**Assignment:**

**Assignment module 3 : Understanding and Maintenance of**

**DHRUMIT CHAUDHARY:**

**Section 1: Multiple Choice**

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

1. Assigning IP addresses to devices
2. Providing wireless connectivity to devices
3. Forwarding data packets between networks
4. Managing user authentication and access control

ANS. c) Forwarding data packets between networks

* **Explanation:**

 A router's main job is to analyze incoming data packets, determine their destination network, and then send them along the most efficient path to reach that destination.

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

1. Encrypting data transmissions for security
2. Assigning IP addresses to devices dynamically
3. Converting domain names to IP addresses
4. Routing data packets between network segments

ANS. c) Converting domain names to IP addresses

* **Explanation:**
* **Domain Name System (DNS):** Its primary function is to translate human-readable domain names ("[www.google.com](https://www.google.com/)") into machine-readable IP addresses, allowing computers to locate each other on the network.

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

1. Star
2. Bus
3. Ring
4. Mesh

ANS. a) star

* **Explanation:**

Star topology uses a central hub or switch to connect all devices. In this topology, each device is connected to the central point, and all communication passes through this central node.

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

1. HTTP
2. FTP
3. SMTP
4. POP3

ANS. b) FTP

* **Explanation:**
* **FTP (File Transfer Protocol):**This protocol is designed specifically for transferring files between computers on a network. While not inherently secure, it can be used with secure protocols like SSH to encrypt data during transfer.

**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: DHCP (Dynamic Host Configuration Protocol) assigns dynamic IP addresses to network devices automatically, not static ones. Static IP addresses are manually configured, while DHCP automates the process of assigning temporary IP addresses from a pool.

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 and a switch in a computer network.

* A network hub and a network switch both connect devices in a network, but they differ significantly in how they handle data traffic. A hub broadcasts all incoming data to every connected device, while a switch intelligently forwards data only to the intended recipient based on MAC addresses. This makes switches more efficient and preferred for modern networks.

Here's a more detailed explanation:

* Hub:
* **Physical Layer Device:**

Hubs operate at the Physical Layer of the [OSI model](https://www.google.com/search?sca_esv=c2f43ffb7082dce8&cs=0&sxsrf=AE3TifMqwJ1Hw8Tvcnqwrsdda3M0miDDbw%3A1755258618762&q=OSI+model&sa=X&ved=2ahUKEwjmrK_z34yPAxX_fjABHXf2KXkQxccNegQIHhAB&mstk=AUtExfCMLobPiVcDSUZFV1ir_js0Td1rNoruc4J3pguaDezGA7yseEuOXDVf3bnCmCZVAYwuNOipkwEnnQ8_lwFiJ63d1Vthq3FdU6iG-x0rdWtYuckStI97aoDuoR_pPYAQctA0CU41uboIw6kdf6hJqJ__bZ7BQFs-02h_HS1a8A7QO_cIKsyNJnRY8hJvhYnErSRkvLeaHZSW8YARJny8sxBXAcHkHhn6K-_F1ZleQjINabiEuLy-lVRuzKN9rjAISCV77ErTjoDs9fneTEf6LiC1aOREBHABTjPPnTKn8V914pSe0Igcp_SCWDwnw8Jwb8AdfH9PPSWeErw65SSz8fujWji5K14Zr8On784tbNwBi2ELec5mwqKRgGTxFs98-aGBGQrtsHgqkCqemfnH3qZWWDq-aW2EshiV6jatxs0&csui=3), meaning they simply transmit electrical signals.

* **Broadcasting:**

When a hub receives data on one port, it transmits that data to all other ports, regardless of the intended recipient.

* **Collision Domain:**

All devices connected to a hub share the same [collision domain](https://www.google.com/search?sca_esv=c2f43ffb7082dce8&cs=0&sxsrf=AE3TifMqwJ1Hw8Tvcnqwrsdda3M0miDDbw%3A1755258618762&q=collision+domain&sa=X&ved=2ahUKEwjmrK_z34yPAxX_fjABHXf2KXkQxccNegQIHxAB&mstk=AUtExfCMLobPiVcDSUZFV1ir_js0Td1rNoruc4J3pguaDezGA7yseEuOXDVf3bnCmCZVAYwuNOipkwEnnQ8_lwFiJ63d1Vthq3FdU6iG-x0rdWtYuckStI97aoDuoR_pPYAQctA0CU41uboIw6kdf6hJqJ__bZ7BQFs-02h_HS1a8A7QO_cIKsyNJnRY8hJvhYnErSRkvLeaHZSW8YARJny8sxBXAcHkHhn6K-_F1ZleQjINabiEuLy-lVRuzKN9rjAISCV77ErTjoDs9fneTEf6LiC1aOREBHABTjPPnTKn8V914pSe0Igcp_SCWDwnw8Jwb8AdfH9PPSWeErw65SSz8fujWji5K14Zr8On784tbNwBi2ELec5mwqKRgGTxFs98-aGBGQrtsHgqkCqemfnH3qZWWDq-aW2EshiV6jatxs0&csui=3), meaning only one device can transmit data at a time to avoid collisions.

* **Half-duplex Communication:**

Hubs typically support half-duplex communication, where devices can only send or receive data at a time.

* **Less Intelligent:**

Hubs are considered less intelligent because they don't understand network addresses or intelligently route data.

* **Example:**

Imagine a room where someone yells a message to everyone in the room, even if it's meant for only one person.

* Switch:
* **Data Link Layer Device:**

Switches operate at the Data Link Layer of the OSI model and can understand MAC addresses.

* [**MAC Address Table**](https://www.google.com/search?sca_esv=c2f43ffb7082dce8&cs=0&sxsrf=AE3TifMqwJ1Hw8Tvcnqwrsdda3M0miDDbw%3A1755258618762&q=MAC+Address+Table&sa=X&ved=2ahUKEwjmrK_z34yPAxX_fjABHXf2KXkQxccNegQIMxAB&mstk=AUtExfCMLobPiVcDSUZFV1ir_js0Td1rNoruc4J3pguaDezGA7yseEuOXDVf3bnCmCZVAYwuNOipkwEnnQ8_lwFiJ63d1Vthq3FdU6iG-x0rdWtYuckStI97aoDuoR_pPYAQctA0CU41uboIw6kdf6hJqJ__bZ7BQFs-02h_HS1a8A7QO_cIKsyNJnRY8hJvhYnErSRkvLeaHZSW8YARJny8sxBXAcHkHhn6K-_F1ZleQjINabiEuLy-lVRuzKN9rjAISCV77ErTjoDs9fneTEf6LiC1aOREBHABTjPPnTKn8V914pSe0Igcp_SCWDwnw8Jwb8AdfH9PPSWeErw65SSz8fujWji5K14Zr8On784tbNwBi2ELec5mwqKRgGTxFs98-aGBGQrtsHgqkCqemfnH3qZWWDq-aW2EshiV6jatxs0&csui=3)**:**

Switches maintain a table that maps MAC addresses to specific ports, allowing them to forward data only to the intended recipient.

* **Collision Domain:**

Switches create separate collision domains for each port, allowing multiple devices to transmit data simultaneously.

* **Full-duplex Communication:**

Switches typically support full-duplex communication, where devices can send and receive data at the same time.

* **More Intelligent:**

Switches are more intelligent than hubs because they can identify the destination device and forward data accordingly.

* **Example:**

Imagine a switchboard where calls are directed to the specific extension, rather than everyone hearing the call.

9. Describe the process of troubleshooting network connectivity issues.

* Troubleshooting network connectivity issues involves a systematic process of identifying, diagnosing, and resolving problems affecting network communication. The process typically includes checking physical connections, verifying device status, testing connectivity with tools like ping and traceroute, and potentially contacting the ISP for assistance.

Here's a more detailed breakdown:

1. Identify the Problem:

* **Gather Information:** What's not working? When did the issue start? Is it affecting one device or many?
* **Define the Scope:** Is it a local issue, a segment issue, or a global issue.

2. Develop a Theory:

* **Possible Causes:** Based on the symptoms, develop possible causes such as faulty cables, configuration errors, DNS issues, or firewall restrictions.

3. Test the Theory:

* **Use Tools:** Employ tools like ping, traceroute, ipconfig, and nslookup to verify or eliminate each possibility.
* **Check Connections:** Ensure all cables are properly plugged in and that devices are powered on.
* **Inspect Hardware:** Check for any physical issues with the network hardware.
* **Review Configurations:** Verify IP addresses, DNS settings, and other relevant configurations.
* **Check for Outages:** Contact the ISP to inquire about any potential service outages in the area.

4. Implement a Solution:

* **Reconfigure Devices:** Adjust settings or configurations on affected devices.
* **Replace Hardware:** If a hardware component is faulty, replace it.
* **Flush DNS:** Clear the DNS cache to resolve potential DNS issues.
* **Update Drivers:** Ensure all drivers are up to date.
* **Adjust Routing Rules:** Modify routing rules if necessary.

5. Verify the Fix:

* **Test the Network:**

Ensure the issue is resolved and that no new problems have been introduced.

* **Document the Process:**

Record the steps taken, the solutions implemented, and the results for future reference.

By following these steps in a logical and systematic manner, network issues can be effectively identified and resolved, restoring network connectivity and functionality.

**Section 4: Practical Application**

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

* To enhance wireless router security, prioritize strong encryption, unique passwords, and disabling WPS. Enable the router's firewall, update firmware, and consider creating a guest network for visitors. Additionally, change the default router credentials and SSID.

Detailed Steps:

* **Strong Encryption:**
  + **WPA3 (Recommended):** If your router supports it, enable WPA3 encryption. It offers the strongest security.
  + **WPA2 (Minimum):** If WPA3 isn't available, use WPA2 with AES encryption (WPA2-PSK (AES)). Avoid older protocols like WEP or WPA.
  + **Finding the Setting:** Locate the security settings within your router's configuration interface (usually under "Wireless" or "Security").
* **Unique Passwords:**
  + **Router Login:** Change the default administrator username and password for accessing the router's settings. These are different from your Wi-Fi password.
  + **Wi-Fi Password:** Create a strong, unique Wi-Fi password (at least 12 characters, with a mix of uppercase, lowercase, numbers, and symbols). Avoid using easily guessable information.
* **Disable WPS:**
  + **Vulnerability:** WPS (Wi-Fi Protected Setup) has known vulnerabilities. Disable it to prevent unauthorized access.
  + **Finding the Setting:** The WPS setting is usually found within the router's wireless or security settings.
* **Enable Firewall:**
* **Built-in Protection:** Most routers have a built-in firewall. Ensure it's enabled to block unauthorized incoming traffic.
* **Finding the Setting:** The firewall setting is typically under "Security" or "Advanced Settings" in the router's interface.
* **Update Firmware:**
  + **Security Patches:** Router manufacturers regularly release firmware updates to fix bugs and security vulnerabilities. Check for and install updates regularly.
  + **Finding the Setting:** Firmware updates are usually found under the "Administration" or "System" settings.
* **Change SSID:**
  + **Avoid Default Names:** Change the default SSID (network name) to something unique and avoid including personal information or the router model.
* **4. Guest Network:**
* **Separate Network:** If your router supports it, create a guest network for visitors. This isolates their devices from your main network.
* **5. Disable Remote Management:**
* **Security Risk:** Unless you need remote access to manage your router, disable remote management to minimize security risks.

**Section 5: Essay**

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

* Network documentation is crucial for efficient network management, troubleshooting, and security. It provides a comprehensive record of the network's design, components, configurations, and operational procedures, enabling faster issue resolution, smoother upgrades, and improved overall network health.

Importance of Network Documentation:

* **Troubleshooting:**

Detailed documentation allows for quicker identification and resolution of network issues by providing a clear understanding of the network's structure and functionality.

* **Scalability and Upgrades:**

As networks grow, documentation helps plan and execute upgrades and expansions smoothly, ensuring new devices integrate without causing disruptions.

* **Security:**

Documentation helps in identifying potential vulnerabilities and implementing security measures effectively.

* **Knowledge Transfer:**

It facilitates knowledge sharing among team members, preventing single points of failure and ensuring continuity of operations.

* **Onboarding:**

New hires can quickly learn about the network and its components through well-maintained documentation, accelerating their integration into the team.

* **Disaster Recovery:**

Documented recovery plans are essential for minimizing downtime and ensuring business continuity in case of network failures or disasters.

* **Compliance:**

Network documentation can be used to demonstrate compliance with industry regulations and standards.

Examples of Information to Document:

* **Network Topology:**

A visual representation of the network's physical and logical layout, including devices, connections, and their relationships.

* **IP Addressing Scheme:**

Documentation of IP address ranges, subnet masks, and how addresses are allocated.

* **Device Inventory:**

Detailed information about each network device, including make, model, serial number, and installed software versions.

* **Configuration Details:**

Specific configurations for routers, switches, firewalls, and other network devices.

* **Cabling Diagrams:**

Illustrations of cabling infrastructure, including cable types, lengths, and connection points.

* **Access Control Lists (ACLs):**

Documentation of network access rules and permissions.

* **Security Policies:**

Detailed security policies, including password management, encryption methods, and firewall rules.

* **Change Management Procedures:**

Documentation of how changes to the network are planned, implemented, and tested.

* **Disaster Recovery Plan:**

A comprehensive plan outlining procedures for restoring network services in case of a disaster.

* **Floor Plans and Rack Diagrams:**

Visual representations of the physical layout of network equipment in facilities and server rooms.