MODULE:3 UNDERSTANDING AND MAINTENANCE OF NETWORK

**SECTION:1 MULTIPLE CHOICE**

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

* Forwarding data packets between network.

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

* Converting domain names into IP addresses.

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

* Star.

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

* 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.

**TRUE.**

**6.TRUE OR FALSE: DHCP (Dynamic Host Configuration Protocol) assigns static IP addresses to network devices automatically.**

FALSE.

7**. TRUE OR FALSE: VLANs (Virtual Local Area Networks) enable network segmentation by dividing a single physical network into multiple logical networks.**

* TRUE.

SECTION:3 SHORT ANSWER

**8. Explain the difference between a hub or switch in a computer?**

|  |  |  |
| --- | --- | --- |
| **Feature** | **Hub** | **Switch** |
| OSI Layer | Physical (Layer 1) | Data Link (Layer 2) |
| Data Transmission | Broadcast to all devices | Unicast to specific device |
| Speed | Up to 10 Mbps | 10/100/1000 Mbps or higher |
| Duplex Mode | Half-duplex | Full-duplex |
| Collision Domains | One shared | One per port |
| MAC Address Learning | No | Yes |
| Security | Low | Higher |

**9**. Describe the process of troubleshooting network connectivity issues**?**

**1.** Check Physical Connections

Make sure all cables (Ethernet, power) are securely plugged in.

Inspect for damaged wires or loose connectors.

If using Wi-Fi, verify you're connected to the correct network.

2. Restart Devices

Reboot the computer, router, and modem.

Sometimes a quick restart clears out temporary glitches.

3. Verify Network Setting

Ensure airplane mode is turned off.

Check IP configuration:

Run ipconfig /all (Windows) or ipconfig (Mac/Linux).

Confirm you're getting an IP address from the router.

4. Test Internet Access

Try pinging a known website like ping google.com.

Access websites from a browser—if some load and others don’t, it might be a DNS issues.

5. Run Diagnostics Tools

Use built-in OS tools:

Windows: Network Troubleshooter

macOS: Wireless Diagnostics

Use tracert or ping to find out where packets are failing.

6. Check Firewall and Antivirus

These might block access to certain sites or services.

Temporarily disable and test, but be cautious about leaving them off.

7. Try Another Device or Network

If another device works on the same network, your issue is likely device-specific.

If no devices work, the problem might be with your router or ISP.

8. Contact Support

If all else fails, your Internet Service Provider or IT department can help identify outages or deeper configuration issues.

**SECTION:4 PRACTICAL APPLICATION**

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

1. Log Into Your Router

Connect to the router via Wi-Fi or Ethernet.

Open a browser and enter your router’s IP address (commonly 192.168.1.1 or 192.168.0.1).

Log in using the admin credentials (printed on the device or set by you).

2. Change Default Admin Username & Password

Navigate to the Administration or System Settings section.

Replace the default login info with a strong, unique username and password.

This prevents unauthorized access to your router settings.

Select WPA3-Personal (recommended) or WPA2-Personal if WPA3 isn’t available.

Avoid outdated protocols like WEP or WPA—it’s like locking your door with tape.

3. Rename Your SSID (Network Name)

Change it from the default to something custom that doesn’t include personal details.

Example: use something quirky like QuantumFrostNet instead of Linksys123.

4. Disable Remote Management

Turn off Remote Access, Remote Management, or WAN Access to prevent external tampering.

Keep router control strictly local unless you really need remote access.

5. Hide Your SSID (Optional)

You can disable SSID broadcast so your network isn’t visible to casual users.

Note: it adds obscurity, but savvy users can still find it.

6. Enable Firewall

Most routers have built-in firewall settings—make sure they’re turned on.

You may also want to block anonymous internet requests.

7. Update Firmware Regularly

Check the Firmware Update section and install the latest version.

These updates often patch known vulnerabilities.

Bonus Tips

Set up a guest network for visitors to avoid exposing your main devices.

Schedule automatic reboots to refresh connections and performance.

Disable features you don’t use—like WPS, UPnP, or IPv6 if unnecessary.

**SECTION:5 EASSAY**

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

Troubleshooting Efficiency: Speeds up diagnosis and resolution when network issues arise.

* Continuity & Handover: Crucial for team transitions, new hires, or external contractors to understand the network setup.
* Security & Compliance: Helps ensure systems adhere to regulations and internal policies.
* Disaster Recovery: Provides a clear guide for restoring systems after outages or cyberattacks.
* Scalability & Planning: Essential when expanding or modifying the network—no one wants to build on an unstable foundation!

Key Information to Document

Here’s a breakdown of what should be included in effective network documentation:

|  |  |
| --- | --- |
| Category | Examples of Information |
| Network Topology | Diagrams showing how devices (routers, switches, firewalls, etc.) are connected |
| IP Addressing | IP allocation plans, DHCP scopes, subnetting details |
| Hardware Inventory | Device names, models, serial numbers, physical locations |
| Configuration Details | Router, switch, and firewall configs; VLAN setups |
| Access Controls | User roles, permissions, remote access policies |
| Service Information | DNS, DHCP, web services, email servers |
| Monitoring & Alerts | Tools used, alert thresholds, escalation procedures |
| Change Logs | Records of changes to configurations or infrastructure |
| Backup Procedures | What’s backed up, how often, and where backups are stored |