ISHub AAU Summer Bootcamp Networking Track

Assignment 004 – Networking Basics Comprehensive Assessment Covers: Full Fundamentals of Networking–Concept, Devices, Models, Addressing, and More 📌Instructions: Answer all questions clearly and concisely. Show calculations where applicable (e.g., IP/Subnetting questions). You may illustrate your answers using diagrams or tables. This is an individual assignment. Submit by July 30. � � Networking Basics – Comprehensive Questions Networking Concepts

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

Answer: A computer network is a system that connects many independent computers to share information (data) and resources. Its main purpose is to enable communication and data exchange between different devices, allowing them to work together efficiently.

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

Answer: A. Local Area Network (LAN)
Size and Coverage: LANs are limited to a relatively small area, such as a single building, home, office, or school campus.
Speed and Cost: They offer high data transfer speeds and are cost-effective to set up and maintain.
Usage: Commonly used to connect computers, printers, and other devices within small spaces for sharing resources like files and internet access.
Example: A school using a LAN to connect all its computers and share a central server.

B. Wide Area Network (WAN)
Size and Coverage: WANs operate over large geographic areas, such as cities, countries, or even continents. The Internet is the most common example of a WAN.
Speed and Cost: These networks generally have slower data transfer speeds compared to LANs and are more expensive to implement and maintain.
Usage: Primarily used to connect multiple LANs and enable global communication.
Example: A multinational company connecting branch offices across different countries using a WAN.

C. Personal Area Network (PAN)

Size and Coverage: PANs cover a personal range, typically within a few meters of the user. They are designed for short-distance communication.

Speed and Cost: PANs are low-cost networks with moderate data speeds suitable for personal device connectivity.

Usage: Used to connect personal devices such as smartphones, tablets, laptops, and wearable technology. Bluetooth and USB connections are common forms of PAN.

Example: A person connecting their smartphone, smartwatch, and wireless headphones using Bluetooth.

D. Metropolitan Area Network (MAN)

Size and Coverage: MANs are larger than LANs but smaller than WANs, spanning a city or a large campus area. These networks link multiple LANs within the defined territory.

Speed and Cost: MANs offer faster speeds compared to WANs but are more complex and expensive than LANs.

Usage: Often used by governments, universities, and large organizations to connect resources across a city or metropolitan region.

Example: A university campus using a MAN to connect different departments spread across multiple buildings.

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

Answer: Client-Server Network Model: a central, powerful computer, known as a server, provides resources and services to other computers, called clients. Clients request services or data from the server, and the server responds by providing the requested information or performing the requested action.

Characteristics:

Centralized control and management of resources.

Servers are typically dedicated machines with robust hardware and software.

Clients depend on the server for most functionalities and data storage.

Easier to manage security, backups, and updates centrally.

Examples: World Wide Web: Web browsers (clients) request web pages and resources from web servers.

Email Systems: Email clients send and receive emails through mail servers.

Corporate Networks: Employees' computers (clients) access shared files, databases, and applications hosted on central servers.

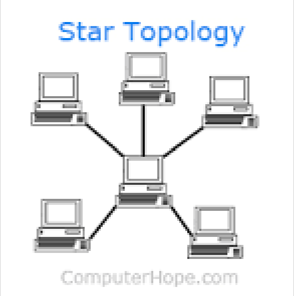
Peer-to-Peer (P2P) Network: In a P2P network, all connected computers, or peers, have equal capabilities and can act as both clients and servers. Each peer can directly share resources and services with other peers without requiring a central server.
Characteristics:
Decentralized control, with no single point of failure.
Each peer stores and manages its own files and resources.
Resource sharing occurs directly between peers.
Often simpler to set up for smaller networks.
Examples:
File Sharing Applications: Users directly share files with each other without a central server facilitating the transfer (e.g., BitTorrent).
Some Online Gaming: In certain games, players' computers directly connect to each other for gameplay, rather than relying on a central game server for all interactions.
Small Home or Office Networks: Computers within a small network might share printers or files directly with each other without a dedicated server.

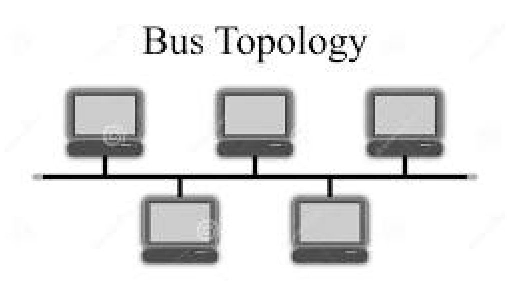
4. What are the benefits of using a network in an organization?

Answer: File sharing:- you can easily share data between different users, or access it remotely if you keep it on other connected devices.
Resource sharing:- using network-connected peripheral devices like printers, scanners, and copiers, or sharing software between multiple users, saves money.
Sharing a single internet connection:- It is cost-efficient and can help protect your systems if you properly secure the network.
Increasing storage capacity:- you can access files and multimedia, such as images and music, which you store remotely on other machines or network-attached storage devices.

Network Topologies
5. 6. 7. List and explain four common network topologies.
Network Devices
Draw a star and bus topology. Mention one advantage and one disadvantage of each.
Which topology is most commonly used in modern LANs? Why?

Answer:





A. Star Topology

Advantage: If one device or cable fails, it doesn't affect the rest of the network. Adding or removing devices is also easy.

Disadvantage: A failure of the central hub will cause the entire network to go down.

B. Bus Topology

Advantage: Simple to set up and requires fewer cables than a star topology.

Disadvantage: If the main cable fails, the entire network goes down. Performance degrades as more devices are added.

The most common topology used in modern LANs is the star topology. It offers better performance, easier management, and more scalability than other topologies like the bus topology.

8. Define the function of the following devices:

Switch

Router

Hub

Access Point.

Answer: Hub: Operates at the physical layer of the OSI model and simply repeats incoming data signals to all connected devices. It's not very efficient because every device receives all the traffic, even if it's not intended for them.

Switch: Operates at the data link layer and uses MAC addresses to identify devices and forward data only to the intended recipient. This significantly reduces network traffic and improves performance.

Router: Operates at the network layer and connects different networks together, like your home network to the internet. It uses IP addresses to determine the best path for data packets to travel and directs them accordingly.

Access Point: Acts as a bridge between a wired and a wireless network, allowing devices to connect to the wired network wirelessly. It essentially provides a wireless signal that devices can connect to using Wi-Fi.

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

Answer: A modem converts analog signals from the internet to digital signals for computers and vice versa, while a router enables multiple devices to share an internet connection.

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

Answer: A switch primarily operates at the Data Link layer (Layer 2) of the OSI model, while a router primarily operates at the Network layer (Layer 3).

Communication Channels

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

Answer: A. Guided (Wired) Media: use physical cables to transmit data.

I. Twisted Pair Cable: Consists of two insulated copper wires twisted together. Used in local area networks (LANs) for connecting computers to routers, and in telephone lines.

II. Coaxial Cable: Has a central conductor surrounded by an insulator, a shield, and an outer jacket. Used in cable TV and some internet connections (like cable internet).

III. Fiber Optic Cable: Uses light signals transmitted through thin glass or plastic fibers. Known for high speed and bandwidth, often used for high-speed internet (fiber optic internet) and long-distance communication.

B. Unguided (Wireless) Media: transmit data through the air or space.

I. Radio Waves: Used in Wi-Fi networks, Bluetooth, and cellular communication.

II. Microwaves: Used for satellite communication and some point-to-point wireless connections.

III. Infrared: Used for short-range communication like remote controls and some wireless connections.

12. Compare STP and UTP cables.

Answer: The primary difference is that UTP requires far less maintenance and comes at a lower cost, making it the ideal choice for smaller businesses.

Unshielded Twisted Pair (UTP) cables are unshielded, and their frequency range makes them suitable for transmitting data and voice. Mainly used in telecommunications and IT departments.. Physically, UTP cables are insulated copper wires twisted together with no shielding, such as aluminum foil.

Shielded Twisted Pair (STP) cabling are the same twisted copper wires, but they're protected by either a copper braid jacket or extra wrapping foil. STP cables are more adept at blocking interference and preventing physical damage that leads to bandwidth loss. Since STP cables are a superior product, they cost more to run and require more maintenance to keep them in prime condition.

13. What are BNC and RJ45 connectors used for?

Answer: BNC connectors are often found in video and radio frequency applications like CCTV, broadcast video, and test equipment. RJ45 connectors are primarily used for Ethernet connections in computer networking, connecting devices like computers, routers, and switches.

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

Answer: Bandwidth: Single-mode fibers have a higher bandwidth capability than multimode fibers due to no modal dispersion effects, which means that they can transmit larger amounts of data over greater distances. Their small core size prevents multiple modes of propagation, thus permitting higher volumes of data to be dispersed without interruption.

Distance: Single-mode fibers are better suited for long-distance applications due to their high bandwidth capability. Since multimode fibers have a larger core size, the modal dispersion, or the overlapping of pulses, increases over larger distances; thus, positioning this type of fiber to be the best choice for shorter-distance applications.

Attenuation: Multimode fibers tend to have higher attenuation than single-mode fibers since the intrinsic loss of the multimode fiber is higher due to the natural loss of the fiber in the operating wavelengths of 850 nm and 1300 nm.

Cost: Since multimode fiber has shorter runs with more setup time, it tends to be the more expensive option, unlike single-mode fibers, which have higher volumes and more continuous, efficient runs. However, single-mode fibers require more expensive active equipment, such as electronics and laser transmitters, to hit the small core target of 8.3 µm. Multimode fibers utilize cheaper electronics, thus leading to lower overall system costs.

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

Answer: connecting cable television and internet service providers (ISPs) to homes and businesses, transmitting video signals in security systems, and some legacy local area networks (LANs).

Crimping and Cables

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

Answer: The T568A and T568B Ethernet cable standards both use eight wires with four pairs, but the order of the green and orange pairs is swapped between them.

A. T568A

Pin 1: Green/White
Pin 2: Green
Pin 3: Orange/White
Pin 4: Blue
Pin 5: Blue/White
Pin 6: Orange
Pin 7: Brown/White
Pin 8: Brown

B. T568B

Pin 1: Orange/White
Pin 2: Orange
Pin 3: Green/White
Pin 4: Blue
Pin 5: Blue/White
Pin 6: Green
Pin 7: Brown/White
Pin 8: Brown

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

Answer: A. Crossover Cables: Connects similar network devices directly, such as computer to computer, switch to switch, or router to router. It is used when connecting two devices of the same type (e.g., two computers) directly.

B. Straight-through cables: Connects devices of different types within a network, like a computer to a switch or a router to a switch. It is used to connect a computer to a switch, a router to a switch, or a computer to a router.

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

Answer: A. Wire Stripper: used to remove the outer plastic jacket of the Ethernet cable, exposing the internal twisted pairs of wires. It helps prevent damage to the conductors during the stripping process.
B. Crimping Tool: essential for attaching the RJ45 connectors to the ends of the Ethernet cable. It securely crimps the connector onto the cable, ensuring a reliable connection between the wires and the connector pins.
C. Cable Tester: verifies the connectivity and wiring of the Ethernet cable. It checks for proper pin-to-pin connections and can identify issues like shorts, opens, or miswires.

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

Answer: A.Simplex: The communication is unidirectional. Only one of the two devices on a link can transmit; the other can only receive.
e.g, keyboard sending data to a computer
B. Half-duplex: Only one of the two devices on a link can transmit; the other can only receive.
e.g, Walkie-talkie
C. Full-duplex: In full-duplex mode, both devices can transmit and receive.
e.g, telephone

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

Answer: A. Sender: The origin of the message or information to be communicated. This could be a person speaking, a computer generating data, or any entity producing information.
B. Receiver: This component receives the signal from the channel and decodes it to recover the original message. It reverses the process done by the transmitter.
C. Message: The information that the sender wants to send to the receiver..

D. Channel: The physical medium through which the signal travels from the transmitter to the receiver. This could be a wire, a radio wave, or even free space.
E. Protocol: A set of rules and standards that govern how communication occurs, ensuring clarity and proper interpretation of the message.

21. Why are protocols important in communication?

Answer: They provide a standardized set of rules and conventions that ensure devices and systems can understand each other and exchange information reliably. Without protocols, communication would be chaotic and inefficient, akin to trying to understand a conversation where everyone speaks a different language or uses different rules.

OSI and TCP/IP Models
22. List and explain the 7 layers of the OSI model.

Answer: 1. Physical Layer: handles the transmission of raw bitstream over the physical medium (cables, wireless signals, etc.). It defines the physical characteristics of the network, like voltage levels, data rates, and physical topologies.
2. Data Link Layer: focuses on node-to-node communication within a local network. It provides reliable data transfer between two directly connected nodes by framing data, performing error detection, and managing access to the physical medium (e.g., using MAC addresses).
3. Network Layer: responsible for logical addressing and routing of data packets across networks. It determines the best path for data to travel from source to destination, often using IP addresses.
4. Transport Layer: ensures reliable end-to-end data delivery. It handles segmentation of data, flow control, and error control (e.g., using TCP or UDP protocols).
5. Session Layer: manages connections between applications, establishing, maintaining, and terminating sessions. It also handles synchronization and checkpointing of data transfer.
6. Presentation Layer: handles data formatting, encryption, and compression. It ensures that the data is in a usable format for the application layer and can translate between different data formats (e.g., ASCII, EBCDIC).
7. Application Layer: closest to the user and provides the interface for applications to access network services (e.g., email clients, web browsers).

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

Answer: HTTP and DNS- application layer(Layer 7)
IP- network layer (Layer 3)
TCP- transport layer (Layer 4)
Ethernet operates- both the data link layer and the physical layer (Layers 2 and 1)
ARP- the network layer (Layer 3).

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

Answer: The Transport layer is responsible for providing end-to-end communication between applications on different hosts. It manages data transfer, error recovery, and flow control. Two key protocols used in the Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

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

Answer: Similarity: both models use a layered approach to network communication and divide the process into distinct functions.
Difference: the OSI model has seven layers, while the TCP/IP model has four.

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

Answer: 1. Network Access Layer: responsible for the physical transmission of data, including how bits are sent over the network medium (like Ethernet cables or Wi-Fi). It defines the physical and data link aspects of communication.
2. Internet Layer: handles addressing and routing of data packets, ensuring they reach the correct destination network. The Internet Protocol (IP) is the key protocol used here, providing unique IP addresses to devices.
3. Transport Layer: establishes connections between applications on different hosts. It provides reliable or unreliable data transfer using protocols like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP provides ordered, reliable delivery with error checking, while UDP offers faster, less reliable transmission.
4. Application Layer: provides network services to applications. It includes protocols like HTTP (for web browsing), FTP (for file transfer), and SMTP (for email). This layer interacts directly with the user's applications.

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

Answer: In both the OSI and TCP/IP models, IP addressing is handled at the Network Layer.

IP Addressing and Subnetting

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

Answer: An IP address is a unique numerical identifier assigned to every device connected to a network.

I. Address Length

IPv4: 32 bits

IPv6: 128 bits

II. Notation Format

IPv4: Dotted decimal (e.g., 192.0.2.1)

IPv6: Hexadecimal with colons (e.g., 2001:db8::1)

III. Number of Available Addresses

IPv4: 4.3 billion (2^{32})

IPv6: 340 undecillion (2^{128})

29. Convert 192.168.1.1 to binary.

Answer: 192-> 11000000

168 -> 10101000

1 -> 00000001

1 -> 00000001

The binary representation is 11000000.10101000.00000001.00000001.

30. Convert 11000000.10101000.00000001.00000100 to decimal.

Answer: 11000000 = 128+64=192

10101000 = 128+32+8=168

00000001 = 1

00000100 = 4

Decimal representation: 192.168.1.4

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

Answer:Class A: 1.0.0.0 to 126.255.255.255 (for large networks)
Class B: 128.0.0.0 to 191.255.255.255 (for medium-sized networks)
Class C: 192.0.0.0 to 223.255.255.255 (for smaller networks)

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

Answer: Static IPs are manually configured, making them suitable for servers and devices requiring consistent network identification, while dynamic IPs are automatically assigned by a DHCP server and are common for general internet use.

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

Answer: A private IP address is a non-routable IP address used within a local network, such as a home or office network, for internal communication and is not directly accessible from the public internet.
10.0.0.0/8: This range includes addresses from 10.0.0.0 to 10.255.255.255.
172.16.0.0/12: This range includes addresses from 172.16.0.0 to 172.31.255.255.
192.168.0.0/16: This range includes addresses from 192.168.0.0 to 192.168.255.255.

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

Answer: he loopback address is a special IP address used to test network functionality and internal communication within a single machine. It’s used for:

Testing Network Stack: You can ping `127.0.0.1` to ensure that the device's networking software and hardware are functioning properly.

Local Services: Developers often bind services (like web servers or databases) to `127.0.0.1` so they are only accessible locally.

Security Purposes: Restricting access to loopback ensures a service won’t be exposed to external traffic unintentionally.

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

Answer: 32-24 = 8 bits = 2^8= 256 addresses.
But 2 of those addresses are reserved for network and broadcast address.
So, 256 - 2 = **254 usable host addresses**

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

Answer: A subnet mask of /26 has a corresponding subnet mask of 255.255.255.192. It supports 62 usable hosts per subnet.

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

Answer: 32 - 27= 5 bits are for hosts.
That gives 2^5 = 32 total IP addresses.
The range starts at 192.168.20.0 and spans 32 addresses, ending at 192.168.20.31.

Network Address: the first IP in the range(192.168.20.0)
Broadcast address: the last IP in the range(192.168.20.31)

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

Answer: Borrowing 3 bits from the host portion increases the network portion to 27 bits.
32 - 27 = 5 bits. Each bit can be either 0 or 1, so with 3 bits, you have 2 * 2 * 2 = 8 possible combinations.

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

Answer: A MAC address is a unique hardware identifier assigned to a network interface card (NIC) and is used for communication within a local network.

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

Answer: ARP is a communication protocol that resolves IP addresses to their corresponding MAC addresses within a local network. Devices must be located on the same network segment for data transmission.
ARP enables devices to find the physical, or MAC, address of another device on the same network when they only know the device's IP address.

Protocols and Ports

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

Answer: HTTP is a protocol used for transmitting hypertext, which is used mainly for web browsing. It operates on port 80 as its default port.

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

Answer: DNS translates human-readable domain names (like www.google.com) into machine-readable IP addresses (like 192.0.2.1) that computers use to communicate with each other. It solves the problem of needing to memorize long, complex IP addresses to access websites. Instead of remembering "172.217.160.142", you can simply type "google.com" into your browser.

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

Answer: DHCP is a network protocol used to automatically assign IP addresses and other critical configuration details to devices on a network. Its useful of :

Automation: No need to assign IPs manually, especially vital in large networks.
Avoids Conflicts: DHCP tracks who has what, preventing duplicate IPs.
Scalability: New devices can join the network seamlessly.
Flexibility: Devices can move between networks and get fresh configurations.

44. List five common networking protocols and their functions. Switching and Routing

Answer: 1. TCP/IP: This is the fundamental protocol suite for the internet. TCP ensures reliable, ordered, and error-checked delivery of data packets, while IP handles routing and addressing of packets across the network.
2. DNS: translates human-readable domain names (like "example.com") into the numerical IP addresses that computers use to locate resources on the network. This allows users to access websites using easily remembered names instead of complex IP addresses.
3. HTTP: foundation of data communication for the World Wide Web. It defines how messages are formatted and transmitted, and how web servers and browsers respond to commands.

4. DHCP: automates the process of assigning IP addresses to devices on a network. It eliminates the need for manual configuration, reducing the risk of errors and simplifying network management.
5. FTP: enables the transfer of files between computers. It allows users to upload, download, and manage files on remote servers.

45. What is the difference between switching and routing?

Answer: A. Switching
Layer: Data Link Layer (Layer 2) of the OSI model.
Function: Forwards data frames (Ethernet frames) based on MAC addresses.
Purpose: Connects devices within the same local network (LAN).
Example: A switch in your home connecting your computer, printer, and other devices.
Key Feature: Creates a single broadcast domain.
B. Routing
Layer: Network Layer (Layer 3) of the OSI model.
Function: Forwards data packets based on IP addresses.
Purpose: Connects different networks (LANs, WANs, etc.).
Example: A router connecting your home network to the internet.
Key Feature: Creates multiple broadcast domains (usually one per port).

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

Answer: VLAN is a logical segmentation of a physical network. It allows administrators to create separate broadcast domains and manage network traffic more efficiently. VLANs are used to improve network security, simplify network management, and optimize traffic flow. Its purposes:

Segmentation: Devices in the same VLAN can communicate directly, while those in different VLANs need routing. This enforces boundaries.
Security: You can isolate sensitive systems (like finance or HR) from public traffic or guest users.
Performance: Limits broadcast domains, reducing unnecessary traffic and improving efficiency.
Flexibility: VLANs aren’t tied to physical locations. Devices across different buildings can still be in the same VLAN.
Simplified Management: Makes it easier to control and monitor groups of users or services.

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

Answer: The Default Gateway is the IP Address of a device (router) on a network through which a SUBNET will communicate with other devices across the network.
A default gateway is a network node (usually a router) that serves as the access point to external networks when a device doesn't know where to send data. And this is why it's important:-
Enables External Communication: Devices rely on the gateway to reach the internet or other remote networks.
Manages Routing: It knows how to forward traffic intelligently based on destination IP addresses.
Network Isolation and Security: Controls what goes in and out of the local network—often filters or logs traffic.
Fallback Path: If no specific route matches a packet's destination, the default gateway is the last resort.

Security Basics
48. Name three common types of network threats.

Answer: malware, phishing, and Distributed Denial of Service (DDoS) attacks

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

Answer: A firewall is a cybersecurity solution that protects your computer or network from unwanted traffic coming in or going out. It inspects and authenticates all data packets in network traffic before they are allowed to move to a more secure environment. It protect a network by:
Traffic Filtering: Blocks suspicious or unauthorized data packets based on IP, port, protocol, or content.
Access Control: Prevents users or apps from reaching restricted parts of the network.
Preventing Malware Spread: Stops infected traffic from spreading across devices.
Logging and Alerts: Records activity for audits and sends alerts on unusual behavior.
Intrusion Prevention (with advanced firewalls): Detects and halts potential attacks in real time.

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

Answer: It acts as a security layer, scanning files, emails, and network traffic to detect and neutralize threats before they can cause damage or compromise the system.

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

Answer: Network Address Translation (NAT) is a method that allows multiple devices on a private network to share a single public IP address when communicating with the internet. It essentially acts as a translator, modifying the IP addresses in network packets as they pass through a router or gateway. This technique is widely used to conserve public IPv4 addresses and enhance network security.