**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 control

Ans: c) Forwarding data packets between networks

1. 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

1. 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

1. 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 (File Transfer Protocol)

**Section 2: True or False**

1. 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

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

**Ans:** False

DHCP (Dynamic Host Configuration Protocol) assigns dynamic IP addresses to network devices automatically, not static IP addresses.

* Dynamic IP addresses change periodically and are assigned by a DHCP server.
* Static IP addresses are manually configured and remain fixed.

1. 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**

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

| **Feature** | **Hub** | **Switch** |
| --- | --- | --- |
| **Functionality** | Broadcasts data to all devices | Forwards data only to the intended device |
| **Network Traffic** | Higher congestion due to broadcasting | Lower congestion as data is sent only to the recipient |
| **Bandwidth** | Shared among all devices | Dedicated bandwidth per device |
| **Collision Domain** | Single collision domain (more collisions) | Separate collision domain for each device (fewer collisions) |
| **Layer of Operation** | Works at Layer1 (Physical Layer) | Works at Layer 2 (Data Link Layer); Layer 3 switches can perform routing |
| **Speed & Performance** | Slower due to repeated transmission | Faster due to efficient data forwarding |
| **Usage** | Suitable for small, simple networks | Preferred for larger, performance-focused networks |

1. Describe the process of troubleshooting network connectivity issues.

Network Connectivity Troubleshooting Process

Troubleshooting network connectivity involves a systematic approach to identify and resolve issues. Below are the key steps:

**1. Identify the Problem**

* Gather information about the issue:
  + Is the problem affecting one device or multiple devices?
  + Is it a wired or wireless connection issue?
  + When did the issue start?

**2. Check Physical Connections**

* Ensure network cables are properly plugged in and not damaged.
* Verify that the router, switch, and modem have power and are functioning.
* Check for loose or disconnected Ethernet cables for wired connections.
* For wireless connections, ensure Wi-Fi is enabled on the device.

**3. Verify IP Configuration**

* Use the command prompt to check network settings:
  + Windows: ipconfig /all
  + Linux/Mac: ifconfig or ip a
* Ensure the device has a valid IP address from the DHCP server.
* If using a static IP, confirm it is correctly assigned.

**4. Test Network Connectivity**

* Ping the local router/gateway: ping 192.168.1.1 (or router IP).
* Ping an external website: ping google.com
  + If the local ping works but the external fails, there may be an internet issue.

**5. Restart Network Devices**

* Restart the computer, router, switch, and modem to refresh connections.
* Power cycle the modem and router:
  + Unplug for 30 seconds, then plug back in.

**6. Check DNS Configuration**

* If websites don’t load but the internet is working:
  + Try changing the DNS server to Google’s DNS (8.8.8.8 and 8.8.4.4).

**7. Disable Firewall/Antivirus Temporarily**

* Sometimes firewalls or security software block network connections.
* Disable them briefly and test the connection.

**8. Test with Another Device**

* If other devices connect successfully, the issue is with the specific device.
* If multiple devices fail, the issue is likely with the network/router/modem.

**9. Contact the ISP (If Needed)**

* If external connectivity issues persist, check if there is an ISP outage.
* Contact the Internet Service Provider (ISP) for further assistance.

**10. Advanced Troubleshooting (If Needed)**

* Check router logs for errors.
* Update network drivers on the computer.
* Reset the router to factory settings if nothing works.

**Section 4: Practical Application**

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

**How to Secure Your Wireless Router**

1. **Log in to Your Router**
   * Open a web browser and enter 192.168.1.1 or 192.168.0.1.
   * Enter the router’s username and password (found on the router label).
2. **Change the Default Admin Password**
   * Set a strong password to prevent hackers from accessing your router.
3. **Use Strong Wi-Fi Encryption (WPA3 or WPA2)**
   * Go to Wireless Security Settings and select WPA3-Personal (or WPA2 if not available).
   * Set a strong Wi-Fi password (at least 12 characters).
4. **Hide Your Wi-Fi Name (Optional)**
   * Disable SSID broadcast so your network is not visible to outsiders.
5. **Enable MAC Address Filtering**
   * Allow only specific devices to connect by adding their MAC addresses.
6. **Reduce Wi-Fi Signal Range (If Needed)**
   * Lower the transmit power to keep the signal inside your home.
7. **Update Router Firmware**
   * Check for firmware updates in the System Settings to fix security issues.
8. **Turn Off WPS**
   * Disable Wi-Fi Protected Setup (WPS) to prevent easy hacking.
9. **Enable Firewall**
   * Turn on the router’s built-in firewall for extra protection.
10. **Set Up a Guest Network**

* Use a separate guest Wi-Fi for visitors to keep your main network safe.

1. **Disable Remote Access**

* Turn off remote administration so hackers can’t access your router from outside.

1. **Check Connected Devices Regularly**

* Monitor the list of connected devices and remove unknown ones.

By following these steps, your Wi-Fi will be much more secure.

**Section 5: Essay**

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

**Importance of Network Documentation**

Network documentation is essential for managing, troubleshooting, and securing a network. It provides a clear blueprint of the network’s structure, making it easier for IT teams to maintain and upgrade the system efficiently.

**Why Network Documentation is Important?**

1. Simplifies Troubleshooting – Helps diagnose and fix network issues quickly.
2. Enhances Security – Identifies vulnerabilities and prevents unauthorized access.
3. Aids in Network Expansion – Makes upgrades and scaling easier.
4. Reduces Downtime – Speeds up recovery after failures or cyberattacks.
5. Standardizes IT Processes – Ensures consistency in network setup and maintenance.
6. Compliance & Auditing – Helps organizations meet legal and industry regulations.

**Examples of Information to Document**

1. **Network Topology Diagram**
   * A visual map showing how devices are connected.
   * Example: A diagram of switches, routers, and servers.
2. **IP Addressing Scheme**
   * A list of assigned IP addresses, subnets, and VLANs.
   * Example: 192.168.1.10 assigned to a file server.
3. **Device Inventory**
   * Details of network hardware (routers, switches, firewalls).
   * Example: Model numbers, serial numbers, and firmware versions.
4. **Configuration Settings**
   * Backup of router and switch configurations.
   * Example: Firewall rules, access control lists (ACLs).
5. **User Access and Permissions**
   * Documentation of who has admin access to network devices.
   * Example: A list of IT staff with login credentials (secured separately).
6. **ISP and Service Provider Details**
   * Contact information for Internet Service Providers (ISP).
   * Example: ISP name, support contact, and bandwidth details.
7. **Backup and Disaster Recovery Plan**
   * Steps to restore network services after a failure.
   * Example: Backup locations for configurations and data.
8. **Security Policies**
   * Guidelines on firewall rules, password policies, and encryption methods.
   * Example: "Employees must change passwords every 90 days."
9. **Network Performance Logs**
   * Record of network uptime, latency, and bandwidth usage.
   * Example: Reports showing average download speeds.
10. **Wi-Fi Settings & SSIDs**

* List of wireless network names (SSIDs) and encryption settings.
* Example: Office\_WiFi uses WPA3 encryption.