**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**

**Ans:** The primary function of a router is not assigning IP addresses to devices. Its primary function is to forward data packets between different networks. While routers can use protocols like DHCP to assign IP addresses, this is a secondary function to their core purpose of routing traffic.

Here's a more detailed explanation:

* **Routers connect networks:**

Routers act as a gateway between different networks, like your home network and the internet, or between different local area networks (LANs).

* **Data packet forwarding:**

When data is sent from one network to another, it's packaged into data packets. Routers examine the destination IP address within each packet and use a routing table to determine the best path for the packet to reach its destination.

* **IP address assignment (DHCP):**

Routers can use protocols like DHCP to dynamically assign IP addresses to devices within a network. This allows devices to have a unique IP address for communication within that network. However, this is a separate function from routing data packets across networks

**b)Providing wireless connectivity to devices**

**Ans:** allows devices to connect to networks and the internet without physical cables, using technologies like Wi-Fi and Bluetooth. Devices need a wireless network interface, like a Wi-Fi adapter, to connect.

1. Wireless Network Interface:

* **Network Interface Cards (NICs):**

These are essential for enabling devices to connect to wireless networks. They can be built-in or external, allowing older equipment to connect to wireless networks.

* **Wi-Fi Adapters:**

Also known as wireless network adapters, these devices allow computers or other devices to connect to wireless networks.

2. Wireless Network Technologies:

* **Wi-Fi:**

A widely used technology based on the IEEE 802.11 standards, allowing devices to connect to local area networks and the internet using radio waves.

* **Bluetooth:**

A short-range wireless technology used for connecting devices, like smartphones and headphones.

3. Connecting Devices to Wireless Networks:

* **Access Points:**

These devices allow wireless-capable devices to connect to a wired network, creating a Wi-Fi network.

* **Routers:**

These devices connect a home or small office to the internet and provide wireless connectivity to multiple devices.

* **Modem:**

Modems convert the signal from your internet provider to signals that your router can understand.

4. Securing Wireless Networks:

* **Encryption Protocols:**

Wi-Fi networks can be secured with encryption protocols, ensuring the privacy of data transmission.

* **Firewalls:**

Routers and modems often have built-in firewalls to protect your network from unauthorized access.

5. Examples of Wireless Devices:

* **Laptops and Desktops:** Can connect to Wi-Fi networks for internet access and network communication.
* **Mobile Devices (Smartphones, Tablets):** Use Wi-Fi and cellular networks for communication and internet access.
* **Printers and Other Equipment:** Can be connected to wireless networks for printing and other tasks.

In essence, wireless connectivity allows devices to communicate and access the internet without physical cables, enabling a wide range of applications and services.

**c) Forwarding data packets between networks.**

**Ans**: Data packets are forwarded between networks by using a router, which is a networking device that connects two or more packet-switched networks. Routers use routing tables to determine the best path for a packet to reach its destination. When a packet arrives at a router, it examines the destination IP address and uses its routing table to decide which interface the packet should be sent out to. This process continues until the packet reaches its intended recipient on another network.

Here's a more detailed explanation:

* **What is a router?**

A router is a device that connects different networks, such as a home network to the internet.

* **Packet Forwarding:**

Routers forward data packets by examining the destination IP address in the packet header.

* **Routing Tables:**

Routers use routing tables to store information about how to reach different networks.

* **Next-Hop:**

When a packet arrives at a router, the router uses its routing table to identify the next-hop router or interface where the packet should be sent to reach its destination.

* **Destination IP Address:**

The router uses the destination IP address to determine which network the packet should be routed to.

* **Iterative Process:**

The process of packet forwarding and routing continues until the packet reaches its final destination, which could be another router or a host.

**d) Managing user authentication and access control.**

**Ans:** Managing user authentication and access control is crucial for ensuring system security and compliance. It involves verifying user identities (authentication) and determining their permitted access to resources (access control). This process is typically handled by an Identity and Access Management (IAM) system, which includes functions like user provisioning, access review, and revocation.

**Here's a more detailed look at the process:**

**1. Authentication:**

* **Verification of Identity:**

This step ensures that the person attempting to access the system is who they claim to be.

* **Methods:**

Common authentication methods include passwords, biometrics (fingerprints, facial recognition), multi-factor authentication (MFA), and smart cards.

* **Security:**

Strong authentication is essential for preventing unauthorized access and mitigating security risks.

**2. Access Control:**

* **Authorization:**

Once a user's identity is verified, access control determines what resources they can access and what actions they can perform.

* **Permission Management:**

This involves assigning specific permissions based on user roles, group memberships, or organizational policies.

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

ACLs specify which users or groups have access to specific resources**.**

* **Principles:**

Key principles include least privilege (granting only necessary access) and multi-layered access control.

**3. User Access Management (UAM):**

* Provisioning: Adding new users to the system and granting them appropriate access.
* Deprovisioning: Revoking access when users leave or their roles change.
* Access Reviews: Regularly reviewing user access to ensure it aligns with current roles and policies.
* Compliance: UAM helps organizations maintain compliance with regulatory requirements.

**4. Identity and Access Management (IAM):**

* **Overarching Framework:**

IAM encompasses the policies, processes, and technologies used to manage digital identities and control user access.

* **Tools and Technologies:**

IAM systems often include features like single sign-on (SSO), multi-factor authentication, and privileged access management.

* **Benefits:**

IAM systems streamline access management, enhance security, and improve compliance.

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

**a) Encrypting data transmissions for security**

**Ans:** The primary purpose of the Domain Name System (DNS) in a computer network is to translate human-readable domain names (e.g., www.google.com) into IP addresses (e.g., 142.250.190.14). This translation is essential because computers use IP addresses to communicate, while humans find it easier to remember and use domain names.

**Elaboration:**

* **IP addresses are numeric:**

Computers use IP addresses (e.g., 192.168.1.1) to identify each other on a network. These addresses are difficult for humans to remember and use.

* **Domain names are easier to remember:**

Domain names (e.g., google.com) are easier for humans to remember and use than IP addresses.

* **DNS translates:**

The DNS system translates domain names into their corresponding IP addresses. This allows users to type domain names into their web browsers and access websites without needing to remember IP addresses.

* **Hierarchical structure:**

The DNS operates as a hierarchical and distributed database, with different levels of servers working together to resolve domain names.

* **Seamless website access:**

DNS ensures that users can access websites using easy-to-remember domain names, making the internet more user-friendly.

**b) Assigning IP addresses to devices dynamically.**

**Ans:** Assigning IP addresses to devices dynamically means automatically allocating a unique IP address to each device on a network as it connects, rather than having a fixed address assigned manually. This process is handled by a DHCP (Dynamic Host Configuration Protocol) server.

**How it works:**

**1. Client Request:**

When a device (client) joins a network, it sends a request to the DHCP server for an IP address.

**2. Server Response:**

The DHCP server assigns a unique IP address from its pool of available addresses to the requesting client.

**3. Lease:**

The assigned IP address is given for a specific period (lease time), after which the client must renew the address or it will be released back to the pool.

**4. Other Network Configuration:**

DHCP also provides other necessary network configuration information, such as the subnet mask and default gateway, to the client.

**Benefits:**

* **Simplified Network Management:**

DHCP eliminates the need for manual IP address assignment, saving time and reducing errors**.**

* **Dynamic IP Addresses:**

Devices can be assigned IP addresses based on their location or connection status without requiring manual reconfigurations**.**

* **Reduced IP Address Conflicts:**

DHCP ensures that each device on the network has a unique IP address, preventing conflicts.

* **Efficient Use of IP Addresses:**

IP addresses are managed and recycled effectively, maximizing their use within the network.

**c) Converting domain names to IP addresses.**

**Ans: The process of converting a domain name (like www.example.com) to an IP address (like 192.0.2.1) is handled by the Domain Name System (DNS). DNS acts as a directory for the internet, mapping domain names to their corresponding IP addresses.**

****

**Here's how it works:**

**1. User Input:**

When you type a domain name into your browser, your computer initiates a DNS query.

**2. Local DNS Server:**

Your computer first checks its local DNS cache. If the IP for that domain is already stored, it's returned.

**3. Recursive DNS Query:**

If the IP isn't in the cache, your computer sends a query to your Internet Service Provider's (ISP's) DNS server (a recursive resolver)

**4. DNS Hierarchy:**

**If the ISP's DNS server doesn't have the IP, it may need to query other DNS servers in a hierarchical structure:**

* + Root DNS Servers: These are the top-level servers, providing general information about the DNS structure.
  + Top-Level Domain (TLD) Servers: These servers handle the specific domain extensions (like .com, .org, .net).
  + Authoritative DNS Servers: These servers contain the specific IP addresses for the domain you're looking for.

**5. IP Address Retrieval:**

Once the IP address is found, it's returned to the ISP's DNS server, which then provides it to your computer.

**6. Webpage Load:**

Your browser uses the IP address to connect to the web server and load the webpage.

**d) Routing data packets between network segments.**

**Ans:** using network devices like routers to direct data packets (containing information) from a source network to a destination network.

**Here's a more detailed explanation:**

**1. Network Segments:**

* A network segment is a portion of a larger network that is logically separated from other segments. Think of it like different rooms in a house, each with its own electrical circuit.
* These segments can be based on various factors, such as physical location, security policies, or the types of users or devices they serve.

**2. Routing:**

* **Definition:**

Routing is the process of selecting the best path for data packets to travel from the source network to the destination network.

* **Mechanism:**

Routers use information like IP addresses (which uniquely identify each network segment) to determine which path a packet should take to reach its destination.

* **Importance:**

Routing ensures that data packets reach their intended destination efficiently and reliably, even if the network topology is complex.

**3. Routers:**

* **Role:**

Routers are network devices that act as the "gatekeepers" between different network segments. They examine the destination IP address of data packets and make decisions about which path to forward them.

* **Function:**

Routers facilitate the flow of data between networks, allowing devices on one network to communicate with devices on another.

**4. Example:**

* Imagine you have two network segments: one for employees' computers and another for the company's server.
* When an employee wants to access the server, their computer sends a data packet to the server's IP address.
* A router will then analyze the packet's destination IP address and forward it to the appropriate segment (the server's network).

In essence, routing is the process of directing data packets across a network to reach their destination by using the right network path, with routers playing a crucial role in this process

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

**a) Star**

**Ans:** In a star topology, all devices (nodes) are connected to a central hub or switch. The hub or switch acts as a central point through which all data passes. This setup makes it easy to manage and troubleshoot the network, but if the central hub fails, the entire network is affected.

**b) Bus**

**Bus Topology:**

* All devices are connected to a single central cable (the "bus").
* Data travels in both directions along the bus.
* If the main cable fails, the entire network goes down.
* It's simple and cheap but not very scalable.

**c) Ring**

* Devices are connected in a circular loop.
* Each device has exactly two neighbors.
* No central hub or switch.
* Data travels in one direction (or both in dual-ring topologies).

**d) Mesh**

* In a mesh topology, each device connects directly to every other device.
* No centralized hub or switch.
* Provides high redundancy and reliability.
* Used in critical systems (like military or telecommunications).

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

**Ans:**

**a) HTTP**

* Stands for HyperText Transfer Protocol.
* Used for browsing web pages, not secure by itself.
* For secure browsing, we use HTTPS, not HTTP.

**Common correct answer (not yet listed but likely in your options):**

**SFTP (SSH File Transfer Protocol)**

* Securely transfers files over SSH (Secure Shell).
* Encrypts both commands and data.
* Commonly used for secure file transfer over a network.

Other secure file transfer protocols include:

* FTPS (FTP Secure): FTP over SSL/TLS.
* SCP (Secure Copy Protocol): Also uses SSH but is more limited than SFTP.

**b) FTP**

FTP (File Transfer Protocol)

* Used for file transfer, but not secure — data (including usernames and passwords) is sent in plain text.
* It can be secured using FTPS (FTP Secure), but plain FTP is not secure**.**

**To securely transfer files, you typically use:**

* SFTP (SSH File Transfer Protocol)
* FTPS (FTP over SSL/TLS)
* SCP (Secure Copy Protocol)

Please provide options c and d, and I’ll confirm the best (correct) one. Right now, neither a) HTTP nor b) FTP is correct for secure file transfer.

**c) SMTP**

SMTP (Simple Mail Transfer Protocol)

* Used to send emails, not for file transfer.
* It can send attachments via email, but it's not a file transfer protocol.

We’re still missing option d, but based on what we have:

All options (a, b, c) are not secure file transfer protocols.

**To securely transfer files over a network, the correct answer should be:**

SFTP (SSH File Transfer Protocol)  
or  
 FTPS (FTP Secure)  
or  
 SCP (Secure Copy Protocol)

Would you mind sharing option d so I can confirm the correct choice? Right now, none of the options a–c are correct for secure file transfer.

**d) POP3**

Correct Answer (Not listed, but what should be correct):

* SFTP (SSH File Transfer Protocol)
* FTPS (FTP Secure)
* SCP (Secure Copy Protocol)

These are all secure protocols for file transfer.

**Final Answer:**

None of the options (a–d) are correct for *securely* accessing and transferring files.  
If this is a multiple-choice question and you're forced to choose the *closest*, then:

FTP is related to file transfer but it’s not secure.  
If "SFTP" or "FTPS" were an option, that would be the correct answer.

Let me know if you want a revised version of this question with the correct answer included!

**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  
Explanation: DHCP assigns dynamic IP addresses automatically. Static IP addresses are manually assigned**.**

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.**

**Ans:**  A hub is a basic networking device that connects multiple devices in a network. When it receives data from one device, it broadcasts that data to all connected devices, regardless of the destination. This can lead to network congestion and collisions.

A switch is more intelligent. It connects multiple devices but only sends data to the specific device it’s intended for, using MAC addresses to direct traffic. This reduces unnecessary data transmission and improves network efficiency.

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

**Ans:**

**Identify the problem:** Gather information from the user or device about the issue (e.g., no internet, slow connection).

**Check physical connections:** Verify cables, switches, routers, and power are properly connected and powered on.

**Verify device settings:** Check IP configuration (using ipconfig or ifconfig), ensure the device has a valid IP address.

**Test network connectivity:** Use commands like ping to check connection to the local gateway and external sites.

**Check for hardware issues:** Test with different cables or ports to rule out faulty hardware.

**Check network devices:** Verify router, modem, and firewall settings.

Restart devices: Power cycle the computer, switches, routers, or modems.

**Escalate if needed:** If the issue persists, consult network administrators or escalate to higher-level support.