Monitoring Network Traffic & Performance

Part 1: Office Roleplay Dialogue

Scenario: An IT Technician, Jake, is working with his colleague, Linda, to diagnose slow network performance in the office.

Linda: Hey Jake, some employees are complaining about slow internet speeds. Do you know what's causing it?

Jake: Let's check the network traffic. I'll start with **packet sniffing**, which allows us to capture and analyze data packets moving through the network. That should give us an idea of what's slowing things down.

Linda: That sounds useful. Is it possible that our bandwidth is being overused?

Jake: It could be. We'll measure the **throughput**, which tells us how much data is successfully transmitted over the network in a given time. If throughput is low, we might have congestion.

Linda: That makes sense. Can we prioritize certain types of traffic?

Jake: Yes, we use **QoS (Quality of Service)** settings to prioritize essential applications like video calls and business software over less important traffic, such as file downloads or social media.

Linda: That's good to know. But what if there's an unauthorized device causing the slowdown?

Jake: We can run a **port scanning** test to check which devices are connected and whether any unusual activity is happening on specific network ports.

Linda: That sounds like a great way to identify potential issues. If the slowdown is caused by an external connection, can we trace where it's coming from?

Jake: Exactly. That's where **traceroute** comes in. It maps out the path data takes from our network to its destination, helping us pinpoint delays or disruptions.

Linda: That's really helpful. Let's check the packet data and see what's going on!

Jake: Sounds like a plan! I'll start the analysis now.

Part 2: Comprehension Questions

1. What is packet sniffing used for?
(A) To capture and analyze network data packets
(B) To increase Wi-Fi signal strength
(C) To block all network traffic
(D) To physically repair network cables

2. What does throughput measure?
(A) The number of users connected to a Wi-Fi router
(B) The total number of computers in an office
(C) The strength of a firewall
(D) The amount of data successfully transmitted over a network

3. What does QoS (Quality of Service) help with?
(A) Encrypting confidential emails
(B) Prioritizing important network traffic
(C) Creating stronger passwords for employees
(D) Installing software updates automatically

4. How does traceroute help diagnose network issues?
(A) It resets a slow internet connection
(B) It automatically removes malware from a computer
(C) It maps the path data takes to its destination
(D) It increases the storage capacity of a server

Part 3: Key Vocabulary Definitions in Japanese

1. **Packet Sniffing (パケットスニッフィング)** – ネットワーク上のデータパケットを監視・解析し、トラブルシューティングやセキュリティ対策に活用する技術。
2. **Throughput (スループット)** – 一定時間内にネットワークを通じて正常に送信されるデータ量。
3. **QoS (Quality of Service) (品質保証)** – ネットワーク上の特定のトラフィックを優先し、重要な通信をスムーズにする設定。
4. **Port Scanning (ポートスキャニング)** – ネットワーク上の開いているポートを調査し、不正アクセスや脆弱性を確認するプロセス。

5. **Traceroute (トレースルート)** – データが目的地に到達する経路を追跡し、遅延や通信障害の原因を特定するツール。

Part 4: Questions & Correct Answers

1. **What is packet sniffing used for?**
   ✅ (A) To capture and analyze network data packets
2. **What does throughput measure?**
   ✅ (D) The amount of data successfully transmitted over a network
3. **What does QoS (Quality of Service) help with?**
   ✅ (B) Prioritizing important network traffic
4. **How does traceroute help diagnose network issues?**
   ✅ (C) It maps the path data takes to its destination