Module 3: Understanding and Maintenance of Networks

Section 1: Multiple Choice

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

Answer: c) Forwarding data packets between networks

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

Answer: c) Converting domain names to IP addresses

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

Answer: a) Star

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

Answer: b) FTP

Section 2: True or False

5. A firewall is a hardware or software-based security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Answer: True

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

Answer: False

7. VLANs (Virtual Local Area Networks) enable network segmentation by dividing a single physical network into multiple logical networks.

Answer: True

Section 3: Short Answer

8. Explain the difference between a hub and a switch in a computer network.

Answer:

- **Hub:** A basic network device that broadcasts data to all connected devices regardless of the destination. It operates at Layer 1 (Physical Layer) and creates a single collision domain. Hubs are inefficient as all devices share bandwidth.
- **Switch:** An intelligent device that forwards data only to the specific destination device based on MAC addresses. It operates at Layer 2 (Data Link Layer), creates

separate collision domains for each port, and provides better performance and security than hubs.

9. Describe the process of troubleshooting network connectivity issues.

Answer: The troubleshooting process typically follows these steps:

1. **Identify the Problem:** Gather information about the issue (what's not working, when it started, error messages)
2. **Check Physical Connections:** Verify cables are properly connected and network devices are powered on
3. **Verify IP Configuration:** Use commands like ipconfig (Windows) or ifconfig (Linux) to check IP address, subnet mask, and gateway
4. **Test Local Connectivity:** Ping the local machine's IP address (127.0.0.1) to verify TCP/IP stack
5. **Test Gateway Connectivity:** Ping the default gateway to ensure local network communication
6. **Test DNS:** Use nslookup or ping domain names to verify DNS resolution
7. **Test Remote Connectivity:** Ping external IP addresses or websites to check internet connectivity
8. **Check Firewall/Security Settings:** Verify no security software is blocking connections
9. **Review Network Device Configuration:** Check router, switch, or firewall settings
10. **Document and Implement Solution:** Record the problem and resolution for future reference

Section 4: Practical Application

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

Answer:

Steps to Configure Wireless Router Security:

1. **Access Router Admin Panel:**
    - Connect to the router via Ethernet or WiFi
    - Open web browser and enter router's IP address (typically 192.168.1.1 or 192.168.0.1)
    - Log in with admin credentials
2. **Change Default Admin Credentials:**

- Navigate to Administration/Management settings
- Change default username and password to strong, unique credentials

3. **Configure Wireless Security:**
   - Go to Wireless Security settings
   - Select **WPA3** or **WPA2-PSK (AES)** encryption (avoid WEP - it's insecure)
   - Create a strong WiFi password (12+ characters with mixed case, numbers, symbols)
4. **Change Default SSID:**
   - Modify the network name (SSID) to something unique
   - Disable SSID broadcast if needed (though this provides minimal security benefit)
5. **Enable Router Firewall:**
   - Turn on the built-in firewall
   - Configure to block incoming connections by default
6. **Disable WPS (WiFi Protected Setup):**
   - WPS has security vulnerabilities; disable it
7. **Enable MAC Address Filtering (Optional):**
   - Create whitelist of allowed device MAC addresses
   - Note: This can be bypassed but adds an extra layer
8. **Update Router Firmware:**
   - Check for and install latest firmware updates
   - Enable automatic updates if available
9. **Disable Remote Management:**
   - Turn off remote access unless specifically needed
10. **Change Default IP Subnet (Optional):**
    - Change from common 192.168.1.x to less common subnet
11. **Save and Apply Settings:**
    - Save all configuration changes
    - Reboot router if required

Section 5: Essay

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

Answer:

Importance of Network Documentation:

Network documentation is crucial for effective network management, troubleshooting, and security. Proper documentation serves multiple critical purposes:

1. Troubleshooting Efficiency: Well-maintained documentation significantly reduces downtime during network issues. When problems arise, technicians can quickly reference network diagrams, device configurations, and IP address schemes rather than spending hours trying to understand the network structure.

2. Knowledge Transfer: Documentation ensures that network knowledge isn't locked in one person's head. When staff members leave or are unavailable, comprehensive documentation allows others to maintain and manage the network effectively.

3. Change Management: Before making changes to the network, administrators can review documentation to understand potential impacts. After changes, updating documentation creates an audit trail of network evolution.

4. Security and Compliance: Documentation helps identify security vulnerabilities, track access controls, and demonstrate compliance with industry regulations and standards.

5. Planning and Scalability: Accurate documentation enables better planning for network expansion, upgrades, and capacity management.

Essential Information to Document:

Network Infrastructure:

- Physical and logical network topology diagrams
- Network device locations (routers, switches, firewalls, access points)
- Device make, model, serial numbers, and firmware versions
- Rack layouts and data center floor plans
- Cable types, runs, and labeling schemes

IP Address Management:

- IP address allocation schemes and subnets
- DHCP scope configurations
- DNS server information and zone files

- VLAN assignments and purposes

Configuration Details:

- Device configuration files (backed up regularly)
- Port assignments and descriptions
- Routing protocols and routing tables
- Access Control Lists (ACLs)
- Quality of Service (QoS) policies

Security Information:

- Firewall rules and policies
- VPN configurations
- Authentication systems
- Wireless security settings
- Security policies and procedures

Contact Information:

- Vendor support contact details
- Internal IT team contact information
- Service level agreements (SLAs)
- Maintenance contracts and warranty information

Procedures and Policies:

- Standard operating procedures
- Disaster recovery plans
- Backup and restoration procedures
- Change management processes
- User access policies

History and Changes:

- Change logs with dates, descriptions, and responsible parties
- Incident reports and resolutions
- Maintenance schedules
- Performance baseline data