Network Troubleshooting Checklist: The PureIoT Rapid Response Guide

Introduction

Network issues can halt business operations instantly. A systematic, step-by-step approach is essential for rapid diagnosis and resolution. This checklist provides a methodology for IT teams and end-users to efficiently troubleshoot common network problems.

Phase 1: Identify and Define the Problem

The first step is to gather information and define the scope of the issue.

Step	Action	Expected Outcome/Tool
1. User Report	Document the exact error message, time of failure, and the user's last action.	Clear problem statement (e.g., "Cannot access shared drive since 10:30 AM").
2. Scope Check	Is the problem affecting one user, one department, or the entire network?	Determines if the issue is local (client-side) or global (server/network-side).
3. Baseline Check	Can the user access the internet? Can they access local resources?	Isolates the problem to LAN, WAN, or a specific application/server.
4. Check Recent Changes	Has any new hardware, software, or configuration been deployed recently?	Often, the last change made is the cause of the new problem.

Phase 2: Physical and Local Checks (OSI Layer 1 & 2)

Start with the simplest, most common causes.

Step	Action	Expected Outcome/ Tool
5. Physical Connection	Check the cable connection at the device and the wall/switch. Ensure the link light is on.	Confirms Layer 1 connectivity.
6. Reboot Device	Perform a simple reboot of the affected device (PC, printer, etc.).	Clears temporary software glitches and IP conflicts.
7. Check IP Address	Run `ipconfig` (Windows) or `ifconfig` (Linux/Mac). Ensure the device has a valid IP address and subnet mask.	Confirms Layer 3 addressing.
8. Check Local Gateway	Ping the default gateway (usually the router's IP address).	Confirms connectivity to the local network.

Phase 3: Network and Server Checks (OSI Layer 3 & Above)

If the local checks pass, the issue is likely deeper in the network or server.

Step	Action	Expected Outcome/Tool
9. Ping External Site	Ping a reliable external IP address (e.g., Google's DNS: `8.8.8.8`).	Confirms Internet connectivity is working.
10. Check DNS Resolution	Ping an external domain name (e.g., `google.com`).	Confirms DNS is resolving names to IP addresses correctly.

Step	Action	Expected Outcome/Tool
11. Trace Route	Run `tracert` (Windows) or `traceroute` (Linux/Mac) to the destination.	Identifies the exact point (router/hop) where the connection is failing.
12. Check Server/Service	Verify the target server is up and the specific service (e.g., web server, file share) is running.	Confirms the application layer is functioning.

Phase 4: Advanced Diagnostics

If the problem persists, escalate to advanced tools and system logs.

- **Check Network Logs:** Review logs on the switch, router, and firewall for error messages, port flapping, or security blocks.
- **Protocol Analyzer:** Use a tool like Wireshark to capture and analyze network traffic to identify protocol errors or packet drops.
- **Configuration Review:** Compare the current configuration of network devices against the last known good configuration.

Conclusion

Following this structured checklist ensures no simple steps are missed and allows for efficient escalation. For persistent or complex issues, contact the PureIoT 24/7 support team for expert intervention.