Module – 5 : 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

Reason : Router connects different networks and selects the best path for forwarding data packets.

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

Reason : DHCP automatically and dynamically assigns IP address to devices, so they can communicate in network without manual configuration.

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

Reason : Switch works at Layer 2 at the OSI model and forward frames based on MAC addresses.

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

Reason : In Bus topology, all devices are connected via central cable or backbone.

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

Reason : VLAN splits one physical network into multiple logical networks, each with its own broadcast domain.

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

Reason : TCP is a connection-oriented protocol, not connectionless. It ensures reliable, ordered and error-checked delivery of data packets.

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

Reason : Firewall filters network traffic based on defined security rules, protects the network from unauthorized access.

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

Ans. **Steps :**

1) Need of wireless router and internet connection from internet service provider.
2) Plug the router into modem and turn on power.
3) Open web browser and type router's ip and log in with default credentials.
4) Give your network name(SSID) and strong password.
5) Turn off remote admin and enable firewall settings for safety.
6) Keep router in a central spot so wi-fi covers home/office fully.
7) Connect devices with wi-fi name and password.

8) Check internet speed and coverage to make sure that everything is working properly.

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

Ans. **Steps :**

1) Connect ISP modem to router's WAN port. Connect your computer to router via LAN cable or Wi-Fi.
2) Open web browser, type router's ip address, and log in with admin credentials.
3) Navigate to router's WAN or internet settings page. Choose DHCP as the connection type.
4) Save the settings and reboot router if required. This allows router get IP address automatically from ISP.
5) Go to wireless settings selection in router. Enter Wi-Fi name for your network.
6) Set a strong Wi-Fi password ans select WPA2 or WPA3 for security. Save settings.
7) Place router in central area for better coverage.
8) Connect devices to Wi-Fi using SSID and password. Test the internet access to confirm setup.

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

Ans. **Importance :**

- Network documentation gives clear view of network design and devices.
- It helps in troubleshooting problems quickly.
- Support easy upgrades and future expansion.
- Improves network security and policy management.
- Keeps configurations consistent and standardized.
- Helps new staff to understand the network easily.
- It is required for compliance and edits.