Troubleshooting Activity

- **Problem:** A corporate office is experiencing intermittent internet connectivity issues. Employees report frequent drops in their network connection, slow internet speeds, and problems accessing critical online applications. Some users cannot connect to the VPN, while others face inconsistent connection quality.
- **Symptoms:**
    - Users report connectivity loss every 10-15 minutes.
    - Internet speed tests show bandwidth fluctuating dramatically.
    - VPN connections are frequently dropped.
    - Network latency is high, especially during video calls and file uploads.
    - Some employees report being unable to access external websites, while internal resources seem unaffected.
- **Goal:** Work through the troubleshooting process to identify the root cause of the connectivity issues and propose a solution.

Key Details to Diagnose:

- **Router/Firewall:** Configuration or hardware issue causing packet loss or traffic filtering.
- **ISP:** Possible internet service provider outages or bandwidth throttling.
- **Wi-Fi Network:** Signal interference or channel overlap causing unstable Wi-Fi connections.
- **Network Equipment:** Overloaded network switches or outdated hardware in the office.
- **Cabling Issues:** Damaged or improperly connected Ethernet cables causing physical connectivity problems.

Expected Troubleshooting Process:

1. **Identify the Problem:**

    - Review logs from the office router, firewall, and other network equipment for any signs of packet loss, drops, or errors.
    - Run network diagnostics (ping, traceroute) to identify where packet loss or high latency occurs.
    - Check if the problem is isolated to specific users, locations (e.g., Wi-Fi vs. wired connections), or times of day.

2. **Hypothesize Possible Causes:**

    - Router or firewall misconfiguration, hardware failure, or bandwidth limitations.
    - External issues with the ISP or bandwidth throttling during peak usage times.
    - Wi-Fi signal interference from neighboring networks or devices.
    - Malfunctioning network hardware (e.g., switches or routers), cabling issues, or improper network configurations.

3. **Test Hypotheses:**

    - Run speed tests on multiple devices and compare performance over time.

- Conduct Wi-Fi signal analysis using tools like Wireshark to identify interference or channel congestion.
- Test VPN connectivity directly to identify if the issue lies with the VPN server or the local network.
- Inspect and test network cabling to identify any physical issues.

4. **Implement the Solution:**

- Reboot network hardware (router, firewall) and apply proper configurations if errors are found.
- If the issue is with the ISP, contact them to report the problem and request diagnostics.
- Adjust Wi-Fi channels to avoid interference and reduce overlap with neighboring networks.
- Replace faulty network equipment or repair/replace damaged cabling.

5. **Monitor Results:**

- After applying fixes, monitor the network using tools like NetFlow or Nagios to ensure connectivity stability.
- Test the network performance (ping, traceroute, bandwidth tests) at regular intervals to verify improvement.
- Confirm that employees can connect to the internet and VPN reliably.

6. **Document the Issue:**

- Record the root cause of the issue, the troubleshooting steps taken, and the implemented solution.
- Include lessons learned and any preventive measures to avoid future connectivity issues.