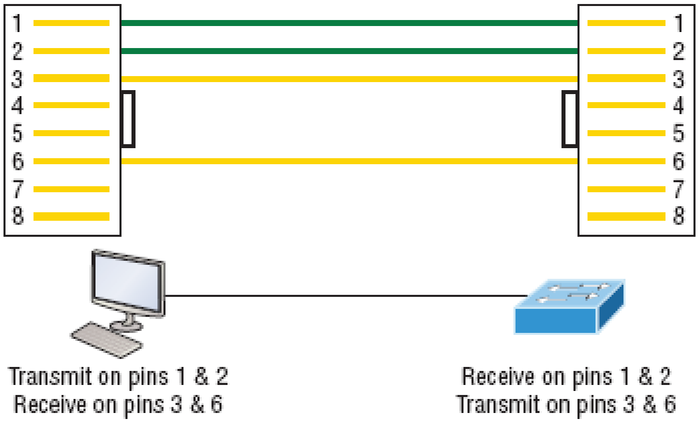
Ethernet at the Physical Layer

- Most common IEEE Ethernet standards:
    - 10Base-T (IEEE 802.3)
        - 10 Mbps
        - CAT3
        - Runs up to 100 meters
        - Physical star topology and logical bus
    - 100Base-T (IEEE 802.3u)
        - Known as Fast Ethernet
        - CAT5, 5E or 6
        - Runs up to 100 meters
        - Physical star topology and logical bus
    - 100Base-FX (IEEE 802.3u)
        - Fiber cabling 62.5/125-micron multimode fiber
        - Point to Point topology
        - Runs up to 412 meters
        - Uses ST and SC connectors (Media-Interface connectors)
    - 1000Base-CX (IEEE 802.3z)

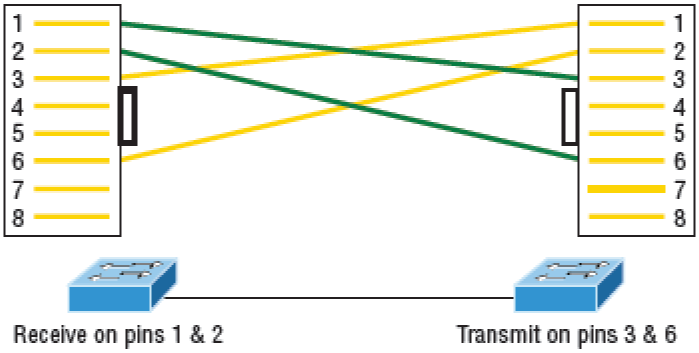
    - Copper twisted paid, called Twinax
    - Coaxial twisted pair
    - Runs up to 25 meters
    - Uses 9-pin High Speed Serial Data Connector (HSSDC)
    - Used in Cisco’s new Data Center technologies
  - 1000Base-T (IEEE 802.3ab)
    - CAT5
    - 4 pairs of UTP wires
    - Up to 100 meters
    - Speeds up to 1 Gbps
  - 1000Base-SX (IEEE 802.3z)
    - MMF (Multi-Mode Fiber)
    - 62.5 – and 50-Micron core
    - 850 nanometer laser
    - Up to 220 meters with 62.5-micron core
    - Up to 550 meters with 50-micron core
  - 1000Base-LX (IEEE 802.3z)
    - Single-Mode Fiber
    - 9-micron core
    - 1300 nm laser
    - Can be from 3-10 Kilometers
  - 1000Base-ZX (Cisco Standard)
    - Standard for Gigabit Ethernet communication
    - Single-Mode fiber
    - Spans up to 43.5 miles
  - 10GBase-T (802.3an)
    - Proposed by the IEEE to provide 10 Gbps connections over conventional UTP cables (CAT5E, 6, or 7)

<u>Ethernet Cabling</u>

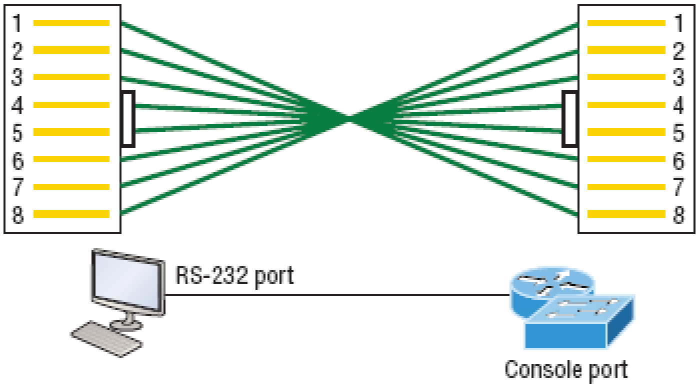
- Three types of cables
  - Straight-Through
    - Used to connect unlike devices together
      - (1) Host to Switch or Hub
      - (2) Router to Switch or Hub
      - (3) Only pins 1, 2, 3 and 6 are used
        - (a) Connect pin 1 to pin 1, 2 to 2, 3 to 3 and 6 to 6 on each side of the cable



- Crossover
  - Used to connect like devices
    - (1) Switch to Switch
    - (2) Hub to Hub
    - (3) Host to Host
    - (4) Hub to Switch
    - (5) Router direct to Host
    - (6) Router to Router
  - Only pins 1, 2, 3 and 6 are used (like the Straight-Through cable)
    - (1) Unlike the Straight-Through cable, connect pins 1 to 3 and 2 to 6 on each side of the cable



- Rollover
  - Used to connect a host to the console port of a router which is used for configuration
    - (1) All pins are reversed from one side to the other



Fiber Optic

- Immune to interference / crosstalk
- Main components of a fiber optic cable
  - Core
    - Holds the light
    - The smaller the core, the faster the speeds
  - Cladding
    - Confines the light within the core
  - Buffer
    - Protects the delicate glass
- Two major types of fiber optic modes:
  - Single-Mode
    - More expensive
    - Tighter cladding
    - Goes much further than multimode
    - Only 1 mode of light propagates down the fiber at a time
  - Multimode
    - Cheaper
    - Looser cladding which allows more than 1 mode of light to travel at a time

Data Encapsulation

- Each layer uses a PDU (Protocol Data Unit)
  - As information is being moved from the top layers down, the information is encapsulated with the PDU designated at the layer
  - When the information is received, the receiving node strips off one PDU per layer as it moves up in the OSI stack
- Control information is attached at each layer
  - Upper layer user data is converted for transmission and handed down to the Transport Layer
  - Transport layer sets up a virtual circuit to the receiving device by sending a SYN packet
  - The data stream is broken up into smaller pieces and a Transport layer header is created and attached
  - When the Transport layer encapsulates the data and adds its header, the PDU is called a **SEGMENT**
    - Each segment can be sequenced so that when the receiving computer receives multiple segments for a file, it can put it back in proper order
  - Each segment is handed to the Network layer
  - The Network layer adds IP information and attaches a header, turning the segment into a **PACKET** or **DATAGRAM**
  - The network layer hands the packet down to the Data Link layer
  - The Data Link layer then adds a header to the packet that contains physical address information (MAC Address), thus turning the packet into a **FRAME**

FIGURE 2.21 Data encapsulation

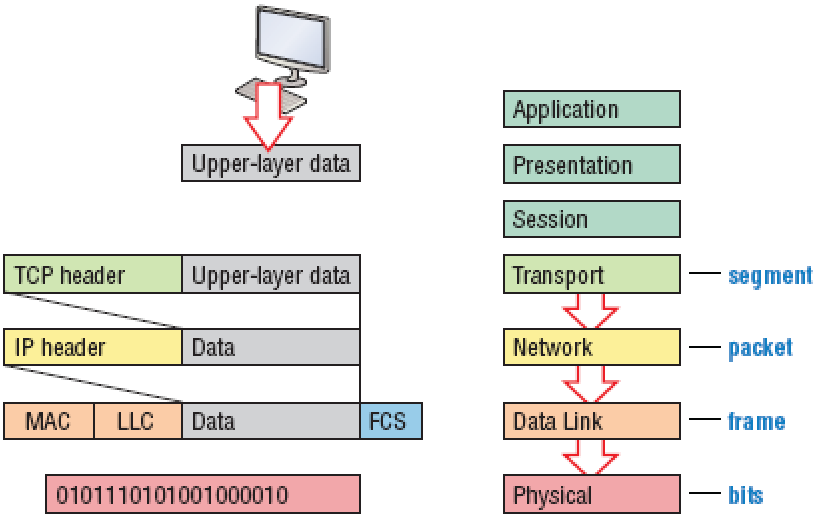
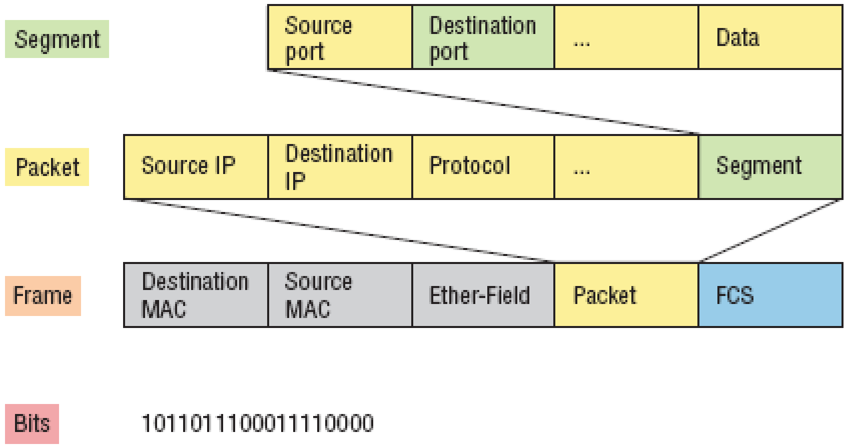


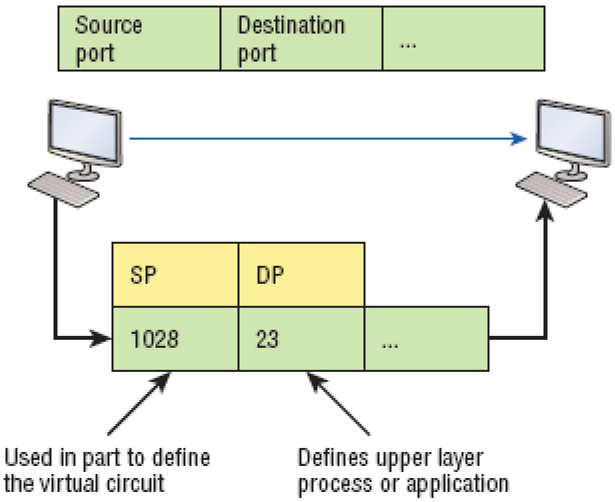
FIGURE 2.22 PDU and layer addressing



Port Numbers

- Transport Layer uses port numbers to define the virtual circuit and upper-layer processes

FIGURE 2.23 Port numbers at the Transport layer


Source port
Destination port
...
SP
DP
1028
23
...
Used in part to define the virtual circuit
Defines upper layer process or application

The Cisco three-Layer Hierarchical Model

INSERT IMAGE ON PAGE 71 HERE

The Core Layer

- Is the core of the network
- Responsible for transporting large amounts of data reliably and quickly
- Only purpose is to switch traffic as fast as possible
- If there is a failure at this layer, every user can be affected
- Fault tolerance is important at this layer
- Things you don't want to do at this layer, since speed is so crucial:
  - Don't slow down traffic by using access lists, routing between VLANS and implementing packet filtering
  - Don't support workgroup access
  - Avoid expanding the core, if you need more speed, don't add devices, upgrade existing ones
- Things you want to do at this layer:
  - Use data link technology that focus on speed and redundancy
  - Select routing protocols with low convergence times
  -

The Distribution Layer

- Sometimes referred to as the workgroup layer

- Communication point between the core layer and access layer
- Primary functions:
  - Provide routing, filtering, and WAN access and to determine how packets can access the core
  - Determines the fastest way network requests are handled
- Things that should be handled at this layer:
  - Routing
  - Access lists, packet filtering and queuing
  - Security and network policies, address translation and firewalls
  - Redistributing between routing protocols, including static routing
  - Routing between VLANS
  - Define broadcast and multicast domains
- Things that should not be handled by this layer:
  - Everything handled by the other two layers

The Access Layer

- Controls user and workgroup access to internetwork resources
- AKA desktop layer
- Things done at this layer:
  - Continued used of access lists and policies
  - Network segmentation to separate collision domains
  - Provide connectivity to the distribution layer
- Gigabit and Fast Ethernet are frequently used at this layer