Assignment module 3:

Understanding and Maintenance of

Section 1: Multiple Choice

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

Ans: C) Forwarding data packets between networks

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

Ans: C) Converting domain names to IP addresses

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

Ans: A) Star Topology

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

Ans: B) FTP (file transfer protocol)

Section 2: True or False

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

Ans: FALSE

1. 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: HUB:

* Layer 1 device
* Does not recognize MAC (Media Access Control Address)
* Broadcast device, slower in operation
* Cheap device

SWITCH:

* Layer 2 device
* Recognize MAC (Media Access Control Address)
* Unicast device, faster in operation
* Expensive device

1. Describe the process of troubleshooting network connectivity issues.

Ans: Troubleshooting network connectivity issues:

1. Identify symptoms
2. Gather information (network settings, physical connections.)
3. Isolate the issue (test devices, network segmentation)
4. Analyze and test (ping, traceroute, logs)
5. Resolve the issue (apply fixes, restart devices)
6. Verify and document

Section 4: Practical Application

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

Ans: Scenario: An employee's computer cannot connect to the company network.

Step-by-Step Troubleshooting:

1. Identify symptoms: Employee reports unable to access company intranet.
2. Gather information:

- Verify network settings (IP address, DNS, gateway).

- Check physical connections (Ethernet cable, Wi-Fi).

1. Isolate the issue:

- Test connectivity on another device.

- Check network segmentation (VLANs, subnets).

1. Analyze and test:

- Ping gateway and DNS.

- Run traceroute to identify bottlenecks.

1. Resolve the issue:

- Restart router and employee's computer.

- Update network adapter drivers.

1. Verify and document:

- Confirm employee's connection.

- Document solution for future reference.

Tools used:

* Ping
* Traceroute
* Network adapter configuration
* Router restart

Skills applied:

* Network fundamentals (TCP/IP, DNS)
* Troubleshooting methodologies
* Analytical thinking
* Problem-solving

Real-world impact:

* Quick resolution minimizes productivity loss.
* Efficient troubleshooting reduces downtime.
* Documenting solutions enhances future troubleshooting.

Essav: Benefits:

1. Reduced downtime
2. Faster troubleshooting
3. Improved collaboration
4. Simplified maintenance
5. Enhanced security
6. Compliance with regulations

Examples of information to document:

Network Diagrams:

1. Physical topology
2. Logical topology
3. IP address schema
4. VLAN configurations

Device Information:

1. Router/Switch configurations
2. Firewall rules
3. Server configurations
4. Network appliance settings

Network Services:

1. DNS settings
2. DHCP configurations
3. Email server settings
4. VPN configurations

Security Information:

1. Passwords (encrypted)
2. Access control lists (ACLs)
3. Firewall rules
4. Intrusion detection/prevention systems

Change Management:

1. Change logs
2. Update history
3. Backup and recovery procedures

Troubleshooting Guides:

1. Common issues and solutions
2. Step-by-step troubleshooting procedures

Contact Information:

1. Network administrator contact details
2. Vendor support information

Documentation Tools:

1. Microsoft Visio (diagramming)
2. Confluence (collaborative documentation)
3. Excel/CSV (inventory management)
4. Wiki platforms (knowledge bases)
5. Network documentation software (e.g., Net Brain, SolarWinds)

Best Practices:

1. Regularly update documentation
2. Standardize documentation formats
3. Limit access to authorized personnel
4. Use version control
5. Automate documentation where possible

By maintaining accurate and up-to-date network documentation, organizations can ensure:

* Efficient network management
* Reduced errors
* Improved compliance
* Enhanced collaboration
* Faster troubleshooting