Name: Kishan Barvaliya

Batch: Hardware (Abdul Hamid Sir) 9:30am to 10:30am

Assignment

A+ - Understanding And Maintenance Of Networks

Section 1: Multiple Choice

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

Ans: Forwarding data packets between networks

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

Ans: Converting domain names to IP addresses

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

Ans: Star

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

Ans: FTP

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

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

Ans: False

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

Ans: True

Section 3: Short Answer

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

Network

Ans:

Feature	Hub	Switch
Function	Broadcasts data to all connected devices	Forwards data only to the intended recipient device
Efficiency	Less efficient – causes network congestion	More efficient – reduces unnecessary traffic
Data Handling	Works at Layer 1 (Physical Layer)	Works at Layer 2 (Data Link Layer)
Bandwidth Sharing	Shared among all devices	Dedicated bandwidth per port
Intelligence	No MAC address learning or filtering	Learns and uses MAC addresses to route data
Security	Low – all data is sent to all ports	Higher – data is sent only to the target device

9. Describe the process of troubleshooting network connectivity issues.

Ans:

Step 1: Define the Problem

Ask: What is not working? (e.g., no internet, slow network)

Let me know what happens in the comments (e.g., any error messages or behavior such as 'No Internet' or 'Limited Connectivity' etc..)

Step 2: Verify the Physical Connections

Confirm whether Ethernet cables connectors are firmly inserted countersunkPORTS on the back of XJR-00Please check whether interfaces are inserted directly XJR-00 counterbore1.

Make sure that Wi-Fi is turned on and connected

Observe router/switch/power lights anomalies

Step 3: Verify Device Settings

Try ipconfig (Windows) or ifconfig (Linux/Mac) to see one IP address.

Check that the device has a good IP, SubNet Mask, GW, and DNS.

Step 4: Test Connectivity

Ping your open IP ping 127.0.0.1 (tests the network adapter)

Ping gateway, for example (local network test): ping

Ping public DNS: ping 8.8.8.8 (checks Internet connectivity)

Ping domain: ping google. com (tests DNS resolution)

Step 5: Restart Devices

Restart the router, modem and switch as well as your computer

This can fix the temporary bugs or the IP conflicts

Step 6: Make sure there aren't any IP conflicts

Verify through each device that there is no possible way there could be two devices with a static IP the same.

DHCP or assign specifc static IPs to each of these.

Step 7: Inspect Firewall/Antivirus Settings Here are some settings you need to take care of.

Try disabling it for now to see if it's obstructing the network traffic.

Step 8: Reset Network Settings

On windows: netsh int ip reset & ipconfig /flushdns

Also as a bonus: forget how to do things, and forget Wi-Fi networks.

Step 9: Change The Broken Hardware

Finally, switch cables, move to another port etc., of even better use another router/switch if available.

Step 10: Talk to your ISP or Network Admin

If everything runs locally fine the problem is most likely outside

Section 4: Practical Application

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

enhance network security.

Ans: Done

Section 5: Essay

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

Ans: The Network documentation is a key aspect of infrastructure management. This includes detailed records of how your network is designed, the hardware and software running, and their individual configurations. Good documentation is key for reliability, efficiency and security.

The Importance of Network Documentation:

1.Faster Troubleshooting:

->Assists in rapid root cause analysis of outages or other issues.

->Minimizes down time and dependence on human memory.

2.Easier to Maintain & Upgrade:

->Facilitates seamless hardware changeovers, software upgrades and network expansions.

->Prevent types of configuration clashes or unwanted misconfigurations.

3.Improves Network Security:

->Tracks devices and access points and can help detect any modifications not authorized.

->Assists in the enforcement of policies and regulations.

4.Serves as a Tool for Onboarding and KnowledgeFD Transfer:

->Helps new team members understand and manage the network.

->Minimizes knowledge loss when staff members leave.

<u>Examples of Information to Document</u>

->Network Topology Diagrams:

Diagrams with device relationships (routers, switches, servers, etc)

->IP Address Management:

IP Address ranges and assignments (including reserved/static IPs).

->Device Inventory:

Router, switch, firewall, server, and access points details (model, serial number, place).

->Configuration Files:

Device configuration and backups, firewall rules, vlan settings.

->User access logs and permissions:

Who is who User list, and what point are they able to reach in the network?

->Software Versions and Licenses:

OS, FW versions and licenses.

->Cabling and Port Mapping:

What cables come from where, ports that are labeled, and wall jack assignments.

->Change Logs:

History of any changes in network and to whom these changes were made.