SkillNewton

Network Troubleshooting Checklist

A bottom-up OSI troubleshooting routine with Windows and Linux commands for cabling, VLANs, IP, DNS, ports, Wi-Fi and apps.

This checklist gives you a repeatable, bottom-up way to find network faults instead of guessing. It follows the OSI model from cables and link lights through switching, IP addressing, DNS and ports to the application, with Windows and Linux commands for each step. It is for students, help desk staff and junior network engineers. Confirm each layer works before moving up, and write down what you find as you go.

How to use it

1. **Define the problem.** Ask who is affected, what exactly fails, since when and what changed. One user or everyone is the first big clue.
2. **Work from Layer 1 upwards.** Confirm the physical link, then switching, IP, DNS, ports and finally the application, ticking off each check.
3. **Change one thing at a time.** Test after every change so you know which fix worked.
4. **Document the fix.** Record the cause, the fix and how you verified it, so the next person solves it faster.

Before you start

- ☐ Find out the scope: one user, one site or everyone
  If only one device fails, start with that device. If everyone fails, look at shared equipment or the ISP.
- ☐ Ask what changed recently
  New cables, moved desks, updates, password changes and firewall rules cause many faults.
- ☐ Reproduce the problem yourself
  Note the exact error message, time and destination name or IP address.
- ☐ Check whether a known outage exists
  Look at your ISP or cloud provider status page and internal change logs.
- ☐ Have the network diagram and IP plan to hand
  You need to know the expected VLAN, subnet, gateway and DNS servers to spot what is wrong.

Layer 1: physical

- ☐ Check the cable is firmly connected at both ends
  Reseat it at the device, wall port and patch panel.
- ☐ Check link and activity lights on the NIC and switch port
  No link light usually means a cable, port or NIC fault, or a disabled port.
- ☐ Swap the cable and try a known-good port
  This quickly separates a bad cable or port from a device problem.
- ☐ Check the interface link state and speed
  Windows: `Get-NetAdapter`. Linux: `ip link show` and `ethtool eth0` (use your interface name).

- [ ] Look for duplex mismatch or interface errors
  On a managed switch, check the port for CRC errors and that speed and duplex match the device.
- [ ] Check power to switches, routers and access points
  Including PoE budgets for phones, cameras and access points.

Layer 2: data link

- [ ] Confirm the switch port is in the correct VLAN
  A port moved to the wrong VLAN gives the device an address from the wrong subnet or none at all.
- [ ] Check the port is not shut down by port security
  Look for err-disabled or blocked status on the switch.
- [ ] Find the device MAC address
  Windows: `ipconfig /all` or `getmac`. Linux: `ip link show`.
- [ ] Check the ARP or neighbour table for the gateway
  Windows: `arp -a`. Linux: `ip neigh`. A missing or incomplete gateway entry points to a Layer 2 problem.
- [ ] Check the switch MAC address table
  Confirm the device MAC appears on the expected port and VLAN.
- [ ] Watch for loops or broadcast storms
  A sudden network-wide slowdown with all lights flashing suggests a loop; check spanning tree.

Layer 3: network

- [ ] Check the IP address, mask, gateway and DNS servers
  Windows: `ipconfig /all`. Linux: `ip a`, `ip r` and `resolvectl status`.
- [ ] Spot a 169.254.x.x address
  An APIPA or link-local address means the device got no DHCP lease. Check DHCP and Layer 2.
- [ ] Renew the DHCP lease
  Windows: `ipconfig /release` then `ipconfig /renew`. Linux with NetworkManager: `nmcli connection up <name>`.
- [ ] Ping the loopback address
  `ping 127.0.0.1` confirms the local TCP/IP stack works.
- [ ] Ping the default gateway
  Windows: `ping 192.168.1.1`. Linux: `ping -c 4 192.168.1.1`. Replace with your gateway address.
- [ ] Ping a public IP address
  For example `ping 1.1.1.1`. Success here but failure by name points to DNS.
- [ ] Trace the path to the destination
  Windows: `tracert example.com` or `pathping example.com`. Linux: `traceroute example.com`, `tracepath` or `mtr`.
- [ ] Check the routing table
  Windows: `route print`. Linux: `ip route`. Look for a missing or wrong default route, often left by a VPN.
- [ ] Remember that ICMP may be blocked
  A failed ping does not always mean the host is down; some firewalls drop ping by design.

DNS

- [ ] Resolve the name
  Windows: `nslookup example.com` or `Resolve-DnsName example.com`. Linux: `dig example.com`.

- [ ] Query a different DNS server to compare

  `nslookup example.com 8.8.8.8` or `dig @1.1.1.1 example.com`. Different answers point to your DNS server.

- [ ] Clear the local DNS cache

  Windows: `ipconfig /flushdns`. Linux with systemd-resolved: `resolvectl flush-caches`.

- [ ] Check the hosts file for overrides

  Windows: `C:\Windows\System32\drivers\etc\hosts`. Linux: `/etc/hosts`.

- [ ] Check record types and TTL

  Use `dig example.com A`, `AAAA`, `MX` or `CNAME`. Recently changed records may still be cached until the TTL expires.

Layer 4: transport and ports

- [ ] Test whether the port is reachable

  Windows PowerShell: `Test-NetConnection example.com -Port 443`. Linux: `nc -zv example.com 443`.

- [ ] Check the service is listening on the server

  Windows: `netstat -ano` or `Get-NetTCPConnection -State Listen`. Linux: `ss -tulpn`.

- [ ] Check host and network firewalls

  Windows Defender Firewall, `ufw status` or `nft list ruleset` on Linux, plus any perimeter firewall or cloud security group.

- [ ] Check the service is bound to the right address

  A service listening only on `127.0.0.1` cannot be reached from other machines.

- [ ] Look for MTU problems

  Pages that half-load over a VPN can be an MTU issue. Test with `ping -f -l 1472` (Windows) or `ping -M do -s 1472` (Linux).

Application and wireless

- [ ] Test the application directly

  `curl -I https://example.com` shows the HTTP status code and headers. Works on Linux and current Windows.

- [ ] Check certificates and proxies

  Certificate errors, wrong system time and proxy settings often look like network failures.

- [ ] Read the application and server logs

  Error logs usually name the real cause once the network is confirmed working.

- [ ] Check Wi-Fi signal and connection details

  Windows: `netsh wlan show interfaces`. Linux: `nmcli dev wifi list` or `iw dev wlan0 link`.

- [ ] Look for channel congestion and interference

  Use a Wi-Fi analyser app; prefer 5 GHz or 6 GHz bands where clients support them.

- [ ] Check the device joined the right SSID and band

  Guest networks are often isolated from internal servers and printers by design.

- [ ] Forget and rejoin the network

  This clears a saved wrong password or stale settings.

Documenting and closing

- [ ] Record symptoms, tests run and results

  Include commands and output; it saves time if the fault returns.

- [ ] Record the root cause, not just the fix

  "Port moved to guest VLAN during desk change" is more useful than "fixed port".

- [ ] Confirm with the user that the problem is solved
  Test the exact task they could not do.
- [ ] Update diagrams, IP plans and configuration backups
  Keep documentation in step with the network.
- [ ] Suggest a prevention step
  For example port labelling, monitoring alerts or a change approval process.

Online version, with the matching free guide: skillnewton.com/resources/templates/network-troubleshooting-checklist/
Learn this hands-on: Networking & Cybersecurity: Foundation & Practical Implementation – skillnewton.com/courses/networking-foundation-course/