Assignment 2

Q1) Explain the difference between FTP and FTPS protocol?

Ans→

FTP (File Transfer Protocol)	FTPS (File Transfer Protocol Secure)
i) FTP is a standard network protocol used to transfer files between a client and a server.	i) FTPS is an extension of FTP that incorporates SSL/TLS encryption to secure file transfers.
ii) Lacks built-in encryption.	ii) Encrypts data in transit using SSL/TLS, ensuring the confidentiality and integrity of data.
iii) Data, including usernames and passwords, is transferred in plain text, making vulnerable to interception and attacks.	iii) Authentication can involve certificates for added security.
iv) Often used in trusted networks where security is not a primary concern or for transferring non-sensitive files.	iv) Used in scenarios where secure file transfer is essential, such as transferring sensitive or confidential data.

2) Explain the steps involved in the DHCP 4-way hand shake process.

Ans→ The DHCP 4-way handshake dynamically assigns IP address and network settings to clients.

i) DHCP Discover → The client broadcasts a request to locate DHCP servers on the network.

ii) DHCP Offer → DHCP servers respond with available IP addresses and configuration details.

iii) DHCP Request → The client selects an offer and requests the chosen IP address from the server.

iv) DHCP Acknowledge (ACK) → The server confirms the lease, providing the client with the requested IP and configuration.

3) ~~The Cis~~ Differentiate between Cisco 3-tier and 2-tier architecture referred by the network professionals while designing a network for an organisation.

Ans→ ① Cisco 3-Tier Architecture →

i) Structure → Composed of three layers:

a) Core layer: High-speed backbone for fast interconnection between distribution layers.

b) Distribution Layer: Connects access layers to the core, implements policies (e.g., routing, filtering)

c) Access Layer: Provides end-user devices access to the network.

ii) Scalability → Highly scalable; suitable for large ~~optimisation~~ organisations or networks with multiple branches.

Name:_____ Regd No.:_____

iii) Performance: Enhanced performance by isolating traffic flows and offloading tasks across layers.

iv) Cost: Higher due to additional hardware and complexity.

v) Use case: Large enterprises requiring scalability and redundancy.

Cisco 2-Tier Architecture

i) Structure: Combines core and distribution layers into a single layer, with the access layer below:

a) Collapsed Core / Distribution → Merges the core and distribution functions.

b) Access layer → Connects directly to the collapsed core/distribution layer.

ii) Scalability: Limited scalability compared to 3-tier.

iii) Performance: Adequate for smaller networks, but less optimised for larger/scale environments.

iv) Cost: Lower due to fewer devices and simpler design.

v) Use case: Small to medium-sized organisations with simpler network requirements.

4) How do the cloud service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Desktop as a Service (DaaS) differ in terms of its use?

Ans → i) IaaS (Infrastructure as a Service):

a) Use: Provides virtualized infrastructure (servers, storage, networking).

b) Users: IT teams needing full control over the environment.

c) Examples: AWS EC2, Azure VMs.

ii) PaaS (Platform as a Service):

a) Use: Offers a platform for app development and deployment.

b) Users: Developers building and deploying apps quickly.

c) Examples: Heroku, Google App Engine.

iii) SaaS (Software as a Service):

a) Use: Delivers ready-to-use software applications.

b) Users: End-users needing functional tools.

Name:_____ Regd No.:_____

c) Examples → Google Workspace, Salesforce

iv) DaaS (Desktop as a Service) →

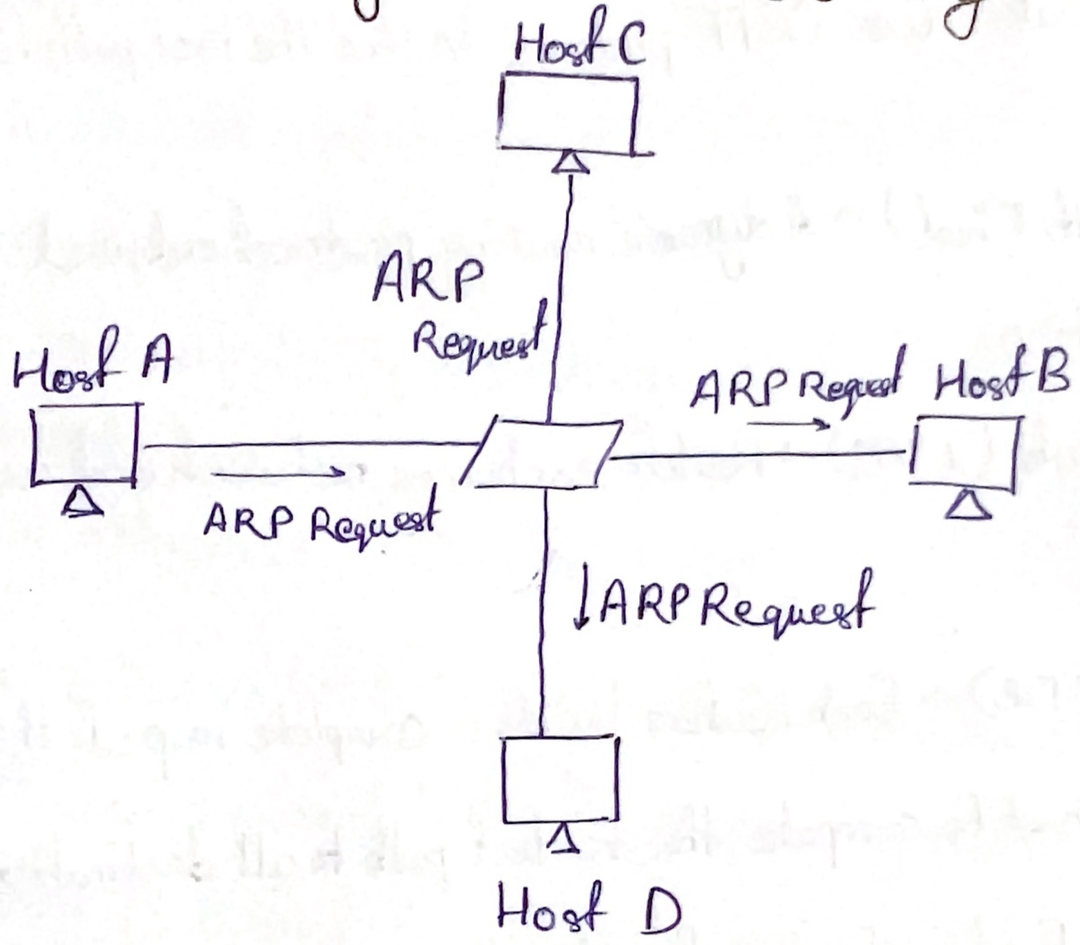
a) Use → Provides virtual desktops for secure remote work.

b) Users → Remote workers, IT admins.

c) Examples → Amazon WorkSpaces, Citrix DaaS.

5) With the help of a neat diagram discuss the working of Address Resolution Protocol (ARP).

Ans →



6) State the ~~availab~~ similarity and difference between access point and wifi router.

Ans → Similarity between Access Point and Wifi Router →

i) Both provide wireless connectivity to devices, enabling them to join a network.

ii) Both can extend a network by connecting devices wirelessly.

iii) Both may have ethernet ports to allows wired connections to devices like computers printers or switches.

Access Point	Wifi Router
i) Extends an existing wired network to provide wireless access.	i) Combines the functions of a router, switch, and access point. Create and manages a local network.
ii) Used in large networks to provide additional wireless coverage.	ii) Designed for smaller networks like homes or small offices.
iii) No built-in DHCP server.	iii) Includes a built-in DHCP server to assign IP addresses to devices.

Name:_____ Regd No.:_____

7) Explain why modems are important in internet connectivity from household hosts.

Ans→ Modems are essential for household internet connectivity as they convert digital signals from your devices into analog signals for transmission over ISP infrastructure and vice versa. They establish a connection with the ISP, manage IP addresses and enable communication, between your home network and the internet without a modem, devices in your home cannot access the internet.

8) Briefly explain how does router use OSPF protocol to find the best path for a destination host/ network.

Ans→ OSPF (Open Shortest Path First) → A dynamic routing protocol used by routers to find the best path to a destination.

i) Link-State Advertisements (LSAs) → Router exchanges network and cost information with neighbours.

ii) Link-State Database (LSDB) → Each router builds a complete map of the network topology.

iii) Dijkstra's Algorithm → Used to compute the shortest path to all destination based on link costs.

iv) Routing Table Update → Best ports are stored in the routing table for forwarding traffic.

v) Dynamic Update → Automatically recalculates routes when network topology changes.

9) Can QoS be used as a solution for controlling the traffic with better performance in a network? List out the matrics used in this approach for measurement of traffic over a network.

Ans→ Yes, QoS (Quantity of Service) can be used as a solution to control network traffic & improve perform once by prioritizing certain types of traffic over others.

Metrics used in QoS for Traffic Measurement:

i) Bandwidth → The ~~latency~~ maximum data rate that can be transmitted over a network link.

ii) Latency → The times it takes for a packet to travel from the source to destination.

iii) Jitter → The variation in latency over time.

iv) Packet Loss → The percentage of packets lost during transmission.

Name:_____ Regd No.:_____

10) What is a Bridge Protocol Data Unit (BPDU) frame? How this is used to find the route bridge in a network comprising of multiple switches having redundancy paths among them and that employs spanning tree protocol?

Ans→ A Bridge Protocol Data Unit (BPDU) is a data frame used by network switches that implement the spanning tree protocol (STP) to maintain loop free topologies in Ethernet networks. BPDU's carry information about the network topology, specifically to help Switches determine the root bridge and the best paths for forwarding the frames, preventing loops in a network with redundant paths.

BPDU is used to find the root bridge →

i) Root bridge election process.
ii) BPDUs are sent periodically to exchange topology info.
iii) Handling redundant paths.
iv) Bridge role assignment.

11) Name and discuss various VLAN that are supported in computer networking.

Ans→ i) Data VLAN → Carries user data traffic, separating different group of users.
ii) Voice VLAN → Dedicated to VoIP traffic, ensuring high priority and low latency.
iii) Management VLAN → Used for network devices management and configuration, ~~VLAN 1 by default~~.
iv) Native VLAN → Carries untagged traffic on trunk links, typically VLAN 1 by client.
v) Storage VLAN → Segregates storage network traffic for SAN or NAS.
vi) Private VLAN → Isolates devices within the same VLAN for security.
vii) Guest VLAN → Provides internet access for guest users, isolated from internal networks.
viii) Multimedia VLAN → Dedicated to multimedia traffic like video and streaming for quality

12) Describe the role of Dynamic Host Configuration Protocol (DHCP) in a wireless protocol.

Ans→ The Dynamic Host Configuration Protocol (DHCP) plays a critical roles in managing IP address allocation and network configuration in a wireless network.

i) When a device connects to wireless network, it needs an IP address to communicate with other devices and access the internet. DHCP automatically assigns a unique IP address.

Name:_____ Regd No.:_____

ii) DHCP eliminates the need at for manual IP configuration. (Simplified Network Configuration)

iii) Efficient Resource Management

iv) Integration within wireless Access Pointer works with DHCP servers to provide IP address.

v) Network flexibility → In dynamic environments like wireless hotspots, DHCP adapts quickly to changing conditions.

13) Mention and describe the relevance and importance of the different performance metrics for operation of any networking device.

Ans → i) Throughput → Measures the data transfer rate, ensuring efficient data flow across the network.

ii) Latency → Tracks the time delay in data transmission, critical for real-time

iii) Packet Loss → Monitors dropped data packets, which impact connection quality and reliability.

iv) Bandwidth → Indicates the maximum data capacity of a device, defining the network's potential speed.

v) Jitter → Examines variations in data, delivery timing, affecting services like video and voice calls.

vi) Reliability → Measures operational availability, ensuring consistent service delivery.

14) Write the default format of a syslog message? Explain each component.

Ans → The default syslog message format address to RFC 5424 →

<PRI> VERSION TIMESTAMP HOSTNAME APP-NAME PROC ID MSG ID MESSAGE

i) <PRI> → (Priority) A numeric value enclosed in angular brackets (<>).

PRI = Facility + Security.

ii) VERSION → Indicates the syslog protocol version.

iii) TIMESTAMP → Provides the time the event occurred.

iv) HOSTNAME → The name or IP address of the device generating the log message.

v) APP-NAME → The name of the application or process generating the message.

vi) PROC ID → The process ID (PID) of the application or domain that created the message.

vii) MSG ID → A unique identifier for the type of message being logged.

viii) MESSAGE → The actual content of the log message.

16) What are the different recovery concepts used in any networking organisation for overcoming sudden network disasters? Explain the process of network device backup and restoration in the event of disaster recovery?

Ans → Recovery concepts for Network disasters →

i) Disaster Recovery Planning
ii) Business Continuity Planning
iii) Redundancy and High Availability
iv) Data Backup and offsite storage
v) Failure and Load Balancing
vi) Cloud based recovery

Network device backup →

i) Scheduled Backups → Regular backup device configurations.
ii) Backup Storage → Store backup locally and offsite (cloud) for redundancy.
iii) Configuration Tools → Use tools for automatic backups.
iv) Secure Backup → Encrypt and use secure protocols.

Restoration Process →

i) Disaster detection → Identify affected devices.
ii) Restore Backup → Retrieve and apply the latest backup configuration.
iii) Reconfiguration → Apply settings like IP addressing, routing, etc.
iv) Testing → Verify device functionality and connectivity.
v) Documentation → Record recovery steps for future reference.

15) What does change management focus in a network implanted organisation? State different phases and the functionality of each associated with the process of its implementation.

Ans → Focus ensures network changes are implemented systematically to minimize disruption, risk and improve efficiency.

Process of Change Management →

i) Initiation/Request for change → Submit a formal request outlining the change details.
ii) Change Assessment and Approval → Recieves and assess risks, impact and benefits by the Change Advisory Board.
iii) Planning and Scheduling → Plan the change including timing and resources, to minimise disruption.
iv) Apply the change according to the plan, test to ensure success.

v) Monitor network performance post-change, gather feedback to address issues.

17) Mention some of the most common guidelines for defining password policies created by system administrators.

Ans → i) Minimum length and complexity → Passwords should be at least 8-12 characters, including alphabets, numerical values & unique values.

ii) Password expiry and history → Require password changes every 60-90 days.

iii) Account Lockout → Lock accounts after 3-5 failed login attempts to prevent brute force attacks.

iv) Multi-factor Authentication → Implement MFA for added security.

v) Encryption → Store passwords securely using encryption.

18) Name and define the key terminologies must be referred when implementing the high availability techniques within a network.

Ans → i) High Availability → Ensures system remains operational with minimal down time.

ii) Redundancy → Duplication of critical components to provide backups.

iii) Failure → Automatic switch to a standby system during failure.

iv) Load balancing → Distributes traffic across resources to prevent over load.

v) Replication → Copies data across systems to ensure availability and consistency.

vi) Fault tolerance → Ability to keep running despite component failures.

vii) Disaster Recovery → Restores services after major failures or disasters.

viii) SLA (Service Level Argument) → Guarantees uptime and performance expectations.

19) Assume a critical server operates for 8,745 hours per year and experienced 10 failures within the same year. Further, the IT professionals engaged spends a total of 60 hours in the same year for repairing all the failure. Find i) Mean time to repair. ii) Mean time between failures.

Ans → Given, Total operating hours per year = 8745 hours

Total failures = 10

Total repair time = 60 hours

$$\text{Mean time to repair} = \frac{\text{Total repair time}}{\text{total failures}} = \frac{60}{10} = 6 \text{ hrs.}$$

Name:_____ Regd No.:_____

Mean time between Failures = $\frac{\text{Total operating time}}{\text{Total failures}}$

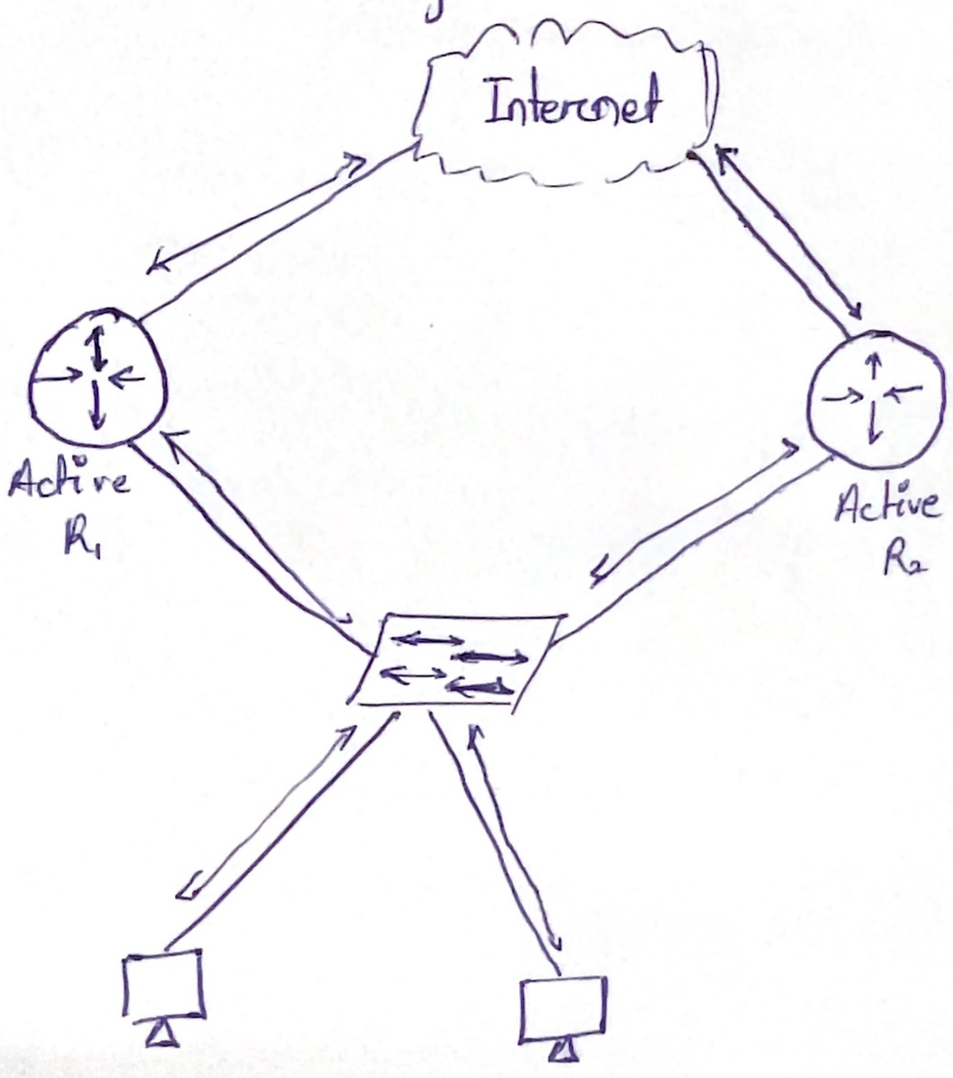
$= \frac{8745}{10} = 874.5$ hrs.

20) State the difference between active-active and active-passive configuration with suitable diagram.

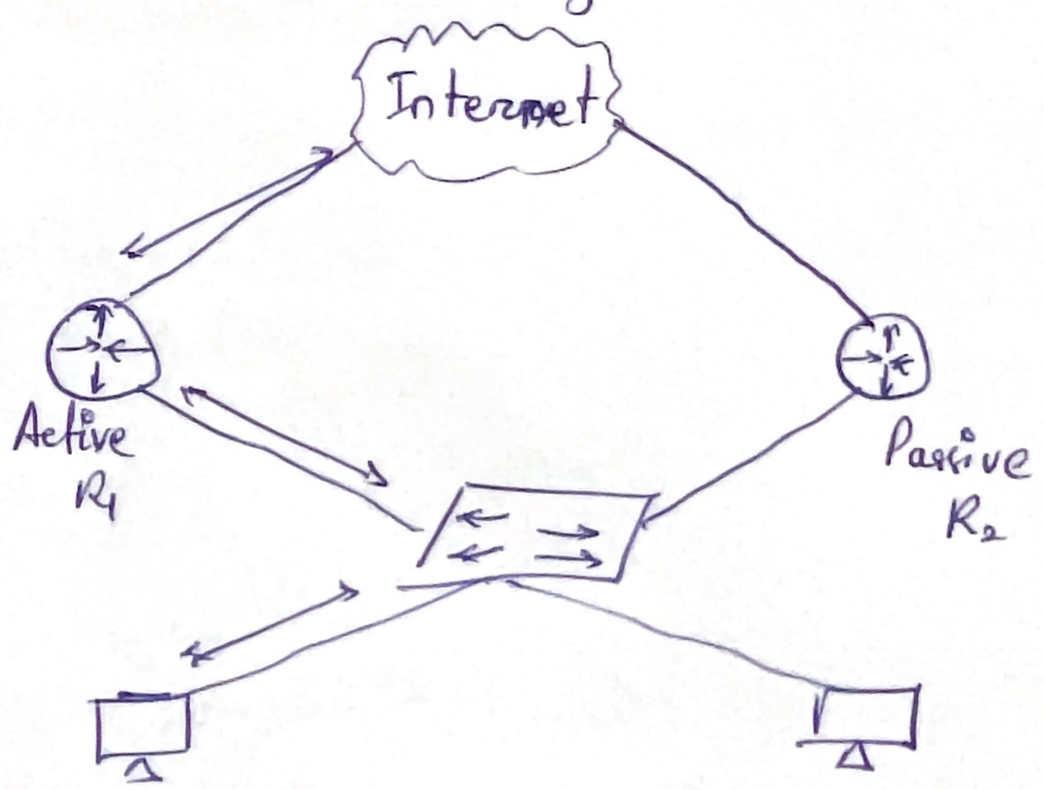
Ans →

Active - Active configuration	Active - Passive Configuration
i) All nodes or system actively handle traffic simultaneously.	i) One system is active while the other remains on standby.
ii) Used for load balancing and maximising resource utilisation.	ii) Used for failover and high availability.
iii) Both nodes are already operational, so failure is seamless.	iii) Failover occurs by activating the standby mode.
iv) More complex to configure and manage.	iv) Simpler ~~est~~ setup with minimal configurations.

Active - Active Configuration.



Active - Passive Configuration.



Name:_____ Regd No.:_____