1. **What are the different communication modes? Give example for each.**

Transferring data between two devices is known as a communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected.

**Simplex transmission**

In simplex transmission mode, the communication between sender and receiver occurs in only one direction. The sender can only send the data, and the receiver can only receive the data. The receiver cannot reply to the sender.

**Ex**:

* Simplex transmission can be thought of as a one-way road in which the traffic travels only in one direction—no vehicle coming from the opposite direction is allowed to drive through.
* To take a keyboard/monitor relationship as an example, the keyboard can only send the input to the monitor, and the monitor can only receive the input and display it on the screen. The monitor cannot reply, or send any feedback, to the keyboard.

**Half Duplex**

The communication between sender and receiver occurs in both directions in half-duplex transmission, but only one at a time. The sender and receiver can both send and receive the information, but only one is allowed to send at any given time. Half-duplex is still considered a one-way road, in which a vehicle travelling in the opposite direction of the traffic has to wait till the road is empty before it can pass through.

**Ex:**

For example, in walkie-talkies, the speakers at both ends can speak, but they have to speak one by one. They cannot speak simultaneously.

**Full Duplex**

In full-duplex transmission mode, the communication between sender and receiver can occur simultaneously. The sender and receiver can both transmit and receive at the same time. The full-duplex transmission mode is like a two-way road, in which traffic can flow in both directions at the same time.

**Ex:**

For example, in a telephone conversation, two people communicate, and both are free to speak and listen at the same time.

1. **What are the advantages of layered model of computer communication?**

The primary purpose of all models, and especially the OSI model, is to allow different vendors to interoperate. The benefits of the OSI and Cisco (Layered) models include, but are not limited to, the following:

• Dividing the complex network operation into more manageable layers

• Changing one layer without having to change all layers. This allows application

developers to specialize in design and development.

• Defining the standard interface for the “plug-and-play” multivendor integration

1. **Give ISO/OSI reference model for computer communication?**

The International Organization for Standardization (ISO) developed the OSI reference model. The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.

The OSI model is the primary architectural model for networks. It describes how data and network information are communicated from applications on one computer, through the network media, to an application on another computer. The OSI reference model breaks this approach into layers.

The OSI reference model has seven layers:

• The Application layer

• The Presentation layer

• The Session layer

• The Transport layer

• The Network layer

• The Data Link layer

• The Physical layer

**7. Application Layer**

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

**6. Presentation Layer**

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

**5. Session Layer**

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

**4. Transport Layer**

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

**3. Network Layer**

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

**2. Data Link Layer**

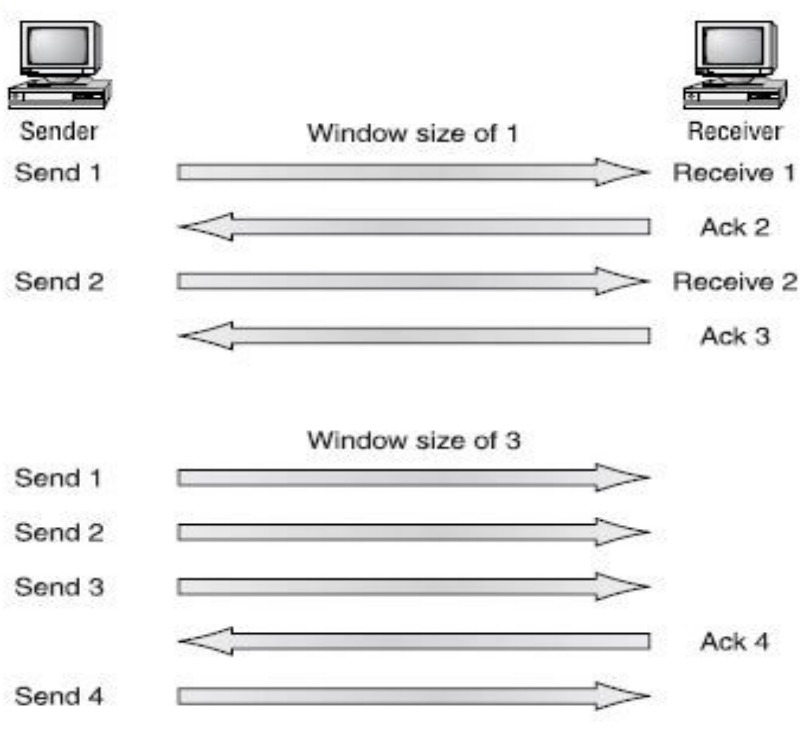
The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

**1. Physical Layer**

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

1. **Explain sliding window protocol for flow control between sending and receiving with a window size 3?**

Data throughput would be low if the transmitting machine had to wait for an acknowledgment after sending each segment. Because there’s time available after the sender transmits the data segment and before it finishes processing acknowledgments from the receiving machine, the sender uses the break to transmit more data. The quantity of data segments the transmitting machine is allowed to send without receiving an acknowledgment for them is called a window. Windowing controls how much information is transferred from one end to the other. While some protocols quantify information by observing the number of packets, TCP/IP measures it by counting the number of bytes.

****

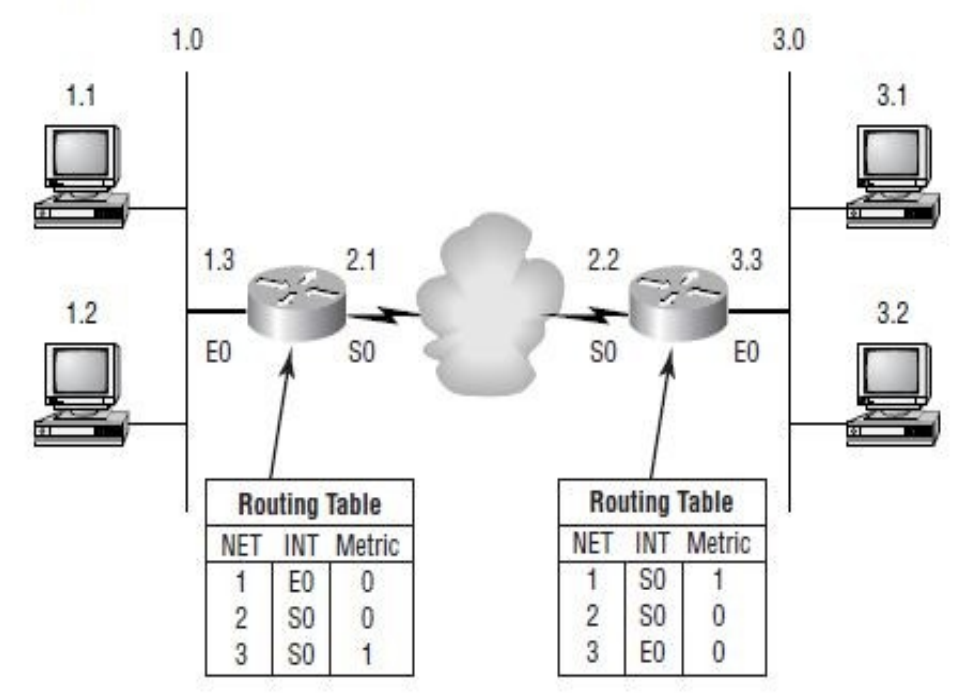
In the figure there is a window size of 1 and a window size of 3. When a window size of 1 is configured, the sending machine waits for an acknowledgment for each data segment it transmits before transmitting another.

Configured to a window size of 3, it’s allowed to transmit three data segments before an acknowledgment is received. In our simplified example, both the sending and receiving machines are workstations. Reality is rarely that simple, and most often acknowledgments and packets will commingle as they travel over the network and pass through routers.

1. **What is routing table? What is the content of routing table?**

When a packet is received on a router interface, the destination IP address is checked. If the packet is not destined for the router, then the router will look up the destination network address in the routing table.

Once an exit interface is chosen, the packet will be sent to the interface to be framed and sent out on the local network. If the entry for the destination network is not found in the routing table, the router drops the packet.

****

The routing table used in a router includes the following information:

**Network addresses (NET)**: Protocol-specific network addresses. A router must maintain a routing table for individual routing protocols because each routing protocol keeps track of a network with a different addressing scheme. Think of it as a street sign in each of the different languages spoken by the residents on a street.

**Interface (INT):** The exit interface a packet will take when destined for a specific network.

**Metric:** The distance to the remote network. Different routing protocols use different methods of computing this distance. Some routing protocols use hop count (the number of routers a packet passes through when routing to a remote network), while others use bandwidth, delay of the line, or even tick count (1/18 of a second).

1. **Give different Ethernet Implementations with its parameter?**

Ethernet was first implemented by a group called DIX. Ethernet use a registered jack (RJ) connector with a 4 5 wiring sequence on unshielded twisted pair (UTP) cabling (RJ-45).

Different Ethernet media requirements:

1. **10Base2:** 50-ohm coax, called thinnet. Up to 185 meters and 30 hosts per segment. Uses a physical and logical bus with AUI connectors.
2. **10Base5:** 50-ohm coax called thicknet. Up to 500 meters and 208 users per segment. Uses a physical and logical bus with AUI connectors. Up to 2500 meters with repeaters and 1024 users for all segments.
3. **10BaseT:** Using two-pair unshielded twisted-pair (UTP) wiring. One user per segment; up to 100 meters long. Uses an RJ-45 connector with a physical star topology and a logical bus
4. **100BaseTX:** EIA/TIA category 5, 6, or 7 UTP two-pair wiring. One user per segment; up to 100 meters long. Uses an RJ-45 MII connector with a physical star topology and a logical bus.
5. **100BaseFX:** Uses fiber cabling 62.5/125-micron multimode fiber. Pointto-point topology; up to 400 meters long. Uses an ST or SC connector, which are duplex media-interface connectors.
6. **1000BaseCX:** Copper shielded twisted-pair that can only run up to 25 meters.
7. **1000BaseT:** Category 5, four-pair UTP wiring up to 100 meters long.
8. **1000BaseSX:** MMF using 62.5 and 50-micron core; uses a 780-nanometer laser and can go up to 260 meters.
9. **1000BaseLX:** Single-mode fiber that uses a 9-micron core, 1300-nanometer laser and can go from 3 km up to 10 km.
10. **Explain the working of CSMA/CD?**

Ethernet networking uses what is called Carrier Sense Multiple Access with Collision Detect (CSMA/CD), which helps devices share the bandwidth evenly without having two devices transmit at the same time on the network medium.

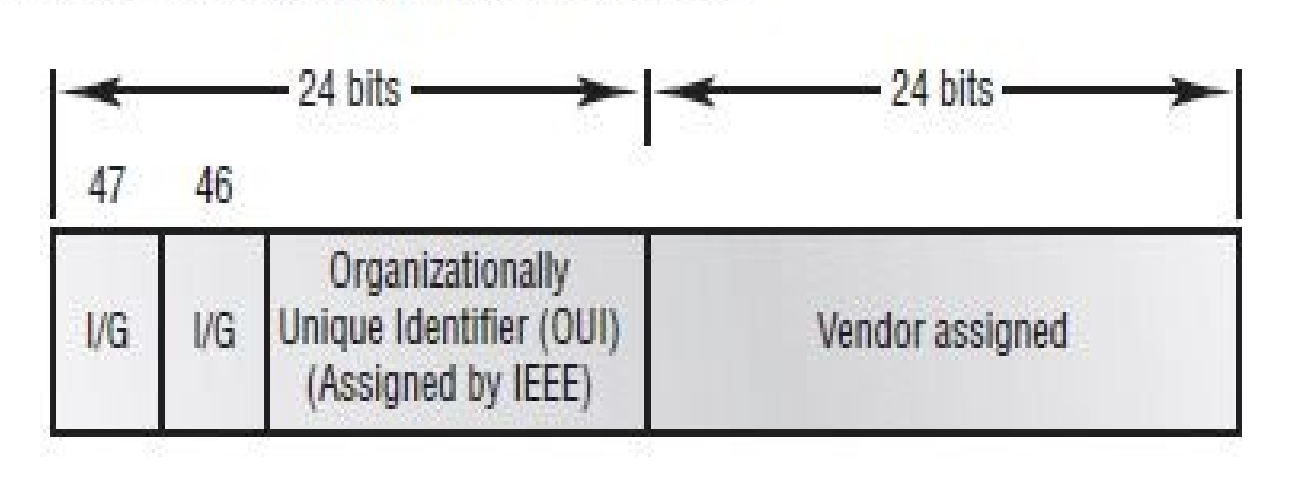
CSMA/CD was created to overcome the problem of collisions that occur when packets are transmitted simultaneously from different nodes. Good collision management is important, because when a node transmits in a CSMA/CD network, all the other nodes on the network receive and examine that transmission. Only bridges and routers effectively prevent a transmission from propagating through the entire network.

**The CSMA/CD protocol works like this:**

* When a host wants to transmit over the network, it first checks for the presence of a digital signal on the wire.
* If all is clear (no other host is transmitting), the host will then proceed with its transmission.
* And it doesn’t stop there. The transmitting host constantly monitors the wire to make sure no other hosts begin transmitting.
* If the host detects another signal on the wire, it sends out an extended jam signal that causes all nodes on the segment to stop sending data.
* The nodes respond to that jam signal by waiting a while before attempting to transmit again.
* Backoff algorithms determine when the colliding stations retransmit.
* If after 15 tries collisions keep occurring, the nodes attempting to transmit will then time-out.

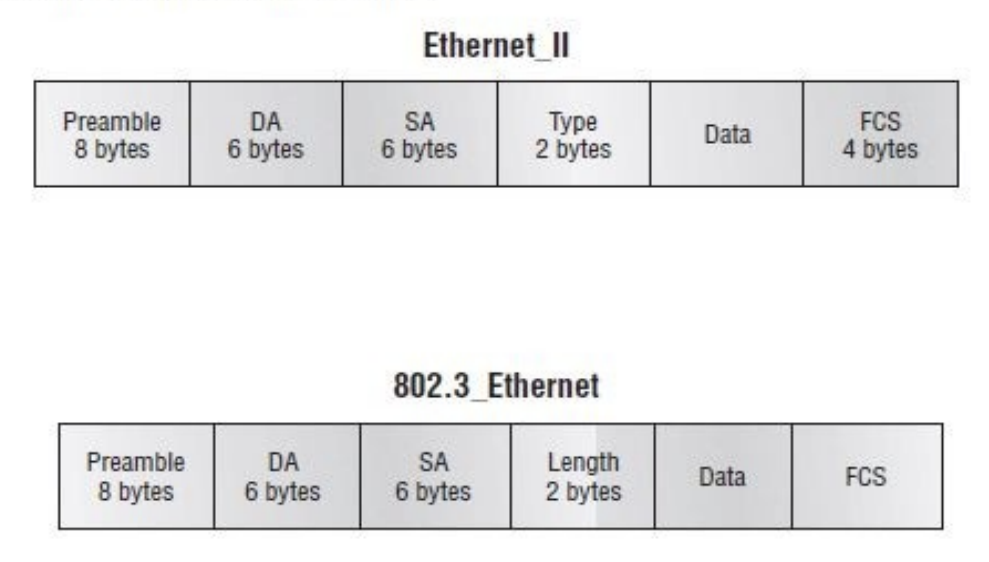
1. **Explain the Ethernet addressing with diagram.**

Ethernet addressing uses the Media Access Control (MAC) address burned into each and every Ethernet Network Interface Card (NIC). The MAC address, sometimes referred to as a hardware address, is a 48-bit address written in a canonical format to ensure that addresses are at least written in the same format, even if different LAN technologies are used. Figure 1.10 shows the 48-bit MAC addresses and how the bits are divided.

****

The Organizationally Unique Identifier (OUI) is assigned by the IEEE to an organization (24 bits or 3 bytes). The organization, in turn, assigns a globally administered address (24 bits or 3 bytes) that is unique (supposedly) to each and every adapter they manufacturer. Notice bit 46. Bit 46 must be 0 if it is a globally assigned bit from the manufacturer and 1 if it is locally administered from the network administrator.

1. **Explain structure of Ethernet frame format as per IEEE 802.3 standard.**



**Preamble**: An alternating 1,0 pattern provides a 5MHz clock at the start of each packet, which allows the receiving devices to lock the incoming bit stream. The preamble uses either an SFD or synch field to indicate to the receiving station that the data portion of the message will follow.

**Start Frame Delimiter (SFD)/Synch**: SFD is 1,0,1,0,1,0, etc., and the synch field is all 1s. The preamble and SFD/synch field are 64 bits long.

**Destination Address (DA):** This transmits a 48-bit value using the Least Significant Bit (LSB) first. DA is used by receiving stations to determine if an incoming packet is addressed to a particular node. The destination address can be an individual address, or a broadcast or multicast.

**Source Address (SA):** SA is a 48-bit MAC address supplied by the transmitting device. It uses the Least Significant Bit (LSB) first. Broadcast and multicast address formats are illegal within the SA field.

**Length or Type field:** 802.3 uses a length field, whereas the Ethernet frame uses a type field to identify the Network layer protocol. 802.3 cannot identify the upper-layer protocol and must be used with a proprietary LAN, for example, IPX.

**Data:** This is a packet sent down to the Data Link layer from the Network layer. The size can vary from 46–1500 bytes.

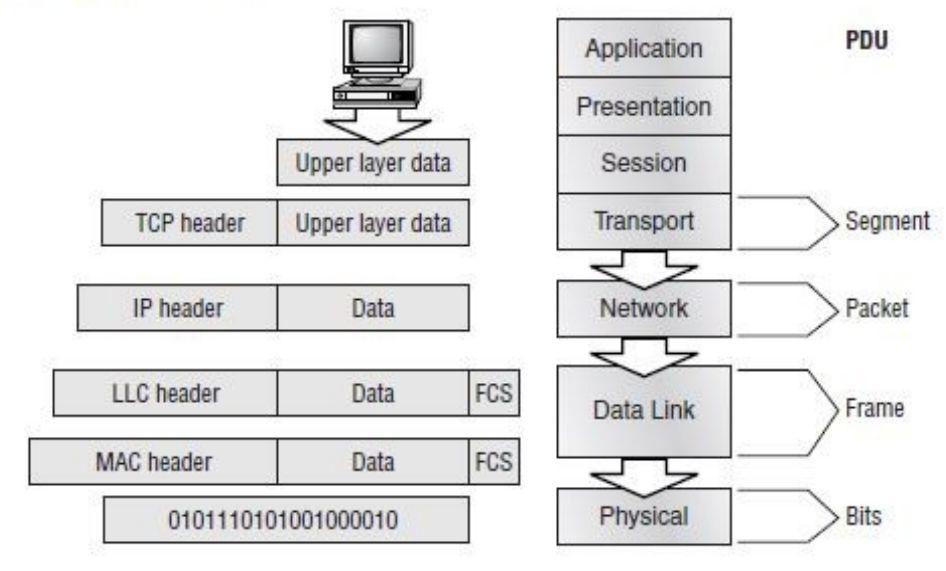
**Frame Check Sequence (FCS):** FCS is a field at the end of the frame that is used to store the cyclic redundancy check (CRC).

1. **What is data encapsulation? Explain with diagram?**

When a host transmits data across a network to another device, the data is encapsulated with protocol information at each layer of the OSI model. Each layer communicates only with its peer layer on the receiving device.

To communicate and exchange information, each layer uses what are called Protocol Data Units (PDUs). These hold the control information attached to the data at each layer of the model, which is typically attached to the header of the data field but can also be in the trailer, or end of the data field.

Each PDU is attached to the data by encapsulating it at each layer of the OSI model. Each PDU has a specific name depending on the information each header has. This PDU information is only read by the peer layer on the receiving device and then is stripped off and the data is handed to the next upper layer.

****

At a transmitting device, the data encapsulation method works as follows:

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

2. Data is converted to segments and a reliable connection is set up between the

transmitting and receiving hosts.

3. Segments are converted to packets or datagrams, and a logical address is placed in the

header so each packet can be routed through an inter- network.

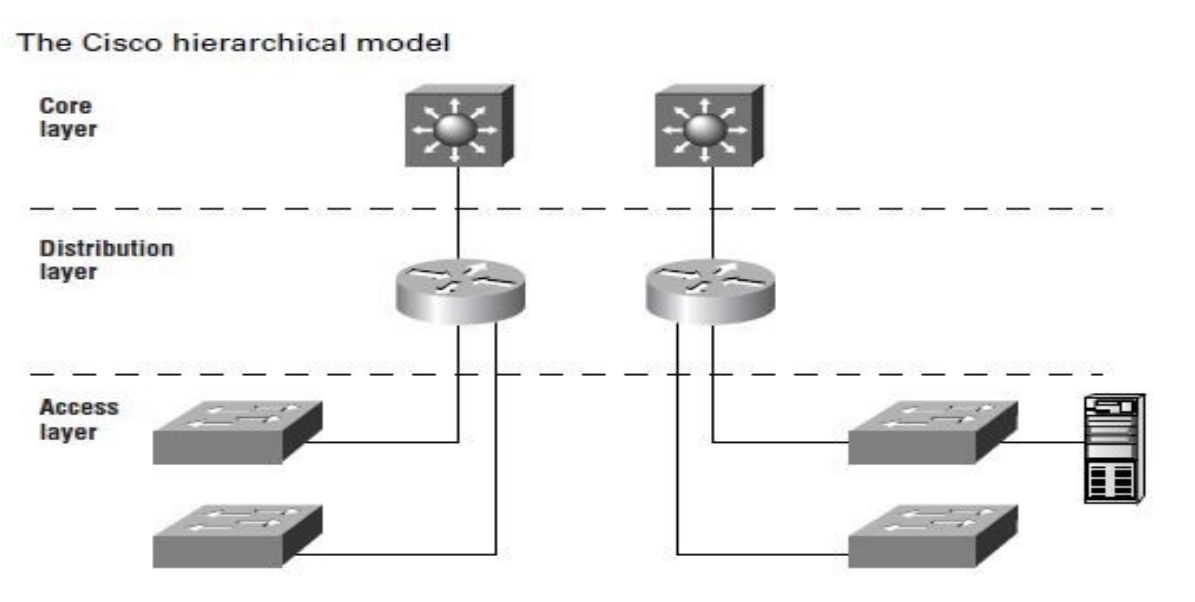
4. Packets or datagrams are converted to frames for transmission on the local network.

Hardware (Ethernet) addresses are used to uniquely identify hosts on a local network

segment.

5. Frames are converted to bits, and a digital encoding and clocking scheme is used.

1. **Explain CISCOs three-layer hierarchical model of networking.**

****

**Core Layer:**

At the top of the hierarchy, the core layer is responsible for transporting large amounts of traffic both reliably and quickly. The traffic transported across the core is common to a majority of users User data is processed at the distribution layer, and forwards the requests to the core only if needed. If there is a failure in the core, every single user can be affected The core is likely to see large volumes of traffic, so speed and latency are driving concerns here

**The Distribution Layer:**

The distribution layer is sometimes referred to as the workgroup layer and is the communication point between the access layer and the core. The primary function of the distribution layer is to provide routing, filtering, and WAN access Also to determine how packets can access the core, if needed. The distribution layer must determine the fastest way that network service requests are handled For example, how a file request is forwarded to a server. After the distribution layer determines the best path, it forwards the request to the core layer. The core layer then quickly transports the request to the correct service. The distribution layer is the place to implement policies for the network

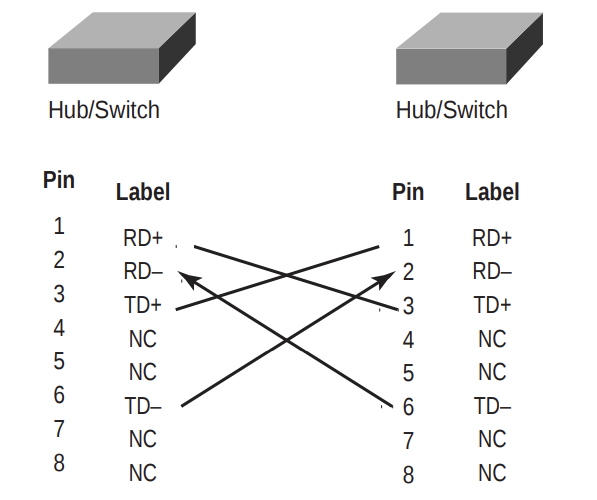
**The Access Layer:**

The access layer controls user and workgroup access to internetwork resources The network resources most users need will be available locally. The distribution layer handles any traffic for remote services.

1. **What is cross over cable? give the different use of cross over cables used?**

In the implementation of a crossover, the wires on each end of the cable are crossed. Transmit to Receive and Receive to Transmit on each side, for both tip and ring.

**UTP crossover implementation.**

****

Notice that pin 1 on one side connects to pin 3 on the other side, and pin 2 connects to pin 6 on the opposite end.

You can use a crossover cable for the following tasks:

• Connecting uplinks between switches

• Connecting hubs to switches

• Connecting a hub to another hub

• Connecting a router interface to another router interface

• Connecting two PCs together without a hub or switch

1. **Significance of roll over cables?**

All Cisco devices are shipped with console cables and connectors, which allow you to connect to a device and configure, verify, and monitor it. The cable used to connect between a PC is a rollover cable with RJ-45 connectors.

The pinouts for a rollover cable are as follows:

1–8

2–7

3–6

4–5

5–4

6–3

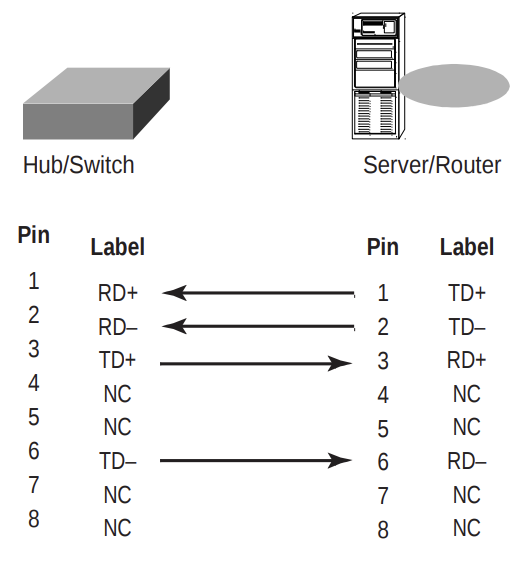
7–2

8–1

You can see that you just take a straight-through RJ-45 cable, cut the end off, flip it over, and reattach a new connector. Typically, you will use the DB9 connector to attach to your PC and use a com port to communicate via HyperTerminal. Most Cisco devices now sup- port RJ-45 console connections. However, the Catalyst 5000 series switch still uses a DB25 connector. Set up the terminal emulation program to run 9600bps, 8 data bits, no parity, 1 stop bit, and no flow control. On some routers, you need to verify that the terminal emulation program is emulating a VT100 dumb-terminal mode, not an auto-sense mode, or it won’t work. Most routers also have an aux port, which is an auxiliary port used to connect a modem. You can then dial this modem and connect the router to the aux port. This will give you console access to a remote router that might be down and that you cannot telnet into. The console port and aux port are considered out-of-band management since you are configuring the router “out of the network.” Telnet is considered in-band.

1. **Give the pin connection to create a straight through cable and also specify where cables are used?**In a UTP implementation of a straight-through cable, the wires on both cable ends are in the same order. Below figure shows the pinouts of the straight-through cable.

**UTP straight-through pinouts**

****

You can determine that the wiring is a straight-through cable by holding both ends of the UTP cable side by side and seeing that the order of the wires on both ends is identical.

You can use a straight-through cable for the following tasks:

• Connecting a router to a hub or switch

• Connecting a server to a hub or switch

• Connecting workstations to a hub or switch

**PART - II**

1. **What is IOS? Why IOS is used?**

The Cisco Internetwork Operating System (IOS) is the kernel of Cisco routers and most switches. The IOS was created to deliver network services and enable networked applications. The Cisco IOS runs on most Cisco routers and on some Cisco Catalyst switches, like the Catalyst 1900 switch.

The Cisco router IOS software is used to complete the following on Cisco hardware:

* Carry network protocols and functions.
* Connect high-speed traffic between devices.
* Add security to control access and stop unauthorized network use.
* Provide scalability for ease of network growth and redundancy.
* Supply network reliability for connecting to network resources.

You can access the Cisco IOS through the console port of a router, from a modem, or even through Telnet. Access to the IOS command line is called an EXEC session.

1. **What is the different alternative to have an access to Cisco device?**

You can connect to a Cisco router to configure the router, verify the configuration, and check statistics. There are different ways to connect to a Cisco router.

First way, you typically would connect to is the console port. The console port is usually a RJ-45 connection on the back of the router. This is used to connect to and configure the router. No password is set on the console port by default.

Another way to connect to a Cisco router is through an auxiliary port. This is really the same as a console port and can be used as such. However, it also allows you to configure modem commands to allow a modem connection to the router. This means you can dial up a remote router and attach to the auxiliary port if the router is down and you need to configure it.

The third way to connect to a Cisco router is through the program Telnet. Telnet is an emulation program that emulates a dumb-terminal. You can then use Telnet to connect to any active interface on a router like an Ethernet or serial port.

1. **Describe the procedure of bringing up or booting router?**

* When you first bring up a Cisco router, it will run a power-on self-test (POST)
* If that passes, it will look for and load the Cisco IOS from Flash memory if a file is present. Flash memory is an electronically erasable programmable read-only memory (EEPROM).
* The IOS will load and then look for a valid configuration called startup-config that is stored by default in non- volatile RAM (NVRAM).
* If there is no configuration in NVRAM, then the router will bring up what is called setup mode.

This is a step-by-step process to help you configure a router. You can also enter setup mode at any time from the command line by typing the command setup from global configuration mode. Setup only covers some very global commands, but is helpful if you don’t know how to con-figure certain protocols, like bridging or DEC net, for example.

1. **What are different working modes in Cisco router? Explain.**

To configure from a CLI, you can make global changes to the router by typing config terminal (config t for short), which puts you in global configuration mode and changes what is known as the running-config.

You can type config from the privileged mode prompt and then just press Return to take the default of terminal.

**Router#**config

Configuring from terminal, memory, or network [terminal]? return Enter configuration commands, one per line. End with CNTL/Z.

**Router(config)#**

To change the running-config, which is the current configuration running in Dynamic RAM (DRAM), you would use the command config terminal, or just config t. To change the configuration stored in NVRAM, which is known as startup-config, you would use the command config memory, or config mem for short. If you wanted to change a router configuration stored on a TFTP host you would use the command config network, or config net.

1. **What is the different interface available with a Cisco router?**

Cisco routers offer various interfaces to connect and interact with other devices and networks. Here are some of the most common interface types available in a Cisco router:

1. **Ethernet Interfaces:**

**Fast Ethernet (FE) and Gigabit Ethernet (GE):** These interfaces are used to connect routers to local area networks (LANs) and wide area networks (WANs) using Ethernet cables. Fast Ethernet offers speeds of 100 Mbps, while Gigabit Ethernet provides speeds of 1 Gbps.

1. **Serial Interfaces:**

**Serial WAN Interface Cards (WICs):** These interfaces are used for connecting to wide area networks (WANs) like T1, E1, T3, or E3 leased lines. They are commonly used for point-to-point connections between routers.

1. **Voice Interfaces:**

**Voice Interface Cards (VICs):** VICs are used to connect analog or digital voice devices, such as telephones or fax machines, to the router. These interfaces allow for voice-over-IP (VoIP) and other voice-related services.

1. **ISDN Interfaces:**

**Integrated Services Digital Network (ISDN) BRI and PRI Interfaces:** These interfaces are used to connect to ISDN networks and provide digital communication services, including voice, data, and video.

1. **Frame Relay Interfaces:**

**Frame Relay Interfaces:** Frame Relay interfaces are used to connect to Frame Relay networks, which are packet-switched networks commonly used for WAN connectivity.

1. **Console Interface:**

**Console Port:** The console interface is used for initial configuration and troubleshooting. Administrators can connect to the router directly through the console port using a terminal or console cable.

**7. Auxiliary Interface:**

**Auxiliary Port**: The auxiliary interface is used for out-of-band management and backup access. It allows administrators to connect modems or other devices for remote management and recovery purposes.

**8. USB Interfaces:**

**USB Ports:** Some modern Cisco routers may include USB ports for connecting USB storage devices or other peripherals. These can be used for various purposes, including software updates and data transfer.

**9. Wireless Interfaces:**

Wireless LAN Interfaces: In routers with integrated wireless capabilities, there are wireless interfaces for connecting to Wi-Fi networks. These interfaces are used for wireless LAN connectivity and can support various Wi-Fi standards like 802.11ac or 802.11ax.

**10.** **VPN Interfaces:**

**Virtual Private Network (VPN) Interfaces:** These interfaces are used for creating encrypted VPN tunnels, allowing secure communication between remote sites or users over untrusted networks.

1. **Give the procedure to apply user mode password as well as privilege mode password for Cisco router?**

**User mode passwords:** To configure user mode passwords, use the line command.

**Router#**config t

Enter configuration commands, one per line end with CNTL/Z.

**Router(config)#**line ?

<0-70> First Line number

Aux Auxiliary line

console Primary terminal line

Tty Terminal controller

Vty Virtual terminal

**Aux:** Is used to set the user-mode password for the auxiliary port. This is typically used for configuring a modem on the router but can be used as a console as well. To configure the auxiliary password, go to global configuration mode and type line aux ? .

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#line aux ?

<0-0> First Line number

Router(config)#line aux 0

Router(config-line)#login

Router(config-line)#password todd

**Privilege mode password:**

You can only view and change the configuration of a Cisco router in privileged mode, which you enter with the command enable.

Router>enable

Router#

You now end up with a Router#, which indicates you are in privileged mode. You can both view and change the configuration in privileged mode.

Router#config t

Router(config)#enable password cisco

To check if our password “cisco” works, get out of enable mode:

Router#disable

Router>enable

Password:

1. **Write a note on banners with available with Cisco IOS with example?**

You can set a banner on a Cisco router so that when either a user logs into the router or an administrator telnet into the router, for example, a banner will give them the information you want them to have. Another reason for having a banner is to add a security notice to users dialing into your internetwork. There are four different banners available:

**Router(config)#**banner ?

LINE c banner-text c, where 'c' is a delimiting character

exec Set EXEC process creation banner

incoming Set incoming terminal line banner

login Set login banner

motd Set Message of the Day banner

**Exec banner:** You can configure a line-activation (exec) banner to be dis-played

when an EXEC process (such as a line-activation or incoming connection to a

VTY line) is created.

**Incoming banner**: You can configure a banner to be displayed on terminals

connected to reverse Telnet lines. This banner is useful for providing instructions

to users who use reverse Telnet.

**Login banner:** You can configure a login banner to be displayed on all connected

terminals. This banner is displayed after the MOTD banner but before the login

prompts. The login banner cannot be disabled on a per-line basis. To globally

disable the login banner, you must delete the login banner with the no banner

login command.

**The Message of the Day:** It is the most used and gives a message to every person dialing in or connecting to the router via Telnet, auxiliary port, or console port.

**Router(config)#**banner motd ?

LINE c banner-text c, where 'c' is a delimiting character

**Router(config)#**banner motd #

Enter TEXT message. End with the character '#'.

1. **Give the procedure to assign an IP address for a specific interface?**

You don’t have to use IP on your routers; however, IP is typically used on all routers. To configure IP addresses on an interface, use the ip address command from interface configuration mode.

**Router(config)#**int e0

**Router(config-if)#**ip address 172.16.10.2 255.255.255.0

**Router(config-if)#**no shut

Turn on an interface with the no shut command.

Remember to look at the command show interface e0, for example, which will show you if it administratively shut down or not. Show running-config will also show you if the interface is shut down.

If you want to add a second subnet address to an interface, then you must

use the secondary command. If you type another IP address and press Enter. it

will replace the existing IP address and mask.

To add a secondary IP address, use the secondary command.

**Router(config-if)#**ip address 172.16.20.2 255.255.255.0 secondary

**Router(config-if)#**^Z

You can verify both addresses are configured on the interface with the

show running-config command (sh run for short).

**Router#**sh run

Building configuration...

Current configuration: [output cut]

!

interface Ethernet0

ip address 172.16.20.2 255.255.255.0 secondary ip address 172.16.10.2 255.255.255.0

!

1. **Give the procedure to configure a serial interface with the proper clock rate and bandwidth?**

To configure a serial interface, there are a couple of specifics that need to be discussed. Typically, the interface will be attached to a CSU/DSU type of device that provides clocking for the line. However, if you have a back-to-back configuration used in a lab environment, for example, one end must provide clocking.

This would be the DCE end of the cable. Cisco routers, by default, are all DTE devices, and you must tell an interface to provide clocking if it is to act as a DCE device. You configure a DCE serial interface with the clock rate command.

**Router#**config t

Enter configuration commands, one per line. End with CNTL/Z

**Router(config)#**int s0

**Router(config-if)#**clock rate ?

Speed (bits per second)

1200

2400

4800

9600

19200

38400

56000

64000

72000

125000

148000

250000

500000

800000

1000000

1300000

2000000

4000000

<300-4000000>

Choose clockrate from list above

**Router(config-if)#**clock rate 64000

%Error: This command applies only to DCE interfaces

**Router(config-if)#**int s1

**Router(config-if)#**clock rate 64000

It does not hurt anything to try and put a clock rate on an interface. Notice that the clock rate command is in bits per second. Every Cisco router ships with a default

serial link bandwidth of a T1, or 1.544Mbps. This has nothing to do with how data is transferred over a link. The bandwidth of a serial link is used by routing protocols such as IGRP, EIGRP, and OSPF to calculate the best cost to a remote network.

**Router(config-if)#**bandwidth ?

<1-10000000> Bandwidth in kilobits

**Router(config-if)#**bandwidth 64

Notice that unlike the clock rate command, the bandwidth command is c

configured in kilobits

1. **What is difference between start up configuration and running configuration and give the procedure?**

To configure from a CLI, you can make global changes to the router by typing config terminal (config t for short), which puts you in global configuration mode and changes what is known as the running-config.

You can type config from the privileged mode prompt and then just press Return to take the default of terminal.

**Router#**config

Configuring from terminal, memory, or network [terminal]? return Enter configuration commands, one per line. End with CNTL/Z.

**Router(config)#**

To change the running-config, which is the current configuration running in Dynamic RAM (DRAM), you would use the command config terminal, or just config t. To change the configuration stored in NVRAM, which is known as startup-config, you would use the command config memory, or config mem for short. If you wanted to change a router configuration stored on a TFTP host you would use the command config network, or config net.