Name :- Naitrik Solanki

Assignments :-

Module – 3 :- Understanding And Maintenance of Networks

Section 1: Multiple Choice

1. What is the primary function of a router in a computer network?

a) Assigning IP addresses to devices

b) Providing wireless connectivity to devices

c) Forwarding data packets between networks

d) Managing user authentication and access control

Ans. C) Forwarding data packets between networks

Note :- A router primary function is to connect multiple networks together and forward data packets between them, ensuring that data reaches its intended destination. It is routing tables and algorithms that determine the best path of data transmission.

2. What is the purpose of DNS (Domain Name System) in a computer network?

a) Encrypting data transmissions for security

b) Assigning IP addresses to devices dynamically

c) Converting domain names to IP addresses

d) Routing data packets between network segments

Ans. C) Converting domain names to IP addresses

Note :- The DNS is like the phonebook of the internet. While humans use domain name (like www.google.com) to access website, computer and networking use to IP address (like 142.250.190.78).

3. What type of network topology uses a centralized hub or switch to connect all devices?

a) Star

b) Bus

c) Ring

d) Mesh

Ans. A) Star

Note :- In a Star topology is all devices (nodes) are connected to a central hub or switch. This central device acts as a point of communication for all data transmission between device on the network.

4. Which network protocol is commonly used for securely accessing and transferring files over a network?

a) HTTP

b) FTP

c) SMTP

d) POP3

Ans. B) FTP

Note :- FTP is commonly used for transferring files over a network. However, traditional FTP lacks security. FTPS and SFTP provide secure file transfer capabilities, protecting data from unauthorized access.

Section 2: True or False

5. True or False: A firewall is a hardware or software-based security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Ans. True

Note :- They help prevent unauthorized access, data breaches, and malicious activity by allowing or blocking data packets based on rules defined by the network administrator.

6. True or False: DHCP (Dynamic Host Configuration Protocol) assigns static IP addresses to network devices automatically.

Ans. False

Note :- DHCP assigns dynamic IP addresses to network devices automatically, not static IP addresses. Dynamic IP addresses can change over time, whereas static IP addresses remain fixed.

7. True or False: VLANs (Virtual Local Area Networks) enable network segmentation by dividing a single physical network into multiple logical networks.

Ans. True

Note :- VLANs enable network segmentation by dividing a single physical network into multiple logical networks, each with its own set of rules, security policies, and configurations.

Section 3: Short Answer

8. Explain the difference between a hub and a switch in a computer network.

Ans.

Hub	Switch
A hub is a basic networking device that simply broadcast data it receives all connected devices.	A switch is more intelligent it learns the MAC addresses of devices connected to it and forwards data only to the specific device.

Every data packet is sent to every port.	Uses MAC address to send data directly to the intended recipient.
Inefficient and causes a lot of unnecessary traffic, especially in larger network.	Much more efficient, with less network congestion.
Less secure since data is sent to all devices, any device can potentially to the traffic.	More secure data is only sent to the intended device.
Operates at OSI Model Layer 1 Physical Layer.	Operates at OSI Model Layer 2 Data Link Layer.
Usually slower speed typically 10/100 Mbps.	Faster and more suitable for modern networks support 100 Mbps, 1 Gbps or more.

9. Describe the process of troubleshooting network connectivity issues.

Ans. The process of troubleshooting network connectivity issues.

Step 1: Identify the problem

- Gather information about the symptoms are (e.g., no internet access, slow speeds).
- Determine the scope is the issue affecting one device, multiple devices, or the entire network.

Step 2: Check Physical Connections

- Verify cables are properly connected (Ethernet, power cables, etc.)

- Check for damaged cables or hardware (routers, switches, modems).
- Ensure devices are powered on.

Step 3: Verify Device Settings

- Check the device network settings (IP address, subnet mask, default gateway).
- Confirm the device is set to obtain an IP automatically via DHCP or has correct static IP settings.
- Check Wi-Fi settings.

Step 4: Test Connectivity and Ping

- Use ping to test reachability to:
- The local router/gateway.
- External IP addresses (e.g. 8.8.8.8).
- Domain name to test DNS (e.g. google.com).
- Use tracert (Windows) or traceroute (Linux/macOS) to identify where packets are dropping.

Step 5: Check Network Devices

- Restart or power cycle routers, modems, switches.
- Check router/modem status lights for errors.
- Access router interface to check WAN status and logs.

Step 6: Check for Software Issues

- Disable firewalls or security software temporarily to rule out interference.
- Check for recent changes in device software or settings.

- Ensure drivers or firmware are up to date.

Step 7: Test Alternate Devices or Connections

- Try connecting another device to the same network.
- Try connecting the device to a different network.
- Use a wired connection instead of wireless to isolate the problem.

Step 8: Check for ISP or External Issues

- Confirm if the ISP is having outages.
- Check online outage maps or contact ISP support.
- Test the modem connection status.

Step 9: Document Findings and Apply Fixes

- Based on the gathered info, apply fixes (e.g. resetting network adapters, reconfiguring settings, replacing hardware).
- Document what was done for future reference.

Step 10: Verify Resolution

- Confirm network access is restored.
- Test multiple services (web browsing, email, file sharing).

Section 4: Practical Application

10. Demonstrate how to configure a wireless router's security settings to enhance network security.

Ans. Configuring a wireless router security settings is essential for protecting your home or office network from unauthorized access and cyber threats.

Step 1: Access the Router Admin Interface

- Connect to the router via Wi-Fi or Ethernet.
- Open a web browser and enter the router IP address.
- Log in using the router admin username and password and change the default password immediately.

Step 2: Change Default Login Credentials

- Navigate to Administration and Management.
- Change Admin Username and Password to a strong password at least 18 (Characters, Number, Symbols).
- Default credentials are publicly known and a major security risk.

Step 3: Enable WPA3 or WPA2 Encryption

- Navigate to wireless settings or wireless security.
- Set best Wi-Fi Security WPA3-Personal and WPA2-Personal.
- WEP is hack easily.
- WPA/WPA2 is a mixed it can allow fallback to weaker encryption.

Step 4: Set a Strong Wi-Fi Password

- Choose a strong, unique passphrase.

- Do not use your name, address, or simple dictionary words.

Step 5: Disable WPS (Wi-Fi Protected Setup)

- Navigate to WPS setting.
- Disable WPS to prevent brute-force attacks on the Wi-Fi password.

Step 6: Update Router Firmware

- Navigate to Firmware or system update.
- Check for updates and install them.
- Consider enabling automatic firmware updates.

Step 7: Disable Remote Management

- Navigate to remote management / Remote Access / WAN Access.
- Disable unless absolutely necessary.
- Remote access should be limited and secured with strong credentials and encryption.

Step 8: Change the default network name

- Navigate to wireless settings.
- Use a unique that doesn’t reveal your identity or location.
- Avoid including personal info like your name, address, ISP.

Step 9: Enable network firewall and Dos protection

- Navigate to security or advanced settings.
- Ensure the built-in firewall is enabled.
- Enable denial of service (DoS) protection if available.

Step 10: Set Up a guest network

- Navigate to guest network settings.
- Enable a separate network for guests.
- Use isolation mode to prevent access to your main devices.
- Secure the guest network with WPA2/WPA3 and a different password.

Step 11: Disable unused services

- Turn off
- UPnP unless required by certain application.
- Telnet or SSH access (unless managed securely).
- IPv6 (if not used).
- These can be entry point for attackers if not properly secured.

Section 5: Essay

11. Discuss the importance of network documentation and provide examples of information that should be documented.

Ans. **Importance of Network Documentation**

1. Troubleshooting & Maintenance

- When network issues arise, detailed documentation helps IT staff quickly identify and resolve problems.
- It reduces downtime and the time needed to trace configurations or identify faulty components.

2. Knowledge Transfer

- Documentation ensures continuity when employees leave or when new staff are onboarded.
- It serves as a guide for training and daily operations.

3. Network Security

- Helps in identifying unauthorized devices or changes.
- Supports compliance with security policies and regulations.

4. Disaster Recovery

- In the event of a failure, documentation provides a roadmap to rebuild or restore services accurately and efficiently.

5. Capacity Planning & Scalability

- Allows for informed decisions on upgrades, expansions, or migrations.
- Helps anticipate and avoid potential bottlenecks.

6. Regulatory Compliance & Auditing

- Many industries require detailed IT documentation to pass audits and meet legal requirements.

Examples of information to document

1. Network Topology

- Diagrams showing physical and logical layout of the network.
- Includes switches, routers, firewalls, and how devices are connected.

2. IP Addressing Scheme

- Assigned IP addresses (static and dynamic).
- Subnets, VLANs, and addressing rules.

3. Device Inventory

- List of all networking hardware routers, switches, servers, firewalls, etc.
- Include manufacturer model, serial number, firmware version, and location.

4. Configuration Files

- Backup configurations of routers, switches, and firewalls.
- Version control of changes made over time.

5. Access Control & Credentials

- Administrative usernames and passwords.
- VPN access information, role-based access permissions.

6. Network Services Information

- DNS, DHCP, NTP servers and configurations.
- Email servers, file servers, and authentication systems.