Network Troubleshooting Checklist

A practical incident flow: scope first, evidence next, layers as the structure.

The OSI model is useful, but it is not a ritual. Start with impact, recent change, and facts.

First Five Questions

1. Who is affected: one user, one VLAN, one site, many sites?
2. What changed: config, cable, circuit, firewall, DNS, identity, app?
3. What still works?
4. Can you reproduce the failure?
5. What is the rollback or containment option?

Evidence Before Action

- Capture timestamps.
- Save show command output.
- Record source, destination, protocol, port, and error.
- Check monitoring and logs.
- Make one change at a time.

LAYERED CHECKS

LAYER	CHECK	GOOD EVIDENCE
Physical	Link, speed, duplex, errors, light levels, cable path.	Interface counters, transceiver data, known-good cable.
Layer 2	VLAN, trunk, MAC table, STP, port security.	MAC learned in expected VLAN, trunk allows VLAN, no blocked surprises.
Layer 3	IP, mask, gateway, route, ARP/ND.	Correct route, next hop reachable, ARP/ND entry present.
Services	DNS, DHCP, NAT, firewall, TLS, app listener.	Named test, port test, logs, packet capture.

MODERN REACHABILITY TESTS

PLATFORM	USE	EXAMPLE
macOS/Linux	TCP port	`nc -vz host 443`
Windows	TCP port	`Test-NetConnection host -Port 443`
HTTP/S	App path	`curl -vk https://host/path`
TLS	Certificate and handshake	`openssl s_client -connect host:443 -servername host`
DNS	Resolver test	`dig name @resolver` or `Resolve-DnsName name -Server resolver`

Do Not Overread Counters

Giants, runts, CRCs, drops, and resets are clues, not final answers. Consider MTU, tagging, cabling, optics, NIC drivers, congestion, duplex, and capture point.

Packet Capture Rule

Capture near the source and near the destination when the path is disputed. One capture point tells you what happened there, not everywhere.

CISCO QUICK REFERENCE

```
show interfaces status
show interfaces counters errors
show vlan brief
show interfaces trunk
show spanning-tree blockedports
show mac address-table dynamic
show ip interface brief
show ip route <prefix>
show arp
show logging
```

Dangerous Debugs

Do not run `debug ip packet` in production without a tight ACL, a stop plan, and CPU monitoring. Packet captures, logs, and targeted debugs are usually safer.

Close The Loop

1. State root cause or best evidence.
2. State fix or workaround.
3. State customer impact.
4. State prevention or monitoring improvement.
5. Update the diagram or runbook.