**Name: Chhaya Deep M**

**Assignment: Network Fundamentals and Building Networks**

**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 primary function of a router in a computer network is to forward data packets between different networks.

**2. What is the purpose of DHCP (Dynamic Host Configuration Protocol) in a computer network?**

**a) Assigning static IP addresses to devices**

**b) Resolving domain names to IP addresses**

**c) Managing network traffic and congestion**

**d) Dynamically assigning IP addresses to devices**

**Ans.** d) Dynamically assigning IP addresses to devices This allows devices to receive their IP address configurations automatically, simplifying network management and reducing the need for manual IP address assignment.

**3. Which network device operates at Layer 2 (Data Link Layer) of the OSI model and forwards data packets based on MAC addresses?**

**a) Router**

**b) Switch**

**c) Hub**

**d) Repeater**

**Ans.** b) Switch

**4. Which network topology connects all devices in a linear fashion, with each device connected to a central cable or backbone?**

**a) Star**

**b) Bus**

**c) Ring**

**d) Mesh**

**Ans**. b) Bus

**5. True or False: A VLAN (Virtual Local Area Network) allows network administrators to logically segment a single physical network into multiple virtual networks, each with its own broadcast domain.**

**Ans**. True because A VLAN allows network administrators to logically segment a single physical network into multiple virtual networks.

**6. True or False: TCP (Transmission Control Protocol) is a connectionless protocol that provides reliable, ordered, and error-checked delivery of data packets over a network.**

**Ans**. False TCP is a connection-oriented protocol, not connectionless.

**7. 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 It helps protect a network by filtering traffic and preventing unauthorized access while allowing legitimate communications.

**8. Describe the steps involved in setting up a wireless network for a small office or home office (SOHO) environment**

**Ans.**

1. **Choose the Right Equipment**

**Router Access Point:** Select a wireless router or access point that supports the desired Wi-Fi standards (e.g., Wi-Fi 5 or Wi-Fi 6) and provides sufficient coverage for the office space.

**Network Devices:** Ensure you have network devices such as computers, printers, and smartphones that are compatible with the wireless standards.

**2. Connect the Router**

**Physical Setup:** Place the router in a central location within the office to maximize coverage. Connect the router to your internet modem using an Ethernet cable, plugging one end into the router's WAN (Wide Area Network) port and the other end into the modem.

**3. Power Up and Access the Router’s Admin Interface**

**Power On:** Plug the router into a power source and turn it on.

**Connect to the Router:** Use a computer or mobile device to connect to the router’s default Wi-Fi network or use an Ethernetcable to connect directly to one of the router’s LAN ports.

**Access Admin Interface:** Open a web browser and enter the router’s IP address usually 192.168.1.1 or 192.168.0.1 to access the router’s admin interface. Log in using the default credentials.

**4. Configure Wireless Settings**

**Set SSID Network Name:** Change the default SSID to a unique and recognizable name for your network.

**Set Wi-Fi Security:** Choose a security protocol (WPA2 or WPA3) and create a strong password to secure the network. Avoid using WEP, as it is outdated and less secure.

**Select Wireless Channels:** If necessary, configure the wireless channel settings to minimize interference from other networks. Most routers have automatic settings, but manual adjustments can be made if needed.

**5. Configure Additional Settings**

**Update Firmware:** Check for and install any firmware updates to ensure the router has the latest security patches and features.

**Enable Guest Network:** If needed, set up a guest network with a separate SSID and password to provide internet access to visitors without giving them access to your main network.

**Configure DHCP:** Ensure the router’s DHCP server is enabled to automatically assign IP addresses to connected devices. Adjust the IP address range if needed.

**9. Demonstrate how to configure a router for Internet access using DHCP (Dynamic Host Configuration Protocol)**

**Ans.**

**1. Connect to the Router**

**Power On:** Plug in and power on your router.

**Physical Connection:** Connect your computer or device to the router using an Ethernet cable or wirelessly. If using Ethernet, plug one end of the cable into one of the router's LAN ports and the other end into your computer's Ethernet port.

**2. Access the Router’s Admin Interface**

**Open a Web Browser:** On your computer, open a web browser e.g., Chrome, Firefox.

**Enter Router’s IP Address:** Type the router’s default IP address into the address bar and press Enter. Common IP addresses for routers are 192.168.1.1 or 192.168.0.1. This information is typically found in the router’s manual or on a label on the router itself.

**Login:** You will be prompted to enter the router’s admin credentials. The default username and password are usually something like admin/admin or admin/password. Check the router’s documentation if these defaults do not work.

**3. Configure the WAN Settings**

**Navigate to WAN Settings:** Once logged in, look for a section related to WAN (Wide Area Network) or Internet settings. This is often found under headings like Setup, Network, Internet.

**Set Connection Type**: In the WAN settings, select “Dynamic IP” or DHCP as the connection type. This tells the router to obtain an IP address from your Internet Service Provider (ISP) automatically**.**

**Save Settings:** After selecting DHCP, save or apply the changes. The router will attempt to obtain an IP address from the ISP.

**4. Configure Wireless Settings**

**Access Wireless Settings:** Go to the Wireless or Wi-Fi settings section.

**Set SSID:** Change network name to something unique and recognizable.

**5. Verify Internet Connectivity**

1. **Check Router Status**: Look for a status or overview page in the router’s admin interface that shows the connection status. It should indicate whether the router is successfully connected to the internet.
2. **Test Connectivity:** On your computer or device, open a web browser and try to visit a website. If the page loads successfully, the router is correctly configured for Internet access.
3. **Troubleshoot if Necessary: If you cannot access the internet, check the following:**

Ensure the modem is connected and powered on.

Verify that the Ethernet cable between the modem and the router’s WAN port is securely connected.

Reboot the router and modem if necessary.

**6. Update Router Firmware**

Check for Updates: In the router’s admin interface, look for a section related to firmware updates, often found under Administration or System.

Download and Install: Follow the instructions to check for and install any available firmware updates. This ensures that the router has the latest security patches and features.

**7. Secure the Router**

**Change Default Admin Password:** Go to the admin settings and change the default router admin password to something secure.

**Review Security Settings:** Make sure the wireless network is secured with WPA2/WPA3 encryption and that the SSID is not broadcasting the network name if desired.

**10. Discuss the importance of network documentation in the context of building and managing networks**

**Ans.**

**The Importance of Network Documentation in Building and Managing Networks:**

Network documentation is a critical aspect of building and managing networks, offering numerous benefits that contribute to the efficiency, security, and reliability of network infrastructure. It involves creating detailed records of network configurations, designs, components, and operational procedures. This documentation is essential for network administrators, IT professionals, and organizations to effectively manage and troubleshoot their network environments.

**1. Facilitates Network Planning and Design**

Network documentation plays a crucial role in the planning and design phase of network development. Detailed network diagrams, topology maps, and configuration documents help network engineers visualize the network layout, understand the interconnections between devices, and plan for scalability. By documenting the network architecture, including hardware components, IP addressing schemes,connection types, organizations can design networks that meet their current needs and accommodate future growth.

**2. Aids in Troubleshooting and Problem Resolution**

When network issues arise, well-maintained documentation can significantly expedite the troubleshooting process. Detailed records of network configurations, device settings, and connection paths enable IT professionals to quickly identify potential problem areas and apply targeted solutions. For example, if a network segment is experiencing connectivity issues, documentation of IP address assignments, VLAN configurations, and routing protocols can help diagnose the root cause and resolve the problem efficiently.

**3. Enhances Network Security**

Effective network documentation is vital for maintaining network security. Detailed records of network components, configurations, and access controls help in monitoring and managing security risks. Documentation of firewall rules, intrusion detection systems, and security policies ensures that security measures are consistently applied and easily reviewed. Additionally, keeping track of network changes and updates through documentation helps in identifying potential security vulnerabilities and implementing appropriate countermeasures.

**4. Supports Compliance and Auditing**

Many industries are subject to regulatory requirements and compliance standards that mandate proper documentation of network systems and processes. Network documentation provides a comprehensive record of network configurations, security controls, and operational procedures, which is essential for audits and compliance checks. It ensures that organizations can demonstrateadherence to regulatory requirementsand industry best practices, helping to avoid penalties and maintain trust with stakeholders.

**5. Streamlines Network Management and Maintenance**

Network documentation simplifies ongoing network management and maintenance tasks. Having accurate records of network configurations, device inventories, and maintenance schedules allows IT teams to manage changes, upgrades, and repairs more effectively. For instance, when replacing or upgrading network hardware, documentation of the existing setup ensures that new components are integrated seamlessly, minimizing disruptions and maintaining network stability.

**6. Facilitates Knowledge Transfer and Training**

Network documentation serves as a valuable resource for knowledge transfer and training within an organization. Comprehensive documentation provides new team members with essential information about network configurations, operational procedures, and troubleshooting techniques. It helps ensure that institutional knowledge is preserved and transferred effectively, reducing the learning curve for new staff and maintaining continuity in network management.

**7. Improves Disaster Recovery and Business Continuity**

In the event of a network failure or disaster, having detailed documentation is crucial for effective disaster recovery and business continuity. Documentation of network topologies, configurations, and backup procedures enables IT teams to quickly restore network operations and recover lost data. By having a clear plan and documented procedures, organizations can minimize downtime, protect critical assets, and ensure that business operations can continue smoothly in the face of unexpected events.