Answers

1) i) Physical Layer (Layer 1) → Responsible for the physical connection between devices, it transmits raw bit streams over a physical medium.

ii) Data Link Layer (Layer 2) → Provides node-to-node data transfer and handles error ~~from~~ correction from the physical layer.

iii) Network Layer (Layer 3) → Determines how data is forwarded to its destination by identifying the best path across the network.

iv) Transport Layer (Layer 4) → Ensures reliable data transfer between systems, handling data segmentation and reassembly.

v) Session Layer (Layer 5) → Manages sessions or connections between applications, ensuring they remain open and operational during communication.

vi) Presentation Layer (Layer 6) → Transforms data into that the application layer or end-user applications can understand.

vii) Application Layer (Layer 7) → The layer closest to the end user, it provides network services directly to applications.

2) Similarities →

i) Layered Approach → Both divide network functions into layers, making networking easier to understand and troubleshoot.

ii) End to End Communication → Both support data transfer across networks.

iii) Standardisation → Ensure interoperability between devices from different manufactures.

Differences →

i) Layers → OSI has 7 layer, while TCP/IP has 4.

ii) Function Distribution → OSI separates functions, while TCP/IP combines them, especially in its ~~layer~~ application layer.

iii) Usage → OSI is theoretical; TCP/IP is practical and widely used, forming the basis of the internet.

iv) Protocols → OSI is a reference model; TCP/IP includes specific protocols like TCP, IP, HTTP.

Name:_____ Regd No.:_____

3) Data Encryption secures data by converting it into an unreadable format, only accessible to those with the decryption key. In the OSI model, encryption typically occurs at the Presentation Layer (Layer 6), though it can also happen at other layers, like the Application layer (e.g., HTTPs) or Network layer (e.g. IPsec).

4) a) Star Topology →

Advantages →

i) Easy to set up & manage.

ii) Fault isolation is straightforward; if one device fails, others are unaffected.

iii) Scalable; adding or removing devices is simple.

Disadvantages →

i) High dependency on the central hub or switch; if it fails, the entire network goes down.

ii) Can be costly due to cabling and the central device.

Ideal ~~Be~~ Use Case → Common in home and office networks where centralized management is useful and reliability is essential.

b) Bus Topology →

Advantages →

i) Simple and inexpensive to set up.

ii) Uses less cabling compared to other topologies.

Disadvantages →

i) Network performance decreases as more devices are added.

ii) If the main cable fails, the entire network is disrupted.

Ideal Use Case → Small networks or temporary setups, where low cost and simplicity are prioritized over scalability and reliability.

c) Ring Topology →

Advantages →

i) Predictable network performance as data travels in a single direction.

ii) Reduced chance of data collisions.

Disadvantages →

i) A failure in any one node or connection can bring down the entire network unless a dual-ring is used.

ii) Difficult to scale as each new connection impacts the whole ring.

Ideal Use Case → Used in simple or smaller networks with a predictable, one directional data flow, like a factory setup.

d) Mesh Topology →

Advantage →

i) High redundancy and reliability; multiple paths for data prevent a single point of failure.

ii) Excellent for high traffic as nodes can direct data through multiple paths.

Disadvantage →

i) Expensive and complex to set up due to extensive cabling and configuration.

ii) Difficult to maintain and manage.

Ideal Use Case → Used in mission-critical networks where uptime is paramount & redundancy is crucial.

5)

Topology	Number of links
Mesh	$\frac{n(n-1)}{2}$
Ring	n
Bus	1
Star	n

Name:_____ Regd No.:_____

6) Fiber optic cables have key advantages over copper:

i) Higher Bandwidth and Speed: Fiber supports faster, higher-capacity data transfer

ii) Longer Distance: Can transmit data farther without signal loss.

iii) Less Interference: Immune to electromagnetic and radio interference.

iv) Better Security: Harder to tap without detection.

v) Smaller and Lighter: Easier to install and route.

vi) Greater Durability: More resistant to environmental factors.

7) Private IP Address →

i) Definition → A private IP address is assigned to devices within a local network and is not accessible directly over the internet.

ii) Purpose → ~~Use~~ Used for internal communication within the network, allowing devices to connect and share resources without being visible to the wider internet.

iii) Address Ranges → Typical private IP ranges include 10.0.0.0 to .10.255.255.255, 172.16.0.0 to 172.31.255.255 and 192.168.0.0 to 192.168.255.255.

Public IP Address →

i) Definition → A public IP address is globally unique and assigned by an ISP for communication on the internet.

ii) Purpose → It allows devices on networks to communicate with other networks and devices globally, acting as the "address" for each device on the internet.

iii) Accessability → Public IPs are visible and accessible from anywhere on the internet.

Why Use Private IPs?

Private IPs conserve are the limited pool of the public IP addresses and add security by keeping internal devices isolated from directly internet access. Devices with private IPs connect to the internet through a Network Address Translation (NAT) process, which uses a single public IP address to communicate externally, hiding individual device IPs within a network.

8) How NAT Works →

i) When a device with a private IP sends a data to the internet, the NAT-enabled router replaces the private IP address with the router's public IP address.

ii) The router also records information about each outgoing request, so it can route the response back to the correct private IP.

iii) When the response comes back, NAT translates the public IP back to the device's private IP and forwards the data to the correct device in the network.

Why NAT is Essential?

i) IP Conservation → NAT helps conserve the limited pool of IPv4 addresses ~~from the outside~~ by allowing multiple devices to share a single public IP.

ii) Security → NAT provides a layer of security by hiding internal IP addresses from the outside world, making it harder for external entities to access specific devices directly.

Purpose of NAT in Private IP communication →

NAT enables devices with private IPs, which aren't directly routable on the internet to access and communicate with external networks by using the Public IP of the NAT router.

9i) Static NAT →

a) Assignment → Maps a specific private IP address to a specific public IP address on a one-to-one basis.

b) Mapping Maintenance → The mapping is fixed and manually configured. Each private IP always corresponds to the same public IP.

c) Use Case → Useful when a particular internal device needs a consistent, unchanging public IP for external access.

d) Limitation → Requires a unique public IP for each private IP, making it less scalable for larger networks.

Name:_____ Regd No.:_____

ii) Dynamic NAT →

a) Assignment → Maps private IP addresses to public IP addresses dynamically, from a pool of available public IPs.

b) Mapping Maintenance → Each time a private IP initiates a connection, it is temporarily assigned a public IP from the pool. When the session ends, the public IP becomes available for other devices.

c) Use Case → Useful in situations where multiple internal devices, need internet access but don't need a fixed IP, conserving public IPs.

d) Limitation → If the pool of the public IPs is exhausted, additional private IPs can't access the internet until a public IP is freed up.

10) a) How PAT works →

i) When a device with a private IP address sends data to the internet, PAT assigns a unique port number to the session on the public IP address.

ii) The public IP address, combined with this unique port number, creates a distinct identifier for each ~~identifier~~ internal device and connection.

iii) The NAT router keeps a table that maps each internal IP and port to the corresponding external port on the public IP. This way, incoming responses can be routed back to the correct internal device.

b) Port Mapping in PAT →

i) Port Mapping → PAT dynamically assigns and tracks port numbers for each internal device's outgoing connection.

ii) Managing Traffic → When responses arrives at the router, PAT checks the port number, referring to the mapping table to identify the originating private IP and port, then forwards the response to the correct device.

Benefits of PAT →

i) IP Conversation → PAT allows many devices to share a single public IP, conserving the limited number of IPv4 addresses.

Name:_____ Regd No.:_____

Name:_____

ii) Effective Traffic Management → Port mapping enables unique session identification, allowing traffic to be correctly routed even when multiple devices communicate with the same external server.

11) Purpose of EUI-64 →

EUI-64 allows IPV6 addresses to be generated automatically by embedding a device's MAC address into the IPV6 address. This helps streamline address assignment, particularly for devices that need global unicast addresses on IPv6 networks.

How EUI-64 works →

i) MAC address modification → A ~~mac~~ MAC address is typically a 48-bit identifier. EUI-64 extends this to 64 bits by splitting the MAC address in half and inserting FFFE @in the middle.

ii) Inverting the 7th Bit (Universal/Local Bit) → The 7th Bit in the first byte of the MAC address is inverted to indicate that this address was modified. If it's originally set to 0, it's flipped to 1 in EUI-64.

iii) Constructing the IPv6 Address → The modified EUI-64 identifier becomes the Interface ID of the IPv6 address. Combined with the network prefix, this gives each device a unique IPv6 address.

12) In SLAAC (Stateless Address Autoconfiguration), an IPv6 device configures its IP address automatically.

i) Generate Link-Local Address → The device creates a link-local address using its MAC address or a random identifier.

ii) Duplicate Address Detection (DAD) → Checks if the link-local address is unique; assigns it if no duplicate is found.

iii) Recieve Router Advertisement (RA) → The device listens for RA messages from routers, which provide the network prefix and configuration details.

iv) Generate Global Unicast Address → The device combines the network prefix from the RA with its identifier to create a unique IPv6 address for internet use.

Name:_____ Regd No.:_____

13) IP address range → 192.168.10.0/24

- Subnet mask → /24 corresponds to 255.255.255.0, meaning the first 24 bits are for the network, leaving 8 bits for the host ~~opt~~ portion.
- Total Host address → With 8 bits for hosts, there are $2^8 = 256$ possible addresses.
- Usable Host addresses → The first address (192.168.10.0) is reserved for the network identifier, and the last address (192.168.10.255) is for the broadcast address. This leaves 256 − 2 = 254 usable addresses.

14) No, the pool of ~~the~~ public IPs (203.0.113.10 to 203.0.113.15) will not be sufficient for 50 devices to access the internet simultaneously.

To allow 50 devices to access internet simultaneously, the company would 50 − 6 = 44 additional public IP addresses.

15) i) Address Format and Size →

a) IPv4 → Uses a 32-bit address format, allowing around 4.3 billion unique addresses.

b) IPv6 → Uses a 128-bit address format, allowing for approximately 340 undecillion addresses.

ii) Notation →

a) IPv4 → Notated in dotted decimal format, divided into four octets.

b) IPv6 → Notated in colon-hexadecimal format, divided into eight 16-bit blocks separated by colons.

iii) Why IPv6 was developed →

a) IPv4 Address Exhaustion → IPv4's limited address space became insufficient as the number ~~the~~ of internet-connected devices grew.

b) Need for Scalability → IPv6 addresses the need for a vast number of unique addresses ~~internet-connected devices grew~~ to support the expanding internet.

iv) Advantages of IPV6 over IPv4 →

a) Larger Address Space → Vastly more IP addresses, supporting the growth of ICT and future technologies.

Name:_____ Regd No.:_____

b) Improved Security → IPv6 natively support IPsec for secure communication.

c) Simplified Address Configuration → Supports SLAAC allowing devices to automatically configure their own addresses without a DHCP server.

d) Better Routing Efficiency → IPv6 reduces the size of routing tables and enhances routing speed and efficiency.

Examples →

IPv4 → 192.168.1.1

IPv6 → 2001:d58:85a3::8ade:370:7334

16) Host address → 10.45.67.32/19

/19 means the first 19 bits are for the network, and the remaining 13 bits are for hosts and its mask is 255.255.224.0

IP address → 10.45.67.32 ⇒ in binary → 00001010.00101101.01000011.00100000

Subnet Mask → 255.255.224.0 ⇒ in binary → 11111111.11111111.11100000.00000000

Caculation →

IP address: 00001010.00101101.01000011.00100000

Subnet mask: 11111111.11111111.11100000.00000000

Network Address: 00001010.00101101.01000000.00000000

Now, result back in decimal 10.45.64.0

The host 10.45.67.32/19 belongs to the subnet 10.45.64.0/19.

17) Address → 192.168.46.234/26

/26 means first 26 bits are for the network and rest 6 bits are for hosts. The subnet mask for /26 in decimal notation is 255.255.255.192.

Calculation →

IP Address → 11000000.10101000.00101110.11101010

Subnet Mask → 11111111.11111111.11111111.11000000

Network Mask → 11000000.10101000.00101110.11000000

Name:_____ Regd No.:_____

Converting the network address back to decimal gives us 192.168.46.192. So, the first usable address is next to network address is 192.168.46.193.

18) Network → 172.30.56.48/28

/28 means the first 28 bits are for the network, and the remaining 4bits are for the hosts. Subnet mask for /28 is 255.255.255.240

The IP address 172.30.56.48 falls within the network starting at 172.30.56.48 for a /28 subnet.

In a /28 subnet:

i) There are 16 addresses per subnet ($2^4 = 16$)

ii) The network address is 172.30.56.48.

The broadcast address is the last address in the subnet, which can be found by adding 15 to the network address.

So, the broadcast address for the 172.30.56.48/28 network is 172.30.56.63.

19) IMAP (Internet Message Access Protocol) allows email clients to access and sync messages with a server, keeping emails consistent across multiple devices.

Key Points →

a) Server-Based Storage → Emails stay on the server, so they're accessible from any device.

b) Two-way Sync → Actions like reading, deleting or moving messages sync across all devices.

c) Folder Management → Users can create and organise server-based folders, which stay synced.

d) Efficient Access → Only headers are initially downloaded, saving bandwidth until full content is needed.

IMAP typically uses port 143 or port 993. It enables real time updates and centralized email access across devices.

Name:_____ Regd No.:_____

20) The main types of ICMP (Internet Control message Protocol) messages used to check connectivity between host on a network ~~dest~~ include →

i) Echo Request (Type 8) and Echo Reply (Type 0): Used in ping tests to check if a host is reachable and responding.

ii) Destination Unreachable (Type 3) → Indicates that a packet could not reach its destination.

~~iii~~ Common codes include → Network Unreachable (Code 0), Host Unreachable (Code 1), Port Unreachable (Code 3)

iii) Time Exceeded (Type 11) → Indicates that the Time-to-Live (TTL) of a packet expired often used in traceroute to identify the path to a destination.

iv) Redirect (Type 5): Sent by routers to inform hosts of a better route for packets, optimising network paths.

v) Router Advertisement (Type 9) and Router Solicitation (Type 10) → Used in IPV6 networks for hosts to discover available routers and configure themselves automatically.

Name:_____ Regd No.:_____