**CHAPTER 1**

**Switch:**  Deals with frames (MAC addy).A switch can segment a network. However, it cannot create separate broadcast domains. It operates at Layer 2. It seeks for MAC addresses for each of the host attached to the switch in order to establish a communication between hosts. The switch holds a table with the MAC address of all attached hosts

**Router:**  Deals with packets (IP addy). It creates separate broadcast **and** collision domains. They can connect two or more networks. They seek other networks and they forward the packets to the appropriate router via the use of routing protocols. They operate at Layer 3 by using Logical IP addressing. Routers also usepacket filtering. In addition routers do not allow broadcasts to reach other networks. Routers can use access lists, created by an administrator, to control security based on the types of packets allowed to enter or exit an interface. Routers can provide layer 2 bridging functions if needed and can simultaneously route through the same interface. Layer 3 devices— in this case, routers— provide connections between virtual LANs. In addition, with routing you also have Badnwidth control and QOS.

* + **packet filtering:** Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.
  + **routing protocols:** A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network
  + **Routing Table:** A routing table is used to match the info in the packet header with the destination route and forwards it. The routing table consists from entries for connected networks and remote networks. The connected networks are directly connected to the router’s interface. Remote networks are not directly connected to the router but the routing table of the routers will enable the routers to forward the packet to a specific remote network. The decision on what path the packet will take depends on routing protocols being used. One route entry can refer to a larger general network or to a specific subnet on that same network. If the subnet is not part of the routing table then the packet will be forwarded to the general network and from there it is assumed that there will be a route that will know where to forward the packet in order to reach the intended subnet. A routing table contains the following information.
    - **Network Address:** The routing addresses from different routing protocols (IP,IPV6, etc).
    - **Interface:** The exit interface a packet will take when destined for a specific network.
    - **Metric:** The distance to the remote network. Each routing protocol uses a different method to calculate distance from one router to another.
  + **How do routers learn about routes?** 
    - **Static Routing:** Each router is statically configured with the routing information. This is very reliable but it adds a lot of administration cost.
    - **Dynamic Routing:**  Routers learn automatically about changes on the network through the use of routing protocols (RIP-EIGRP-OSPF). Routers share dynamically information about their routing.

**What can cause a LAN traffic congestion:**

* Too many hosts in a Collision or Broadcast Domain
* Broadcast storms
* Too much multicast traffic
* Low bandwidth
* Existence of Hubs
* Lots of ARP broadcasts which can lead to a broadcast storm.

**OSI MODEL:**

**Key thing to remember:**

Transport layer --> Segments

Network layer --> packets (Datagram at the IP model)

Data Link layer --> frames

Physical --> bits

**PDU Vs SDU**

Both terms are used to describe the process of **encapsulation/decapsulation**. The PDU holds the control information. The PDU is the encapsulation of data at the current layer in order to be passed at the next layer. Each PDU from each layer is read only by the peer layer of the receiving device. When the PDU is received by the next layer, that same PDU is treated like a SDU (data), which in turn will be turned into a PDU (encapsulation) to be passed along to the next lower layer. The above describes the process of a top to down direction at the OSI model.

**Application -** File, print, message, database, and application services. The Application layer works as the interface between actual application programs.

**Presentation -** Data encryption, compression, and translation services. It presents data to the Application layer and is responsible for data translation and code formatting

**Session -** Dialog control. The Session layer is responsible for setting up, managing, and dismantling sessions between Presentation layer entities and keeping user data separate

**Transport -** End-to-end connection. The Transport layer ensures the reliable arrival of messages and provides error checking mechanisms and data flow controls. When using a connection-oriented protocol like TCP, the Transport layer takes the data stream, makes segments out of it, and establishes a reliable session by creating a virtual circuit. The Transport layer is responsible for providing mechanisms for multiplexing upper-layer applications, establishing sessions, and tearing down virtual circuits.  
The Transport layer provides services for both "**connection-mode**" transmissions and for "**connectionless-mode**" transmissions.

**Connection - mode - TCP:** Under UDP mode Segments are being used.A connection oriented service needs to meet the following requirements.

* 1) Handsake
* 2) Sequences
* 3) AKCs
* 4) Flow control.

In order for a connection to be established a three way handshake needs to take place. The three way handshake is a set of rules being established before exchange of information is established between two hosts. TCP also provides error checking on its segments. Remember that all connections are IP (no error checking) but TCP makes up for the deficiencies of the IP.

* + **Segments:** Contain the encapsulated data from the application layer. The size of the segment is being determined by the smallest MTU value encountered across the network. The MTU (A maximum transmission unit) is the physical limitation of what a router is willing to handle at any point. Each segment has a **sequence number** which is being used to re-assemble the data when it reaches the destination. For each segment being sent an ACK is being sent back. If the ACK is not sent then the segment is being resent.
  + **MTU (Maximum Transmit Unit):** Is determined by the data link layer and the requirements are passed to the network layer. Each router determines the MTU size. Initially the host will do an MTU discovery. If the size of the packet is larger than the MTU allowed by a router, the router will request for a smaller size. This request is being sent over to the host and the host adjust the size accordingly. If there is a router that demands a smaller MTU, the router then will fragment the packets before sending them over to the next router. The fragments are being assembled at the host. The transport layer is not aware of any of this.
  + **Flow control.** Flow control prevents a sending host on one side of the connection from overflowing the buffers in the receiving host. The receiving end can set a "Not Ready" signal to the sender is order to pause the transmission of segments if it needs to. Flow control specifies the amount of segments can be sent before an ACK is expected by the sender. The receiver is always the one who specifies the window size. The sender cannot sent any more segments before the ACK has been received (by the sender). If the ACK is not received then the sender will put the data it wants to send into a buffer. Reliable data transport employs a connection-oriented communications session between systems, and the protocols involved ensure that the following will be achieved:
    - The segments delivered are acknowledged back to the sender upon their reception. Any segments not acknowledged are retransmitted.
    - Segments are sequenced back into their proper order upon arrival at their destination.
    - A manageable data flow is maintained in order to avoid congestion, overloading, or worse, data loss.
  + **Windowing (type of flow control):** The quantity of data segments, measured in bytes, that the transmitting machine is allowed to send without receiving an acknowledgment is called a window. Windows are used to control the amount of outstanding, un-acked data segments. The size of the window controls how much information is transferred from one end to the other before an acknowledgement is required. While some protocols quantify information depending on the number of packets, TCP/ IP measures it by counting the number of bytes.
  + **Acknowledgments:** The sender documents each segment measured in bytes, then sends and waits for this acknowledgment before sending the next segment. Also important is that when it sends a segment, the transmitting machine starts a timer and will retransmit if it expires before it gets an acknowledgment back from the receiving end.
  + **Session Multiplexing:** and it happens when a client connects to a server with multiple browser sessions open. The client data from each browser session must be separate when the server application receives it.
* **Connectionless - mode - UDP:** Under UDP mode datagrams are being used. In this mode there is no error checking. The data is being requested and the remote host sends the data with out concerning it self if the client machine received the data in a proper format/sequence nor does it care if it received the data at all for that matter. Datagrams are received by the client and are assembled in the order they were received and not by the use of sequence numbers.
  + **Datagrams:** UDP uses datagrams which are smaller than Segments because they do not have sequence numbers. As mentioned above, error checking is not performed and it is of no concern.

**Network -** Routing Deals with packets. It forwards/moves packets through paths created by logical paths within the network. The Network layer is responsible for finding the destination hardware address that dictates where the packet should be sent on the local network. It does this by using the Address Resolution Protocol (ARP) Routers operate at this layer. Routers may know about directly connected networks or remote networks. There are a variety of routing protocols that allow routers to be aware of the logical topology of the network. All this is done by using IPs/Network Masks. The packet has a protocol field that describes where the segment came from (either UDP or TCP) so it can hand the segment to the correct protocol at the Transport layer when it reaches the receiving host. There are two types of packets going through routers.

**Data Packets** which contains the actual data.

**Route Update Packets** which contain information/updates in order to update neighborhood routers for the state of other routers/networks.

**Network Addresses** A router must maintain a routing table for individual routing protocols because each routed protocol keeps track of a network with a different addressing scheme.

**Metric:** The distance to the remote network. Different routing protocols use different ways of computing this distance. Some protocols use hop count, or bandwidth, delay of the line, tick count, in order to determine the best path.

**Data Link** - Framing Deals with frames. It encapsulated the packets it received from the network layer into a frame and it puts it on the wire. The Data Link layer will add a header to the front of the packet and the piece of data then becomes a frame. The frame uses an Ether-Type field to describe which protocol the packet came from at the Network layer. The frame's header carries the hardware address of the source and the destination host. This is where switches operate. IP is not used here but the physical address MAC of each network card. The data link also handles network topology, and flow control.

This is where the **Ethernet Frames** live.

* + **Preamble:** Used for clock sync
  + **Start Frame Delimeter**: Indicates the preamble's end and that the MAC addy will follow.
  + **FCS:** It is an error detection operation. Sender generates a value by running CRC against the data contained in the frame. That value is placed in the FCS and the fame is transmitted. The receiver will run the same CRC against the frame's data and compare it to the answer provided by the incoming CRC. If there is a miss match the frame is considered corrupt but there is no special notification sent back to the sender. It is an error detection and not correction function.

**Physical:** Is responsible for encoding digits from the data link into a digital signal which are being read by devices in the same network. The devices will receive this signal and reconstruct the frames and run a CRC and check their answer against the FCS field.

Overall:

At a transmitting device, the data encapsulation method works like this:

User information is converted to data for transmission on the network.

Data is converted to segments, and a reliable connection is set up between the transmitting and receiving hosts.

Segments are converted to packets or datagrams, and a logical address is placed in the header so each packet can be routed through an internetwork.

Packets or datagrams are converted to frames for transmission on the local network.

Hardware (Ethernet) addresses are used to uniquely identify hosts on a local network segment.Frames are converted to bits, and a digital encoding and clocking scheme is used.

**CHAPTER 2**

**Collision Domain:**  Collision Domain is where data packets collide when being sent over a shared medium. This is a problem with Hubs. On switches each port is its own collision domain.

**Broadcast Domain:** Is a logical division of a computer network in which all nodes can reach one another. All devices attached to a switch compose a broadcast domain and are by default part of the same broadcast domain. This means you may have a root switch that has other switches attached to it with hosts attached to them. However, such a setup will create a lot of congestion due to the ARP requests or broadcast storm.

**Broadcast storms:** A broadcast storm is the situation in which messages broadcast on a network cause multiple hosts to respond simultaneously by broadcasting their own messages.

**Segmentation:** Breaking a network to smaller networks. Each segment can then be attached to a switch thus making each segment its own collision domain.

**CSMA/CD aka carries Sense multiple Access with Collision Detection. It is used in half duplex envs**

It helps devices share the bandwidth evenly while preventing two devices transmitting at the same time on the same network medium. This tech was initiall created to avoid collisions from two different nodes when TRed at the same time.

The transmitting host monitors the wire for any other hosts that might send out signals. If it sees another host trying to send out data then it puts a jam which prevents all other hosts from sending data as well. The other hosts will wait for a while till they attempt to send again data. This is in a half duplex environment and it has major delays. Hubs operate in a half duplex mode.

**Half Duplex and Full duplex ethernet.**

Hubs operate in a **half duplex** mode. Also a half duplex env can only use 30%-40% efficiency because due to overhead it can only give you 30 to 40 Mbps on a 100Base-T network.

In a **full duplex** environment there are two pairs of wires used. One for RX and one for TX. In theory all hosts can talk at the same time. It is also supposed to offer 100 effiency in both directions.

Last, remember these important points:

* There are no collisions in full-duplex mode.A dedicated switch port is required for each full-duplex node.
* The host network card and the switch port must be capable of operating in full-duplex mode.
* The default behavior of 10Base-T and 100Base-T hosts is 10 Mbps half-duplex if the autodetect mechanism fails, so it is always good practice to set the speed and duplex of each port on a switch if you can.

**Ethernet at the Data Link Layer:**

Ethernet at this layer is responsible for MAC addressing which is a 48bit address in hex format.

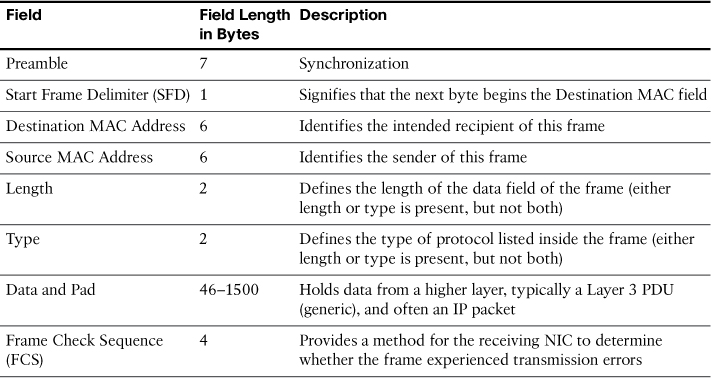
The organizationally unique identifier (OUI) is assigned by the IEEE to an organization. It’s composed of 24 bits. The reaming 24bits are assigned by the vendor.

The Data Link Layer combines bits into bytes and bytes into frames. Frames encapsulate packets handed by the network layer.

Data frames are passed between each node using the MAC frame format. It provides error detection via CRC.

An Ethernet Frame is composed by the following:

* Preable:
* Start Frame Delimiter/Sync:
* Destination Address (DA):
* Source Address(SA):
* Length of Type:
* Data:
* Frame Check Sequence: used to store the cyclic redundancy check (CRC) answer.



**Ethernet at the Physical Layer:**

Most cables are **UTP** (unshielded twisted pair). They consist of pairs of twisted copper cables. The twisting minimizes the effect of EMI. The most commonly used cable is CAT5. It can handle speeds up to 1Gbit with a distance of 100meters. CAT6 is rated for 10Gbps.

We also have **STP** which is shielded twisted pair. The problem with this type is that slight damage can introduce EMI.

REVISIT THESE.

**Copper based standards:**

All copper standards have a mix length of 100 meters.

**Ethernet:** 802.2 (10Base-T) : Ethernet runs on 10Mbps - Uses two pairs of wires

**Fast Ethernet:** 802.3u. It runs on 100Mbps. - Uses two pairs of wires.

**Gigabit Ethernet:** 802.3ab. It runs on 1000Mbps. Uses all fours pair of wires.

**10 Gigabit Ethernet:** 802.3an.

**Fiber Optic Standard:** They jump right in the 1000Mbps. 802.3z

**Ethernet Cabling:**

* **Straight-through cable:**
  + Host to switch. Router to switch.
  + Pins 1-2-3-6 are being used only. Supports only 100MBs
* **Crossover cable:** 
  + Sw to SW. Hb to Hb. Host to Host. Hb to SW. Router to host. Router to Router.
  + We connect pins 1 to 3 and 2 to 6.
* **Rolled cable:**
  + Although rolled cable isn’t used to connect any Ethernet connections together, you can use a rolled Ethernet cable to connect a host EIA-TIA 232 interface to a router console serial communication (COM) port.
* **Fiber Optic:** Is made either from glass or plastic and transmits light. It is immune to interference and it is becoming more popular in the ethernet world. There are two major types of cabling. Single mode and multimode. Single mode can go much further distances. Single mode allows only one mode of light down the fiber.

**Host to switch Connections - Straight Through cable**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Pin1 | Pin2 | Pin3 | Pin4 |
| PC | T | T | R | R |
| Switch | R | R | T | T |

**The Cisco Three-Layer Hierarchical Model**

**The core layer** is literally the core of the network. At the top of the hierarchy, the core layer is responsible for transporting large amounts of traffic both reliably and quickly. The only purpose of the network’s core layer is to switch traffic as fast as possible.

Not to do list of cores:

* Never do anything to slow down traffic. This includes making sure you don’t use access lists, perform routing between virtual local area networks, or implement packet filtering.
* Don’t support workgroup access here.
* Avoid expanding the core (e.g., adding routers when the internetwork grows). If performance becomes an issue in the core, give preference to upgrades over expansion.

To do list:

* Design the core for high reliability. Consider data-link technologies that facilitate both speed and redundancy, like Gigabit Ethernet with redundant links or even 10 Gigabit Ethernet.
* Design with speed in mind. The core should have very little latency.
* Select routing protocols with lower convergence times. Fast and redundant data-link connectivity is no help if your routing tables are shot!

**The Distribution layer** The primary functions of the distribution layer are to provide routing, filtering, and WAN access and to determine how packets can access the core, if needed. The distribution layer must determine the fastest way that network service requests are handled. There are several things that should generally be handled at the distribution layer:

* Routing
* ACLs, packet filtering, queing.
* Securtity/network policies, address translation and firewalls.
* Redistribution between routing protocols.
* Routing between VLANs
* Defining broadcast and multicast domains.

**The access layer:** The access layer controls user and workgroup access to internetwork resources. The access layer is sometimes referred to as the desktop layer.

The following are some of the functions to be included at the access layer:

* Continued (from distribution layer) use of access control and policies
* Creation of separate collision domains (microsegmentation/switches)
* Workgroup connectivity into the distribution layer
* Device connectivityResiliency and security servicesAdvanced technology capabilities (voice/video, etc.)

**CHAPTER 3 Introduction to TCP/IP**

**TCP/IP The DOD model**

It is condensed version of the OSI model.

* **Process/Application layer:**  Defines protocols for node to node application communication.
* **Host To Host layer or Transport layer:** Parallels the functions of the Transport layer.
* **Internet layer(IP) :** Corresponds to the OSI's model network layer. IP is connectionless. Packets are being sent without notifying the receiving end. There is no check at the IP level for any missing information. Is a best effort delivery of data from point to point. If reliability is important it must be paired with TCP, otherwise it is a UDP. Packets in the IP layer are called Datagrams. This is taken care of by TCP at the transport layer.
  + **IP** uses the **ICMP** protocol and it provides error reporting and testing. Its messages are carried as datagrams. It is being used to diagnose the network. If a router can’t send an IP datagram any further, it uses ICMP to send a message back to the sender, advising it of the situation. This can be because a buffer is full, Hops/Time exceeded, ping, traceroute.
  + **Network Access layer or Link layer:** Corresponds to the Data Link layer on the OSI model.

**IP ADDRESSING:**

**LOOPBACK**

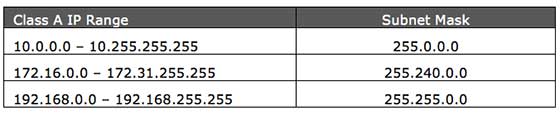
IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback i.e. a Host’s self-address. Also known as localhost address. This loopback IP address is managed entirely by and within the operating system.

**Link-local Addresses**  
In case of the Host is not able to acquire an IP address from DHCP server and it has not been assigned any IP address manually, the host can assign itself an IP address from a range of reserved Link-local addresses. Link local address range is 169.254.0.0 - 169.254.255.255. In absence of DHCP server, every host machine randomly chooses an IP address from the above mentioned range and then checks to ascertain by means of ARP, if some other host also has not configured himself with the same IP address.

**IPV4 Address Classes**

|  |  |  |  |
| --- | --- | --- | --- |
| **Class** | **Theoretical Address Range** | **Binary Start** | **Used for** |
| **A** | 0.0.0.0 to 127.255.255.255 | 0 | Very large networks |
| **B** | 128.0.0.0 to 191.255.255.255 | 10 | Medium networks |
| **C** | 192.0.0.0 to 223.255.255.255 | 110 | Small networks |
| **D** | 224.0.0.0 to 239.255.255.255 | 1110 | Multicast |
| **E** | 240.0.0.0 to 247.255.255.255 | 1111 | Experimental |

**Reserved IPs**



**CHAPTER 6**

**The CISCO IOS.**

You can connect to a CISCO device by:

* Auxiliary port
* Console port
* SSH or Telnet

**What happens during boot.**

* It does a POST.
* Loads the IOS from flash memory and expands it in RAM.
* Then it will load a valid configuration known as the startup-config which is stored in NVRAM.
* Then it will be copied into RAM.
* If not valid config file is found then the device will enter into config mode.

**Types of config modes:**

|  |  |
| --- | --- |
| * User Exec mode | Monitoring Commands |
| * Priveleged exec mode | Access to all other router commands |
| * Glogal Configuration mode | Commands that change the whole device |
| * Specific config modes | Commands that affect specific interfaces |
| * Setup mode | Interactive config dialog. |