MODULE:5 NETWORK FUNDAMENTALS AND BULDING NETWORKS

SECTION:1 MULTIPLE CHOICE

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

* Forwarding data packets between networks.

1. What is the purpose of DHCP (Dynamic Host Configure Protocol) in computer network?

* Dynamically assigning IP addresses to devices.

1. Which network device operates at layers 2(Data link layer) of the OSI model and forwards data packets based on MAC addresses?

* Switch.

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

* Bus topology.

SECTION:2 TRUE OR FALSE

1. 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.

* TRUE.

1. TRUE OR FALS E: TCP (Transmission Control Protocol) is connectionless protocol that provides reliable, ordered, and error-checked delivery of data packets over a network.

* 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.

* TRUE.

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

* 1. Assess Your Needs

Determine number of devices (computers, phones, printers, etc.)

Identify coverage area and any physical obstacles like walls

Consider internet usage (video conferencing, streaming, file sharing)

* 2. Choose an Internet Service Provider (ISP)

Select a reliable ISP offering the speed and bandwidth you need.

Consider fiber, DSL, or cable options depending on availability.

* 3. Select Suitable Hardware

Modem: Connects to your ISP

router or Gateway device: Provides Wi-Fi coverage

Wireless Router Consider a mesh network if the space is large or multi-level

* 4. Connect and Configure Hardware

Connect modem to router using an Ethernet cable

Plug both into power and allow them to boot up

Use a computer or mobile device to access the router settings

* 5. Configure Network Settings

Change default login credentials for the router

Set a unique SSID (network name)

Enable Wi-Fi encryption (WPA3 or WPA2) for security

Set a strong Wi-Fi password

* 6. Optimize Network Performance

Place router in a central, elevated location

Select a less congested Wi-Fi channel

Enable QoS (Quality of Service) settings for priority tasks like VoIP or video calls

* 7. Connect Devices

Add all devices to the network using the SSID and password

Verify connectivity and internet access

* 8.Implement Network Security

Disable remote management unless necessary

Set up a guest network for visitors

Regularly update firmware on your router

Consider using a firewall and antivirus software on connected devices

* 9.Monitor and Maintain

Log into router settings periodically to monitor traffic

Keep backups of configurations

Adjust settings as network needs evolve

SECTION:4 PRACTICAL

1. Demonstrate how to configure a router for internet access using DHCP (Dynamic Host Configure Protocol).

Steps to Configure DHCP on Your Router

1. Access the Router’s Admin Page

* + Open a web browser.
  + Type your router’s IP address into the address bar and press Enter.
  + Log in using the router’s username and password (often “admin” / “admin” by default).

2. Enable DHCP

* + Navigate to the Network Settings, LAN Settings, or Administrator tab (varies by brand).
  + Look for DHCP Server settings.
  + Make sure DHCP Server is enabled.

3. Set DHCP Parameters

* + Define the IP address range (e.g., 192.168.1.100 to 192.168.1.200).
  + Set the subnet mask (usually 255.255.255.0).
  + Specify the default gateway (typically the router’s IP).
  + Add DNS servers (e.g., 8.8.8.8 and 8.8.4.4 for Google DNS).

4. Save and Reboot

* + Click Save or Apply to confirm changes.
  + Reboot the router to apply the new settings.
  + Verifying DHCP Is Working
    - Connect a device to the router.
    - Check the device’s IP settings — it should receive an IP address automatically from the router.
  + On Windows, open Command Prompt and type ipconfig to view the assigned IP.
* On macOS, go to **System Preferences > Network > Advanced > TCP/IP**.
* Pro Tip

If you want certain devices (like printers or servers) to always get the same IP, look for DHCP Reservation settings in your router’s admin page. This lets you assign a fixed IP based on the device’s MAC address.

SECTION:5 EASSAY

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

* Network documentation refers to the written records, diagrams, configurations, andprocedures that describe how a network is designed, deployed, and maintained. It includes:
* Network topology maps
* IP address allocations
* Device configurations (routers, switches, firewalls)
* Cable layouts
* Cloud architecture diagrams
* Security police and access controls
* Disaster recovery plans
* Why It Matters

1. Troubleshooting & Diagnostics

* Speeds up issue resolution by providing a clear reference.
* Reduces guesswork during outages or performance problems.
* Helps identify root causes and dependencies quickly.

2. Scalability & Planning

* Enables smooth network expansion by showing existing infrastructure.
* Helps forecast hardware/software needs and budget accordingly.
* Supports capacity planning and future upgrades.

3. Security & Compliance

* Documents access controls, firewall rules, and patch schedules.
* Essential for audits and regulatory compliance (e.g., GDPR, HIPAA).
* Helps identify vulnerabilities and enforce consistent security policies.

4. Disaster Recovery

* Provides a roadmap for restoring services after failures.
* Ensures continuity even if key personnel are unavailable.
* Minimizes downtime and data loss.

5. Team Collaboration & Onboarding

* New IT staff can get up to speed faster with clear documentation.
* Promotes consistency in operations and standard procedures.
* Reduces reliance on tribal knowledge.

6. Cost Efficiency

* Prevents unnecessary purchases by revealing existing resources.
* Avoids costly misconfigurations and downtime.
* Supports smarter vendor negotiations and upgrades.
* Best Practices
* Keep it updated: Outdated documentation is almost worse than none.
* Use visuals: Diagrams make complex systems easier to understand.
* Automate where possible: Tools can help track changes and generate reports.
* Secure access: Only authorized personnel should view sensitive documentation.
* Network documentation isn’t just paperwork — it’s the blueprint, safety net, and playbook for your entire digital ecosystem.