NETWORK CONNECTIVITY TROUBLESHOOTING GUIDE

Version 1.8 | Last Updated: January 2025

SECTION 1: WIRELESS CONNECTION ISSUES

SYMPTOMS:
- Device cannot connect to Wi-Fi network
- Intermittent connection drops
- "Cannot connect to network" error message
- Slow or unstable wireless connection
- Device shows connected but no internet access

ROOT CAUSES:
1. Incorrect Wi-Fi password
2. Router/access point configuration issues
3. Signal interference or weak signal strength
4. Network adapter driver problems
5. IP address conflicts
6. Router firmware issues

TROUBLESHOOTING STEPS:

Step 1: Verify Network Credentials
- Confirm SSID (network name) is correct
- Verify Wi-Fi password (case-sensitive)
- Check if network requires WPA2/WPA3 encryption
- Ensure device supports network security protocol

Step 2: Check Signal Strength
- Move device closer to router/access point
- Check signal strength indicator (should be 3+ bars)
- Identify and remove sources of interference:
  * Microwave ovens
  * Bluetooth devices
  * Other 2.4GHz/5GHz devices
  * Physical obstructions (walls, metal objects)

Step 3: Restart Network Components
- Power cycle router: Unplug for 30 seconds, then reconnect
- Restart access point if separate device
- Restart device network adapter:
  * Windows: Disable/enable Wi-Fi adapter
  * macOS: Turn Wi-Fi off/on
  * Mobile: Airplane mode on/off

Step 4: Forget and Reconnect Network
- Remove network from saved networks list
- Clear network credentials
- Scan for available networks
- Reconnect with correct credentials

- Verify connection status

Step 5: Update Network Adapter Driver
- Check current driver version in Device Manager
- Download latest driver from manufacturer website
- Uninstall old driver
- Install new driver
- Restart device

AUTOMATED RESOLUTION:
- Script: reset-wifi-connection.ps1
- Command: Reset-NetAdapter -Name "Wi-Fi"
- Verification: Test-NetConnection -ComputerName 8.8.8.8

SECTION 2: ETHERNET CABLE CONNECTION PROBLEMS

SYMPTOMS:
- "Network cable unplugged" error
- No link light on network port
- Intermittent connection with cable
- Slow wired connection speeds
- Device shows "Limited connectivity"

ROOT CAUSES:
1. Damaged or faulty Ethernet cable
2. Loose cable connection
3. Faulty network port (device or switch)
4. Incorrect cable type (Cat5 vs Cat6)
5. Network switch/router port failure

TROUBLESHOOTING STEPS:

Step 1: Physical Cable Inspection
- Check cable for visible damage (kinks, cuts, fraying)
- Verify cable is fully inserted at both ends
- Ensure cable clicks into place (RJ-45 connector)
- Try different Ethernet cable if available
- Test cable with cable tester if available

Step 2: Verify Port Status
- Check link/activity lights on network port
- Link light should be solid (connection established)
- Activity light should blink (data transmission)
- Try different port on switch/router
- Test with known working device

Step 3: Check Cable Type and Length
- Verify cable meets Cat5e or Cat6 standard
- Ensure cable length is under 100 meters (328 feet)
- Check cable rating (solid vs. stranded)

- Use appropriate cable for installation type

Step 4: Test Network Port
- Try connecting to different switch/router port
- Test device port with known working cable
- Check port configuration (auto-negotiation settings)
- Verify port is not disabled in switch management

Step 5: Update Network Driver
- Check Ethernet adapter driver version
- Download latest driver from manufacturer
- Update driver through Device Manager
- Restart device after driver update

AUTOMATED RESOLUTION:
- Script: reset-ethernet-adapter.ps1
- Command: Restart-NetAdapter -Name "Ethernet"
- Verification: Get-NetAdapterStatistics

SECTION 3: IP ADDRESS CONFIGURATION ISSUES

SYMPTOMS:
- "IP address conflict" error message
- Device assigned 169.254.x.x (APIPA) address
- Cannot obtain IP address from DHCP
- "Limited connectivity" or "No internet access"
- Network shows connected but cannot access resources

ROOT CAUSES:
1. DHCP server not responding
2. IP address conflict with another device
3. Incorrect static IP configuration
4. Subnet mask mismatch
5. Default gateway configuration error

TROUBLESHOOTING STEPS:

Step 1: Release and Renew IP Address
Windows:
- Open Command Prompt as Administrator
- Run: ipconfig /release
- Run: ipconfig /renew
- Verify new IP address assignment

macOS/Linux:
- Open Terminal
- Run: sudo ipconfig set en0 DHCP
- Or: sudo dhclient -r && sudo dhclient

Step 2: Check for IP Address Conflicts

- Note current IP address
- Ping the IP address from another device
- If ping succeeds, another device has same IP
- Change IP address or resolve conflict
- Restart network adapter

Step 3: Verify DHCP Server
- Check router/switch DHCP settings
- Verify DHCP scope is configured correctly
- Check DHCP lease pool has available addresses
- Restart DHCP service on router if possible
- Check DHCP server logs for errors

Step 4: Configure Static IP (If Required)
- Obtain available IP address from network admin
- Configure static IP in network settings:
  * IP Address: [assigned address]
  * Subnet Mask: [usually 255.255.255.0]
  * Default Gateway: [router IP]
  * DNS Servers: [primary and secondary DNS]
- Verify connectivity after configuration

Step 5: Flush DNS Cache
Windows:
- Run: `ipconfig /flushdns`

macOS:
- Run: `sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder`

Linux:
- Run: `sudo systemd-resolve --flush-caches`

AUTOMATED RESOLUTION:
- Script: reset-network-config.ps1
- Command: `Reset-NetIPConfiguration -InterfaceAlias "Ethernet"`
- Verification: `Get-NetIPAddress`

==

SECTION 4: DNS RESOLUTION PROBLEMS

==

SYMPTOMS:
- Websites load slowly or not at all
- "DNS server not responding" error
- Can access sites by IP but not by domain name
- Intermittent website access issues
- "This site can't be reached" errors

ROOT CAUSES:
1. DNS server unreachable or slow
2. Incorrect DNS server configuration
3. DNS cache corruption

4. Firewall blocking DNS queries
5. ISP DNS server issues

TROUBLESHOOTING STEPS:

Step 1: Test DNS Resolution
- Open Command Prompt/Terminal
- Run: nslookup google.com
- Check if DNS query returns IP address
- Try different domain name if first fails
- Note response time (should be under 100ms)

Step 2: Change DNS Servers
- Use public DNS servers:
  * Google: 8.8.8.8, 8.8.4.4
  * Cloudflare: 1.1.1.1, 1.0.0.1
  * OpenDNS: 208.67.222.222, 208.67.220.220
- Configure in network adapter settings
- Set both primary and secondary DNS
- Apply changes and test connectivity

Step 3: Flush DNS Cache
- Clear local DNS cache (see Section 3, Step 5)
- Restart DNS client service if needed
- Verify cache is cleared
- Test DNS resolution after flush

Step 4: Check Firewall Settings
- Verify firewall allows DNS traffic (port 53)
- Check both UDP and TCP port 53
- Review firewall logs for blocked DNS queries
- Temporarily disable firewall to test (re-enable after)

Step 5: Test Router DNS Configuration
- Access router admin interface
- Check DNS server settings
- Update router DNS if using ISP default
- Restart router after DNS change
- Verify devices receive new DNS via DHCP

AUTOMATED RESOLUTION:
- Script: fix-dns-resolution.ps1
- Command: Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 8.8.8.8,8.8.4.4
- Verification: Resolve-DnsName google.com

SECTION 5: VPN CONNECTION ISSUES

SYMPTOMS:
- Cannot establish VPN connection

- VPN connects but no internet access
- Slow VPN connection speeds
- Frequent VPN disconnections
- "VPN authentication failed" error

TROUBLESHOOTING STEPS:

Step 1: Verify VPN Credentials
- Confirm username and password are correct
- Check if account is locked or expired
- Verify two-factor authentication if required
- Test credentials on different device

Step 2: Check VPN Server Status
- Contact VPN administrator for server status
- Verify VPN server is online and accessible
- Check for scheduled maintenance windows
- Review VPN server logs if accessible

Step 3: Update VPN Client
- Check current VPN client version
- Download latest version from vendor
- Uninstall old client
- Install updated client
- Reconfigure VPN connection

Step 4: Firewall and Port Configuration
- Verify required VPN ports are open:
  * PPTP: TCP 1723
  * L2TP/IPSec: UDP 500, 4500
  * OpenVPN: UDP/TCP 1194
  * IKEv2: UDP 500, 4500
- Check firewall allows VPN traffic
- Test with firewall temporarily disabled

Step 5: Network Adapter Issues
- Disable other network adapters temporarily
- Check for conflicting network configurations
- Reset network adapter (see Section 2)
- Restart device and retry VPN connection

AUTOMATED RESOLUTION:
- Script: reset-vpn-connection.ps1
- Command: Restart-VpnConnection -Name "CompanyVPN"
- Verification: Get-VpnConnection

==

ESCALATION CRITERIA
==

Escalate to Network Team if:
- Multiple devices affected simultaneously

- Network infrastructure failure suspected
- Router/switch hardware issues
- Complex network configuration changes required
- Security breach or unauthorized access detected

Contact Information:
- Network Team: network@company.com
- Emergency: 1-800-NETWORK
- On-call Engineer: Check IT portal for current rotation

```
====================================================================
============
END OF DOCUMENT
====================================================================
============
```