**Question 1:- You are working as a network administrator in a large company. Your task is to troubleshoot and resolve network issues reported by users in the organization. You have access to various network monitoring tools and command-line utilities. 1. TCP and UDP Analysis: Use a network monitoring tool to analyse the traffic on the network. Identify and classify the traffic based on whether it is using TCP or UDP. Look for any anomalies or patterns that may indicate network issues. 2. HTTP Analysis: Monitor HTTP traffic to identify any slow or failed requests. Check for any errors or timeouts that could indicate problems with web servers or network congestion. Use tools like Wireshark to capture and analyse HTTP packets. 3. HTTPS Analysis: Similar to HTTP analysis, monitor HTTPS traffic to ensure that encrypted connections are being established correctly. Check for any certificate errors or handshake failures that could indicate security issues. 4. ICMP Analysis: Use the ping command to test network connectivity to various servers and devices. Check for any packet loss or high latency, which could indicate network congestion or hardware issues.**

**Answer 1:**

As a network administrator in a large company, troubleshooting and resolving network issues is a crucial part of my role.

1.TCP and UDP Analysis: I've used Wireshark to analyse TCP and UDP packets. This helps identify anomalies and patterns that may indicate network issues. For example, high TCP retransmissions can suggest congestion or packet loss, while dropped UDP packets may indicate app or service issues.

2.HTTP Analysis: I've monitored HTTP traffic using Wireshark to detect slow or failed requests. By analysing HTTP packets, I've identified errors, timeouts, and long response times that may indicate web server or network congestion issues.

3.HTTPS Analysis: I've analysed HTTPS traffic to ensure secure connections. Using Wireshark, I've checked for certificate errors or handshake failures that could compromise data integrity or confidentiality.

4.ICMP Analysis: I've used the ping command to test network connectivity. By analysing ICMP responses, I've identified packet loss or high latency issues that may indicate congestion, hardware failures, or misconfigurations.

My Learning

Regular Monitoring: Regular network monitoring helps identify issues before they escalate.

Timely Alerts: Automated alerting systems can help address issues promptly.

Performance Evaluation: Periodic performance evaluations can identify areas for improvement.

Security-First Approach: Prioritizing security ensures the integrity of network data and communications.