Name: Ashish kumar sahni

Assignment 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**

**Ans: c)** Forwarding data packets between networks. The main work of router is to make sure that data packet can move between different networks effectively to decides the best path for data to travels so that it reaches its destination efficiently.

**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**

**Ans: c)** The purpose of DNS (domain name system) is to converting domain names to IP addresses such as (192.168.10.12) in a computer network thorough internet. This translation enables users to access websites and other online services using simple, easy to remember domain names instead of needing to known the specific numerical IP addresses.

**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 because in a star network all devices such as computers, printers are connected individually to a central hub or switch which controls the flow of data between devices.

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

**a) HTTP**

**b) FTP**

**c) SMTP**

**d) POP**

**Ans: b)** FTP because in the network protocol commonly used for securely accessing and transferring file over a network is FTP on the port number 21 and 22. However people often use FTPS or SFTPS (SSH file transfer protocol).

**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 because a firewall is hardware or software based security system that monitor and control incoming and outgoing network traffic based on predetermined security rules. Firewall is like a security guard of your computer network. It is working on a set of rules it decides which data is safe and should be allowed through and which data might be harmful should be blocked. In that way our network should be away from unauthorized access and cyber threats.

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

**Ans:** False because DHCP automatically gives devices temporary IP addresses that can change making it easier to manage the network where static IP addresses are manually set and don’t change.

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

**Ans:** true because VLANs this allows for improving management, security and efficiency within a network.

**Section 3: Short Answer**

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

**Ans:**

|  |  |
| --- | --- |
| **HUB**   1. This is layer 1 device 2. Does not recognize MAC address 3. It is a broadcast device 4. Slower in operation 5. It is low in cost device. | **Switch**   1. This is layer 2 device 2. It recognize MAC address 3. Its unicast device 4. Faster in operation 5. It is a expansive device. |

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

Ans: Troubleshooting network connectivity issues

1. identify the problem first of all we ask the person what’s wrong and see if its just one device or many or the whole network.
2. Check physical connections that making sure cables are plugged in and not broken and check if all devices have power.
3. Verify device configuration where see if the device has a good IP address or not and check also subnet mask and gateway settings.
4. Test connectivity while using the command “PING” to check connection to local router and the internet and another command is “traceroute” to find where the connection breaks or slows down.
5. Check network equipment where look at the status light on routers and switches or try to rebooting the modem, router and switch.
6. Review network configuration were make sure that router setting are correct and verify DNS settings.
7. Examine software issue check if a firewall or antivirus is blocking network access.
8. Check for external issues while call the ISP to see if there’s and outage or try a different cable or port.
9. Advanced diagnostics while using this tool like Wireshark to analyze network traffic look at logs on network devices.

**Section 4: Practical Application**

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

**Ans:** here are the steps for configure wireless router security are

1. Access router setting for connect to the routers IP address in a web browser and login with the router’s username and password.
2. Change admin credentials first of all change the default admin username and password to something strong.
3. Update firmware then check for and install the latest firmware updates.
4. Configure wireless security while change the SSID to a unique name and enable WPA3 or WPA2-PSK (AES) encryption and set a strong wi-fi password.
5. Disable WPS to reduce security risks.
6. Enable network firewall and ensure that the firewall is activated.
7. Set up guest network while create a guest network with a separate SSID and password.
8. Disable remote management features.
9. Monitor regularly and check connected devices and update passwords.

**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 and maintenance helps quickly fix problems and reduce downtime.
2. Network security keeps track of security settings and spots vulnerabilities.
3. Efficient management makes upgrades and changes easier and help plan for the future.
4. Knowledge sharing helps new team members learn and keeps everyone on the same page.
5. Compliance and audits ensures you meet rules and can prove it during checks.

**Example of Information to Document**

1. Network layout maps showing how everything connects.
2. Device list like names and details of all network devices.
3. Settings and configurations how devices are up and work together.
4. IP addresses and access who can use what and how they get in.
5. Security plans rules and tools that keep your network safe.
6. Backups and fixes plan for when things go wrongs and how to get back on track.
7. Performance data how well things are running and what to watch out for.
8. Support contacts who to call when you need fixing things.