Network Troubleshooting Playbook
Procedural Documentation

Author: ***Darius Ceazar A. Luna***
Email: ***Ceazar.luna@gmail.com***
Portfolio: ***github.com/DariusLuna/IT-Support***
Date: ***November 22, 2025***

Objective

The Network Troubleshooting Playbook aims to provide a clear, procedural guide for resolving the most common network issues encountered in a help desk environment. Users frequently report problems such as Wi-Fi connection failures, slow network performance, VPN access errors, IP addressing conflicts, and missing network devices. These issues can typically be resolved quickly by following structured steps. Verifying connectivity, checking configurations, testing DNS and DHCP functions, and isolating faults at each network layer.

This playbook equips technicians with a consistent method to identify root causes and apply effective solutions, improving and ensuring reliable network access for end users.

Cannot Connect to Network

Assessment

- Identify the exact error message.
- Confirm the SSID the user is attempting to join.
- Check whether other devices can connect to that SSID.
- Verify the device's Wi-Fi is enabled and the wireless adapter is active.

Troubleshooting Procedure

1. Restart the Wi-Fi adapter.
2. Toggle Airplane Mode ON/OFF.
3. "*Forget*" the network and re-enter correct credentials.
4. Check for NIC driver updates.
5. Reboot the device.
6. Verify the access point is online, not overloaded, and broadcasting properly.
7. Move the user closer to the access point to rule out weak signal.

Slow Internet / Network Performance

Assessment

- Determine whether the issue is isolated or widespread.
- Identify which applications or services are affected.
- Run a ping test to check latency and packet loss.

Troubleshooting Procedure

1. Restart the computer and network device.
2. Check for high-bandwidth tasks (updates, downloads, cloud sync).
3. Scan for malware or unnecessary background processes.
4. Perform a speed test or check monitoring tools.
5. Review network logs for congestion.
6. If on Wi-Fi, test using Ethernet to rule out wireless issues.
7. Move the user closer to the access point.

VPN Connection Issues

Assessment

- Collect the specific VPN error message.
- Verify the user's VPN permissions/subscription are active.
- Confirm basic internet connectivity.
- Check whether the VPN server or gateway is reachable/online.

Troubleshooting Procedure

1. Verify user credentials.
2. Restart the VPN client and the device.
3. Update the VPN client to the latest version.
4. Check firewall/antivirus settings that may block VPN ports or protocols.
5. Test connectivity to the VPN server (*ping*, *traceroute*).
6. Reinstall the VPN client if damaged or misconfigured.
7. Update or regenerate VPN certificates if authentication fails.

IP Address or DHCP Problems

Assessment

- Review the device's IP address, subnet mask, and default gateway.
- Check whether the issue affects a single device or multiple devices.

Troubleshooting Procedure

1. Release and renew the IP address (*ipconfig /release*, *ipconfig /renew*).
2. Restart or disable/enable the network adapter.
3. Verify DHCP server availability and ensure there are free addresses in the pool.
4. Check for duplicate IPs or conflicts on the network.
5. Assign a temporary static IP to test connectivity and isolate DHCP issues.

Printer or Network Device Not Found

Assessment

- Determine whether the issue is isolated or widespread.
- Confirm the device is powered on, connected, and showing normal status indicators.

Troubleshooting Procedure

1. Ping the device's IP address to test reachability.
2. Ensure the device is not in sleep or low-power mode.
3. Restart the device if unresponsive.
4. Check if the device received a new DHCP address.
5. Look for firewall or port-blocking issues.
6. Reinstall or update drivers/software.
7. Confirm the device and user are on the same VLAN/subnet.

DNS Resolution Issues

Assessment

- Test accessing a site directly via IP address (to confirm DNS-specific failure).
- Ask whether multiple devices experience the same problem.

Troubleshooting Procedure

1. Flush local DNS cache (*ipconfig /flushdns* on Windows).
2. Check the device's configured DNS servers.
3. Test using a public DNS server (8.8.8.8, 1.1.1.1).
4. Restart the router or DNS server if the issue is network-wide.
5. Check for firewall rules blocking DNS traffic.

OSI Model as a Troubleshooting Framework

The OSI (Open Systems Interconnection) model serves as the foundation for the procedures in this playbook. By dividing troubleshooting into layers such as Physical, Data Link, Network, Transport, Session, Presentation, and Application, technicians can narrow down issues efficiently and avoid skipping critical diagnostic steps.

Examples of OSI-based troubleshooting:

- Physical Layer: Check cables, power, signal strength, and link lights.
- Data Link / Network Layers: Validate IP addressing, DHCP leases, VLAN assignments, routing, and ARP behavior.
- Transport / Application Layers: Test VPN connectivity, DNS resolution, authentication services, Ports, and application availability.

Using this structured, layer-by-layer method ensures consistency and improves troubleshooting accuracy.

Note

Issues that fall outside the help desk scope, such as infrastructure failures, firewall or routing changes, server-level authentication issues, or problems requiring elevated permissions must be escalated to the appropriate support, network or systems team.