

IT SUPPORT L1

INTERVIEW STUDY WORKBOOK

A 5+ Hour, 50+ Page Practical Preparation Guide

Windows • Networking • Active Directory • Microsoft 365 • Hardware • Security • ITSM • Scenario
Troubleshooting

How to use this workbook: Study it in four passes: learn the concepts, practice the commands, walk through the scenarios out loud, then complete the mock interview without notes.

Table of Contents

#	Section
1	How to Use This Workbook / 5-Hour Plan
2	L1 Role, Mindset, Scope and Ticket Lifecycle
3	Troubleshooting Methodology and Decision Trees
4	Windows 10/11 Fundamentals and Administration
5	Windows Command-Line Toolkit
6	Networking Fundamentals
7	DNS, DHCP, TCP/IP and Connectivity Troubleshooting
8	Active Directory and Group Policy
9	Microsoft 365, Outlook, Teams and OneDrive
10	Hardware, Peripherals and Printers
11	VPN, Remote Support and Access Issues
12	Security, Phishing and Endpoint Incidents
13	ITSM, SLA, Priority, Documentation and Escalation
14	80+ L1 Troubleshooting Scenarios
15	Behavioral and Customer-Service Interview Questions
16	Rapid-Fire Technical Questions
17	Hands-On Lab Exercises
18	Final 100-Question Mock Interview
19	7-Day Revision Schedule and Final Cheat Sheets

1. How to Use This Workbook / 5-Hour Study Plan

This workbook is intentionally practical. The goal is not to turn you into an L2 administrator; it is to make you capable of handling the first-contact support problems that arrive in a corporate service desk queue, while knowing exactly when and how to escalate.

Recommended 5-hour learning path

Time	Focus	What you should be able to do
0:00-0:30	L1 role + ITSM	Explain incident/request/problem, SLA, priority, escalation and ticket hygiene.
0:30-1:20	Windows	Diagnose slow PC, login, app, update, driver, disk and profile issues.
1:20-2:10	Networking	Use IP/gateway/DNS/DHCP logic and commands to isolate connectivity problems.
2:10-2:50	AD + identity	Handle password reset, lockout, group membership, domain and GPO basics.
2:50-3:40	M365	Troubleshoot Outlook, Teams, OneDrive, MFA and mailbox access issues.
3:40-4:20	Hardware + security	Handle monitor, printer, docking, VPN, phishing and endpoint incidents.
4:20-5:00	Scenarios + mock interview	Answer out loud using structured troubleshooting and escalation language.

The L1 answer pattern to memorize

1. Confirm the exact symptom and business impact.
2. Check whether the issue affects one user, a device, a location or many users.
3. Ask what changed and when it started.
4. Start with simple, reversible checks before destructive changes.
5. Use evidence: error messages, logs, IP information, service status, task/resource usage.
6. Isolate the fault domain: device, identity, application, network, server/service or user action.
7. Apply the lowest-risk fix within your authorization.
8. Re-test the original function with the user.
9. Document what happened, what you checked and what fixed it.
10. Escalate with useful evidence when the issue is outside your scope, access or SLA.

Interview tip: Do not say "I would restart it" as your entire answer. Restarting can be a valid step, but interviewers want to see diagnosis, isolation, verification and documentation.

2. L1 Role, Mindset, Scope and Ticket Lifecycle

What an L1 analyst owns

- First-contact diagnosis and resolution for common end-user issues.
- Password/account and access requests within policy.
- Basic workstation, printer, peripheral and software troubleshooting.
- Basic network and VPN triage.
- Microsoft 365 application support.
- Remote support and user communication.
- Ticket categorization, notes, SLA tracking and escalation.
- Following security, privacy and change-control procedures.

What L1 normally should NOT do without authorization

- Disable security controls just to make a user productive.
- Make unapproved firewall, server or production changes.
- Grant privileged access based on verbal pressure.
- Delete logs, evidence or user data.
- Reset or modify accounts without identity verification.
- Apply a “known fix” that changes production configuration when the change is not approved.

Ticket lifecycle

Stage	What good looks like
Open	Accurate category, user, device, symptom, impact and time started.
Triage	Check priority/SLA and determine whether outage or high-impact incident exists.
Investigate	Record tests and findings, not just “troubleshooting done.”
Resolve	Document the root/likely cause and exact corrective action.
Verify	Confirm the original issue is resolved, ideally with user confirmation.
Close	Complete notes, knowledge article reference and closure code.
Escalate	Send evidence, scope, steps tried, errors, timestamps and requested action.

Impact vs urgency

Impact answers “how many people or how much business is affected?” Urgency answers “how quickly must this be restored?” Priority is normally calculated by the organization from those and other factors. A single executive issue is not automatically a P1; follow the documented matrix.

3. Troubleshooting Methodology and Decision Trees

The fault-domain model

Domain	Evidence to collect	Typical examples
User/identity	Username, account status, MFA, sign-in time	Locked account, expired password
Device/OS	Hostname, OS, resource usage, Event Viewer	Slow PC, driver, profile corruption
Network	IP, gateway, DNS, Wi-Fi/VPN, scope	No internet, DNS failure
Application	Version, add-ins, logs, cache/profile	Outlook/Teams crash
Service/server	Service health, scope, status page, backend dependency	M365 outage, print server issue
Data/access	File path, permissions, group membership	SharePoint/file share access

General decision tree

USER REPORT -> VERIFY SYMPTOM -> CHECK SCOPE -> CHECK RECENT CHANGE ->
ISOLATE DOMAIN -> TEST LOW-RISK HYPOTHESIS -> APPLY FIX -> VERIFY -> DOCUMENT -> ESCALATE IF NEEDED

Good questions

- What exactly happens when you try?
- What error message do you see?
- When did it last work?
- Did anything change before the issue started?
- Is anyone else affected?
- Does the issue happen on another device or network?
- Can you reproduce it now?
- Is there a deadline or business impact?
- What have you already tried?

Avoiding confirmation bias

If you suspect DNS, still prove it. If you suspect a bad cable, swap the cable and retest. Good troubleshooting is evidence driven. Interviewers often reward candidates who explain why a test is useful, not merely which command they know.

Escalation rule: Escalation is not failure. A strong L1 analyst escalates early enough to protect the SLA, but only after collecting enough evidence to make the next team faster.

4. Windows 10/11 Fundamentals and Administration

Core areas to know

- User profiles and permissions
- Task Manager and resource usage
- Device Manager and drivers
- Event Viewer
- Services
- Windows Update
- Storage/Disk Management
- Startup applications
- Safe Mode
- System Restore / recovery concepts
- Local accounts and sign-in
- Remote Desktop / Quick Assist concepts

Task Manager troubleshooting

Use CPU, Memory, Disk and Network columns to find resource pressure. A high number by itself is not always a fault: look for the process, duration, resource behavior and whether the user can reproduce the slowdown.

Symptom	What to inspect	Possible cause
CPU near 100%	Processes + duration	Runaway app, updates, indexing
Memory consistently high	Processes + committed memory	Too many apps, browser tabs, memory leak
Disk near 100% active time	Process + disk health	Updates, antivirus scan, paging, storage issue
Slow startup	Startup apps + boot time	Too many startup programs, disk pressure
Random freeze	Event Viewer + reliability history	Driver, hardware, app crash, memory/storage

Device Manager

Look for warning icons, device status and driver details. A driver problem can cause no audio, no Wi-Fi, display issues, USB failures and unstable behavior. Before removing a driver, confirm the device and have a rollback/recovery plan.

Event Viewer

Know the three high-level log families: Windows Logs > System, Windows Logs > Application, and Security. L1 does not need to memorize every Event ID; learn to correlate timestamps, source names and the user-reported symptom.

Services

Use services.msc to inspect service status, startup type and dependencies. Restarting a service should be done only when appropriate and authorized, especially on shared or production systems.

5. Windows Command-Line Toolkit

Command	What it does	Interview/use case
ipconfig /all	View IP address, gateway, DNS, DHCP state and adapter details.	First-line network evidence.
ipconfig /flushdns	Clear local DNS resolver cache.	After stale/wrong DNS resolution is suspected.
ipconfig /release	Release DHCP lease.	Useful when refreshing DHCP state; use carefully on remote connections.
ipconfig /renew	Request a new DHCP lease.	DHCP troubleshooting.
ping <host>	Test reachability using ICMP where permitted.	Separate basic connectivity from name-resolution problems.
tracert <host>	Trace route toward destination.	Routing/path investigation.
nslookup <name>	Query DNS.	Name resolution troubleshooting.
arp -a	Show ARP cache.	Local IPv4 neighbor troubleshooting.
netstat -ano	Show connections/listening ports and owning PIDs.	Basic connection/port investigation.
whoami	Show current security identity.	Identity context checks.
hostname	Show computer name.	Confirm endpoint identity.
gpupdate /force	Refresh Group Policy.	After approved policy changes or client-side policy troubleshooting.
gpresult /r	Show resulting Group Policy information.	Determine applied user/computer policy.
sfc /scannow	Check protected system files.	Windows corruption scenarios.
DISM /Online /Cleanup-Image /RestoreHealth	Repair Windows component store.	More advanced OS repair with appropriate permissions.
tasklist	List running processes.	Process triage.
taskkill /PID <pid> /F	Force terminate a process.	Only when appropriate; risk of data loss.
shutdown /r /t 0	Restart immediately.	Use only when user impact and policy allow.
systeminfo	System configuration details.	Basic endpoint inventory/troubleshooting.
powercfg /batteryreport	Generate battery report.	Laptop battery diagnostics.

How to talk about commands in an interview

Do not recite commands without purpose. Say: “I would run `ipconfig /all` to check whether the endpoint has a valid address, gateway and DNS configuration; that tells me whether I am dealing with local configuration, DHCP or name-resolution symptoms.”

PowerShell awareness

```
Get-Process
Get-Service
Get-NetIPConfiguration
Test-NetConnection example.com -Port 443
```

For L1, understanding the intent is more important than becoming a PowerShell expert. Be comfortable reading output and knowing when to escalate.

6. Networking Fundamentals

The concepts you must explain clearly

Concept	Interview explanation
IP address	Logical address assigned to an endpoint on a network.
Subnet mask/prefix	Defines which part identifies the network versus the host.
Default gateway	The router used to reach destinations outside the local subnet.
DNS	Maps names to IP addresses and supports service discovery.
DHCP	Automatically provides network configuration such as IP, gateway and DNS.
MAC address	Layer-2 hardware/network interface identifier used on local networks.
VPN	Encrypted or authenticated tunnel that extends/controls access to a network or service.
NAT	Translates address/port information between network boundaries.
TCP	Connection-oriented transport with reliability features.
UDP	Connectionless transport with lower overhead and no built-in delivery guarantee.

The three-hop connectivity test

- 1) ping <default-gateway>
- 2) ping 8.8.8.8
- 3) nslookup example.com
- 4) ping example.com (where ICMP is allowed)

Interpretation: if gateway fails, focus on local connectivity/VLAN/Wi-Fi. If gateway works but public IP fails, investigate upstream routing/firewall/VPN. If public IP works but name resolution fails, focus on DNS. Real environments may block ICMP, so use additional tests such as Test-NetConnection and an actual browser/application test.

Common ports worth memorizing

Port	Service	Why it matters to L1
22	SSH	Remote administration on Linux/network devices
25	SMTP	Mail relay
53	DNS	Name resolution
67/68	DHCP	Address assignment
80	HTTP	Web traffic
110	POP3	Mail retrieval
143	IMAP	Mail retrieval
443	HTTPS	Secure web/application traffic
445	SMB	Windows file sharing
587	SMTP submission	Authenticated mail submission
3389	RDP	Windows remote desktop
993	IMAPS	Secure IMAP
995	POP3S	Secure POP3

7. DNS, DHCP, TCP/IP and Connectivity Troubleshooting

DHCP DORA

Discover -> Offer -> Request -> Acknowledge. An L1 analyst should connect that sequence to practical symptoms: no DHCP response can leave a machine without a usable address; a bad scope or exhausted scope can affect multiple clients; a single endpoint may instead have a disabled adapter or local issue.

APIPA 169.254.x.x

A 169.254.x.x IPv4 address usually indicates that the client did not obtain a normal DHCP lease. Check adapter state, physical/Wi-Fi connectivity, VLAN/switch path, DHCP server/scope and local firewall or client configuration.

DNS troubleshooting sequence

11. Test whether the device has a valid IP/gateway.
12. Query the configured DNS server with nslookup.
13. Compare result with a known-good client if appropriate.
14. Check whether only one domain is affected or all names fail.
15. Check VPN/proxy behavior because corporate DNS may be available only on the VPN.
16. Flush the local cache only after gathering evidence; do not treat it as a magic fix.
17. Escalate if server-side records, conditional forwarding or DNS infrastructure are involved.

Wi-Fi troubleshooting

- Check whether Wi-Fi is enabled and the correct SSID is selected.
- Check signal quality and whether the issue follows the user to another location.
- Forget/rejoin the network when credential/profile corruption is plausible.
- Check DHCP address and gateway.
- Compare with another device at the same access point/location.
- Determine whether the issue is authentication, RF/signal, DHCP, DNS or upstream connectivity.

High-value interview phrase: "I would compare the failing endpoint with a known-good endpoint on the same network. That quickly tells me whether the fault is likely local to the device or shared by the network path."

8. Active Directory and Group Policy

AD building blocks

Term	Practical meaning for L1
Domain	Centralized identity and management boundary.
Domain Controller	Server providing AD authentication and directory services.
User object	Identity record containing attributes and group memberships.
Security group	Group used to assign permissions/access.
Distribution group	Primarily for email distribution rather than authorization.
OU	Container used to organize objects and target management policies.
GPO	Central policy configuration applied to users/computers.
Domain join	Associates an endpoint with the corporate domain.
Account lockout	Security state triggered by repeated failed authentication according to policy.

Password reset vs account unlock

A password reset changes the credential. An unlock changes the account lockout state. A user can have one, the other, or both problems. Always verify identity and follow the organization's reset procedure.

Group membership troubleshooting

18. Confirm the exact resource the user needs.
19. Identify the group that grants the access, using approved documentation or admin tools.
20. Check current membership.
21. Apply the approved change.
22. Allow for token/replication/policy timing as applicable.
23. Have the user sign out/in or reconnect as required.
24. Test access and document the change.

Group Policy troubleshooting

```
gpupdate /force
gpresult /r
```

If a policy is not applying, consider OU placement, security filtering, inheritance, connectivity to a domain controller, policy conflicts and whether the user/computer has refreshed policy. L1 should gather evidence before escalating rather than repeatedly running gpupdate.

9. Microsoft 365, Outlook, Teams and OneDrive

Identity stack to understand

- Microsoft Entra ID identity
- Microsoft 365 licensing
- MFA and authentication methods
- Conditional Access at a conceptual level
- Exchange Online mailbox
- Outlook desktop/mobile/web
- Teams
- OneDrive
- SharePoint

Outlook troubleshooting framework

25. Test webmail/Outlook on the web if available.
26. Check whether the issue is send, receive, sync, authentication or application-specific.
27. Check service health if multiple users are affected.
28. Check mailbox storage/quota and recipient/addressing.
29. Check rules/junk/focused inbox.
30. Check Outlook connection state and credentials.
31. Use Safe Mode for add-in isolation when appropriate.
32. Create/rebuild the Outlook profile only after gathering evidence and understanding local data impact.
33. Retest and document.

Teams troubleshooting framework

- Confirm microphone/camera permissions in Windows and Teams.
- Confirm the correct input/output device is selected.
- Test with another application such as a sound recorder when appropriate.
- Check whether the issue affects only Teams or the device generally.
- Restart Teams and sign in again if authentication/client state is suspect.
- Test Teams web to separate client-side from service/account issues.
- Check whether other users have the same symptom.

OneDrive troubleshooting

- Check sign-in/account identity.
- Check sync status and error icons.
- Check storage quota and path/file-name limitations.
- Check whether files are online-only and whether local availability is required.
- Check whether the issue is one file, a folder, the client or a service/site issue.
- Use web access to determine whether the data exists in the cloud.

MFA/SSO troubleshooting

Determine whether the user reaches the authentication prompt, whether MFA is delivered, whether the device is registered, whether the account is blocked by policy, or whether the issue occurs only from a particular network/location/device. Never ask a user to share a password or one-time verification code with support.

10. Hardware, Peripherals and Printers

Hardware isolation principles

Swap one variable at a time. For a monitor problem, test a known-good cable or known-good display. For a docking problem, bypass the dock. For a headset problem, test another USB port or device. The goal is to identify the failing component, not merely make the issue disappear.

Printer troubleshooting checklist

- Power and physical status
- Network/USB connectivity
- Printer IP/hostname
- Queue stuck or paused
- Correct default printer
- Print Spooler
- Driver
- Paper/toner and hardware status
- Server-side shared printer vs local printer

```
services.msc -> Print Spooler  
Control Panel / Settings -> Printers & scanners  
Optional: ping printer-IP (where ICMP is allowed)
```

Docking station checklist

34. Check power to dock and laptop.
35. Confirm dock connection is secure.
36. Check whether USB/network/audio/display functions all fail or only one.
37. Bypass dock to test laptop directly.
38. Try another known-good port/cable/device.
39. Check driver/firmware only according to support policy.
40. Replace dock if the fault follows the dock.

Battery and charging

- Check adapter seating and indicator LEDs.
- Try a known-good charger of correct specification.
- Check whether the laptop runs on AC without battery.
- Inspect battery health and Windows battery report.
- Look for thermal/charging errors.
- Escalate suspected battery swelling or electrical damage immediately according to safety procedures.

11. VPN, Remote Support and Access Issues

VPN fault domains

Layer	Questions
Local network	Can the user browse normally before VPN?
Client	Does the VPN app launch and show a profile?
Authentication	Does username/password/MFA succeed?
Policy	Is the device compliant/managed/authorized?
Tunnel	Does the VPN show connected?
Internal access	After connection, can the user reach required internal resources?
Service side	Are other users affected?

Remote support best practices

- Verify the user and ticket before remote control.
- Tell the user what you are about to do.
- Avoid viewing unrelated personal data.
- Do not ask for passwords or MFA codes.
- Use approved remote support tooling.
- Record meaningful observations, not personal content.
- End the session and confirm the user can continue working.

Shared drive / file share access

41. Verify the path and whether it is a Windows file share, SharePoint or other system.
42. Check whether other users can access the same path.
43. Check network/VPN connectivity.
44. Check the user's account and group membership.
45. Check whether the issue is authentication, authorization or availability.
46. Test from a known-good endpoint if possible.
47. Escalate permissions/server issues with evidence.

12. Security, Phishing and Endpoint Incidents

Core concepts

Concept	What L1 should do
Phishing	Identify, contain/report according to policy, preserve evidence, support credential reset if approved.
Malware	Follow security playbook; do not casually delete evidence.
MFA fatigue	Report suspicious repeated prompts and follow identity/security procedures.
Least privilege	Give only the access needed, with approval.
Endpoint isolation	Follow security team procedure if compromise is suspected.
Sensitive data	Minimize exposure and follow privacy rules.

Phishing response sequence

48. Ask the user what they clicked or entered, without blaming them.
49. If credentials were entered, follow the approved credential containment/reset procedure.
50. If malware or execution is suspected, follow endpoint isolation guidance.
51. Capture the email subject/sender/time and relevant indicators as allowed.
52. Report/escalate to the security team.
53. Document the user impact and actions taken.

Security red flags

- Unexpected MFA prompts
- Requests for password/OTP sharing
- Urgent requests to bypass process
- Unknown remote-control software
- Unexpected privilege changes
- Suspicious USB/storage devices
- Browser certificate/security warnings
- Repeated account lockouts with no known cause

Interview answer pattern: "I would follow the incident-response playbook, contain risk without destroying evidence, protect the user's account, document indicators and escalate to security."

13. ITSM, SLA, Priority, Documentation and Escalation

Incident / Request / Problem / Change

Type	Example	Goal
Incident	Outlook stopped working	Restore service
Service Request	Install approved software	Fulfill standard need
Problem	Recurring VPN failures caused by common root cause	Remove root cause
Change	Roll out new VPN client	Control and authorize environment change

What to write in a ticket

- User-reported symptom
- Business impact
- Affected device/application
- Start time
- Scope (one user vs many)
- Exact error text if available
- Troubleshooting steps and results
- Root cause or best-supported diagnosis
- Resolution
- User confirmation
- Escalation destination and requested next action

Bad vs good ticket note

Bad	Good
"Fixed Outlook."	"User unable to send mail from Outlook desktop; OWA worked; Safe Mode reproduced successful send; identified third-party add-in as cause; disabled add-in; Outlook desktop sent test email successfully; user confirmed."
"Network issue."	"User received 169.254.x.x; Wi-Fi connected; gateway unreachable; other users at same location unaffected; adapter reset restored DHCP lease 10.x.x.x; user confirmed internet and internal access."

Escalation template

Subject: User unable to access Finance share – high business impact
 Scope: 1 user, Finance department
 Started: 09:15
 Error: Access denied
 Checks: VPN connected; internet works; group membership verified; peer user can access
 Result: Access still denied
 Request: L2 please check server/share ACL or effective permissions

14. 80+ L1 Troubleshooting Scenarios

The following scenarios are designed to be spoken aloud in an interview. For each one, explain your logic rather than simply listing fixes. "Why did you check that?" is often the hidden follow-up question.

Scenario 1: Windows PC is slow

User report: User reports that the computer takes minutes to open applications.

Objective: Find the bottleneck and rule out simple causes.

Troubleshooting workflow

54. Ask when the slowdown began and whether it is constant or intermittent.
55. Open Task Manager and observe CPU, memory, disk and startup behavior.
56. Check disk free space and whether Windows Update or security scanning is active.
57. Check recently installed software or startup changes.
58. Review Reliability Monitor/Event Viewer for repeated application or system faults.
59. Test with a minimal workload or another user profile if permitted.

Likely diagnosis: One process or startup component is consuming resources, or the device has a broader OS/storage issue.

Resolution / corrective action

60. Stop or disable an unnecessary startup item only if approved.
61. Close or restart the offending application.
62. Free storage or schedule maintenance according to policy.
63. Escalate suspected hardware degradation, recurring crashes or OS corruption with evidence.

Verification

- User opens key applications successfully.
- CPU/memory/disk return to expected levels.
- No new errors during a short retest.

When to escalate

- Hardware health problem, disk failure suspicion, repeated blue screens, or changes requiring L2/admin permissions.

Interview-ready answer: I would first quantify the slowness using Task Manager and scope the problem to the device, user profile or application. I would make the smallest safe correction, verify performance, and document what I found.

Scenario 2: Windows computer will not boot

User report: User sees a boot error or black screen.

Objective: Separate power, display, bootloader, OS and hardware causes.

Troubleshooting workflow

64. Ask whether power LEDs/fans appear.
65. Check external display and cables if the screen is blank.
66. Disconnect nonessential USB devices.
67. Record the exact boot error/message.
68. Try approved recovery options or Safe Mode if available.
69. Check whether BitLocker/recovery prompts appear and follow the organization process.

Likely diagnosis: Possible power/display failure, boot configuration issue, OS corruption or hardware failure.

Resolution / corrective action

70. Apply approved recovery steps.
71. Use vendor diagnostics if available and authorized.

72. If disk health is suspect, avoid destructive repair and escalate.

Verification

- System boots and user reaches sign-in.
- User data and encryption status remain intact.

When to escalate

- Hardware diagnostics fail, encryption recovery is required, or repair risks data loss.

Interview-ready answer: I would identify the boot stage that fails and avoid blindly reinstalling Windows. I would protect user data and escalate if recovery actions could cause loss.

Scenario 3: Blue screen / repeated restart

User report: Machine crashes with a stop error.

Objective: Identify whether a recent driver/software/hardware change is involved.

Troubleshooting workflow

73. Capture the stop code and time.
74. Ask about recent driver, Windows Update or hardware changes.
75. Check Reliability Monitor/Event Viewer.
76. Boot Safe Mode if approved to isolate nonessential drivers.
77. Run approved hardware and memory diagnostics.

Likely diagnosis: Driver, OS, storage or hardware fault.

Resolution / corrective action

78. Roll back a known recent driver/change when approved.
79. Apply vendor/Windows updates if the issue is known and remediation is safe.
80. Escalate hardware or repeated crashes.

Verification

- System stable after reboot and normal workload.
- Crash does not recur during validation.

When to escalate

- Repeated BSODs, hardware errors, data integrity concern.

Interview-ready answer: I would capture the stop code, correlate it with recent changes and logs, then isolate software versus hardware. I would not treat repeated restarts as a simple reboot issue.

Scenario 4: Application crashes on launch

User report: One application closes immediately.

Objective: Determine whether it is app-specific, profile-specific or system-wide.

Troubleshooting workflow

81. Reproduce and capture error text.
82. Try running the app as the same user and, if permitted, a different user.
83. Check Safe Mode/clean startup or the app's repair option.
84. Check Event Viewer Application log.
85. Check whether a recent update/add-in/plugin preceded the issue.

Likely diagnosis: Corrupt app profile/configuration, incompatible add-in, missing dependency or damaged installation.

Resolution / corrective action

- 86. Repair/reset the app.
- 87. Disable problematic add-in.
- 88. Reinstall only after preserving user data/config and following policy.

Verification

- App launches and performs core task.
- User data/settings are preserved where required.

When to escalate

- Application packaging/server issue, repeated crashes, or admin-required remediation.

Interview-ready answer: I would reproduce the crash, use logs and a second-user test to separate profile issues from application-wide issues, then apply the lowest-risk fix.

Scenario 5: Disk almost full

User report: Windows warns that storage is low.

Objective: Recover space safely and determine whether growth will recur.

Troubleshooting workflow

- 89. Check free space and largest categories.
- 90. Use approved cleanup tools.
- 91. Check Downloads, temp files, recycle bin and cached data.
- 92. Determine whether corporate storage/OneDrive is involved.
- 93. Check whether update recovery files are consuming space.

Likely diagnosis: Temporary files, user data growth, application caches or insufficient capacity.

Resolution / corrective action

- 94. Remove only approved nonessential files.
- 95. Move data to approved storage if policy allows.
- 96. Escalate storage-capacity or disk-health issues.

Verification

- Space is restored above operational threshold.
- User can launch apps and updates can proceed.

When to escalate

- Disk health warning, unexplained growth, or need to delete business data.

Interview-ready answer: I would measure the space, identify what is consuming it, clean only approved data, and determine whether the problem is recurring.

Scenario 6: Windows Update fails

User report: Update repeatedly fails with an error.

Objective: Determine whether it is local, policy, storage or service-side.

Troubleshooting workflow

- 97. Capture the error code.
- 98. Check free disk space and restart state.
- 99. Check whether other users/devices have the issue.
- 100. Run the approved Windows Update troubleshooter/repair steps.
- 101. Review Windows Update logs or Event Viewer as appropriate.

Likely diagnosis: Insufficient storage, corrupted update components, policy restriction or service-side issue.

Resolution / corrective action

102. Apply approved update repair steps.
103. Retry update and reboot if required.
104. Escalate if update policy or servicing stack issues require admin action.

Verification

- Update installs successfully.
- Device returns to compliant state.

When to escalate

- Multiple devices affected, policy conflict, or repeated servicing failure.

Interview-ready answer: I would capture the error code and determine whether this is a single-device issue or a wider deployment problem before changing the endpoint.

Scenario 7: User cannot sign in to Windows

User report: User receives invalid credentials or sign-in error.

Objective: Distinguish password, account, domain, network and profile issues.

Troubleshooting workflow

105. Confirm username format and keyboard layout.
106. Verify identity and account status according to policy.
107. Check whether the device has network access when domain authentication is needed.
108. Test whether the same account works elsewhere.
109. Check whether the issue is one device or the identity service.

Likely diagnosis: Wrong/expired password, locked/disabled account, offline domain connectivity, or profile issue.

Resolution / corrective action

110. Reset/unlock account if authorized.
111. Restore network connectivity.
112. Use approved profile remediation for a damaged local profile.

Verification

- User can sign in and access required resources.

When to escalate

- Identity-service failure, domain controller issue, or profile/data-risk situation.

Interview-ready answer: I would verify identity, determine whether the account works elsewhere, check device/network conditions, and then choose between identity remediation and endpoint troubleshooting.

Scenario 8: No Wi-Fi

User report: Wireless networks do not appear or connection fails.

Objective: Separate adapter, driver, authentication, signal, DHCP and upstream causes.

Troubleshooting workflow

113. Check Wi-Fi toggle and airplane mode.
114. Check whether other SSIDs are visible.
115. Check Device Manager for adapter state.
116. Test another device at the same location.

117. Check IP/DHCP after connecting.

Likely diagnosis: Adapter/driver issue, local Wi-Fi profile, access point/RF problem or authentication failure.

Resolution / corrective action

- 118. Enable adapter, reconnect, or update/repair driver if approved.
- 119. Forget and rejoin the network when profile corruption is plausible.
- 120. Escalate if the site/AP is affected.

Verification

- Device connects and receives valid IP.
- User can reach required resources.

When to escalate

- Multiple users affected, AP/controller issue, or hardware fault.

Interview-ready answer: I would first determine whether the adapter can see networks. Then I would compare the endpoint with a known-good device to isolate client versus infrastructure.

Scenario 9: Wi-Fi connects but no internet

User report: User is connected to SSID but websites do not load.

Objective: Use gateway/DNS/path testing.

Troubleshooting workflow

- 121. Check ipconfig /all.
- 122. Ping gateway.
- 123. Test a known public IP where ICMP is permitted.
- 124. Run nslookup.
- 125. Check VPN/proxy behavior.
- 126. Compare another device on the same Wi-Fi.

Likely diagnosis: DHCP/gateway, DNS, captive portal, proxy, VPN or upstream issue.

Resolution / corrective action

- 127. Renew DHCP if justified.
- 128. Correct proxy/VPN state if policy allows.
- 129. Escalate shared network outage.

Verification

- Normal IP/gateway/DNS.
- Browser/application test succeeds.

When to escalate

- Infrastructure outage or policy-controlled network configuration.

Interview-ready answer: I would not assume "Wi-Fi" means the radio is broken; I would test the gateway, IP connectivity and DNS to isolate the failing layer.

Scenario 10: DNS name does not resolve

User report: User can reach an IP but not a hostname.

Objective: Prove a name-resolution failure.

Troubleshooting workflow

- 130. Check current DNS servers with ipconfig /all.

- 131. Run nslookup for the failing name.
- 132. Compare against a known-good host.
- 133. Check VPN/corporate DNS requirement.
- 134. Flush cache only after gathering evidence.

Likely diagnosis: DNS server, record, cache or routing-to-DNS issue.

Resolution / corrective action

- 135. Correct local DNS/VPN state if within scope.
- 136. Escalate DNS record/server issues.

Verification

- Hostname resolves and application opens.

When to escalate

- Record/service-side DNS issue or widespread DNS outage.

Interview-ready answer: The key clue is that IP connectivity works while name resolution fails, so I would focus on DNS rather than reinstalling network drivers.

Scenario 11: 169.254.x.x address

User report: Endpoint receives an APIPA address.

Objective: Determine why DHCP failed.

Troubleshooting workflow

- 137. Check adapter status.
- 138. Check cable/Wi-Fi.
- 139. Run ipconfig /renew.
- 140. Test another client on same network.
- 141. Escalate VLAN/DHCP scope issues if shared.

Likely diagnosis: DHCP response unavailable or client cannot communicate with DHCP.

Resolution / corrective action

- 142. Restore connection/adaptor state.
- 143. Renew lease.
- 144. Escalate if scope or network infrastructure is implicated.

Verification

- Valid corporate IP, gateway and DNS appear.
- User can access required network resources.

When to escalate

- DHCP server/scope or network path issue.

Interview-ready answer: A 169.254 address tells me the client did not obtain normal DHCP configuration. I would prove whether DHCP is failing only for one endpoint or for a larger scope.

Scenario 12: VPN will not connect

User report: VPN client fails before or during connection.

Objective: Separate local internet, client, authentication, policy and service causes.

Troubleshooting workflow

- 145. Confirm normal internet before VPN.

146. Capture VPN error.
147. Confirm time/date and account status.
148. Check MFA behavior.
149. Test whether other users can connect.
150. Check policy/compliance status if applicable.

Likely diagnosis: Authentication, client configuration, certificate, network or service-side problem.

Resolution / corrective action

151. Correct local client state if approved.
152. Retry with known-good connection.
153. Escalate service-side or certificate issues.

Verification

- VPN shows connected.
- Internal resource access works.

When to escalate

- Multiple users affected or privileged/certificate remediation required.

Interview-ready answer: I would first prove that basic internet works, then identify the exact VPN stage that fails: client, authentication, tunnel or internal access.

Scenario 13: Outlook will not open

User report: User clicks Outlook and it closes or hangs.

Objective: Separate client/profile/add-in/OS/service causes.

Troubleshooting workflow

154. Test Outlook Web.
155. Launch Outlook in Safe Mode when appropriate.
156. Check Task Manager for stuck Outlook process.
157. Review add-ins and Event Viewer.
158. Create/rebuild profile only after understanding local data implications.

Likely diagnosis: Add-in, profile corruption, cached state or Office installation issue.

Resolution / corrective action

159. Disable offending add-in.
160. Repair Office or rebuild profile per support policy.

Verification

- Desktop Outlook opens and syncs.
- User can send/receive.

When to escalate

- Office deployment problem or data-risk scenario.

Interview-ready answer: I would use OWA and Safe Mode to isolate service/account versus desktop-client causes before rebuilding the profile.

Scenario 14: Outlook cannot send email

User report: Mail stays in Outbox or returns an error.

Objective: Separate network, authentication, mailbox, recipient and client causes.

Troubleshooting workflow

161. Test OWA send.
162. Check Outlook connection/authentication.
163. Capture error.
164. Check mailbox capacity and recipient address.
165. Review rules/add-ins if client-only.

Likely diagnosis: Client connectivity/profile issue, mailbox restriction, recipient issue or service problem.

Resolution / corrective action

166. Resolve local client state if OWA works.
167. Escalate Exchange/service issue if OWA also fails or multiple users are affected.

Verification

- Test email reaches a controlled recipient.
- User confirms normal sending.

When to escalate

- Mailbox/service or transport issue outside L1 scope.

Interview-ready answer: OWA is a strong separator: if webmail sends successfully, I focus on the desktop client rather than Exchange transport.

Scenario 15: Outlook is not receiving mail

User report: New mail does not appear.

Objective: Check service, mailbox, client sync and filtering.

Troubleshooting workflow

168. Test OWA.
169. Check whether messages arrive in OWA.
170. Inspect junk/rules and focused inbox.
171. Check mailbox quota.
172. Check Outlook connection state.

Likely diagnosis: Client sync/filtering, mailbox issue, quota or service problem.

Resolution / corrective action

173. Correct filters or client sync.
174. Escalate if messages are absent in OWA or wider service issues exist.

Verification

- New test message appears in both web and desktop.

When to escalate

- Transport/service-side issue.

Interview-ready answer: I would first test OWA; that immediately tells me whether the problem is the mailbox/service or just the desktop client.

Scenario 16: Teams microphone not working

User report: User cannot be heard.

Objective: Separate hardware, Windows permissions and Teams device selection.

Troubleshooting workflow

175. Test microphone in Windows sound settings.
176. Check Teams selected input device.
177. Check application privacy permissions.
178. Try another USB port/headset.
179. Test Teams web if needed.

Likely diagnosis: Device, permission, driver or Teams client configuration.

Resolution / corrective action

180. Correct selected device/permissions.
181. Reconnect or replace known-bad peripheral.

Verification

- User can be heard in a test call.

When to escalate

- Device/driver issue across applications or service-side issue affecting many users.

Interview-ready answer: I would first prove the microphone works outside Teams. If it does, I would focus on Teams device selection and permissions.

Scenario 17: OneDrive not syncing

User report: Files show pending/error state.

Objective: Determine whether issue is identity, storage, path, file or client.

Troubleshooting workflow

182. Check signed-in account.
183. Check sync status/error icon.
184. Check cloud/web access.
185. Check quota.
186. Test whether one file or many files are affected.

Likely diagnosis: Sync client state, account, quota, invalid path/file name or service issue.

Resolution / corrective action

187. Restart sync client when appropriate.
188. Resolve file/path issue.
189. Escalate service/account problems.

Verification

- Test file syncs both directions as required.

When to escalate

- Widespread service issue or data integrity concern.

Interview-ready answer: I would use web access to determine whether the cloud copy exists and then isolate whether the failure is one file or the entire sync client.

Scenario 18: Account locked out

User report: User cannot sign in due to logout.

Objective: Unlock safely and identify repeated source if the logout recurs.

Troubleshooting workflow

190. Verify identity.
191. Check lockout state and recent failed attempts.
192. Unlock if authorized.
193. Ask about saved credentials, mobile devices, mapped drives, services or old passwords.
194. Monitor for recurrence.

Likely diagnosis: Repeated authentication attempts from a device or service using stale credentials, or potential compromise.

Resolution / corrective action

195. Unlock per policy.
196. If recurrence continues, isolate the source and escalate security if suspicious.

Verification

- User signs in successfully.
- No immediate repeat lockout.

When to escalate

- Repeated unexplained lockouts or suspected compromise.

Interview-ready answer: I would unlock only after identity verification and then investigate why the account may be locking again rather than repeatedly unlocking it.

Scenario 19: Need access to shared folder

User report: User gets Access Denied.

Objective: Separate network path from authorization.

Troubleshooting workflow

197. Confirm exact path.
198. Check VPN/network.
199. Check whether peers can access.
200. Verify group membership/approved entitlement.
201. Retest after approved change.

Likely diagnosis: User lacks effective permission or is using wrong path/account.

Resolution / corrective action

202. Add to approved group or correct entitlement if authorized.
203. Escalate ACL/server permission issues.

Verification

- User can open, create or modify only as intended.

When to escalate

- Server-side ACL or complex nested permissions.

Interview-ready answer: I would verify the resource and the required business entitlement, then distinguish authentication from authorization before changing access.

Scenario 20: Printer offline

User report: Shared/local printer shows offline.

Objective: Determine physical, network, queue or server cause.

Troubleshooting workflow

- 204. Check printer power/status.
- 205. Check IP/hostname for network printer.
- 206. Ping if permitted.
- 207. Check queue and default printer.
- 208. Restart Print Spooler if appropriate.
- 209. Compare another user.

Likely diagnosis: Printer powered off, network unreachable, queue/spooler, driver or print server issue.

Resolution / corrective action

- 210. Restore power/network.
- 211. Clear stuck jobs or restart spooler.
- 212. Re-add/driver repair if approved.

Verification

- Print test page.
- User test print succeeds.

When to escalate

- Printer hardware fault, print server issue, or widespread outage.

Interview-ready answer: I would isolate the printer path from the local queue: physical status, network reachability, spooler and then server/driver.

Scenario 21: Monitor shows no signal

User report: External display has power but no picture.

Objective: Isolate laptop port, cable, dock and monitor.

Troubleshooting workflow

- 213. Check input source.
- 214. Check cable seating.
- 215. Bypass dock.
- 216. Try known-good cable/monitor.
- 217. Check Windows display detection.

Likely diagnosis: Wrong input, bad cable, dock, port or display hardware.

Resolution / corrective action

- 218. Correct input/cable or reconnect dock.
- 219. Replace failed component if supported.

Verification

- Display stays stable through a test period.

When to escalate

- Hardware replacement or endpoint graphics issue.

Interview-ready answer: Swap one component at a time; the goal is to find which element the fault follows.

Scenario 22: USB headset not detected

User report: Headset does not appear.

Objective: Separate USB port, device, driver and app issues.

Troubleshooting workflow

- 220. Try another USB port.
- 221. Check Device Manager.
- 222. Check Windows Sound settings.
- 223. Test another computer/device if available.
- 224. Check application device selection.

Likely diagnosis: Port/device failure, driver issue or app selection.

Resolution / corrective action

- 225. Use known-good port/device.
- 226. Repair driver or settings if approved.

Verification

- Audio input/output works in OS and target app.

When to escalate

- Hardware fault or driver package issue.

Interview-ready answer: I would first see whether Windows detects the headset at all; if not, Teams/Zoom settings are not the first place to troubleshoot.

Scenario 23: Laptop not charging

User report: Battery percentage is not increasing.

Objective: Separate adapter, port, battery, power policy and hardware.

Troubleshooting workflow

- 227. Check charger and outlet.
- 228. Check charging indicator.
- 229. Try approved known-good adapter.
- 230. Inspect port for damage.
- 231. Check battery health/report.
- 232. Determine whether system runs on AC.

Likely diagnosis: Adapter/port/battery fault or charging subsystem issue.

Resolution / corrective action

- 233. Use known-good adapter where safe.
- 234. Escalate battery/port hardware.

Verification

- Battery charges and reports expected state.

When to escalate

- Swelling, smell, heat, physical damage -> immediate safety escalation.

Interview-ready answer: I would test the charging path safely and escalate physical battery hazards immediately rather than continuing normal troubleshooting.

Scenario 24: Browser cannot open one site

User report: Other sites work.

Objective: Determine site-specific DNS, proxy, authentication, TLS or service issue.

Troubleshooting workflow

- 235. Try private/incognito window if allowed.
- 236. Test same site in another approved browser.
- 237. Test from another network/device.
- 238. Check DNS and proxy.
- 239. Capture error message.

Likely diagnosis: Browser cache/session, DNS, proxy, certificate or site-side problem.

Resolution / corrective action

- 240. Clear site data or try alternate browser.
- 241. Escalate site-side or proxy/certificate issue.

Verification

- Target site loads and user can authenticate.

When to escalate

- Enterprise proxy/security gateway or service-side issue.

Interview-ready answer: Because other websites work, I would narrow scope to the site path rather than resetting the whole network configuration.

Scenario 25: Mapped network drive missing

User report: Drive letter no longer appears.

Objective: Determine whether mapping, authentication, VPN or policy is involved.

Troubleshooting workflow

- 242. Check VPN/network.
- 243. Check whether other users see the drive.
- 244. Test the UNC path directly.
- 245. Check current logon/session state.
- 246. Review mapped-drive policy if applicable.

Likely diagnosis: Login script/GPO, VPN, credentials or server availability.

Resolution / corrective action

- 247. Reconnect or restore policy mapping if within scope.
- 248. Escalate GPO/server issue.

Verification

- Drive appears and user can access expected data.

When to escalate

- Server outage or policy change.

Interview-ready answer: Testing the UNC path tells me whether the drive letter is the problem or the underlying share is unavailable.

Scenario 26: User cannot install software

User report: Installer requests admin or fails.

Objective: Determine whether software is approved and how it should be deployed.

Troubleshooting workflow

- 249. Identify software and business need.

- 250. Check approved software catalog/process.
- 251. Capture exact error.
- 252. Determine whether elevation/admin is required.
- 253. Check whether endpoint management blocks it.

Likely diagnosis: Policy/approval or permissions rather than a technical fault.

Resolution / corrective action

- 254. Use approved software deployment process.
- 255. Escalate packaging/admin requirement.

Verification

- Software launches and is licensed/compliant.

When to escalate

- Security/policy restriction or packaging issue.

Interview-ready answer: I would not bypass endpoint controls. I would verify approval and use the company's standard deployment process.

Scenario 27: User forgot password

User report: Cannot authenticate.

Objective: Reset safely and restore access.

Troubleshooting workflow

- 256. Perform identity verification.
- 257. Check whether account is locked/expired.
- 258. Use approved reset workflow.
- 259. Handle MFA/recovery method if needed.
- 260. Have user sign in and update credentials as required.

Likely diagnosis: Credential forgotten or expired.

Resolution / corrective action

- 261. Reset according to policy and require secure credential handling.

Verification

- User can authenticate and access required resources.

When to escalate

- Identity verification fails, MFA recovery issue, or suspicious activity.

Interview-ready answer: The critical step is secure identity verification before any credential action.

Scenario 28: MFA prompt not received

User report: User cannot complete sign-in because second factor never arrives.

Objective: Determine method/device/policy/service issue.

Troubleshooting workflow

- 262. Confirm registered authentication methods.
- 263. Check phone/app connectivity and notification settings.
- 264. Try an alternate approved method.
- 265. Check time/date and device state.
- 266. Determine whether others are affected.

Likely diagnosis: Wrong method, notification delivery, device registration, policy or service problem.

Resolution / corrective action

- 267. Use approved alternate method or re-register if authorized.
- 268. Escalate identity-service issue.

Verification

- User completes MFA and signs in.

When to escalate

- Account security concern or service-wide outage.

Interview-ready answer: I would never ask for the MFA code; I would troubleshoot the registered method or use the approved recovery process.

Scenario 29: Computer cannot join domain

User report: Join fails.

Objective: Separate DNS, credentials, naming, network and permissions.

Troubleshooting workflow

- 269. Confirm network connectivity and corporate DNS.
- 270. Confirm correct hostname/domain.
- 271. Check time synchronization.
- 272. Verify join credentials and permissions.
- 273. Capture exact error.

Likely diagnosis: DNS/domain controller reachability, time, permissions or duplicate computer object.

Resolution / corrective action

- 274. Correct local DNS/time or use approved join workflow.
- 275. Escalate AD/domain-controller issue.

Verification

- Computer object and sign-in work as expected.

When to escalate

- Domain-controller replication/service or privileged permission issue.

Interview-ready answer: Domain join is more than “put in domain name”; DNS, time, credentials and DC reachability all matter.

Scenario 30: GPO not applying

User report: User says a setting never changed.

Objective: Determine whether policy is targeted and refreshed.

Troubleshooting workflow

- 276. Run gpresult /r.
- 277. Run gpupdate /force.
- 278. Check user/computer scope.
- 279. Check OU/security filtering conceptually.
- 280. Compare with a known-good device.

Likely diagnosis: Policy targeting, refresh, precedence or connectivity issue.

Resolution / corrective action

- 281. Refresh and correct local state if allowed.
- 282. Escalate GPO administration if targeting or policy content must change.

Verification

- Setting changes after policy refresh/re-login.

When to escalate

- Policy design/conflict or domain infrastructure issue.

Interview-ready answer: I would prove whether the policy is actually reaching the machine before changing settings manually.

Scenario 31: Remote desktop unavailable

User report: User cannot RDP to a workstation/server.

Objective: Separate network, host availability, permissions and RDP service.

Troubleshooting workflow

- 283. Confirm target hostname/IP.
- 284. Test network reachability.
- 285. Verify user authorization.
- 286. Check whether other users connect.
- 287. Check target RDP state/service if authorized.

Likely diagnosis: Network path, endpoint offline, authorization or RDP service/configuration.

Resolution / corrective action

- 288. Restore network/host state if within scope.
- 289. Escalate server-side or permission issue.

Verification

- RDP session establishes and user can work.

When to escalate

- Server outage or privileged RDP policy issue.

Interview-ready answer: I would test reachability before troubleshooting RDP itself, because a remote desktop client cannot connect to an unavailable host.

Scenario 32: Teams sign-in fails

User report: Teams repeatedly asks for credentials or errors.

Objective: Determine identity, client and service scope.

Troubleshooting workflow

- 290. Test web sign-in.
- 291. Verify account status/MFA.
- 292. Check date/time and connectivity.
- 293. Compare with another client/device if possible.
- 294. Check service health if multiple users.

Likely diagnosis: Authentication state, cached client credentials, policy or service issue.

Resolution / corrective action

- 295. Sign out/reset client state according to approved procedure.

296. Escalate identity/service issues.

Verification

- User can sign in and join a meeting.

When to escalate

- Conditional Access/identity service problem outside L1.

Interview-ready answer: I would use the web client to distinguish account/service authentication from the local Teams client.

Scenario 33: OneDrive says storage full

User report: Sync stops due to quota.

Objective: Confirm quota and separate personal sync issue from tenant/site limits.

Troubleshooting workflow

297. Check storage status.
298. Identify whether the quota is user, site or device related.
299. Remove/move only approved data.
300. Confirm sync resumes.

Likely diagnosis: Cloud quota or local storage constraint.

Resolution / corrective action

301. Use approved storage cleanup/migration process.
302. Escalate if organizational quota must change.

Verification

- Space is available and sync resumes.

When to escalate

- Quota increase or policy change requiring admin.

Interview-ready answer: I would identify where the capacity limit is occurring before deleting anything.

Scenario 34: Keyboard/mouse intermittent

User report: Input devices drop out.

Objective: Determine whether issue follows device, port or endpoint.

Troubleshooting workflow

303. Check cable/battery.
304. Try another port.
305. Test known-good device.
306. Check Device Manager and power settings.
307. If wireless, check receiver/2.4GHz interference.

Likely diagnosis: Device, cable, port, battery or driver.

Resolution / corrective action

308. Replace battery/cable/device or correct driver.

Verification

- No drops during test.

When to escalate

- Endpoint hardware/controller issue.

Interview-ready answer: I isolate by swapping the device and port so I can tell whether the problem follows the peripheral.

Scenario 35: No audio from laptop

User report: User has no sound.

Objective: Separate mute/output device, driver and hardware.

Troubleshooting workflow

309. Check volume/mute.
310. Check selected output device.
311. Test headphones/speakers.
312. Check Windows sound troubleshooter/settings.
313. Check Device Manager.

Likely diagnosis: Wrong output selection, mute, driver or speaker hardware.

Resolution / corrective action

314. Select correct output or repair driver as approved.

Verification

- Play test audio in Windows and target app.

When to escalate

- Hardware/driver failure.

Interview-ready answer: Start with the simplest explanations—mute and output device—then move to driver/hardware.

Scenario 36: Camera not working in Teams

User report: Camera appears black/unavailable.

Objective: Separate privacy, driver, app and hardware.

Troubleshooting workflow

315. Test Windows Camera app if available.
316. Check privacy permissions.
317. Check Teams device selection.
318. Try another app.
319. Check Device Manager.

Likely diagnosis: Privacy setting, driver, app selection or hardware.

Resolution / corrective action

320. Enable approved permission and choose correct camera.
321. Repair driver or replace device if needed.

Verification

- Camera image works in test call.

When to escalate

- Driver/hardware issue across apps.

Interview-ready answer: I would prove whether the camera works outside Teams before changing Teams settings.

Scenario 37: Print jobs stuck

User report: Jobs remain in queue.

Objective: Determine whether queue, spooler, driver or printer is at fault.

Troubleshooting workflow

- 322. Check queue status and job size.
- 323. Pause/resume or clear only appropriate jobs.
- 324. Check Print Spooler.
- 325. Test another document/user.
- 326. Check printer status.

Likely diagnosis: Stuck queue/spooler, driver or printer problem.

Resolution / corrective action

- 327. Clear stale jobs and restart spooler if appropriate.
- 328. Re-add/driver repair if approved.

Verification

- A new test page prints.

When to escalate

- Print server or printer hardware issue.

Interview-ready answer: I would distinguish a stuck local queue from a printer-side or server-side issue by testing a new job and another client.

Scenario 38: User says “internet is down” but only one app fails

User report: Browser or one application is broken.

Objective: Avoid over-scoping to network.

Troubleshooting workflow

- 329. Test another site/app.
- 330. Test same function in web/alternate client.
- 331. Check application status and sign-in.
- 332. Check proxy/VPN dependence.

Likely diagnosis: Application-specific issue.

Resolution / corrective action

- 333. Repair/restart app or correct credentials/settings.
- 334. Escalate service-specific outage.

Verification

- Application function works.

When to escalate

- Backend/service or widespread outage.

Interview-ready answer: The phrase “internet is down” is a user symptom, not a diagnosis. I would test other services before changing network settings.

Scenario 39: Password works on web but not Outlook

User report: Credential works elsewhere.

Objective: Isolate desktop credential/token/profile state.

Troubleshooting workflow

- 335. Test OWA.
- 336. Check Outlook account state.
- 337. Check cached credentials according to policy.
- 338. Restart/re-authenticate.
- 339. Rebuild profile only if needed.

Likely diagnosis: Outlook client authentication/profile state.

Resolution / corrective action

- 340. Re-authenticate or repair profile.

Verification

- Outlook authenticates and syncs.

When to escalate

- Identity policy issue.

Interview-ready answer: Because the password works in webmail, I would focus on the Outlook client state rather than resetting the password again.

Scenario 40: User cannot access SharePoint site

User report: Site loads for some users but not one.

Objective: Separate licensing/account, membership, browser and Conditional Access concepts.

Troubleshooting workflow

- 341. Test web access and exact URL.
- 342. Verify user account and group/site membership.
- 343. Try private browser session if allowed.
- 344. Check whether other site permissions work.
- 345. Check device/network policy if applicable.

Likely diagnosis: Authorization, session/cached credential or policy issue.

Resolution / corrective action

- 346. Correct approved membership or clear session state.
- 347. Escalate tenant/site permissions.

Verification

- User can access intended site without excess rights.

When to escalate

- Site collection/admin policy issue.

Interview-ready answer: I would distinguish authentication from authorization and avoid granting broad access as a workaround.

Scenario 41: USB storage blocked

User report: User cannot use a flash drive.

Objective: Determine whether blocking is intentional security policy.

Troubleshooting workflow

- 348. Check whether other USB devices work.
- 349. Test whether the drive is recognized.
- 350. Review endpoint policy/message.
- 351. Do not bypass security controls.

Likely diagnosis: Intentional device control or hardware/media issue.

Resolution / corrective action

- 352. Use approved exception/request process.
- 353. Escalate security policy questions.

Verification

- Approved device works or request is correctly routed.

When to escalate

- Endpoint security control.

Interview-ready answer: I would treat a security block as potentially intentional and follow the policy instead of disabling endpoint protection.

Scenario 42: Browser certificate warning

User report: User sees certificate error.

Objective: Do not instruct user to bypass security without understanding cause.

Troubleshooting workflow

- 354. Check exact certificate warning.
- 355. Verify system date/time.
- 356. Determine whether it is one site or many.
- 357. Test from another approved device/network.
- 358. Check enterprise proxy inspection conceptually.

Likely diagnosis: Expired/mismatched certificate, wrong time, interception/proxy or site-side error.

Resolution / corrective action

- 359. Correct local time if wrong.
- 360. Escalate site/certificate/proxy issue.

Verification

- Certificate warning is resolved by approved remediation.

When to escalate

- Security-sensitive TLS issue; do not bypass blindly.

Interview-ready answer: Certificate warnings can indicate real security problems, so I would identify the exact cause before suggesting any bypass.

Scenario 43: Shared mailbox access missing

User report: User was granted access but cannot see mailbox.

Objective: Separate authorization timing, Outlook client state and Exchange-side permission.

Troubleshooting workflow

- 361. Confirm approval and permission assignment.
- 362. Check whether access works in webmail.
- 363. Refresh/restart Outlook.
- 364. Check account/group context.
- 365. Allow for propagation where applicable.

Likely diagnosis: Permission not applied, client cache, or mailbox configuration.

Resolution / corrective action

- 366. Refresh client and verify permission through approved tools.
- 367. Escalate Exchange admin issue.

Verification

- User can open and perform only approved actions.

When to escalate

- Permission assignment or Exchange config issue.

Interview-ready answer: I would verify that the access was actually granted before troubleshooting Outlook.

Scenario 44: Local admin rights requested

User report: User wants permanent admin rights to install a tool.

Objective: Protect least privilege and use approved process.

Troubleshooting workflow

- 368. Understand the business requirement.
- 369. Check software deployment/catalog.
- 370. Determine whether temporary elevation is available.
- 371. Follow approval and security process.

Likely diagnosis: Access-control policy, not a normal troubleshooting ticket.

Resolution / corrective action

- 372. Use approved elevation/deployment path.

Verification

- Software installed with least privilege.

When to escalate

- Security/admin approval required.

Interview-ready answer: I would not grant permanent local admin simply because it is convenient; I would use the approved least-privilege process.

Scenario 45: Login is slow after sign-in

User report: Desktop takes long to become usable.

Objective: Separate profile, startup, policy, network and storage.

Troubleshooting workflow

- 373. Check whether delay occurs before or after desktop appears.
- 374. Review startup apps.
- 375. Check network/domain dependence.
- 376. Check GPO processing symptoms.

377. Test another user on the device.

Likely diagnosis: Profile/startup/GPO/network dependency or storage.

Resolution / corrective action

378. Reduce approved startup load, refresh profile/policy as directed.

379. Escalate repeated GPO/domain latency.

Verification

- Normal sign-in time restored.

When to escalate

- Domain/GPO/server issue or data-risk profile rebuild.

Interview-ready answer: I would identify exactly where the sign-in delay occurs before making changes, because pre-logon and post-logon delays point to different fault domains.

Scenario 46: PC fan is loud

User report: Device is noisy and warm.

Objective: Determine load and thermal risk.

Troubleshooting workflow

380. Check CPU/GPU usage.

381. Check task causing load.

382. Check physical airflow and vents.

383. Check whether noise persists at idle.

384. Observe any shutdown/thermal warning.

Likely diagnosis: High workload, background task or thermal/hardware issue.

Resolution / corrective action

385. Close/remove offending workload if appropriate.

386. Clean/repair hardware only according to policy.

Verification

- Normal load and temperature behavior.

When to escalate

- Thermal alarm, fan failure or hardware service needed.

Interview-ready answer: I would correlate fan noise with system load and thermal symptoms rather than assuming the fan itself is defective.

Scenario 47: Computer has no network after moving desks

User report: Previously worked, now fails at new location.

Objective: Test physical port/VLAN versus endpoint.

Troubleshooting workflow

387. Check cable and link lights.

388. Check IP/gateway.

389. Try known-good port/cable/device.

390. Compare with adjacent desk.

391. Check whether the move changed network segment.

Likely diagnosis: Port/VLAN/cabling issue or DHCP/network-path change.

Resolution / corrective action

- 392. Reconnect cable or move to known-good port if allowed.
- 393. Escalate switch-port/VLAN issue.

Verification

- Valid IP and network access.

When to escalate

- Network infrastructure.

Interview-ready answer: The timing suggests location/path dependency, so I would compare the endpoint and port with a known-good workstation at the new desk.

Scenario 48: User cannot access internal site on VPN

User report: VPN shows connected but internal resource fails.

Objective: Separate tunnel connectivity from name resolution and authorization.

Troubleshooting workflow

- 394. Check VPN status.
- 395. Test internal hostname resolution.
- 396. Test another internal resource.
- 397. Check route/permission context.
- 398. Compare known-good VPN user.

Likely diagnosis: DNS/routing/authorization/VPN split-tunnel or backend issue.

Resolution / corrective action

- 399. Correct local VPN/DNS state if supported.
- 400. Escalate network/security/VPN admin.

Verification

- Internal site opens and user can authenticate.

When to escalate

- Routing/ACL/backend issue.

Interview-ready answer: VPN connected is not the end of the test; I must verify that the required internal route, DNS and authorization actually work.

Scenario 49: User cannot open PDF

User report: One PDF fails or all PDFs fail.

Objective: Separate file corruption, application association and permissions.

Troubleshooting workflow

- 401. Try another PDF.
- 402. Try the same file in approved browser/PDF viewer.
- 403. Check file location/permissions.
- 404. Capture any error.

Likely diagnosis: Bad file, viewer problem, file permissions or storage path.

Resolution / corrective action

405. Repair association/viewer or obtain a clean copy if appropriate.

Verification

- Multiple PDFs open.
- Original file opens if it is valid.

When to escalate

- Corrupt/business-critical file or storage permission issue.

Interview-ready answer: I would test another PDF first; that tells me whether the reader is broken or the specific document is the problem.

Scenario 50: Excel/Word file opens read-only

User report: User expects to edit but cannot.

Objective: Separate permissions, location lock, protected document or application state.

Troubleshooting workflow

- 406. Check file location and permissions.
- 407. Check whether someone else has it open.
- 408. Check file attributes/protection.
- 409. Try web/client version if applicable.

Likely diagnosis: Access rights, file lock, protection or sync state.

Resolution / corrective action

- 410. Use approved permissions/request process.
- 411. Release stale lock through approved support process.

Verification

- User can edit only as authorized.

When to escalate

- SharePoint/Office permission or document-owner issue.

Interview-ready answer: I would identify whether the read-only state is caused by document protection, access control or an active lock.

Scenario 51: User reports ransomware-like filename changes

User report: Files appear renamed/encrypted.

Objective: Contain and escalate immediately.

Troubleshooting workflow

- 412. Avoid opening/modifying affected files.
- 413. Disconnect/isolate endpoint according to security playbook.
- 414. Record symptoms and time.
- 415. Notify security/incident response immediately.

Likely diagnosis: Potential ransomware/security incident.

Resolution / corrective action

- 416. Follow containment and incident-response procedure.
- 417. Do not improvise recovery or delete evidence.

Verification

- Security team confirms containment and recovery path.

When to escalate

- Always escalate to security; possible active compromise.

Interview-ready answer: This is a security incident, not a normal file-support issue. I would follow the incident playbook and prioritize containment and evidence preservation.

Scenario 52: User gets repeated MFA prompts

User report: Unexpected prompts appear repeatedly.

Objective: Treat as possible attack or misconfiguration.

Troubleshooting workflow

418. Ask whether the user initiated any login.
419. Do not approve unknown prompts.
420. Record time/device/application if visible.
421. Escalate to security/identity team.

Likely diagnosis: Possible credential attack, token issue or misconfigured application.

Resolution / corrective action

422. Follow identity/security playbook; reset credentials if directed.

Verification

- Account protected and prompts stop.

When to escalate

- Security escalation is mandatory for suspicious repeated prompts.

Interview-ready answer: I would tell the user not to approve unexpected MFA requests and escalate because repeated prompts can indicate a credential attack.

Scenario 53: User cannot browse while proxy is enabled

User report: Corporate browser errors but direct internet may work elsewhere.

Objective: Determine whether proxy configuration is required or broken.

Troubleshooting workflow

423. Check whether proxy is expected in the environment.
424. Check proxy reachability.
425. Test another managed client.
426. Avoid bypassing policy without approval.

Likely diagnosis: Proxy server or configuration issue.

Resolution / corrective action

427. Restore approved configuration or escalate proxy service.

Verification

- Corporate websites/apps work through expected path.

When to escalate

- Proxy/security gateway issue.

Interview-ready answer: I would not simply disable the corporate proxy if it is a security control; I would verify service reachability and escalate.

Scenario 54: Application license expired

User report: App launches but reports no license.

Objective: Separate user entitlement from local client.

Troubleshooting workflow

- 428. Capture error.
- 429. Check account/license assignment through approved tools.
- 430. Test whether other users have same issue.
- 431. Check sign-in state.

Likely diagnosis: License/assignment/account issue.

Resolution / corrective action

- 432. Restore approved license assignment or escalate licensing team.

Verification

- Application opens with expected licensed features.

When to escalate

- Tenant-wide licensing issue.

Interview-ready answer: A license error is often an entitlement problem, so I would verify assignment before reinstalling the application.

Scenario 55: User cannot print color

User report: Black-and-white prints, color setting ignored.

Objective: Determine whether app, driver or printer policy controls color.

Troubleshooting workflow

- 433. Test printer properties.
- 434. Try print test page or another application.
- 435. Check driver settings/policy.
- 436. Compare with another user.

Likely diagnosis: Driver/app setting or printer policy.

Resolution / corrective action

- 437. Correct approved driver/print preference.
- 438. Escalate server/driver policy.

Verification

- Test print uses expected color.

When to escalate

- Print server policy or hardware.

Interview-ready answer: I would first identify whether the setting follows the user, application or printer by testing from another app/client.

Scenario 56: User sees “Access Denied” after password reset

User report: Password changed, now access fails.

Objective: Separate authentication from cached credentials/permissions.

Troubleshooting workflow

- 439. Confirm sign-in works in web or Windows.
- 440. Check whether specific resource or all resources fail.
- 441. Reconnect VPN/share if needed.
- 442. Check cached sessions/tokens.

Likely diagnosis: Stale session, token, mapped resource credentials or actual permission issue.

Resolution / corrective action

- 443. Re-authenticate/reconnect approved resources.

Verification

- User can access intended resources.

When to escalate

- Permission changes or identity-service issue.

Interview-ready answer: Because the password reset succeeded, I would test whether the failing resource still has a stale session before changing permissions.

Scenario 57: Time is wrong on workstation

User report: Clock differs significantly from corporate time.

Objective: Restore time sync because it can affect authentication.

Troubleshooting workflow

- 444. Check date/time/time zone.
- 445. Determine whether device is domain joined.
- 446. Check time synchronization state.
- 447. Do not manually force arbitrary time on a managed domain device.

Likely diagnosis: Wrong time zone or synchronization issue.

Resolution / corrective action

- 448. Correct time zone or sync configuration using approved method.

Verification

- Time matches corporate source closely.
- Authentication works.

When to escalate

- Domain time infrastructure issue.

Interview-ready answer: Time is not only cosmetic: authentication and certificates can depend on correct time.

Scenario 58: User cannot upload file to web app

User report: Download works but upload fails.

Objective: Separate browser, file constraints, permissions and network security controls.

Troubleshooting workflow

- 449. Try small known-good file.
- 450. Check file extension/size restrictions.
- 451. Try approved browser.
- 452. Check account/site permission.
- 453. Check proxy/security gateway if enterprise policy applies.

Likely diagnosis: File validation, app permission, browser or security control.

Resolution / corrective action

- 454. Use compliant file/browser or correct approved permissions.

Verification

- Upload a test file successfully.

When to escalate

- Backend or security gateway rule.

Interview-ready answer: Using a tiny known-good file helps identify whether the issue is file-specific or the upload path generally.

Scenario 59: User cannot open internal web app but colleagues can

User report: One user affected.

Objective: Separate identity, device and browser state.

Troubleshooting workflow

- 455. Test same app in browser/private session.
- 456. Test another device or network if allowed.
- 457. Verify account/role.
- 458. Check DNS and VPN.

Likely diagnosis: User-specific permission/session/device issue.

Resolution / corrective action

- 459. Clear session state or correct approved access.

Verification

- User opens app and signs in.

When to escalate

- Role/backend issue if user entitlement is correct.

Interview-ready answer: I would compare the same account across paths to determine whether the problem follows the user or the device.

Scenario 60: Multiple users cannot access same application

User report: Several users fail simultaneously.

Objective: Recognize potential outage quickly.

Troubleshooting workflow

- 460. Confirm multiple affected users/locations.
- 461. Check service health/status.
- 462. Stop repeating local fixes.
- 463. Raise incident priority according to impact.

Likely diagnosis: Backend/service/network outage.

Resolution / corrective action

- 464. Open/raise major incident according to process.
- 465. Communicate status to users.

Verification

- Service restored and communication sent.

When to escalate

- Immediately escalate to the owning team.

Interview-ready answer: The scope changes the response. Multiple users failing the same service points toward an incident, so I would pivot from endpoint fixes to service-level investigation.

Scenario 61: User asks for blocked website to be unblocked

User report: User wants security filter bypass.

Objective: Handle policy/security request correctly.

Troubleshooting workflow

- 466. Identify business need.
- 467. Check approved exception process.
- 468. Do not bypass filter locally.
- 469. Route request to security/network if required.

Likely diagnosis: Policy-controlled access.

Resolution / corrective action

- 470. Submit approved exception/request.

Verification

- Access granted only through authorized process.

When to escalate

- Security/network team.

Interview-ready answer: I would not bypass the filter; I would document the business need and use the approved exception workflow.

Scenario 62: Laptop stolen

User report: User reports missing corporate laptop.

Objective: Protect account and company data.

Troubleshooting workflow

- 471. Confirm identity and incident details.
- 472. Record asset information if available.
- 473. Immediately follow lost-device security process.
- 474. Escalate to security/management.

Likely diagnosis: Physical asset loss with possible data exposure.

Resolution / corrective action

- 475. Trigger approved device lock/wipe and account response as directed.

Verification

- Security team confirms containment.

When to escalate

- Immediate security escalation.

Interview-ready answer: This is an information-security incident, not just an asset ticket. I would follow the lost-device process immediately.

Scenario 63: User accidentally deleted important file

User report: Needs restoration.

Objective: Determine source and approved recovery path.

Troubleshooting workflow

476. Identify storage system.
477. Check recycle bin/version history where available.
478. Confirm file name/path/time.
479. Avoid creating conflicting copies.

Likely diagnosis: User deletion with possible recoverable version.

Resolution / corrective action

480. Restore via approved recycle/version process.

Verification

- Recovered file opens and is complete.

When to escalate

- Permanent deletion or backup recovery requires L2/storage team.

Interview-ready answer: I would identify whether the file is in OneDrive, SharePoint, file share or local storage because each has a different recovery path.

Scenario 64: Browser pop-ups and redirects

User report: User reports suspicious ads/redirects.

Objective: Differentiate web-site behavior from browser compromise.

Troubleshooting workflow

481. Ask whether issue occurs only on one site.
482. Check extensions.
483. Test private browser.
484. Run approved endpoint security scan if indicated.
485. Escalate if compromise suspected.

Likely diagnosis: Bad site, unwanted extension or possible malware.

Resolution / corrective action

486. Remove unwanted extension through approved process; scan/escalate if needed.

Verification

- Normal browsing restored and security clear.

When to escalate

- Malware suspicion or persistent compromise.

Interview-ready answer: I would not assume every pop-up is malware, but persistent redirects across sites warrant endpoint and security investigation.

Scenario 65: User hears no audio in Teams but YouTube works

User report: General audio works.

Objective: Prove Teams-specific device/configuration.

Troubleshooting workflow

- 487. Check Teams selected device.
- 488. Check call volume/mute state.
- 489. Test another meeting or Teams web.
- 490. Check exclusive app settings if applicable.

Likely diagnosis: Teams device or app state.

Resolution / corrective action

- 491. Correct device selection/restart client.

Verification

- Test call audio works.

When to escalate

- Service/client issue affecting multiple users.

Interview-ready answer: Because browser audio works, I can deprioritize hardware and focus on Teams's input/output selection and call settings.

Scenario 66: User receives “credential prompt” repeatedly for mapped drive

User report: Share asks for password repeatedly.

Objective: Avoid credential harvesting and isolate authentication/session.

Troubleshooting workflow

- 492. Verify share path.
- 493. Check domain/VPN connectivity.
- 494. Check account status.
- 495. Reconnect using approved methods.
- 496. Avoid storing passwords insecurely.

Likely diagnosis: Authentication/session problem or permission mismatch.

Resolution / corrective action

- 497. Refresh network authentication or escalate server/AD issue.

Verification

- Share opens without repeated prompt.

When to escalate

- Server auth/permissions or security concern.

Interview-ready answer: I would determine whether the user is reaching the domain/share correctly before saving new credentials or changing permissions.

Scenario 67: User cannot install browser extension

User report: Extension blocked.

Objective: Determine whether management policy is intentional.

Troubleshooting workflow

- 498. Check browser policy/message.
- 499. Ask whether extension is approved.
- 500. Do not disable browser management.
- 501. Route request for approval.

Likely diagnosis: Enterprise browser policy.

Resolution / corrective action

- 502. Use approved extension/request process.

Verification

- Extension installed if approved.

When to escalate

- Browser management/security team.

Interview-ready answer: A blocked extension can be a deliberate security control; I would follow the approval path.

Scenario 68: USB keyboard works in BIOS but not Windows

User report: Input works before OS.

Objective: Suggest OS/driver rather than hardware failure.

Troubleshooting workflow

- 503. Check Device Manager.
- 504. Boot with another keyboard if needed.
- 505. Check HID/USB driver state.
- 506. Check Windows updates/policy.

Likely diagnosis: Windows driver/policy issue.

Resolution / corrective action

- 507. Repair driver/settings or restore known-good device.

Verification

- Keyboard works in Windows.

When to escalate

- USB controller/OS issue requiring L2.

Interview-ready answer: Because it works in BIOS, the keyboard hardware is less likely to be the root cause; I would focus on Windows drivers and policy.

Scenario 69: External webcam works in Camera app but not Teams

User report: Camera is healthy at OS level.

Objective: Focus on Teams permission/selection.

Troubleshooting workflow

- 508. Check privacy permissions.

- 509. Check Teams selected camera.
- 510. Check app restart/session.
- 511. Test Teams web.

Likely diagnosis: Teams selection/permission/client state.

Resolution / corrective action

- 512. Correct setting/restart client.

Verification

- Test meeting video works.

When to escalate

- Service issue.

Interview-ready answer: The OS test proves the device path, so I would troubleshoot Teams configuration next.

Scenario 70: User cannot access email on phone

User report: Desktop works.

Objective: Separate mobile authentication, app configuration and device policy.

Troubleshooting workflow

- 513. Check whether webmail works on phone browser.
- 514. Check mobile app sign-in and MFA.
- 515. Check device management/compliance requirement.
- 516. Avoid storing passwords insecurely.

Likely diagnosis: Mobile app token/config or device compliance.

Resolution / corrective action

- 517. Re-authenticate or re-enroll according to policy.

Verification

- Mobile email sync works.

When to escalate

- MDM/Conditional Access identity issue.

Interview-ready answer: Because desktop works, I would focus on the mobile identity/session and device policy rather than Exchange mail delivery.

Scenario 71: Office applications all ask to sign in

User report: Multiple Office apps affected.

Objective: Recognize identity/licensing state.

Troubleshooting workflow

- 518. Check account sign-in and licensing.
- 519. Test web apps.
- 520. Check service health.
- 521. Verify device date/time and connectivity.

Likely diagnosis: Identity token/license/service issue.

Resolution / corrective action

- 522. Re-authenticate through approved process.
- 523. Escalate tenant/license issue.

Verification

- Word/Excel/Outlook open with expected access.

When to escalate

- Tenant-wide authentication issue.

Interview-ready answer: Multiple Office apps failing together suggests shared identity/licensing rather than individual application corruption.

Scenario 72: User cannot connect to conference room Wi-Fi

User report: Only one room/device affected.

Objective: Compare with other room/user to isolate AP/authentication.

Troubleshooting workflow

- 524. Test another device in room.
- 525. Check SSID/signal.
- 526. Check DHCP.
- 527. Test nearby room.
- 528. Escalate AP/site issue if multiple devices fail.

Likely diagnosis: Room AP/RF/authentication/VLAN issue.

Resolution / corrective action

- 529. Reconnect or report AP issue.

Verification

- Device connects and gets network access.

When to escalate

- Wireless infrastructure.

Interview-ready answer: Scope is key: if several devices fail only in one room, it is probably infrastructure rather than one laptop.

Scenario 73: User gets “No bootable device”

User report: Firmware cannot find OS.

Objective: Treat as potential disk/boot configuration issue.

Troubleshooting workflow

- 530. Capture exact message.
- 531. Check whether storage device is detected in firmware.
- 532. Do not format/reinstall immediately.
- 533. Follow approved recovery procedure.

Likely diagnosis: Disconnected/failed drive or boot configuration issue.

Resolution / corrective action

- 534. Reconnect hardware only if authorized; use recovery tools as directed.

Verification

- OS boots without data loss.

When to escalate

- Drive failure or recovery requiring L2.

Interview-ready answer: I would protect data first and determine whether firmware sees the storage device before making boot changes.

Scenario 74: User accidentally installed unapproved software

User report: Security/compliance concern.

Objective: Assess risk and follow policy.

Troubleshooting workflow

- 535. Identify software/source/time.
- 536. Disconnect/isolate if security guidance says so.
- 537. Run approved endpoint scan.
- 538. Notify security/IT as required.

Likely diagnosis: Policy violation or potential malware.

Resolution / corrective action

- 539. Remove/contain per security playbook; preserve evidence as directed.

Verification

- Device is compliant and secure.

When to escalate

- Security incident or uncertain compromise.

Interview-ready answer: I would treat it as a security/compliance event, not simply uninstall it and close the ticket.

Scenario 75: File share is slow for everyone

User report: Multiple users report slowness.

Objective: Recognize shared service issue.

Troubleshooting workflow

- 540. Confirm scope and timing.
- 541. Compare local vs shared file performance.
- 542. Check network/service health.
- 543. Avoid endpoint-by-endpoint rebuilds.

Likely diagnosis: Server/storage/network congestion.

Resolution / corrective action

- 544. Raise incident with evidence and affected location.

Verification

- Shared service normal.

When to escalate

- Infrastructure/service team.

Interview-ready answer: Multiple users on the same share suggests a service-side or network issue; I would consolidate evidence and escalate.

Scenario 76: User cannot access printer after password change

User report: Other network access works.

Objective: Separate print server/session/credential cache.

Troubleshooting workflow

- 545. Test printer web/UI or direct path if appropriate.
- 546. Reconnect shared printer.
- 547. Check server auth.
- 548. Compare another user.

Likely diagnosis: Stale session/credential or print server authorization.

Resolution / corrective action

- 549. Reconnect using approved methods.

Verification

- Test page prints.

When to escalate

- Print server ACL issue.

Interview-ready answer: A password change can invalidate cached sessions; I would reconnect the printer using the approved path before changing permissions.

Scenario 77: User's desktop icons disappeared

User report: Apps/files still exist but desktop looks different.

Objective: Determine profile/shell/view issue.

Troubleshooting workflow

- 550. Check whether user is in correct profile/account.
- 551. Check Desktop folder contents.
- 552. Check OneDrive-known-folder redirection concepts.
- 553. Test another shell/profile symptom.

Likely diagnosis: Wrong profile, sync/redirection or shell/view issue.

Resolution / corrective action

- 554. Restore correct profile/path/view.

Verification

- Icons/data visible and shortcuts work.

When to escalate

- Profile corruption or data-redirection issue.

Interview-ready answer: I would first verify the user is in the correct profile and that the underlying Desktop folder still contains the data.

Scenario 78: Application shortcut broken

User report: Icon gives "file not found".

Objective: Determine whether app moved/updated or shortcut target invalid.

Troubleshooting workflow

- 555. Inspect shortcut target.
- 556. Try app from Start Menu.
- 557. Check installation path.
- 558. Check whether app was upgraded/removed.

Likely diagnosis: Broken shortcut rather than application failure.

Resolution / corrective action

- 559. Recreate shortcut or use approved app repair.

Verification

- App launches normally.

When to escalate

- Packaging/deployment issue.

Interview-ready answer: I would test the application directly before reinstalling it; the shortcut may be the only fault.

Scenario 79: User cannot see newly granted group access

User report: Group membership added but access not present.

Objective: Account for session/token refresh.

Troubleshooting workflow

- 560. Confirm membership is actually applied.
- 561. Have user sign out/in as required.
- 562. Reconnect resource/VPN.
- 563. Retest.

Likely diagnosis: Stale logon token/session or propagation delay.

Resolution / corrective action

- 564. Refresh user session and resource connection.

Verification

- Access appears as intended.

When to escalate

- Replication/group policy issue.

Interview-ready answer: Access changes often require a refreshed session; I would verify membership first and then refresh authentication state.

Scenario 80: User gets “Account disabled”

User report: Sign-in blocked.

Objective: Determine whether account is intentionally disabled.

Troubleshooting workflow

- 565. Verify identity.
- 566. Check account status and offboarding/HR process indicator according to policy.
- 567. Do not re-enable blindly.
- 568. Escalate if business status conflicts with directory state.

Likely diagnosis: Deliberate disablement or directory issue.

Resolution / corrective action

569. Follow approved authorization path.

Verification

- User access restored only if authorized.

When to escalate

- HR/security/identity admin.

Interview-ready answer: An account-disabled state is security-sensitive; I would verify authorization before re-enabling anything.

Scenario 81: Laptop overheating during normal use

User report: Device becomes very hot and performance drops.

Objective: Protect hardware and user safety.

Troubleshooting workflow

- 570. Check CPU load.
- 571. Inspect vents/blocked airflow.
- 572. Check fans/thermal alerts.
- 573. Test on AC/battery conditions.
- 574. Stop use if safety hazard appears.

Likely diagnosis: Blocked airflow, runaway process or cooling-system failure.

Resolution / corrective action

575. Reduce load; arrange hardware service if needed.

Verification

- Normal temperature/load behavior.

When to escalate

- Burn smell, swelling, repeated thermal shutdown.

Interview-ready answer: I would first rule out an abnormal workload but treat physical heat hazards as a hardware-support escalation.

Scenario 82: User cannot open company portal after password reset

User report: Some internal sites work, portal does not.

Objective: Separate cached token/session from account permission.

Troubleshooting workflow

- 576. Test private browser session.
- 577. Test portal URL exactly.
- 578. Check sign-in prompt and error.
- 579. Try web on another managed device if allowed.

Likely diagnosis: Stale session/cookie, SSO token or portal role.

Resolution / corrective action

580. Refresh session or use approved identity remediation.

Verification

- Portal opens and role is correct.

When to escalate

- SSO/portal backend.

Interview-ready answer: Because the password changed, stale SSO state is a strong hypothesis, but I would verify it before resetting more credentials.

Scenario 83: User reports “VPN connected but slow internet”

User report: Internet slows only while VPN is connected.

Objective: Determine whether traffic is intentionally routed through corporate VPN.

Troubleshooting workflow

581. Compare speed before/after VPN.
582. Check whether only internal resources are slow.
583. Test another user/network.
584. Check VPN client status and policy.

Likely diagnosis: Full-tunnel routing, VPN capacity, local network or policy.

Resolution / corrective action

585. Use approved VPN settings; escalate capacity/network issue.

Verification

- Required corporate apps perform within expected range.

When to escalate

- VPN infrastructure/capacity issue.

Interview-ready answer: VPN changes routing and security inspection paths, so I would compare behavior with and without the tunnel and escalate if shared impact exists.

Scenario 84: User says “everything is slow”

User report: Broad perception of slowness.

Objective: Turn subjective symptom into measurable tests.

Troubleshooting workflow

586. Ask which applications and tasks are slow.
587. Measure CPU/memory/disk/network.
588. Check whether issue is local or service-specific.
589. Compare with peer device.

Likely diagnosis: Could be endpoint performance, network, service latency or user environment.

Resolution / corrective action

590. Fix identified bottleneck or escalate shared service issue.

Verification

- Specific tasks return to normal.

When to escalate

- Infrastructure or hardware issue.

Interview-ready answer: I would break “everything” into measurable components rather than troubleshooting blindly.

Scenario 85: User cannot use RDP from home

User report: Local internet works but remote access fails.

Objective: Separate VPN prerequisite, DNS, MFA and endpoint availability.

Troubleshooting workflow

- 591. Confirm VPN requirement.
- 592. Verify VPN connection.
- 593. Resolve target hostname.
- 594. Check target availability/authorization.

Likely diagnosis: Remote access path or endpoint offline.

Resolution / corrective action

- 595. Restore VPN/authorization within scope.

Verification

- RDP connects after VPN.

When to escalate

- Network/server/identity issue.

Interview-ready answer: I would confirm the expected remote-access sequence—often VPN first, then DNS/route, then RDP.

Scenario 86: User's Teams status is stuck

User report: Presence does not update.

Objective: Separate client cache/session from service issue.

Troubleshooting workflow

- 596. Check service health if broad.
- 597. Sign out/in.
- 598. Test Teams web.
- 599. Determine whether chat/calls also fail.

Likely diagnosis: Client state or service presence issue.

Resolution / corrective action

- 600. Refresh client session; escalate if service-wide.

Verification

- Presence updates correctly.

When to escalate

- Tenant-wide Teams issue.

Interview-ready answer: If Teams web has the same presence issue, I would stop focusing on the desktop cache and consider a service-side problem.

Scenario 87: User cannot download attachment

User report: Email/website opens but attachment download fails.

Objective: Determine policy, browser, file, storage and security filtering.

Troubleshooting workflow

- 601. Test another small attachment.
- 602. Check file type/size restrictions.
- 603. Test web vs desktop app.
- 604. Check security gateway/policy.

Likely diagnosis: Policy/filter, browser session or file-specific issue.

Resolution / corrective action

- 605. Use approved alternate method or escalate policy.

Verification

- Allowed file downloads successfully.

When to escalate

- Security gateway or mail-service issue.

Interview-ready answer: I would test a small known-good attachment before assuming the mailbox is broken.

Scenario 88: User cannot use clipboard in RDP

User report: Copy/paste between local and remote not working.

Objective: Determine if feature is disabled by policy or session.

Troubleshooting workflow

- 606. Check whether copy works within local/remote separately.
- 607. Check RDP clipboard settings if authorized.
- 608. Test reconnect.
- 609. Check policy restriction.

Likely diagnosis: RDP session setting or policy.

Resolution / corrective action

- 610. Reconnect or follow approved configuration.

Verification

- Clipboard behaves as expected.

When to escalate

- Security policy/server settings.

Interview-ready answer: Clipboard can be intentionally restricted, so I would verify policy before enabling it.

Scenario 89: User receives fake antivirus pop-up

User report: Scareware-style browser alert.

Objective: Avoid calling a random number or installing software.

Troubleshooting workflow

- 611. Ask whether they interacted with the pop-up.
- 612. Close browser safely if possible.
- 613. Do not call displayed number.
- 614. Run approved security checks if indicated.

Likely diagnosis: Malicious website/scareware, possibly not endpoint compromise.

Resolution / corrective action

615. Close/clean browser session; escalate if interaction/execution occurred.

Verification

- Browser clean and no compromise indicators.

When to escalate

- Security if executable/personal data was provided.

Interview-ready answer: I would prevent further interaction with the pop-up and determine whether the user downloaded or executed anything before escalating.

Scenario 90: User reports lost bookmarks/passwords

User report: Browser profile appears reset.

Objective: Determine whether profile/account changed or sync failed.

Troubleshooting workflow

- 616. Check signed-in browser account.
- 617. Check profile selection.
- 618. Check sync status.
- 619. Test another managed device if applicable.

Likely diagnosis: Wrong profile or sync issue.

Resolution / corrective action

620. Restore correct profile/sync according to policy.

Verification

- Expected bookmarks/settings return.

When to escalate

- Data recovery or account issue.

Interview-ready answer: I would verify profile and sync identity before assuming the data is deleted.

Scenario 91: User cannot open network printer web page

User report: Printer prints but web UI unavailable.

Objective: Treat as nonessential diagnostic unless required.

Troubleshooting workflow

- 621. Check printer IP and network.
- 622. Test ping if allowed.
- 623. Try browser to IP/HTTPS if supported.
- 624. Compare another client.

Likely diagnosis: ICMP/HTTP disabled or printer admin interface unavailable.

Resolution / corrective action

625. Use normal printing path; escalate only if management access is needed.

Verification

- Printing still works.

When to escalate

- Network/printer admin issue.

Interview-ready answer: Not every unavailable management page means printing is broken; I would focus on business impact.

Scenario 92: User says email is missing from inbox

User report: Message may be in another folder or rule.

Objective: Trace message location before assuming deletion.

Troubleshooting workflow

- 626. Search mailbox.
- 627. Check junk/archive/other folders.
- 628. Check inbox rules.
- 629. Test OWA.

Likely diagnosis: Filtering, rule, archive or search issue.

Resolution / corrective action

- 630. Correct rule/filter/move message as appropriate.

Verification

- User can locate new test mail.

When to escalate

- Transport/deletion issue requiring Exchange admin.

Interview-ready answer: I would search and inspect filtering before changing mailbox settings.

Scenario 93: User cannot access company Wi-Fi after password change

User report: Other services work.

Objective: Reconnect wireless profile securely.

Troubleshooting workflow

- 631. Forget/rejoin network if approved.
- 632. Verify correct password entry.
- 633. Check 802.1X/authentication conceptually.
- 634. Check DHCP after reconnect.

Likely diagnosis: Stale wireless credentials/profile.

Resolution / corrective action

- 635. Re-enter credentials through secure workflow.

Verification

- Connected with valid corporate IP.

When to escalate

- Wireless authentication infrastructure.

Interview-ready answer: A password change can leave a stale saved Wi-Fi credential; reconnecting the managed profile is a sensible first-line step.

Scenario 94: User reports keyboard layout changed

User report: Keys produce unexpected characters.

Objective: Determine whether language/layout changed.

Troubleshooting workflow

- 636. Check current keyboard layout.
- 637. Check Windows language settings.
- 638. Test in another app.
- 639. Check whether issue is user-specific.

Likely diagnosis: Wrong input language/layout.

Resolution / corrective action

- 640. Switch to approved layout.

Verification

- Expected characters appear.

When to escalate

- Policy/profile issue.

Interview-ready answer: This is a configuration issue rather than a hardware fault if only character mapping is wrong.

Scenario 95: User cannot open Task Manager

User report: Access is denied/disabled.

Objective: Determine whether restriction is intentional.

Troubleshooting workflow

- 641. Capture message.
- 642. Check whether other admin tools are blocked.
- 643. Do not bypass security policy.
- 644. Escalate management/security policy.

Likely diagnosis: Policy/endpoint control.

Resolution / corrective action

- 645. Use approved diagnostic alternatives or request exception.

Verification

- Required support work completed compliantly.

When to escalate

- Endpoint management/security.

Interview-ready answer: I would not bypass a management restriction just to get Task Manager; I would use approved alternatives or escalate.

Scenario 96: User cannot access network because DNS server is unreachable

User report: IP configuration shows corporate DNS but queries time out.

Objective: Determine whether VPN/network path to DNS works.

Troubleshooting workflow

- 646. Check DNS server IPs.

- 647. Test reachability where allowed.
- 648. Check VPN.
- 649. Compare known-good client.

Likely diagnosis: DNS server path or VPN routing issue.

Resolution / corrective action

- 650. Restore expected connection or escalate DNS infrastructure.

Verification

- nslookup succeeds and applications work.

When to escalate

- Network/DNS infrastructure.

Interview-ready answer: The DNS server address in ipconfig is evidence, not proof that it is reachable; I would test the path.

Scenario 97: User cannot open file due to long path

User report: Specific deeply nested file fails.

Objective: Identify filesystem/path limitation or application restriction.

Troubleshooting workflow

- 651. Try shorter path if policy allows.
- 652. Check exact error.
- 653. Test another file.
- 654. Check share/OneDrive specifics.

Likely diagnosis: Path length or application limitation.

Resolution / corrective action

- 655. Move/rename through approved method.

Verification

- File opens and syncs normally.

When to escalate

- Storage/application limitation.

Interview-ready answer: I would identify whether the file itself is corrupt or the path/filename is the constraint.

Scenario 98: User cannot delete file from shared drive

User report: Delete action denied.

Objective: Separate permission from file lock.

Troubleshooting workflow

- 656. Check whether file is open elsewhere.
- 657. Check user permission.
- 658. Test another file in same folder.
- 659. Escalate ACL if needed.

Likely diagnosis: Permission or lock.

Resolution / corrective action

660. Close stale lock via approved support; adjust permissions only with authorization.

Verification

- User can delete only where authorized.

When to escalate

- Server-side permissions.

Interview-ready answer: A permission problem should not be fixed by giving the user full control; I would identify the exact required operation.

Scenario 99: User says computer is disconnected from domain

User report: Symptoms may be wrong time, login or trust relationship.

Objective: Recognize domain trust issue conceptually.

Troubleshooting workflow

- 661. Capture exact error.
- 662. Check network/DNS/time.
- 663. Determine whether domain resources fail.
- 664. Do not unjoin/rejoin blindly.

Likely diagnosis: Potential secure-channel/trust issue or network/identity problem.

Resolution / corrective action

665. Run approved trust-repair steps only if within scope; otherwise escalate.

Verification

- Domain authentication/resources work.

When to escalate

- AD trust repair or domain controller issue.

Interview-ready answer: A domain-trust symptom can require privileged remediation; I would gather DNS/time/network evidence before escalating.

Additional rapid scenarios (micro-playbooks)

Scenario	L1 playbook
No webcam in browser	Check browser permission, OS privacy, device selection, another browser/app, then escalate driver/hardware.
No VPN after Windows update	Capture client error, verify service/profile, compare another user, check approved client version, escalate if policy/deployment issue.
Cannot map printer by name	Test DNS/name resolution, test IP if approved, compare known-good workstation, check print server/share.
Battery drains quickly	Check battery health, power usage, background apps, brightness and hardware health.
Laptop wakes by itself	Check power events/wake timers, docking/USB/network wake settings; escalate recurring firmware/hardware issues.
Desktop background changed	Check user profile/sync/central policy; avoid treating cosmetic change as incident unless policy/business impact exists.
Windows search not finding files	Check index scope/status, storage location, permissions and whether the issue is local or OneDrive.
User cannot change time zone	May be policy-controlled; request authorized change rather than granting privilege.
Browser says "managed by your organization"	Expected on managed devices; inspect policy only when it blocks a required business function.
User cannot receive Teams meeting invitation	Check mailbox/calendar flow, sender/recipient, junk/rules, service health and licensing.

Printer prints blank pages	Check toner/ink, correct driver, test page and device hardware; compare another printer/job.
Laptop keyboard keys missing	Test external keyboard, check key-specific hardware, input layout, debris/physical damage; hardware if issue follows keyboard.
Windows profile temporarily loaded	Capture error, do not create/delete profiles casually; check profile service and disk/network conditions; escalate if data at risk.
User can browse but cannot reach internal DNS names	Check VPN and corporate DNS routing; public DNS may not know private records.
User sees "Your organization requires more information"	Follow Entra/MFA registration or Conditional Access workflow; do not bypass policy.
Office shows unlicensed product	Check account/license, internet, activation state and service health; escalate tenant/licensing issue.
Teams screen sharing unavailable	Check meeting policy/permissions and client version; test web; escalate policy/service issue.
OneDrive folder missing	Check known-folder backup/sync path and web copy before restoring or moving data.
User cannot access remote application	Verify VPN, DNS, authentication, application launch and service status; compare peer user.
Computer name conflict during deployment	Capture hostname, check directory/device inventory through authorized tools, escalate provisioning issue.

15. Behavioral and Customer-Service Interview Questions

Question	Strong answer structure
Tell me about yourself.	Present: current IT focus -> past support experience -> core technologies -> measurable strengths -> why this role.
Why IT support?	Explain that you enjoy diagnosing problems, helping users and working across endpoints, identity and applications.
How do you handle an angry user?	Listen, acknowledge impact, clarify facts, explain next steps, keep updates coming, resolve/escalate.
What if you do not know the answer?	Use documentation/KB, gather evidence, test safely, consult L2, document the result.
How do you prioritize tickets?	Follow impact/urgency matrix, SLA and business criticality; communicate delays.
What if two urgent tickets arrive?	Assess impact/urgency, start the higher business-risk incident, communicate, parallelize/escalate as possible.
How do you deal with repetitive tickets?	Look for a pattern, improve KB, automate standard fixes where authorized and raise a problem record for root cause.
Describe a difficult troubleshooting case.	Use STAR: Situation, Task, Action, Result; emphasize evidence and verification.
What is good documentation?	Concise, reproducible notes showing symptom, evidence, steps, result and next action.
When do you escalate?	When outside access/skill/scope, risk is high, SLA is at risk, or a shared/service-side issue is suspected.
How do you protect user privacy?	Access only needed information, use approved tools, avoid viewing unrelated personal data and never request secrets.
How would you handle pressure from a senior employee?	Remain respectful, follow policy and authorization; escalate conflict rather than bypassing controls.

STAR answer framework

- Situation: what was happening?
- Task: what were you responsible for?
- Action: what did you actually do and why?
- Result: what improved, and how did you verify it?

Avoid this: "I fixed it by restarting." Instead say what you observed, what hypothesis you tested, what change you made, and how you verified the result.

16. Rapid-Fire Technical Questions

Question	Model answer
What is DNS?	A naming system that resolves hostnames to IP addresses and other records.
What is DHCP?	A service that automatically assigns network configuration to clients.
What is APIPA?	An automatically assigned 169.254.x.x IPv4 address used when DHCP configuration is unavailable.
What is a default gateway?	The local router used to reach other networks.
Authentication vs authorization?	Authentication verifies identity; authorization determines allowed access.
What is MFA?	Authentication using two or more independent factors.
What is Active Directory?	A directory and identity platform used to manage users, computers, groups and policies in Windows environments.
What is Group Policy?	Centralized policy configuration for managed users and computers.
What is an incident?	An unplanned interruption or degradation of an IT service.
What is an SLA?	An agreed service-level target such as response or resolution expectations.
What is VPN?	A secure tunnel/access mechanism used to connect to protected resources over an untrusted network.
What does ping test?	Reachability using ICMP where allowed; it does not prove an application works.
What does nslookup do?	Queries DNS for names/records.
What does ipconfig /all show?	Detailed network configuration including IP, gateway, DNS and DHCP information.
What does gpupdate /force do?	Requests a refresh of Group Policy.
Why test OWA when Outlook fails?	It separates mailbox/service/account problems from desktop Outlook client problems.
Why compare a known-good device?	It helps isolate local endpoint failure from shared network/service issues.
What is least privilege?	Giving only the minimum access needed to perform the task.
Why document?	So the next analyst can reproduce, understand and continue the work and so the organization retains a support history.
When should you not restart a service?	When it risks disrupting other users/production or when policy requires change approval.
What is a false positive?	An alert or symptom that appears harmful/failed but is actually benign or expected.
What is a root cause?	The underlying reason that generated the incident, not merely the visible symptom.
What is a workaround?	A temporary method to restore service without eliminating the underlying cause.
What is a change?	A controlled modification to an IT service/environment.
What is a problem record?	A record focused on the underlying cause of recurring or significant incidents.

17. Hands-On Lab Exercises

Lab 1: Build a network troubleshooting checklist

On a Windows machine, record output for `ipconfig /all`, ping your gateway, perform an `nslookup`, and use Test-NetConnection to a common HTTPS destination. Write one sentence explaining what each result proves and what it does not prove.

Lab 2: Windows performance triage

Open Task Manager, identify the top CPU, memory and disk processes, then explain whether the utilization is sustained, bursty or expected. Inspect Reliability Monitor for recent failures.

Lab 3: Event Viewer

Find one Application and one System event associated with a recent failure. Record source, timestamp, severity and the business symptom that occurred at the same time. Do not change system settings just to make the event disappear.

Lab 4: Group Policy

```
gpupdate /force
gpresult /r
```

Explain which user/computer policies you can observe and how you would use that information in a ticket without guessing at policy configuration.

Lab 5: Safe Mode / application isolation

For a non-critical test application, compare normal launch and Safe Mode/clean-start behavior where supported. The objective is to understand how add-ins and background components can be isolated.

Lab 6: Outlook decision tree

Walk through: Outlook desktop fails -> test OWA -> test Safe Mode -> capture error -> check add-ins/profile -> repair/rebuild only if justified -> verify.

Lab 7: Printer isolation

Test a printer from two endpoints. Record whether the fault follows the printer, endpoint, queue or user. Practice writing the escalation note.

Lab 8: Phishing response tabletop

Pretend the user entered a password into a suspicious site. Practice the safe conversation: no blame, no password/OTP collection, secure reset/containment per policy, security escalation, evidence and documentation.

Lab rule: Do these exercises on a personal/test environment or under authorized IT support procedures. Never disable security controls or alter production systems just to complete a learning exercise.

18. Final 100-Question Mock Interview

Answer these without looking at the model material. For troubleshooting questions, use the L1 structure: verify, scope, recent change, isolate, test, fix, verify, document, escalate.

666. Tell me about yourself and your IT support experience.
667. What is the role of an L1 service desk?
668. What is an incident?
669. Incident vs service request?
670. What is an SLA?
671. How do you prioritize tickets?
672. What is impact vs urgency?
673. When do you escalate?
674. What makes a good ticket note?
675. How do you handle an angry user?
676. How do you troubleshoot a slow Windows PC?
677. What is Task Manager used for?
678. What is Event Viewer?
679. What is Device Manager?
680. How do you troubleshoot a blue screen?
681. What is Safe Mode?
682. What is SFC?
683. What is DISM?
684. How do you troubleshoot Windows Update?
685. What do you do if disk space is low?
686. What is an IP address?
687. What is a subnet mask?
688. What is a default gateway?
689. What is DNS?
690. What is DHCP?
691. Explain DORA.
692. What is APIPA?
693. What does ping do?
694. What does tracert do?
695. What does nslookup do?
696. User has no internet. Walk me through it.
697. User can ping 8.8.8.8 but not a domain name. Diagnose it.
698. User has 169.254.x.x. What do you do?
699. Wi-Fi connects but no internet. Diagnose it.
700. VPN does not connect. Diagnose it.
701. VPN connects but internal app fails. Diagnose it.
702. What is NAT?
703. TCP vs UDP?
704. Name five important ports.
705. What is RDP?
706. What is Active Directory?
707. Domain vs workgroup?
708. What is a Domain Controller?
709. User account locked. What do you do?
710. User forgot password. What do you do?
711. Authentication vs authorization?
712. What is a security group?
713. What is an OU?

- 714. What is GPO?
- 715. How do you troubleshoot a GPO not applying?
- 716. What is Microsoft 365?
- 717. Why test OWA when Outlook fails?
- 718. Outlook does not open. Diagnose it.
- 719. Outlook cannot send. Diagnose it.
- 720. Outlook not receiving. Diagnose it.
- 721. Teams mic not working. Diagnose it.
- 722. Teams camera not working. Diagnose it.
- 723. Teams sign-in fails. Diagnose it.
- 724. OneDrive not syncing. Diagnose it.
- 725. MFA prompt does not arrive. Diagnose it.
- 726. Monitor shows no signal. Diagnose it.
- 727. Laptop not charging. Diagnose it.
- 728. Printer offline. Diagnose it.
- 729. Print jobs are stuck. Diagnose it.
- 730. USB device not detected. Diagnose it.
- 731. No sound. Diagnose it.
- 732. Webcam works in Windows but not Teams. Diagnose it.
- 733. Shared drive is missing. Diagnose it.
- 734. Access Denied on file share. Diagnose it.
- 735. User cannot install software. Diagnose it.
- 736. What is phishing?
- 737. User clicked a suspicious link. What do you do?
- 738. User entered a password on a phishing site. What do you do?
- 739. User receives repeated MFA prompts. What do you do?
- 740. User reports ransomware-like activity. What do you do?
- 741. What is least privilege?
- 742. Why should support never ask for OTP codes?
- 743. What is endpoint security?
- 744. What is the principle of preserving evidence?
- 745. When is a security event more urgent than a normal support ticket?
- 746. What if you do not know the answer?
- 747. How do you deal with multiple high-priority tickets?
- 748. How do you explain technical problems to non-technical users?
- 749. Describe a difficult troubleshooting case.
- 750. Describe a mistake you made and what you learned.
- 751. How do you document a resolution?
- 752. How do you know when to stop troubleshooting?
- 753. How do you avoid making an issue worse?
- 754. How do you handle pressure to bypass policy?
- 755. How do you improve recurring ticket types?
- 756. Explain Authentication vs Authorization in one sentence each.
- 757. Explain DNS failure vs internet failure.
- 758. Explain DHCP failure vs Wi-Fi failure.
- 759. Explain profile corruption vs application corruption.
- 760. Explain local printer vs print-server problem.
- 761. Explain client outage vs service outage.
- 762. Explain workaround vs permanent fix.
- 763. Explain incident vs problem.
- 764. What are your strongest L1 skills?
- 765. Why should we hire you for this L1 role?

19. 7-Day Revision Schedule and Final Cheat Sheets

7-day revision schedule

Day	Study targets	Output
1	Windows + commands	Explain 10 common endpoint incidents and use core commands.
2	Networking + DNS/DHCP	Troubleshoot no internet, DNS, Wi-Fi, VPN.
3	AD + GPO	Handle account lockout, password, group access, domain/GPO basics.
4	M365	Outlook, Teams, OneDrive, MFA and web-vs-client isolation.
5	Hardware + printer + remote support	Solve device/peripheral and remote-access scenarios.
6	Security + ITSM + behavioral	Practice policies, escalation, customer communication.
7	Mock interview	Answer 100 questions out loud; note weak areas; revise those only.

Final command cheat sheet

```

ipconfig /all          -> IP/gateway/DNS/DHCP details
ipconfig /flushdns     -> clear DNS cache
ipconfig /renew        -> request DHCP lease
ping <host>            -> basic reachability test
tracert <host>         -> route/path view
nslookup <name>        -> DNS query
arp -a                -> ARP cache
netstat -ano           -> connections/listeners
whoami                 -> current identity
gpupdate /force        -> refresh Group Policy
gpresult /r            -> resulting policy
sfc /scannow           -> system file check
DISM ...RestoreHealth -> component store repair
tasklist               -> process list
systeminfo             -> system inventory

```

Final interview cheat sheet

- Always start with the symptom and business impact.
- Ask whether one user or many are affected.
- Ask what changed and when.
- Use a known-good comparison when possible.
- Explain why each diagnostic step is useful.
- Do not bypass security or access controls.
- Never ask users for passwords, MFA codes or secrets.
- Re-test the original business function after the fix.
- Document the evidence and action.
- Escalate with a complete handoff, not “please check.”

Final mindset: The best L1 analyst is not the person who knows the most commands. It is the person who can take an unclear user complaint, turn it into a testable problem, solve what is within scope, protect the environment, communicate clearly and leave a useful ticket behind.

Suggested reference areas for continued practice

- Microsoft Learn: Windows client, Microsoft 365, Entra ID and Intune fundamentals.
- Official Windows command documentation and networking reference material.
- Your employer’s own service-desk SOPs, knowledge base, priority matrix and escalation matrix.

- Practice in a safe lab using a Windows VM, test Microsoft account/tenant if available, and a non-production network.

Final Self-Assessment

Score yourself 0–2 for each line: 0 = cannot explain, 1 = can explain with notes, 2 = can explain confidently and troubleshoot aloud.

Topic	Score 0-2	Weak point / next action
Windows performance		
Windows login		
Windows Update		
Drivers/Device Manager		
Event Viewer		
Command line		
IP addressing		
DNS		
DHCP		
Wi-Fi		
VPN		
Active Directory		
Account lockout		
Group Policy		
Microsoft 365		
Outlook		
Teams		
OneDrive		
MFA		
Hardware		
Printers		
Remote support		
Security/phishing		
ITSM/SLA		
Ticket documentation		
Escalation		
Customer handling		
Mock troubleshooting		

Target before the interview: at least 45/56, with no critical topic at zero. More importantly, practice speaking your reasoning aloud because L1 interviews often evaluate how you think under pressure.