Module 6 :- CCNA - Network Troubleshooting

Section 1: Multiple Choice

1. What is the primary purpose of a firewall in a network security infrastructure?

Ans:- Filtering and controlling network traffic

2. What type of attack involves flooding a network with excessive traffic to disrupt normal operation?

Ans:- Denial of Service (DoS)

3. Which encryption protocol is commonly used to secure wireless network communications?

Ans:- WPA (Wi-Fi Protected Access)

Section 2: True or false

True or False: Patch management is the process of regularly updating software and firmware to address security vulnerabilities and improve system performance.

Ans:- True

True or False: A network administrator should perform regular backups of critical data to prevent data loss in the event of hardware failures, disasters, or security breaches.

Ans:- True

True or False: Traceroute is a network diagnostic tool used to identify the route and measure the latency of data packets between a source and destination device.

Ans:- True

Section 3: Short Answer

8. Describe the steps involved in conducting a network vulnerability Assignment.

Ans:-

⍰ **Identify assets**
List all network devices such as routers, switches, servers, firewalls, and endpoints.

⍰ **Define scope**
Decide which systems, IP ranges, and services will be tested.

⍰ **Scan for vulnerabilities**
Use vulnerability scanning tools to detect open ports, outdated software, and misconfigurations.

⍰ **Analyze results**
Check the severity of vulnerabilities and identify potential risks.

⍰ **Remediate vulnerabilities**
Apply patches, change configurations, and strengthen security controls.

⍰ **Verify and re-test**
Re-scan the network to ensure vulnerabilities are fixed.

⍰ **Document and report**
Prepare a report with findings, risk levels, and recommendations.

Section 4: Practical Application

9. Demonstrate how to troubleshoot network connectivity issues using the ping command

Ans:-

Step 1: Check local TCP/IP stack

ping 127.0.0.1

✅ **Success** → TCP/IP is working
❌ **Failure** → Problem with OS network stack

Step 2: Check network interface (NIC)

ping <your_IP_address>

✅ Confirms the network card is functioning properly

Step 3: Check local network connectivity

ping <default_gateway_IP>

✅ Confirms connection between device and router/switch
❌ Failure indicates local network or cable issue

Step 4: Check external network connectivity

ping 8.8.8.8

✅ Internet connection is working
❌ If this fails but gateway works → ISP or routing issue

Step 5: Check DNS resolution

ping google.com

✅ Name resolves → DNS is working
❌ IP works but domain fails → DNS issue

Section 5: Essay

10. Discuss the importance of regular network maintenance and the key tasks involved in maintaining network infrastructure.

Ans:-

Introduction

Regular network maintenance is essential to ensure that a network operates **reliably, securely, and efficiently**. A well-maintained network reduces downtime, prevents security breaches, and improves overall system performance. Without regular maintenance, networks can become slow, vulnerable to attacks, and prone to unexpected failures.

Importance of Regular Network Maintenance

1. **Improves Network Reliability**
   Routine maintenance helps detect and fix issues early, reducing unexpected outages and ensuring continuous network availability.

2. **Enhances Security**
   Regular updates and monitoring protect the network from malware, hacking attempts, and security vulnerabilities.

3. **Optimizes Performance**
   Maintenance activities such as traffic analysis and configuration tuning help reduce latency, packet loss, and congestion.

4. **Prevents Data Loss**
   Regular backups and hardware health checks protect critical data from failures or disasters.

5. **Extends Hardware Life**
   Monitoring hardware conditions and replacing faulty components increases the lifespan of network devices.

Key Tasks Involved in Network Maintenance

1. **Monitoring Network Performance**
   Continuously checking bandwidth usage, latency, and error rates to detect problems early.

2. **Patch and Update Management**
   Applying firmware and software updates to fix bugs and security vulnerabilities.

3. **Backup and Recovery Management**
   Performing regular backups and testing recovery procedures.

4. **Security Management**
   Managing firewalls, access control lists (ACLs), antivirus, and intrusion detection/prevention systems.

5. **Hardware Inspection and Replacement**
   Checking cables, switches, routers, and servers for faults or aging components.

6. **Configuration Management**
   Maintaining proper documentation and backing up device configurations.

7. **Troubleshooting and Incident Response**
   Quickly identifying and resolving network issues to minimize downtime.