**Layer One troubleshooting** refers to diagnosing and resolving issues at the **physical layer** of the OSI model — the foundation of all network communication. Layer One troubleshooting is the first and most fundamental step in resolving network issues.

**Layer Focus**

Layer 1 Physical Issue with Cabling

Layer 2 Data Link MAC Address Conflict, VLAN Misconfiguration

Layer 3 Network IP Address, DHCP Issues, Routing

Step 1: Visual Inspection

☐ Are cables cut, frayed, kinked, or improperly terminated?

☐ Are connectors fully inserted and clicked into place?

Step 2: Cable Testing

☐ Use a cable tester to check for:

☐ Continuity on all 8 wires ☐ Correct wiring (T568A/B) ☐ Shorts or Split Pairs

☐ Use a toner and probe to trace cables and identify endpoints

☐ Test fiber with visual fault locator or light source/power meter (if applicable)

☐ Use a PoE tester to verify power on the line (for cameras, phones, APs)

Step 3: Visual Inspections Light Checks

☐ Are link/activity LEDs on switches, NICs, or devices illuminated? GREEN

☐ No light: Potential Layer One failure

Step 4: Port Swapping

☐ Plug the same device into a known-good port/cable

Loopback and Patch Testing: Verify signal integrity.

Step 5: Known-Good Substitution

☐ Use a known-working cable, device, or laptop to test the same port

Step 6: Re-termination or Replacement

☐ If a cable fails continuity testing, cut and re-terminate or replace entirely

☐ Replace damaged patch cables or wall jacks

Hardware Handling: Racking and stacking servers, switches, routers, etc.

Port Mapping: Identifying and updating the physical port-to-device mapping.

Inventory Checks: Logging serial numbers, asset tags, and confirming part availability.

**Importance:**

Techs are essential in environments where remote administration must be augmented by physical access. Their work ensures the integrity of the physical infrastructure that supports upper-layer network services.

**Notable Characteristics:**

Operates under direction from network/system engineers.

Requires meticulous attention to detail and documentation.

Often adheres to strict change control and escalation procedures.

**Basic Network Configuration & Troubleshooting**

☐ Log into modem/router if credentials provided

☐ Confirm routing, subnet, and gateway settings

☐ Verify DNS and default route

☐ Restart modem/router if no connectivity

☐ Use Putty or console cable to access CLI if applicable

☐ Use TeamViewer or AeroAdmin to allow remote support assistance

☐ Coordinate with client support to validate circuit activation

☐ *Patch Panel and Switch Checks*

☐ *Signal/Speed Verification*

☐ *Confirm IP address is assigned (DHCP or static)*

☐ *PoE Power Verification*

☐ Confirm switch port is PoE-enabled

☐ Use PoE tester to validate proper power output (802.3af/at)

☐ If no power, test with alternate known-good PoE port or injector

☐ Inspect for bad patch cables—especially between patch panel and switch

☐ *SSID and Device Connection Checks*

☐ Confirm SSID is broadcasting (use phone/laptop to scan)

☐ Try connecting to SSID with known password

☐ Verify signal strength in intended coverage area (dBm range below)

☐ *Signal Strength (dBm) Quality*

☐ Check Signal Strength using Command: netsh wlan show interfaces

Use basic tools (e.g., WiFi Analyzer app or inSSIDer) to confirm signal presence

-30 to -50 Excellent

-51 to -65 Good

-66 to -75 Fair (troublesome)

-76 or worse Poor (likely unusable)

☐ *Interference & Channel Planning (Basic)*

☐ Use non-overlapping 2.4 GHz channels: 1, 6, or 11 only

☐ Minimize use of 2.4 GHz in dense deployments; prefer 5 GHz if supported

☐ Avoid nearby APs on same or adjacent channels—watch for co-channel interference

☐ Identify nearby sources of interference:

Bluetooth devices

Cordless phones (2.4 GHz)

Security systems