

Introduction to Network Troubleshooting

Introduction to Network Troubleshooting

Quick-reference guide for beginners and intermediate IT professionals

1. What Is Network Troubleshooting?

Aspect	Description
Definition	Systematic process of identifying, diagnosing, and resolving problems that affect network performance, connectivity, or reliability.
Goal	Restore normal service as fast as possible while minimizing impact on users.
Scope	Covers physical media, hardware, software, configuration, security policies, and external service providers.

2. The Troubleshooting Lifecycle

1. Identify the Problem

- Gather symptoms (e.g., “cannot ping 10.0.0.5”).
- Ask “who, what, when, where, why, how”.

2. Establish a Theory of Cause

- Use the **OSI model** or **TCP/IP stack** to narrow down layers.
- List possible causes (hardware failure, misconfig, DNS issue, etc.).

3. Test the Theory

- Perform targeted checks (cable test, ping, traceroute, port scan).
- Verify whether the symptom is reproduced or eliminated.

4. Establish a Plan of Action

- Choose the most probable fix.
- Document steps, required tools, and any change-control approvals.

5. Implement the Fix

Introduction to Network Troubleshooting

- Apply configuration changes, replace hardware, update firmware, etc.
- Monitor for immediate side effects.

6. Verify Full Restoration

- Confirm that the original problem and any collateral issues are resolved.
- Run performance or connectivity tests to validate.

7. Document the Incident

- Record symptoms, cause, resolution, time spent, and preventive measures.

Tip: Follow the “**Divide and Conquer**” principle – isolate the problem to the smallest possible network segment before expanding the scope.

3. Common Troubleshooting Tools

Tool	Primary Use	Example Command / Action
Ping	Test basic IP connectivity & latency	<code>ping 192.168.1.1</code>
Traceroute / <code>tracert</code>	Map the path packets take	<code>tracert www.example.com</code>
<code>nslookup</code> / <code>dig</code>	DNS query/diagnostic	<code>dig example.com MX</code>
<code>ipconfig</code> / <code>ifconfig</code> / <code>ip a</code>	View/refresh interface settings	<code>ipconfig /renew</code>
<code>netstat</code> / <code>ss</code>	Show active connections & listening ports	<code>netstat -an</code>
Wireshark / <code>tcpdump</code>	Capture and analyze packet flows	<code>tcpdump -i eth0 -c 100</code>
Port scanner (<code>nmap</code>)	Identify open services	<code>nmap -p 22,80 10.0.0.0/24</code>
Cable tester / TDR	Verify physical media integrity	–
SNMP monitoring (e.g., PRTG, SolarWinds)	Real-time health metrics	–
Syslog / Event Viewer	Review device logs	<code>show logging</code> (Cisco)

Introduction to Network Troubleshooting

4. Layer-by-Layer Checklist (OSI Model)

Layer	Typical Issues	Quick Checks
7 – Application	Wrong URL, service down, authentication failure	Test with a web browser or telnet to the service port.
6 – Presentation	Encryption mismatches, codec problems	Verify SSL/TLS certificates, cipher suites.
5 – Session	Session timeouts,	