**Networking Concepts**

1. Define a computer network. What are its main purposes?

Answer: A Computer Network is a system that connects two or more devices to enable them communicate and share resources. Its main purposes are communication (device to device), sharing resources (like servers) etc.

2. What is the difference between LAN, WAN, MAN, and PAN? Provide one example of each

Answer:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | LAN | WAN | MAN | PAN |
| Range | Small area like a home | Large areas like cities | Covers a City or large Campus | Very small area (10m) |
| Speed | High-Speed | Lower than LAN | Better than WAN | High-Speed |
| Cost | Low | Expensive | Lower than WAN | Low |

3. Explain client-server and peer-to-peer network models with examples

Answer: **Client-Server** model is when there is a dedicated device (server) to share the resources and files needed by the user. An example can be email providers, they give you every file and resource without needing the resources of your own personal device.

On the **Peer-to-Peer** model, there will be a collection of connected user-owned devices that facilitate the files and resources that are being shared. The best example I can think of for this is the Bit-torrent system.

4. What are the benefits of using a network in an organization?

Answer: Following from the definition of networks, the main purpose for using networks in an organization is to create communication and resource sharing among workers and departments. The benefit of this is that collaboration and information sharing can be very smooth and streamlined for the employees and they can also share resources like printers, servers (depends on the company) and others.

**Network Topologies**

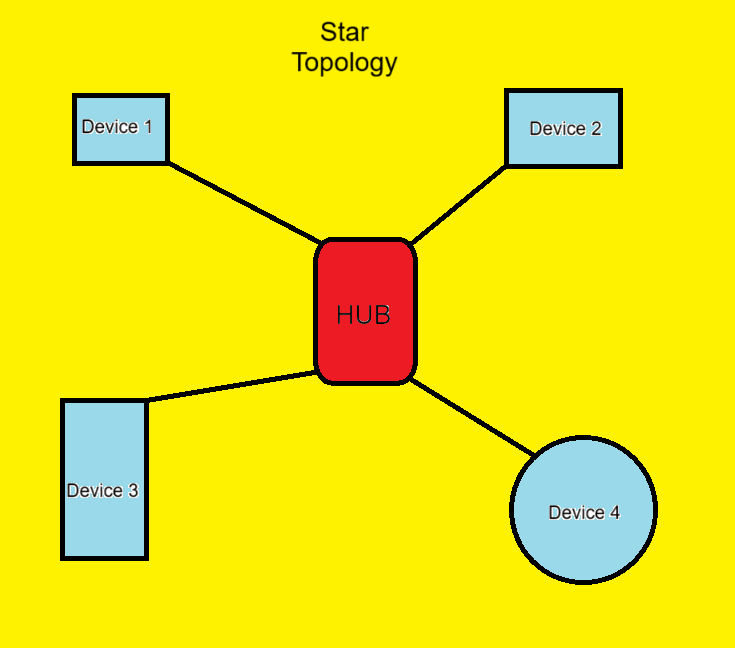
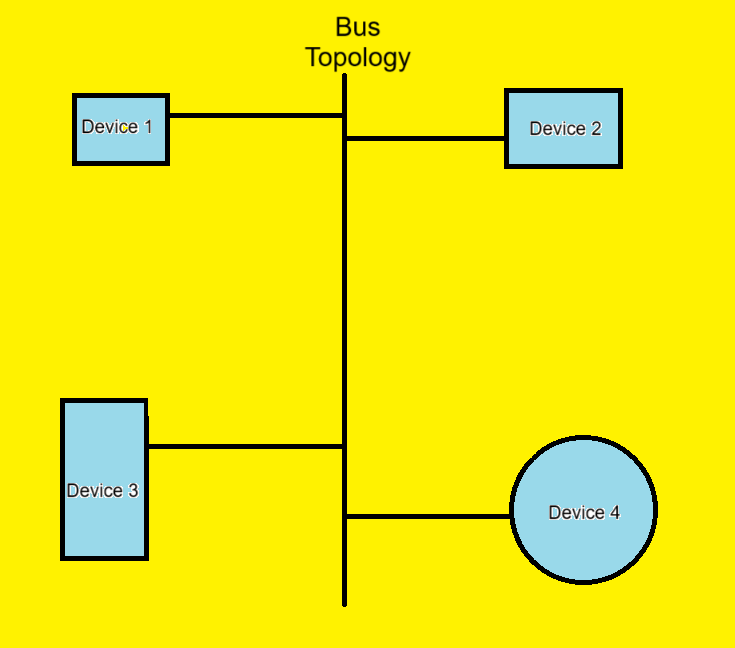
5. List and explain four common network topologies.

Answer:

* **Bus Topology**: When all the devices in a network connect to a central cable (the bus). The negative part is when the “Bus” gets damaged, you’ll lose all communication and network.
* **Star Topology**: Is created when all devices connect to one central hub or switch, all traffic goes through it. If the hub or switch gets damaged then you lose all the network abilities.
* **Ring Topology**: Devices in the network are connected in a circular loop (like seleme seleme but the front and end are connected too). The issue with this topology is when one cable connection or one device fails, then the whole system performs below the desired way.
* **Mesh Topology**: All the devices on the network are connected to each other. Which is complex and expensive to implement.

6. Draw a star and bus topology. Mention one advantage and one disadvantage of each.

Answer:



**Advantage**

* Cheap and easy to install for Bus and if one device fails (except the hub) the rest are still connected and it is also easy to manage for the Star.

**Disadvantage**

* If the Bus cable fails, then it all fails for bus and if the central hub fails, it all fails for Star.

7. Which topology is most commonly used in modern LANs? Why?

Answer: The most common for LAN is the Star topology. This is because LAN is usually used in houses and this houses connect to the internet using routers most of the time.

**Network Devices**

8. Define the function of the following devices:

Switch

Router

Hub

Access Point

Answer: **Switch** controls traffic and forwards it to the correct mac address.

**Router** is used to connect multiple networks together.

**Hub** is a device that connects multiple devices in a network and broadcast data to all of them.

**Access Point** is used to connect wireless devices to a network. It extends the wired network to the wireless devices.

9. What is the difference between a modem and a router?

Answer: A **router** connects multiple networks together while a **modem** translates the digital data from devices to analog that’s understood by the ISP.

10. Which OSI layers do a switch and router operate on?

Answer: **Switch** operates on the Data Link Layer while **Router** operates on the Network Layer.

**Communication Channels**

11. What are the types of transmission media in networking? Give examples.

Answer: The types of transmission media in networking are **Guided Transmission Media (Wired)** and **Unguided Transmission Media (Wireless)**. The twisted pair cable, coaxial cable etc… fall under the **Guided** media while radio waves, infrared etc… are examples of **Unguided**.

12. Compare STP and UTP cables.

Answer:

|  |  |  |
| --- | --- | --- |
|  | STP | UTP |
| Cost | High | Lower |
| Shielding | Yes | No |
| Susceptibility to Interference | Lower | Higher |

13. What are BNC and RJ45 connectors used for?

Answer: **BNC** connector is used to connect a coaxial cable with the intended device to provide a secure and reliable connection. **RJ45** is used to connect a twisted pair cable with the intended device for internet use in most cases.

14. Explain the difference between single-mode and multi-mode fiber optic cables.

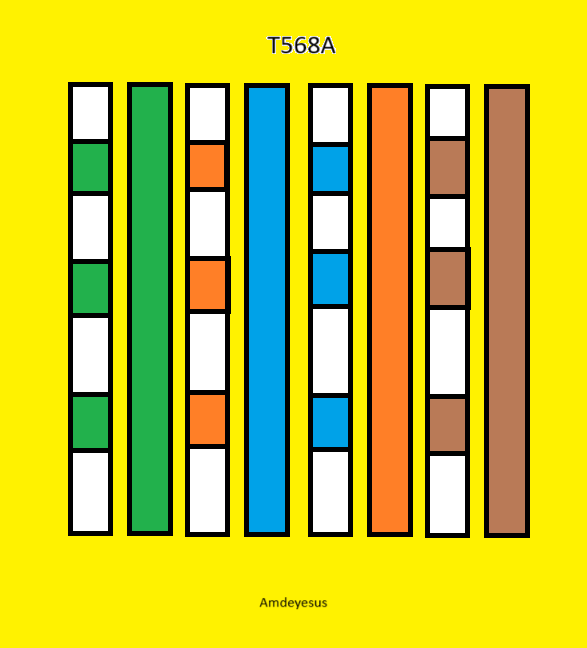
Answer: Single-Mode and Multimode are different in their core radius. Multimode has a large radius which allows multiple light modes to travel in it but after long distances, those rays start to degrade. And Single-Mode has a small radius which only allows a single light mode to pass in it which enables it to go very large distances without degradation and higher bandwidth but as mentioned it only transmits one mode of light.

15. What are the typical uses of coaxial cable in networking?

Answer: It is mostly used in cable TV and CCTV systems.

**Crimping and Cables**

16. List the color codes used in T568A and T568B Ethernet cable standards.

Answer: I have used Microsoft paint and drawn an image to show this.  

17. What is the purpose of crossover and straight-through cables? When are they used?

Answer: A **straight through** cable is usually used to connect two different types of devices in a network. It is used when we need a connection between different devices like a modem and a computer, connecting access points to switches etc.

A **Crossover** cable is usually used to connect two similar types of devices in a network. It is used when we need a connection between similar devices like two computers, although it is less common now.

18. Name three tools used to prepare and test Ethernet cables.

Answer: Crimping tool, scissors (or any sharp object to cut the cable), cable tracer.

**Communication Models**

19. Describe the three types of communication flows: Simplex, Half-Duplex, and Full Duplex.

Answer: **Simplex** is a type of communication flow where data only goes only one way, from the sender to the receiver.

**Half-Duplex** is a type of communication flow where data is transmitted in both directions but not at the same time, one has to finish receiving before sending.

**Full Duplex** is a type of communication flow where data is transmitted in both directions simultaneously.

20. What are the key components of a basic communication system?

Answer: The key components are the **Source** (**Sender**), **Message** (**Data**), **Medium**, **Protocol** (take customs law as an equivalent example), **Receiver** (As the name says)

21. Why are protocols important in communication?

Answer: Because they create order from the chaos. They remember the sender, know the receiver and protect the message while it goes through the medium in a basic explanation.

**OSI and TCP/IP Models**

22. List and explain the 7 layers of the OSI model.

Answer:

**Application Layer** – The top layer, providing network services directly to end-user applications. It's where user interaction with the network occurs.

**Presentation Layer** – Translates, encrypts/decrypts, and compresses/decompresses data. It ensures data is in a format that the receiving application can understand.

**Session Layer** – Establishes, manages, and terminates communication sessions between applications.

**Transport Layer** – Provides end-to-end communication between applications. It handles segmenting data, flow control etc.

**Network Layer** – Responsible for logical addressing (IP addresses) and routing data packets between different networks.

**Data Link Layer** – Provides reliable node-to-node data transfer. It handles physical addressing (MAC addresses), error detection etc.

**Physical Layer** – Deals with the physical transmission of raw bit streams over the network medium.

23. Match the following protocols to OSI layers: HTTP, IP, TCP, Ethernet, DNS, ARP

Answer:

HTTP – **Application** Layer

IP – **Network** Layer

TCP – **Transport** Layer

Ethernet – **Data Link** Layer

DNS – **Application** Layer

ARP – **Data Link** Layer

24. What is the function of the Transport layer? Name two protocols used there.

Answer: As I mentioned above (and assuming the question is about OSI), Transport Layer provides end-to-end communication between applications. It handles segmenting data, flow control and more. To mention, some of its protocols include TCP, UDP, etc.

25. Compare OSI and TCP/IP models. Mention one similarity and one difference.

Answer: Both OSI and TCP/IP are used to define layers of communication and their difference is in how many layers they have.

26. What are the layers of the TCP/IP model?

Answer: **Application Layer** (Layer 4), **Transport Layer** (Layer 3), **Internet Layer** (Layer 2), and **Network Access Layer** (Layer 1)

27. In which layer is IP addressing handled in OSI and TCP/IP models?

Answer: In OSI model IP addressing takes place in the **Network Layer** while on the TCP/IP model, it takes place in the **Internet Layer**.

**IP Addressing and Subnetting**

28. What is an IP address? Differentiate between IPv4 and IPv6.

Answer: An IP (Internet Protocol) address is an identification or label given to devices connected to a given network. IPv4 and IPv6 are both Internet Protocol versions but IPv6 is an improvement on the IPv4 because IPv4 was running out of addresses to assign to devices.

IPv4 uses 32 bit addressing while IPv6 uses 128 bit addressing, IPv4 uses decimal separated with dots while IPv6 uses hexadecimal separated by colons.

29. Convert 192.168.1.1 to binary.

Answer: 192 = **11000000**

168 = **10101000**

1 = **00000001**

1 = **00000001**

The address is **11000000.10101000.00000001.00000001**.

30. Convert 11000000.10101000.00000001.00000100 to decimal.

Answer: 11000000 = **192**

10101000 = **168**

00000001 = **1**

00000100 = **4**

The address is **192.168.1.4**.

31. Define the IP classes A, B, and C with their address ranges.

Answer: **Class A** is designed for very large networks and supports over 16 million hosts per network. It has a range 1.0.0.0 to 126.255.255.255 because all its first bits must be 0. Even though the range 0.0.0.0 to 0.255.255.255 and 127.0.0.0 to 127.255.255.255 may fall under this category, they are reserved for default/unknown network and localhost respectively.

**Class B** is used for medium-size networks and supports around 65,534 hosts per network. It has a range 128.0.0.0 to 191.255.255.255 because all its first bits must be 10.

**Class C** is used for small networks and supports up to 254 hosts per network. It has a range 192.0.0.0 to 223.255.255.255 because all its first bits must be 110.

32. What is the difference between static and dynamic IP addressing?

Answer: **Static** **IP** address never changes and is given to servers and other highly needed infrastructures while **Dynamic IP** address is an address given to ordinary devices like cell phones, computers etc… and they change regularly.

33. What is a private IP address? List the private IP ranges.

Answer: **Private IP** addresses are those given in a specific local network and aren’t accessible from the internet or across any network other than the one it is given in. I usually ranges from **192.168.0.0 – 192.168.255.255**, **10.0.0.0 – 10.255.255.255**, and **172.16.0.0 – 172.31.255.255**.

34. What is the loopback address and what is it used for?

Answer: It helps in testing before deployment. It is used by developers to see their work and progress, errors and results using loopback/localhost to fine tune their product.

35. How many hosts can a /24 subnet support?

Answer: It can support 232 – 24 = 28 = **256** hosts of which 256 – 2 = **254** are usable.

36. What is the subnet mask of /26? How many hosts does it support?

Answer: Since it borrows 2 bits from network, we make their bits’ 1 and get

**255.255.255.192** and it supports

32 – 26 = 6

26 = **64** hosts of which 64 – 2 = **62** are usable.

37. Calculate the network and broadcast address of 192.168.20.0/27.

Answer:

Network Address – **192.168.20.0**

Using the host bits 32 – 27 = 5

Setting all the host bits to 1 will give us

Broadcast Address – **192.168.20.31**

38. From a /24 network, how many subnets can you create by borrowing 3 bits?

Answer: Using the 2n formula

23 = **8**

We can create **8** subnets.

**MAC Address and ARP**

39. What is a MAC address and how is it different from an IP address?

Answer: A MAC address is an address given to a device by the manufacturer and is permanent. It is used to identify a specific device accurately. On the other hand, IP address is an address assigned by a router or other routing device when connecting to the internet and it may change every time.

40. What is ARP and what is its role in networking?

Answer: It is a protocol that helps in identifying the mac addresses of devices for accurate transfer of data. Its role in networking is enabling local communication and more.

**Protocols and Ports**

41. What does HTTP do? On which port does it operate?

Answer: HyperText Transfer Protocol is the set of rules that governs how browsers and servers communicate with each other to exchange information. It operates on the port 80.

42. What is DNS? What problem does it solve in networking?

Answer: A **Domain Name System** is a system that changes the human readable domain names into machine understandable IP address. It solves the problem of memorizing numbers whenever we want to visit any website.

43. Define DHCP. How does it help in IP configuration?

Answer: **DHCP** is a protocol used to assign IP addresses and other parameters to devices automatically. It helps in IP configuration by automatically finding unused and new IP to assign to the device and automates other processes regarding IP addresses that would otherwise be tedious and ineffective when done by humans.

44. List five common networking protocols and their functions.

Answer:

**HTTP (Hypertext Transfer Protocol)** – is the foundation of the World Wide Web and is used by browsers and servers to exchange web pages, images, and other web content.

**IP (Internet Protocol)** – is responsible for logical addressing (IP addresses) and routing data packets across different networks. It ensures data reaches its correct destination on the internet.

**TCP (Transmission Control Protocol)** – is used to provide reliable and efficient data transmission. It ensures data segments arrive in order, without errors, and are retransmitted if lost.

**UDP (User Datagram Protocol)** – is used to provide a fast, connectionless, and unreliable data transmission. It is commonly used for applications where speed is more critical.

**DNS (Domain Name System)** – is used to translate human-readable domain names into IP addresses that computers use to locate resources on a network.

**Switching and Routing**

45. What is the difference between switching and routing?

Answer: In addition to happening in different layers of the OSI model, they are different in other ways. Mainly switching occurs in the same network like a LAN while a router routes data to different parts of the world.

46. Define VLAN. What is its purpose in a network?

Answer: It is a logical segmentation on a normal LAN that acts like its own LAN. VLANs enable network administrators to group hosts together, even if they are not on the same physical switch, as if they are connected to the same network segment.

47. What is default gateway and why is it important?

Answer: It is the gateway used to technically connect to the internet or any other network outside the local network.

**Security Basics**

48. Name three common types of network threats.

Answer: The most common are malware/viruses, phishing and DoS/DDoS (my favorite) attacks.

49. What is a firewall? How does it protect a network?

Answer: It is a device or software that monitors and controls the data flow in a network. It protects the network by only allowing approved and legitimate softwares and/or users access to the internet and only allowing data to enter devices from trusted sources.

50. What is the role of antivirus software in networking?

Answer: The role of **antivirus** in networking is crucial. It is one of the systems that helps in preventing malware and other malicious data or files from entering a device.

**BONUS**

51. Explain what NAT (Network Address Translation) is and where it is commonly used

Answer: **NAT** is a method a router primarily uses to map IP addresses to devices. It works by taking the private IP and port of the sender and changes it to the router’s public IP address and gives it a new port that it records and sends the packet out to the internet.

It is commonly used in corporate, home, office and other networks.