Networking Basics & Troubleshooting – Diagnose, Resolve, and Optimize IT Networks

By Israr Ahmed

This comprehensive DriveInTech guide helps IT professionals and network administrators understand, diagnose, and fix network issues — from LAN, Wi-Fi, and DHCP conflicts to enterprise firewall, VPN, and cloud connectivity problems. Designed for both beginners and advanced users, it provides step-by-step commands, real-world examples, and expert recommendations.

Prepared by Israr Ahmed

Founder of **DriveInTech.com**

info@driveintech.com | support@driveintech.com

▶️ YouTube: @israrahmedy | 💬 WhatsApp: Israr Ahmed Technical

Table of Contents

> 💡 **Pro Tip:** Click any topic to jump directly to that section when viewing this guide in a browser before printing.

Networking Basics and Troubleshooting Overview

Understanding how to identify and fix network problems is a critical skill for IT professionals. This guide explains how to diagnose issues from local LAN to cloud, using effective tools, commands, and evidence-based troubleshooting.

1. Network Layers and Connectivity Overview

A network issue can occur at different layers — from the physical connection to applications. Start troubleshooting from the **bottom-up approach** (Physical → Network → Transport → Application).

> **Quick Example:**
> - **Physical Layer:** Damaged LAN cable, disconnected switch port.
> - **Network Layer:** Wrong IP, DHCP issue, IP conflict.
> - **Application Layer:** ERP app slow due to server maintenance.

2. Checking Basic Network Connectivity

Always verify local and external connectivity step-by-step:

> **Commands to Check Connectivity:**
> `ping 127.0.0.1` – Tests local TCP/IP stack.
> `ping 192.168.1.1` – Tests gateway or router.
> `ping google.com` – Tests Internet and DNS.
> `tracert google.com` – Traces packet path.
> `nslookup driveintech.com` – Tests DNS resolution.
> `ipconfig /all` – Shows IP, gateway, and DHCP info.

> ⚠ **Precaution:** If `ping 127.0.0.1` fails, the TCP/IP stack is corrupted. Run `netsh int ip reset` and reboot.

3. LAN and Wireless Issues

Common LAN/Wi-Fi issues may stem from physical disconnection, DHCP misconfiguration, or interference.

- Check cable or Wi-Fi connection status in **Network & Internet Settings**.
- Ensure correct **IP configuration** (`ipconfig`).
- Restart **network adapter** using `ncpa.cpl`.
- Use `netsh wlan show interfaces` for wireless signal quality.

💡 **Pro Tip:** For Wi-Fi users, check if the issue is only with one access point or all. If limited to one, try changing the channel or reconnecting manually.

4. DHCP and IP Conflict Issues

IP conflicts are one of the most common network disruptions. Two or more devices with the same IP can block access to the entire subnet.

To Identify:
- Use `arp -a` to list all active IP/MAC mappings.
- Use `ipconfig /release` then `ipconfig /renew` to request a new DHCP lease.
- Check DHCP server logs for duplicate IP assignments.

⚠️ **Precaution:** Rogue DHCP servers (e.g., unauthorized Wi-Fi routers) may assign wrong IPs. Use **Wireshark** or **Advanced IP Scanner** to identify them.

5. Firewall and Proxy Issues

Firewalls can block necessary ports or domains unintentionally. Proxy settings may also cause restricted access.

- Check Windows Firewall (`firewall.cpl`).
- Verify proxy settings under **Internet Options → Connections → LAN settings**.
- Use `netstat -an` to see active connections.

💡 **Pro Tip:** When contacting ISP or firewall admin, have screenshots of blocked IPs, timestamps, and traceroute results ready.

6. Cloud and Internet-Level Issues

Sometimes issues are beyond the local network, caused by ISP downtime or cloud outages.

- Check Downdetector or Azure Status Page.
- Ping multiple public servers: `ping 8.8.8.8`, `ping 1.1.1.1`.
- Contact ISP with traceroute, IPs, and timestamps.

💬 **Recommendation:** Maintain a shared logbook of outages with proof (ping, tracert, screenshots) for accountability.

7. Enterprise, Server, and ERP Access Issues

Enterprise apps can face access issues after maintenance or due to configuration errors.

- Check if issue affects all or specific users.
- Test internal vs VPN access.
- Review firewall or SSL updates post-maintenance.

> 💡 **Pro Tip:** If ERP becomes slow after patching, check **database connections** and **app server CPU usage** first.

8. Unwanted Devices or Unauthorized Access Points

Visitors or staff may connect personal hotspots or Wi-Fi routers, causing IP conflicts or proxy bypassing.

- Use **Advanced IP Scanner** to find unknown devices.
- Block unauthorized MAC addresses.
- Restrict guest access via VLAN or firewall segmentation.

> ⚠️ **Precaution:** Rogue access points can leak corporate data — schedule periodic Wi-Fi audits.

9. Bandwidth and Resource Utilization Issues

Applications like personal cloud backups (Google Drive, OneDrive, iCloud) can consume massive bandwidth.

- Monitor via **Task Manager** → **Performance** → **Network**.
- Use **GlassWire** or **Wireshark** for tracking.
- Restrict heavy uploads during office hours.

> 💡 **Pro Tip:** Identify top bandwidth users via router/firewall console and enforce policies.

10. Preparing Recommendations and Reporting

Each investigation should end with evidence-based recommendations.

Report Should Include:
- Issue summary
- Evidence (Logs, Ping, Screenshots)
- Root cause

- Recommendations
- Responsible team

Final Note: Consistent documentation builds trust and proves analytical troubleshooting.

11. Network Performance and Latency Diagnostics

When a connection is slow, test latency, packet loss, and routing hops to find where delays occur.

Tools:

`ping -n 20 google.com`

`tracert 8.8.8.8`

`pathping driveintech.com`

`netstat -e`

`resmon.exe` → Network tab

12. DNS Troubleshooting and Resolution Checks

Domain Name System (DNS) converts domain names into IP addresses. If DNS fails, users may have Internet but cannot reach websites by name.

Essential DNS Checks:

`ipconfig /displaydns` — View cached DNS entries.

`ipconfig /flushdns` — Clear and refresh DNS cache.

`nslookup driveintech.com` — Check domain resolution.

`netsh winsock reset` — Fix corrupted Winsock settings.

`ping 8.8.8.8` — Confirms Internet even if DNS fails.

💡 **Pro Tip:** Always test both **internal** DNS (company resolver) and **external** public DNS like `8.8.8.8` (Google) or `1.1.1.1` (Cloudflare) to isolate the problem.

⚠️ **Precaution:** Incorrect DNS forwarding in Active Directory or outdated records can cause slow logons and resource failures.

13. VPN and Remote Connectivity Issues

Remote employees depend on VPNs for secure access. Common failures include certificate expiration, split-tunnel errors, or routing conflicts.

Key Troubleshooting Steps:
• Verify VPN adapter status (`ncpa.cpl`).
• Run `route print` to check routing tables.
• Confirm DNS suffixes and IP range after connection.
• Test internal servers (ERP, mail) through VPN tunnel.

💡 **Pro Tip:** Correlate disconnect timestamps between client logs and VPN concentrator logs to identify who dropped first.

⚠️ **Precaution:** Split-tunnel VPNs can leak traffic to the Internet. Always enforce corporate DNS and routing policies.

14. Monitoring Tools and Logs for Evidence Collection

Accurate evidence is crucial for problem analysis and management reporting. Use monitoring tools to capture logs, trends, and anomalies.

Recommended Tools:
• **Event Viewer** – Tracks adapter resets and driver issues.
• **Wireshark** – Packet capture and protocol analysis.
• **GlassWire** – Bandwidth usage by application.
• **PRTG / Zabbix** – Centralized network monitoring dashboards.
• PowerShell Cmdlets: `Get-NetAdapterStatistics`, `Test-Connection`.

💡 **Pro Tip:** Export logs with filenames like `NetworkLog_2025-10-13.csv` and store in a central evidence folder for each incident.

📊 **Recommendation:** Centralize monitoring on a NAS or log-server to maintain long-term audit trails and performance history.

15. Security and Spoofing-Related Network Problems

Malicious actions like IP spoofing or ARP poisoning can silently disrupt networks or redirect traffic to rogue hosts.

Detection Methods:

- Run `arp -a` to identify unexpected MAC/IP pairs.
- Use Wireshark filter `arp.duplicate-address-detected`.
- Enable **Dynamic ARP Inspection (DAI)** on managed switches.
- Keep antivirus / EDR signatures updated.

⚠️ **Precaution:** IP spoofing may lead to session hijacking or DoS. Isolate and block suspicious MAC addresses immediately.

💡 **Pro Tip:** Schedule monthly scans using **Nmap** or **Angry IP Scanner** to detect unauthorized devices early.

16. Preventive Maintenance and Network Health Checks

Proactive care prevents future outages and improves service reliability. Create and follow a recurring maintenance plan.

Routine Checklist:

- Update switch / router firmware regularly.
- Backup configuration files monthly.
- Verify UPS uptime and battery health.
- Monitor DHCP lease pool utilization.
- Conduct Wi-Fi channel interference scans quarterly.

💡 **Pro Tip:** Automate weekly reports of ping success rate, interface errors, and link uptime using PowerShell or SNMP scripts.

✅ **Recommendation:** Keep a quarterly "Network Health Snapshot" document — management values trend-based data more than single incidents.

End of Guide — Networking Basics & Troubleshooting

Prepared by Israr Ahmed |