NETBEEZ

Remote Contact Center Call Quality Troubleshooting Checklist

A practical guide for IT, UCaaS, CCaaS, network, and service desk teams

The problem

Your contact center platform may show that a call was bad.
But it often cannot prove whether the root cause was Wi-Fi, ISP, VPN, DNS, endpoint, network path, or the UCaaS/CCaaS provider.

Use this checklist before escalating bad-call incidents to NICE, Genesys, Five9, Amazon Connect, Zoom, Teams, Webex, RingCentral, Vonage, or 8x8.

Where bad calls usually start

Use this map to separate user-side network causes from platform-side issues.

Endpoint

CPU or memory pressure, softphone/browser issues, headset problems, recent updates, VPN client instability.

Local Wi-Fi / LAN

Weak signal, poor link quality, roaming, congestion, home router problems, incorrect SSID, guest Wi-Fi.

ISP

Packet loss, latency spikes, poor upload quality, regional peering, time-of-day congestion, unstable public IP path.

VPN / SASE / ZTNA

Full tunnel vs split tunnel, DNS behavior, routing changes, tunnel instability, unnecessary voice hairpinning.

DNS

Slow or failed lookups, split DNS issues, resolver changes, DNS failures only when VPN is active.

UCaaS / CCaaS path

Platform region, media path, service endpoint, SaaS reachability, provider-side or regional degradation.

NetBeez value proposition

Collect objective performance data directly from the remote agent and the network path so IT can prove whether a bad call was caused by Wi-Fi, ISP, VPN, DNS, endpoint conditions, or the platform path.

The first 15 minutes of troubleshooting

Start with context, then validate endpoint, Wi-Fi, ISP, VPN, DNS, and reachability.

1. Capture incident context

- Agent/workstation ID
- Time and date of issue
- Location: home, office, BPO, offshore site
- Affected app: softphone, browser, VDI, CRM
- Symptoms: dropped call, one-way audio, lag, freeze, reconnect

2. Check endpoint and connection type

- Wi-Fi or wired Ethernet?
- SSID, band, signal strength, link quality
- Dock, USB adapter, or direct Ethernet
- CPU, memory, recent reboot/update
- VPN client state

3. Validate Wi-Fi quality

- Stable signal and link quality
- No frequent disconnect/reconnect events
- No roaming or SSID switching during incident
- Low or zero packet loss
- No obvious congestion or interference pattern

4. Check ISP quality

- ISP name and public IP
- Latency and packet loss to internet targets
- Upload/download speed
- Time-of-day patterns
- Other agents on same ISP or region

5. Check VPN / SASE / ZTNA

- Connected or disconnected?
- Full tunnel vs split tunnel
- Public IP before/after VPN
- DNS behavior with VPN active
- Does issue occur only on VPN?

6. Test DNS and application reachability

- DNS success rate and response time
- Internal vs external resolver behavior
- HTTP response time for web apps
- Ping/TCP reachability where allowed
- Path analysis or traceroute changes

Compare, isolate, escalate

Do not troubleshoot one user in isolation - compare against peers and route the ticket with evidence.

Compare the affected agent against

- Other agents in same region
- Other agents on same ISP
- Other agents using same VPN/SASE path
- Office-based vs remote agents
- Wired vs Wi-Fi users
- Users on same UCaaS/CCaaS target

Escalation guide

Endpoint / desktop team	CPU or memory saturated; softphone/browser crashing; VPN client unstable; recent device update.
Network team	Packet loss or latency appears before provider; VPN/SASE path degrades traffic; multiple users at one site affected.
ISP	Public internet path shows loss; poor upload quality; multiple users on same ISP affected; regional peering issue suspected.
UCaaS / CCaaS provider	User-side Wi-Fi, ISP, VPN, DNS, and network path checks are clean, but platform/region still degrades.

What to include in a bad-call incident report

Use this structure to reduce back-and-forth between service desk, network, EUC, ISP, and UCaaS/CCaaS provider teams.

User context

- User/device
- Location
- Connection type
- ISP
- VPN state

Network evidence

- Latency
- Packet loss
- Jitter
- DNS results
- Path changes

Wireless evidence

- SSID
- Signal strength
- Link quality
- Band
- Disconnect events

Application evidence

- UCaaS/CCaaS target
- CRM/VDI target
- HTTP response
- Reachability
- Provider region

Peer comparison

- Same ISP
- Same region
- Same site
- Same VPN path
- Affected vs healthy

Decision

- Likely root cause
- Owner/team
- Next action
- Escalation path
- Evidence attached

What NetBeez can turn this into

Top 10 worst-performing agents | ISP quality report | Wi-Fi vs wired breakdown | VPN impact summary
UCaaS target performance | Recommended alert thresholds | Service desk playbook

How NetBeez helps remote contact center teams

NetBeez provides user-experience network monitoring for remote workers, offices, and distributed enterprises.

Monitor the user-side path

Remote worker Wi-Fi and wired connectivity
ISP performance
VPN/SASE/ZTNA impact
DNS, HTTP, ping, traceroute, and path analysis
SaaS and UCaaS/CCaaS reachability
Network speed and throughput tests

Reduce troubleshooting guesswork

Identify whether bad calls are likely caused by Wi-Fi, ISP, VPN, DNS, endpoint conditions, network path, or the platform itself.

Give service desk, EUC, voice, and network teams one objective data set for incident review.

Suggested next step: 2-4 week network health assessment

Start with a small group of remote contact center agents and produce a concrete report for IT and operations.

- 25-50 remote agents
- 2-3 network agents for offices, data centers, or offshore/BPO sites
- Monitor UCaaS/CCaaS, CRM, VPN, and DNS targets
- Produce a report with worst agents, ISP quality, VPN impact, Wi-Fi/wired breakdown, and thresholds

NETBEEZ

User-experience network monitoring for remote workers, Wi-Fi networks, and distributed enterprises.