CallerID.com
IDENTIFY | CONNECT | EMPOWER

# Tech Support Real-World Workbook

CallerID.com Academy · 30 September 2026

Practice learning material only. Not an official exam, certification, or customer-specific directive. Read each case's resolution status before taking action.

## Case 1. TCP call setup is not a UDP caller-ID feed

**Tier 3 · Unresolved — requires investigation**

### Scenario

A legacy Vertex sometimes displays a caller although most inbound calls never appear.

### Evidence

- The call INVITE is readable SIP over TCP at a nonstandard transport port.
- Voice packets are labeled OPUS; no matching UDP SIP setup is observed.

### Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the best-supported interpretation?

**A.** An intermittent popup proves compatibility.

**B.** OPUS is audio, while caller identity is in SIP; readable TCP signaling is not a dependable legacy Vertex UDP feed.

**C.** OPUS contains the missing phone number.

**D.** Every TCP session is encrypted.

Selected letter: _____ Why? _____

### 2. What is the safest next step?

**A.** Preserve an inbound capture and ask the provider about an authorized compatible UDP signaling path; test repeated calls.

**B.** Decode the audio stream for caller ID.

**C.** Declare intermittent behavior fixed.

**D.** Disable all network security without approval.

Selected letter: _____ Why? _____

### Verification plan

## Cautions

- No provider change or successful conversion is proved by these captures.

Practice source references: Technical bulletin B002 · Technical bulletin B009

# Case 2. Mixed UDP/TCP port mismatch at the bridge

**Tier 3 · Unresolved — requires investigation**

## Scenario

A phone registers and rings, but the Vertex produces status traffic without a caller number.

## Evidence

- An INVITE appears on UDP/5090; other handsets use TCP/5090.
- The SIP URI mentions 5060, but this capture has no UDP/5060 setup.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** The URI's 5060 does not override the observed wire transport/port; the documented Vertex path is not receiving the expected UDP/5060.

**B.** A URI string proves all packets use UDP/5060.

**C.** RTP carries the identity.

**D.** Status broadcasts prove the POS got caller ID.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Change the URI text in a screenshot.

**B.** Replace the POS before inspecting INVITEs.

**C.** Assume the provider already made the change.

**D.** Confirm live packet transport/port and device compatibility with support, then request an authorized provider change and retest.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- The proposed provider account change is not a demonstrated successful fix; do not generalize this device's port behavior to every model.

Practice source references: Technical bulletin B023

# Case 3. A SIP URI does not specify the packet's transport port

**Tier 3 · Unresolved — requires investigation**

## Scenario

Two phones receive readable inbound calls but the passive caller-ID reader remains silent.

## Evidence

- Outbound REGISTER is UDP source 5060 to proxy destination 5090.
- Inbound INVITE reverses direction: proxy source 5090 to handset destination 5060; the SIP request URI contains 5060.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the best-supported interpretation?

**A.** A URI guarantees the capture reader sees a 5060 source.

**B.** The inbound datagram is destined for proxy port 5090.

**C.** The provider did not deliver an INVITE.

**D.** The URI's 5060 is a logical SIP address, not proof of an inbound packet sourced from 5060.

Selected letter: _____ Why? _____

### 2. What is the safest next step?

**A.** Assume another site's absence of UDP/5060 applies here.

**B.** Rewrite source ports immediately in production.

**C.** Interpret a SIP URI as a UDP header.

**D.** Inspect both packet header ports on a timed inbound call and consult product/provider support before altering transport or NAT.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- The source-port rewrite option is proposed, not validated; NAT rewriting may disrupt SIP and requires network-owner approval.
- This capture has inbound destination UDP/5060, unlike bulletin B023's different site.

Generated by Rod Mac Kenzie · CallerID.com Academy · Tech Support practice · 30SEP26

# Case 4. A blank SIP filter does not prove no traffic

**Tier 3 · Unresolved — requires investigation**

## Scenario

The VCT call log is empty and a technician's Wireshark SIP display filter shows no rows.

## Evidence

- The unfiltered trace includes TLS application data during test calls.
- No readable matching inbound INVITE has yet been found at the Vertex interface.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** TLS application data reveals caller names.

**B.** A VCT test call proves real provider traffic reaches the port.

**C.** A SIP display filter hides encrypted TLS; lack of readable SIP alone does not establish a cable or hardware fault.

**D.** An empty display filter proves no packets crossed the switch.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Infer encryption solely from a blank filtered view.

**B.** Email an unredacted entire capture widely.

**C.** Factory-reset the Vertex.

**D.** Capture unfiltered traffic at the actual observation point and correlate a timed inbound call before deciding topology versus encryption.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Captures contain personal call metadata; restrict access and redact before training or sharing.
- A capture on an ordinary switched laptop port may not see other devices' calls.

Practice source references: Technical bulletin B013 · Technical bulletin B019

# Case 5. Firewall pass-through is not TLS termination

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

An installer proposes enabling SIP ALG on an existing firewall to make SIP-TLS readable to a passive Vertex.

## Evidence

- Provider-facing SIP is TLS.
- The available firewall routes traffic but is not the authorized SIP TLS endpoint.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the best-supported interpretation?

**A.** All TCP SIP is readable by the Vertex.

**B.** SRTP audio must be decrypted to read caller identity.

**C.** Opening ports or enabling SIP ALG does not expose protected INVITE identity to a passive listener.

**D.** A SPAN of ciphertext decrypts it.

Selected letter: _____ Why? _____

### 2. What is the safest next step?

**A.** Disable TLS at every handset.

**B.** Change firewall port alone and claim success.

**C.** Intercept TLS generically without approval.

**D.** Consult provider and qualified network engineer about an explicitly supported TLS-terminating SBC/B2BUA with a compatible, authorized local signaling leg.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- LTE-mode handset signaling may not traverse the LAN.
- The older bulletin's 3520/6699-as-SIP-listen-port and Vertex-as-SBC-trunk diagrams conflict with the later correction: those are output ports, and the Vertex is a passive observer, not a SIP endpoint.

- Do not decrypt SRTP merely for caller identity, expose plaintext broadly, open generic firewall ranges, or change emergency-calling paths without provider approval and rollback.

Practice source references: Technical bulletin B004 · Technical bulletin B006

# Case 6. Ingress classification versus output destination

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

A Vertex sees SIP packets, yet the POS workstation has no records.

## Evidence

- Gateway MAC identifies the SIP router/source for direction classification.
- Destination IP and MAC select where the separate UDP caller-ID output goes.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** The SIP gateway MAC is always the handset MAC.

**B.** POS destination IP determines whether INVITE is inbound.

**C.** A working phone proves POS output destination is correct.

**D.** SIP gateway identification and POS output delivery are distinct settings and failure domains.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Paste a sample site's IP/MAC into production.

**B.** Change the SIP URI instead.

**C.** Discover the inbound gateway MAC on a test call; inspect configured output destination, format and receiver before changing either.

**D.** Assume broadcast is accepted by all switches.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Do not reuse example site IP or virtual MAC across installations.
- A broadcast diagnostic is not proof of final unicast routing.

Practice source references: Technical bulletin B022

# Case 7. A readable call still cannot cross the POS network boundary

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

Calls appear in the device monitor, yet a segmented restaurant POS sees no popup after an upgrade.

## Evidence

- The bulletin documents a site whose switch allowed the caller-ID cable only on its designated port and another whose older device firmware needed an upgrade.
- A separate case required format, gateway classification and destination correction.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the best-supported interpretation?

**A.** Every missing popup is a SIP provider problem.

**B.** A readable INVITE proves that the POS receiver got UDP output.

**C.** Multiple downstream gates can block the POS independently of readable SIP; no single fleet-wide port, IP or firmware assumption is safe.

**D.** Every switch port is equivalent.

Selected letter: _____ Why? _____

### 2. What is the safest next step?

**A.** Flash firmware without approved model/rollback checks.

**B.** Ask the authorized POS/network owner to identify the site-specific allowed port, firmware requirement, listener format and destination; isolate them with captured output.

**C.** Bypass POS network controls unilaterally.

**D.** Copy a different store's host IP and MAC.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- The bulletin reports successful repairs in its historical tickets; they do not establish that the same change fixes a new site.
- A fleet-specific switch port is not a universal hardware requirement.

Practice source references: Technical bulletin B022

# Case 8. Cross-site WAF challenge on a relay request

**Tier 3 · Unresolved — requires investigation**

## Scenario

Many geographically separate POS sites lose popups at the same time; their local caller-ID devices still report events.

## Evidence

- Onsite relay reports HTTP 400 Bad Request; the direct relay uses GET first and may fall back to POST.
- Controlled GET and POST probes returned nominal 202 with a WAF challenge header, not an application receipt; vendor action is pending.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the best-supported interpretation?

**A.** Replace every local analog unit.

**B.** A WAF challenge proves the POS vendor already fixed it.

**C.** HTTP 400 proves a line's analog caller-ID signal is missing.

**D.** The failure is on the relay-to-POS HTTP delivery leg, not evidence of simultaneous device failures.

Selected letter: _____ Why? _____

### 2. What is the safest next step?

**A.** Escalate sanitized HTTP response/request characteristics to the POS vendor for endpoint/WAF review and confirm an approved resolution.

**B.** Reset every site device.

**C.** Disable all WAF controls unilaterally.

**D.** Log full customer payloads in a public issue.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Bulletin says awaiting vendor action; no confirmed restoration is established.
- Current plain-HTTP GET query can expose caller metadata; require an authorized HTTPS/authenticated design rather than assuming a broad WAF exemption is safe.

Generated by Rod Mac Kenzie · CallerID.com Academy · Tech Support practice · 30SEP26

# Case 9. Phone entry versus live popup

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

A POS tablet fills a phone-number field during order entry but shows no live ringing popup.

## Evidence

- One-Touch Phone Entry finds active calls without portal setup.
- Live Call Prompts require a per-device portal enablement and may be suppressed in an active order.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** This necessarily means the device lost SIP.

**B.** Both features require the same portal toggle.

**C.** Working one-touch entry does not establish that the independent live-popup feature is enabled.

**D.** A popup must appear inside any active order.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Claim a portal change fixed every tablet without retesting.

**B.** Confirm requested feature and per-device portal state, then test a ringing call outside an active order.

**C.** Switch analog lines to VoIP without diagnosis.

**D.** Replace hardware despite working one-touch entry.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Configuration instructions are not evidence that this site's popup was actually restored.

Practice source references: Technical bulletin B010

# Case 10. Some lines ring but are absent from order entry

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

One restaurant order terminal lists the first active caller, but a second concurrent caller never appears.

## Evidence

- The POS can display active caller numbers when its device sees them.
- The source warns that provider hunt/rollover and monitoring every active analog line can matter for concurrent calls.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** A per-line service or physical monitoring gap is plausible; intermittent caller display alone does not prove rollover is the root cause.

**B.** A one-line test verifies every concurrent line.

**C.** The live-popup portal toggle controls analog hunt routing.

**D.** All calls on an untapped line must be decoded.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Order a new device without checking line count.

**B.** Declare provider rollover faulty without testing.

**C.** Place controlled calls to each configured line, including simultaneous calls, then compare provider routing, monitored ports and received POS records.

**D.** Enable every popup tablet as a substitute for line capture.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Provider features vary; do not claim hunt/rollover is always the cause.

Practice source references: Technical bulletin B010

# Case 11. Cellular-capable handset versus captured LAN TLS

**Tier 3 · Unresolved — requires investigation**

## Scenario

A cellular-capable desk-phone model appears in a LAN trace as TLS application data, and only one of two lines produces a popup.

## Evidence

- The phone model supports more than one signaling mode.
- The observed call-related LAN flow is encrypted; the other line's path was not established.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the best-supported interpretation?

**A.** A firewall SIP ALG reveals the protected identity.

**B.** Both lines necessarily use the same transport.

**C.** A model suffix cannot prove cellular-only operation, and one LAN TLS flow cannot establish both lines' modes.

**D.** The local Ethernet capture contains the LTE air interface.

Selected letter: _____ Why? _____

### 2. What is the safest next step?

**A.** Assume the popup line proves TLS was decoded.

**B.** Disable provider TLS to test a hypothesis.

**C.** Buy an SBC on model number alone.

**D.** Confirm the configured mode and observe a timed call on each line before selecting an approved analog, provider event, or authorized clear-SIP path.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- B004's detailed SBC diagrams incorrectly portray the passive reader as an endpoint; rely on B006's correction and require provider authority.

Practice source references: Technical bulletin B004 · Technical bulletin B006

# Case 12. A dollar sign inside a fixed packet header

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

A POS intermittently displays punctuation and stray network-looking text instead of a phone number.

## Evidence

- A compressed device header can contain dollar signs.
- Receiving parser searches for the first dollar sign rather than skipping the fixed header.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** A stray hostname proves DNS poisoned the caller ID.

**B.** A dollar sign must mark every record start.

**C.** The receiver can begin parsing inside the header; a header delimiter search is not safe.

**D.** The device is necessarily emitting invalid call records.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Have the POS integrator parse the documented fixed header boundary and validate with sanitized records.

**B.** Publish raw customer packets as test fixtures.

**C.** Change device serial number.

**D.** Silently strip every dollar sign from payload.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- No specific customer serial or raw call number belongs in the training exercise.

Practice source references: Technical bulletin B011

# Case 13. Cloud-parked analog line keeps popup open

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

A popup opens correctly but stays visible when the call is parked in a hosted phone system.

## Evidence

- An ATA presents an analog line to the caller-ID device.
- Cloud parking can leave that analog line active, so the device has no observed hang-up event.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** The device cannot emit an analog hang-up event it never observes; POS clear policy needs separate evaluation.

**B.** Cloud parking always drops the ATA line.

**C.** Correct popup opening proves a matching End exists.

**D.** A SIP-TLS setting on the analog unit necessarily fixes it.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Replace the unit without testing analog line state.

**B.** Ask the POS integrator to review timer/answered-event dismissal against actual line behavior and test call states.

**C.** Claim the suggested POS change was deployed.

**D.** Invent an End event on every ring.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- The proposed POS behavior is guidance, not a measured successful fix.
- The bulletin mixes a raw TCP/3520 diagnostic with other UDP/3520 discussions; establish the integration's configured transport before opening a listener or assuming an End was delivered.

Practice source references: Technical bulletin B012

# Case 14. Forked SIP cancel versus answered-call end

**Tier 3 · Unresolved — requires investigation**

## Scenario

A popup may clear just as one of two ringing extensions answers.

## Evidence

- One branch returns 200 OK; the other receives CANCEL/487 about a second later.
- The answered dialog's BYE is about 23 seconds after that cancellation; output and POS timeline were not captured.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the best-supported interpretation?

**A.** CANCEL closes the losing branch, not the answered dialog; an early device End versus POS clearing remains unproven.

**B.** No packets on an assumed output port proves no End was sent.

**C.** Other TCP/TLS packets prove this call is encrypted.

**D.** Every CANCEL terminates the answered branch.

Selected letter: _____ Why? _____

### 2. What is the safest next step?

**A.** Suppress provider CANCEL traffic.

**B.** Assume the POS listening port is always 3520.

**C.** Capture synchronized SIP, configured device output and POS popup timestamps for a success and failure.

**D.** Claim firmware fix solely from SIP.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Three revised render variants, an earlier HTML and PDF-only supplied copy are one diagnostic family, not separate resolutions.

Practice source references: Technical bulletin B026

# Case 15. Readable inbound SIP, separate POS delivery

**Tier 3 · Unresolved — requires investigation**

## Scenario

A legacy bridge capture has a complete inbound forked call but the POS remains empty.

## Evidence

- One extension answers and two are canceled, followed by normal BYE.
- The bridge-side capture does not observe Management-port UDP output; VCT and POS receiver may contend for the same local UDP listener.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the best-supported interpretation?

**A.** The SIP side is readable; POS delivery must be measured on its separate interface.

**B.** No UDP/3520 in a bridge capture proves none was sent.

**C.** Normal losing-branch CANCEL proves malformed SIP.

**D.** A VCT display always proves the POS also received the packet.

Selected letter: _____ Why? _____

### 2. What is the safest next step?

**A.** Change provider transport before measuring output.

**B.** Treat separate outbound capture as same inbound call.

**C.** Ignore the listener conflict.

**D.** Capture at the Management-port receiver and verify local listener ownership, programmed format and destination.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- No definitive cause or repair is established solely from the reviewed bridge traces.

Practice source references: Technical bulletin B001

# Case 16. Generated sample bypasses live SIP

**Tier 3 · Unresolved — requires investigation**

## Scenario

A sample call appears in VCT but not the restaurant POS; live SIP capture has registration only, plus other TLS flows.

## Evidence

- Generated sample needs no provider INVITE.
- VCT binds UDP 3520 only on its own host/interface; the capture contains no live inbound INVITE.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the best-supported interpretation?

**A.** TLS traffic proves every live call is encrypted.

**B.** Successful registration proves inbound INVITEs use that transport.

**C.** Sample failure isolates an output/receiver path; the capture cannot classify live inbound signaling.

**D.** A laptop VCT binds the server's UDP port.

Selected letter: _____ Why? _____

### 2. What is the safest next step?

**A.** Assume prior analog integration validates this server listener.

**B.** Trace sample UDP output at the POS server and test port ownership, interface and format before a separate live-call capture.

**C.** Change SIP ports to repair generated samples.

**D.** Claim TLS root cause without INVITE.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Both subproblems remain open until measured independently.
- B015 records a Basic/Start receiver profile; B016 leaves this vendor's TCI flag unconfirmed. Verify live catalog and receiver requirements rather than assuming TCI.

Practice source references: Technical bulletin B015

# Case 17. Field spacing is a receiver contract

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

A POS expects TCI-spaced caller-ID fields but rejects an otherwise readable Vertex record.

## Evidence

- TCI changes spacing and termination, not caller-ID field meanings.
- VCT software format selector programs the format; phone setup cannot select it.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** A receiver's expected field spacing can cause a parse failure even when identity was extracted.

**B.** Dial-only phone setup programs any known format.

**C.** TCI is a SIP encryption mode.

**D.** A firmware setting named TCI must be toggled.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Reformat records by guessing field offsets.

**B.** Reflash firmware without evidence.

**C.** With the POS vendor's format requirement verified, select the matching software format in VCT and test a raw sample.

**D.** Change gateway MAC to alter spacing.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Do not assume a particular vendor uses TCI without confirming its specification.
- The related output bulletin calls a restaurant receiver Basic/Start while this bulletin says its TCI requirement is unconfirmed; check the current authoritative software record and actual bytes.

Practice source references: Technical bulletin B016

# Case 18. Call-waiting identity on an analog line

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

A second caller arrives while an analog conversation is active, but staff only sees the first caller.

## Evidence

- Type II caller ID is delivered during a call-waiting interval rather than between initial rings.
- The analog device supports Type II; SIP Vertex uses independent call legs rather than analog Type II.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** A ringing Type I test proves the carrier supplies Type II.

**B.** First distinguish analog call-waiting service and second-call signaling from a VoIP SIP-leg issue.

**C.** Type II requires the Vertex to decode OPUS.

**D.** Every second call is a SIP TLS failure.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Infer service subscription from a single first-ring popup.

**B.** Disable active calls to simulate Type II.

**C.** Confirm carrier Caller ID plus Call Waiting service and capture second-call event and receiver behavior while line is occupied.

**D.** Replace analog device immediately.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Support depends on actual carrier signaling and POS handling, not merely hardware capability.

Practice source references: Technical bulletin B017

# Case 19. Wizard test call has no usable identity

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

A VCT wizard reports that its inbound test call cannot be identified although a ring is seen.

## Evidence

- Test source has private/blocked or missing identity.
- The wizard requires a valid caller number to pass its identification step.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** The wizard identifies all internal PBX calls.

**B.** Ring detection alone does not establish that the test call included usable caller ID.

**C.** A blocked caller should still supply a public number.

**D.** The power supply is proven faulty.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Claim all customer calls are healthy based on one ring.

**B.** Repeat with a known outside line whose caller ID is enabled; inspect identity if the warning persists.

**C.** Disable the POS listener permanently.

**D.** Replace the unit first.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- The warning alone cannot prove hardware is good at this site; validate with controlled identity-bearing calls.

Practice source references: Technical bulletin B018

# Case 20. Dial-only Profi-Touch setup handshake

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

An installer sees the setup-mode test record but never sees the setup-updated record.

## Evidence

- DIP switch 2 down and reboot produced Setup Mode On in the POS.
- The dialed setup sequence is a capture signal, not a number that must connect.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** The first record validates output to POS, but absence of update leaves dial capture/signaling unverified.

**B.** Setup Mode On proves timezone update.

**C.** The procedure is a substitute for diagnosing encrypted VoIP.

**D.** A failed phone connection means setup cannot work.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Claim setup completed.

**B.** Change customer phone provider without approval.

**C.** Leave DIP switches in setup mode.

**D.** Stop repeated blind programming; check whether the Vertex can observe this site's VoIP signaling and escalate if it is encrypted.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- The bulletin's dial string is a setup code; no real outside call completion is expected.

Practice source references: Technical bulletin B020

# Case 21: ATA registration versus local dial tone

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

All PBX desk phones lose inbound and outbound service; a provider IP handset still works and the ATA emits dial tone.

## Evidence

- The direct handset bypasses the ATA/PBX.
- Dial tone and Ethernet link do not prove ATA SIP registration.
- The later recovery runbook explicitly says not to factory-reset before preserving provider-managed line state.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the best-supported interpretation?

**A.** Analog dial tone proves the provider accepted SIP REGISTER.

**B.** Investigate ATA account registration/proxy and the ATA-to-PBX path first.

**C.** Factory reset is the first safe step.

**D.** The working IP handset proves the ATA is registered.

Selected letter: _____ Why? _____

### 2. What is the safest next step?

**A.** Reset every port before taking a backup.

**B.** Preserve settings without copying secrets into tickets; inspect account status, proxy and provider record one line at a time with provider support.

**C.** Change the PBX without isolating the ATA.

**D.** Try default admin passwords in training material.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Earlier outage bulletin suggests factory reset as an option; later safe runbook supersedes that risky first action.
- Do not include passwords, IPs or account identifiers in training.

Practice source references: Technical bulletin B007 · Technical bulletin B008

# Case 22. Handset and ATA may compete for routing

**Tier 3 · Unresolved — requires investigation**

## Scenario

An Ethernet handset stops ringing while an ATA still feeds analog caller ID to the POS; disconnecting the ATA restores handset ringing.

## Evidence

- Provider log records inbound call, but does not prove delivery to handset.
- ATA output proves an ATA call leg, not a handset INVITE.
- Ethernet/PoE handset gets no ringing voltage from ATA.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** The analog Whozz load electrically starves the Ethernet handset.

**B.** ATA caller ID proves the handset received INVITE.

**C.** A distinct extension alone guarantees both endpoints ring.

**D.** Competing registration or provider forking is plausible, but false answer or LAN interference also remains possible.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Use sequential ATA-first hunt.

**B.** Declare a SIP cause based only on disconnect test.

**C.** Request provider binding and per-leg SIP traces, then pilot distinct extensions with explicit simultaneous ringing if shared registration is verified.

**D.** Change credentials blindly on all locations.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Leading hypothesis and recommended architecture are not a confirmed root cause or proven fix.

Practice source references: Technical bulletin B024

# Case 23. Power path collapse after reversed adapter

**Tier 3 · Confirmed resolution**

## Scenario

A Vertex will not power up after an incorrect adapter; correct input is present, the regulator rail sits near 3 V, and series diode tests good.

## Evidence

- The bulletin's bench case found damaged SCR gate branch despite an intact series diode.
- Replacement of the SCR was followed by passing performance tests in that documented repair.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the best-supported interpretation?

**A.** Any barrel connector with a 9 V label has correct polarity.

**B.** The diode must be shorted if the rail is low.

**C.** The regulator must be replaced first solely because its output is low.

**D.** An intact series diode does not exclude damage to the separate SCR gate network upstream of the starved regulators.

Selected letter: _____ Why? _____

### 2. What is the safest next step?

**A.** Probe a powered board without electrical precautions.

**B.** Assume every low rail has this same SCR fault.

**C.** Ship a regulator without inspecting upstream loading.

**D.** Quarantine power, confirm correct center-negative supply and refer board-level testing/replacement to qualified repair personnel.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Confirmed repair applies to the documented symptom set, not every no-power device.

Practice source references: Technical bulletin B021

# Case 24. Duplicate database key is not an analog hardware code

**Tier 3 · Unresolved — requires investigation**

## Scenario

A PC caller-ID program briefly shows caller data, then DBISAM reports duplicate RawNumber key.

## Evidence

- The index rejects a nonunique value.
- The bulletin does not identify the older application's actual database path or repair utility.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** The analog unit produced DBISAM error.

**B.** The software database/write path is implicated; a reboot alone does not prove corruption.

**C.** Any installed program folder is the database folder.

**D.** Deleting index files is a safe generic repair.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Treat a screenshot as proof of shared-server corruption.

**B.** Reinstall on all workstations before collecting logs.

**C.** Delete data/index files immediately.

**D.** Preserve error and version, close clients normally, identify data path and backup, then let product support choose repair.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- No actual repair has been established in the bulletin.

Practice source references: Technical bulletin B025

# Case 25. A working website is not a migration audit

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

A domain is serving HTTPS after an account-to-account DNS migration, and a technician proposes reusing the recorded remote-access/root-user procedure.

## Evidence

- Public HTTPS and DNS checks passed for tested hosts.
- The procedure omitted dashboard-only controls, mail/DNSSEC gates, access cleanup and rollback evidence.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. What is the best-supported interpretation?

**A.** Operational availability does not prove security and all services survived the move.

**B.** One HTTPS response proves mail, WAF and DNSSEC were preserved.

**C.** Public DNS alone proves access links were revoked.

**D.** Root access is required for routine zone transfers.

Selected letter: _____ Why? _____

## 2. What is the safest next step?

**A.** Declare security closure from website uptime.

**B.** Delete source zone before checks.

**C.** Do not reuse the recorded procedure; perform named-user credential cleanup and dashboard-only service/security review with rollback gates.

**D.** Publish the recorded remote session.

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Public checks confirm only tested endpoints, not all zone settings.
- No live secrets or remote links belong in exercises.

Practice source references: Technical bulletin B005

# Case 26. A repaired device still cannot populate the POS

**Tier 3 · Confirmed resolution**

## Scenario

A VoIP-to-POS installation had flashing lights and no network response. After service, the device returned with normal lights, but the POS still showed no caller ID.

## Evidence

- Before service, it could not be pinged even when directly connected to a laptop.
- After return, the technician found the receiving POS port configured for 3520 rather than the required 6699.
- Changing the port was followed by an explicit working report.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What should be checked after the repaired hardware comes online but POS pop-ups still fail?

**A.** Replace the telephone handsets

**B.** Compare the device's data output port against the POS listener

**C.** Assume the repair was ineffective

**D.** Disable the router firewall without testing

Selected letter: _____ Why? _____

### 2. Which observation confirms the second issue was resolved?

**A.** The port was changed and the installation was reported working

**B.** The ticket was placed in Solved

**C.** The customer received return instructions

**D.** The power LED lit

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- A lit link does not prove that the POS listens on the right port.

Practice source references: Technical helpdesk case A01

# Case 27. Scrambled POS output is not proof of encrypted SIP

**Tier 3 · Confirmed resolution**

## Scenario

A POS received scrambled caller data and sometimes rendered the word 'Encrypted'; staff suspected the inline VoIP device was encrypting packets.

## Evidence

- Three bridge lights were lit.
- A packet capture was assessed as unencrypted.
- The POS provider corrected its own setup and reported normal operation.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What evidence should carry most weight in testing the encryption theory?

**A.** A capture of signaling on the relevant link

**B.** The POS's literal 'Encrypted' label

**C.** Whether the ticket is closed

**D.** The age of the device

Selected letter: _____ Why? _____

### 2. What ultimately resolved the symptom?

**A.** A new VoIP carrier

**B.** Correcting the POS configuration

**C.** Replacing the bridge

**D.** Changing the caller's number

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Do not infer encrypted transport from a POS display string alone.

Practice source references: Technical helpdesk case A02

# Case 28. A new router strands an otherwise working integration

**Tier 3 · Confirmed resolution**

## Scenario

After a router replacement, a previously working device stopped displaying caller ID in Toast, although the POS vendor believed its side was healthy.

## Evidence

- The change was the new router.
- Support installed firmware revision 143z and configured the new SIP gateway.
- The case note explicitly states it was working in Toast afterwards.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. Which change should be revisited before replacing the device?

**A.** The age of the POS monitor

**B.** The SIP gateway configuration after the router swap

**C.** The colors of the telephone cords

**D.** The customer's subscription payment

Selected letter: _____ Why? _____

## 2. Can this case isolate firmware upgrade alone as the fix?

**A.** No, firmware and gateway configuration were changed together

**B.** Yes, firmware was mentioned first

**C.** No, because no action was recorded

**D.** Yes, because Toast was involved

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Do not attribute causality to just one of two simultaneous interventions.

Practice source references: Technical helpdesk case A03

# Case 29. All link lights on, but the management path left the POS LAN

**Tier 3 · Confirmed resolution**

## Scenario

After an interruption to the telephone line, phones were restored by bypassing the device, but caller ID no longer reached a Revel POS.

## Evidence

- All amber lights were illuminated.
- The phone-setup simulated call failed to reach POS.
- The IT contact found the switch port used by the device was no longer on the POS LAN; reconfiguring that port restored operation.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What does the failed simulated call suggest in this context?

**A.** The phones have no dial tone

**B.** The device-to-POS management path should be checked

**C.** An encrypted SIP feed must be present

**D.** The caller ID subscription expired

Selected letter: _____ Why? _____

### 2. What was the recorded corrective action?

**A.** Reformat the POS hard drive

**B.** Move the receiving switch port back onto the POS network

**C.** Turn off the phone service

**D.** Replace every handset

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Link lights do not establish VLAN or subnet reachability.

Generated by Rod Mac Kenzie · CallerID.com Academy · Tech Support practice · 30SEP26

# Case 30. Restore detection without guessing at several moving cables

**Tier 3 · Confirmed resolution**

## Scenario

A site stopped receiving POS caller ID. The installer moved phone and management cables repeatedly, obscuring whether the loss was on the voice or data side.

## Evidence

- Support asked to stabilize the management connection before changing phone wiring.
- A capture of a real call identified the SIP gateway.
- Support selected Slow Start SDP because the protocol behaved unusually; the user then observed data in Pulse, despite an empty tool monitor.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is the safest troubleshooting sequence?

**A.** Change both cable sets at once

**B.** Stabilize and test the management path, then capture a real call and set gateway/protocol options

**C.** Treat an empty monitor as proof the POS is empty

**D.** Replace the POS first

Selected letter: _____ Why? _____

### 2. What supports a working outcome?

**A.** A staff hypothesis

**B.** The user's report of data in the Pulse terminal

**C.** The ticket stage alone

**D.** A device serial number

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- A monitoring window and the actual POS may not show identical results.

Generated by Rod Mac Kenzie · CallerID.com Academy · Tech Support practice · 30SEP26

# Case 31: A POS upgrade blocks the push despite an active device

**Tier 3 · Confirmed resolution**

## Scenario

A Domino's POS upgrade was followed by missing pop-ups. The field technician initially suspected phone and management wiring.

## Evidence

- The management cable was tried on a direct POS-network port.
- The later note identifies a new Pulse port setting that blocked UDP traffic to the device.
- After the Pulse technician permitted UDP on port 3520 to that port, pop-ups began working.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

## 1. After an upgrade, which boundary must be inspected?

**A.** The ringtone volume only

**B.** The color of the Ethernet jacket

**C.** The purchase warranty

**D.** UDP allowance on the new POS equipment's device-facing port

Selected letter: _____ Why? _____

## 2. Why not declare the bridge defective from missing pop-ups?

**A.** Link lights prove the entire path

**B.** Every missing popup means encrypted SIP

**C.** An application/network policy can block otherwise valid pushes

**D.** The router can never change

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Confirm UDP, not TCP, for this documented path.

Practice source references: Technical helpdesk case A06

# Case 32. New switch fixes link, not encrypted signaling

**Tier 3 · Confirmed resolution**

## Scenario

A replacement device exhibited the same problem as its predecessor. Swapping a phone-side switch restored correct link lights, but live calls remained unreadable.

## Evidence

- With a compatible switch, the expected lights came on.
- The carrier declined to send unencrypted SIP directly.
- A provisioned Edgewater device was later installed; phone setup completed and Toast was explicitly reported working.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What did the switch replacement actually prove?

**A.** It converted TCP to UDP

**B.** It decrypted SIP

**C.** It fixed the Toast subscription

**D.** It restored physical/network link only

Selected letter: _____ Why? _____

### 2. What made the final result different?

**A.** Turning off the POS

**B.** Replacing all handsets

**C.** Adding a carrier-side device with usable signaling and completing setup

**D.** Repeating the switch swap

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- A generic 10/100 switch does not decrypt encrypted SIP.

Practice source references: Technical helpdesk case A07

# Case 33. A cloud relay will not run on a locked-down host

**Tier 3 · Confirmed resolution**

## Scenario

A POS cloud-relay installation failed on a workstation that could not run the required application; phone traffic also required a careful network layout.

## Evidence

- Initial notes cited a .NET compatibility issue; a less restrictive relay build still did not run on the original PC.
- The technician suspected OS application restrictions but did not prove the precise reason.
- A separate mini computer ran the relay in service mode with a configured store location; the final note says it worked.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What is known about the original PC failure?

**A.** The POS vendor disabled all ports

**B.** The modified installer still failed; the exact restriction remained a suspicion

**C.** The OS restriction was conclusively proven

**D.** SIP encryption caused installation failure

Selected letter: _____ Why? _____

### 2. Why select service mode on the replacement host?

**A.** To turn a switch into a router

**B.** So the relay can run while the host is powered without an interactive login

**C.** To change analog signaling

**D.** To encrypt the phone traffic

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Do not generalize an unverified OS diagnosis to every relay failure.

Practice source references: Technical helpdesk case A08

# Case 34. Voice link recovered, but a POS-side service remains down

**Tier 3 · Unresolved — requires investigation**

## Scenario

After a carrier/network renewal, a PoE switch yielded no VoIP bridge lights. Replacing it initially took down the phones, and a second attempt restored voice-side visibility.

## Evidence

- After correct switch installation, the phones worked and the configuration tool showed incoming calls.
- Caller ID appeared in the device monitor but not in PizzaPOS.
- Changing an INI address allowed a database connection; the POS caller-ID service still did not run, so the POS vendor was asked to investigate.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What should be tested before declaring the whole system repaired?

**A.** Only the power light

**B.** Phone service, device monitor and POS receiver separately

**C.** Only the switch's brand

**D.** The invoice

Selected letter: _____ Why? _____

### 2. What is the proper resolution classification?

**A.** Confirmed device failure

**B.** No troubleshooting occurred

**C.** Confirmed end-to-end

**D.** Documented guidance with POS-side work outstanding

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Do not interpret a Solved ticket stage as end-to-end success.

Generated by Rod Mac Kenzie · CallerID.com Academy · Tech Support practice · 30SEP26

# Case 35. Queue routing and POS broadcast both matter

**Tier 3 · Confirmed resolution**

## Scenario

A legacy device stopped displaying calls after a POS/network change. The team could reach the device, but a simulated push did not appear on Pulse.

## Evidence

- The POS team eventually saw SIP during a phone setup and real caller data appeared after the gateway issue was revisited.
- A ring-group-to-call-queue change preceded tests of multiple simultaneous calls.
- The final working configuration placed the device on the correct POS switch port and targeted the POS host's broadcast address instead of an all-host broadcast.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. Why is a reachable device insufficient proof?

**A.** A ping always carries caller ID

**B.** The phone routing and receiving POS data path can fail independently

**C.** The customer has no phones

**D.** The device must be analog

Selected letter: _____ Why? _____

### 2. What end-to-end test was recorded?

**A.** A single link LED

**B.** A ticket assignment

**C.** A purchase of new equipment

**D.** Four simultaneous calls appearing on screen

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- The notes involve multiple changes; do not claim one change alone caused recovery.

Generated by Rod Mac Kenzie · CallerID.com Academy · Tech Support practice · 30SEP26

# Case 36. Rebuild a VoIP bridge path after a provider change

**Tier 3 · Confirmed resolution**

## Scenario

After changing to a new VoIP provider, Toast displayed no caller ID. During after-hours tests, forwarding to cloud voicemail also prevented useful inbound captures.

## Evidence

- An earlier attempt routed phone signaling through the POS router.
- The installer and carrier rewired the gateway and handset-side connections on the provider's router.
- After moving the gateway feed and rebooting the devices, calls worked and settings held.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. Why should an after-hours capture be treated cautiously?

**A.** The POS requires analog only

**B.** Forwarding can keep the inbound call out of the local signaling path

**C.** Wireshark never captures SIP

**D.** A reboot decrypts packets

Selected letter: _____ Why? _____

### 2. Which verification best closes this case?

**A.** The case was assigned

**B.** The new port arrangement worked and survived a reboot

**C.** The bridge has a serial number

**D.** A PDF was sent

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- No-SIP observations during forwarded calls do not by themselves prove encryption.

Practice source references: Technical helpdesk case A11

# Case 37. A comparison unit narrows a post-outage hardware failure

**Tier 3 · Confirmed resolution**

## Scenario

After a power outage, an analog caller-ID unit stopped delivering data over a serial-to-USB connection. A different unit functioned through the same site setup.

## Evidence

- The serial loop test reported no activity from the affected unit.
- A substitute device worked at the location.
- Bench notes identified a damaged RS-232 chip and other failed components; after replacement, the unit passed tests and was ready to return.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What does the substitute-unit test most strongly suggest?

**A.** The router has no internet

**B.** The carrier encrypted analog calls

**C.** The original hardware or its power supply merits bench diagnosis

**D.** The POS cannot use a serial connection

Selected letter: _____ Why? _____

### 2. What is the documented verification boundary?

**A.** Customer acceptance after reinstall

**B.** Only ticket closure

**C.** Bench testing after component replacement

**D.** An unopened RMA

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Power outage timing is not proof of which component failed.

Generated by Rod Mac Kenzie · CallerID.com Academy · Tech Support practice · 30SEP26

# Case 38. Unreachable on two networks, then recovered on the bench

**Tier 3 · Confirmed resolution**

## Scenario

A previously working VoIP device could no longer be discovered by the configuration tool, including when moved to a different office network.

## Evidence

- Support proposed an RMA rather than treating network discovery failure as certain proof of a broken unit.
- The bench found no power LED and erased memory.
- Technicians reprogrammed it, upgraded its firmware and replaced the old power supply; the bench note states it worked afterwards.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. Which finding moves the diagnosis beyond a single customer LAN issue?

**A.** The POS brand changed

**B.** It also failed discovery in a separate environment

**C.** The ticket contained an RMA

**D.** The device was out of warranty

Selected letter: _____ Why? _____

### 2. Can the exact cause of erased memory be established from these notes?

**A.** Yes, the router certainly erased it

**B.** Yes, firmware alone proves it

**C.** No; reprogramming and power-supply replacement were performed, but cause was not isolated

**D.** Yes, the POS erased it

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Do not present a speculative memory-loss mechanism as a confirmed root cause.

Generated by Rod Mac Kenzie · CallerID.com Academy · Tech Support practice · 30SEP26

# Case 39. An analog device cannot decode a VoIP phone source

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

An analog two-line device no longer pushed caller ID to POS. The customer reported telephone caller ID and tried wiring its inputs directly to a box with telephone-style ports.

## Evidence

- The physical source was later identified as a VoIP cordless-phone base.
- Direct connection to the analog device still produced no caller ID.
- Support advised an appropriately provisioned VoIP device, subject to readable UDP SIP; return/exchange was started but no successful installation was recorded.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What test of the initial analog-splitter hypothesis changed the diagnosis?

**A.** The ticket was closed

**B.** A new paper manual was emailed

**C.** The customer changed the POS theme

**D.** Direct connection still failed and the phone source proved to be VoIP

Selected letter: _____ Why? _____

### 2. What should happen before promising a replacement will work?

**A.** Ignore the telephone architecture

**B.** Order any new unit immediately

**C.** Assume every VoIP source uses readable UDP

**D.** Verify the provider's SIP transport and encryption and the proposed bridge wiring

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- A return authorization is not confirmation of a working replacement.

Practice source references: Technical helpdesk case A14

# Case 40. Reproduce an intermittent second-line complaint

**Tier 3 · Documented guidance — outcome not confirmed**

## Scenario

A customer reported that the second simultaneous call had never popped up consistently, despite the first line working.

## Evidence

- The customer was not initially on site for a shared test.
- On site, support placed simultaneous calls repeatedly.
- Both calls appeared in the device record and POS screen on three attempts, including a check from another POS station.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What does the repeated on-site test establish?

**A.** The fault was permanently repaired

**B.** The symptom was not reproduced under the tested conditions

**C.** Line two is unplugged

**D.** The provider must be at fault

Selected letter: _____ Why? _____

### 2. What should be requested if the complaint recurs?

**A.** A timed real-call example with station/line and device-versus-POS observations

**B.** Immediate replacement without tests

**C.** Only a screenshot of the ticket stage

**D.** A change to all phone numbers

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- This is a verified non-reproduction, not a confirmed permanent fix.

Practice source references: Technical helpdesk case A15

# Case 41: Several sites fail when a POS API challenges the relay

**Tier 3 · Unresolved — requires investigation**

## Scenario

Several independent locations simultaneously reported cloud-relay errors, even though their hardware and the supplier's relay were reported operational.

## Evidence

- The shared failure was attributed in the thread to a POS vendor AWS WAF challenge on programmatic caller-ID requests.
- The relay cannot solve a browser JavaScript challenge, resulting in HTTP 400 responses.
- Support sent the vendor a technical proposal to exempt the API path or provide a machine-friendly authorization mechanism; no vendor-side fix was documented.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What does simultaneous failure across several sites suggest?

**A.** Every site lost its power supply together

**B.** The relay needs a browser popup

**C.** All phones switched to analog

**D.** A shared upstream POS/API policy change

Selected letter: _____ Why? _____

### 2. What status should be communicated?

**A.** Confirmed device repair

**B.** No evidence exists

**C.** Confirmed resolved because the ticket says Solved

**D.** Vendor-side remediation recommended, but no successful follow-up recorded

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Never publish a site's endpoint identifier, customer IP or proposed allowlist values.

Generated by Rod Mac Kenzie · CallerID.com Academy · Tech Support practice · 30SEP26

# Case 42. A popup disappears when the call is picked up

**Tier 3 · Unresolved — requires investigation**

## Scenario

The POS displayed a call initially but cleared its caller-ID card at pickup.

## Evidence

- A packet capture was reviewed.
- The case note identifies a SIP CANCEL with a 'Call completed elsewhere' reason.
- No subsequent provider or POS configuration change, nor recovered display behavior, appears in the case.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What distinguishes this from a missing initial caller-ID problem?

**A.** No call reaches the store

**B.** The device has no lights

**C.** The installer forgot a password

**D.** The popup appears first and clears at pickup

Selected letter: _____ Why? _____

### 2. What should support do next?

**A.** Ignore the capture

**B.** Disable all firewall rules

**C.** Correlate the CANCEL event with device output and POS dismissal; ask the provider/POS vendor about the reason

**D.** Claim a confirmed hardware repair

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Do not equate identifying a SIP reason with fixing the display.

Practice source references: Technical helpdesk case A17

# Case 43. Serial mode changes where to observe data

**Tier 3 · Unresolved — requires investigation**

## Scenario

A Vertex showed calls in its network monitor, but a serial-connected POS did not receive them. Support initially focused on why the network call log was empty after switching output to serial.

## Evidence

- A broadcast/network test demonstrated the device could capture inbound calls.
- In serial mode, the relevant evidence was physical serial output and the receiving COM port, not only a network call-log window.
- The POS vendor opened and selected a COM port, yet the POS remained empty; an RMA/replacement was authorized with the serial fault still unconfirmed.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. Which test would best separate a failed serial output from a POS receiver problem?

**A.** Count the ticket comments

**B.** Capture actual serial output at the configured baud rate with the POS service released from the COM port

**C.** Change the phone provider

**D.** Look only at the network monitor

Selected letter: _____ Why? _____

### 2. What is the defensible final classification?

**A.** Confirmed POS repair

**B.** Unresolved serial-to-POS path with a suspected device issue and pending bench test

**C.** Confirmed defective serial hardware

**D.** Confirmed encryption

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Do not claim a no-charge RMA proves a failed device.

Generated by Rod Mac Kenzie · CallerID.com Academy · Tech Support practice · 30SEP26

# Case 44. Phones still work when the bridge is unplugged

**Tier 3 · Unresolved — requires investigation**

## Scenario

A Toast installation had phones that worked but no caller-ID pop-ups, despite hours spent on POS-side troubleshooting.

## Evidence

- Unplugging the bridge did not interrupt the phones.
- The team found a separate jumper feeding the wireless telephone path.
- Wiring and setup instructions were sent; later test numbers reached POS, but a real call displayed only partial data and further investigation awaited an Ethernet-equipped laptop.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. What does the unplug test reveal?

**A.** Calls are bypassing the intended inline monitoring path

**B.** All phones are defective

**C.** The bridge decrypted SIP

**D.** The POS has no network

Selected letter: _____ Why? _____

### 2. Was the entire installation verified?

**A.** No test was attempted

**B.** No; test numbers reached POS but real-call output remained incomplete

**C.** Yes, simulated tests always prove real calls

**D.** Yes, because all lights were lit

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Test signals cannot establish all real-call formatting and gateway behavior.

Practice source references: Technical helpdesk case A19

# Case 45. Device captures calls, POS provider corrects its receiver

**Tier 3 · Confirmed resolution**

## Scenario

A new POS installation continued to show no pop-ups after the caller-ID device was configured.

## Evidence

- The device's call log showed captured inbound caller ID.
- Reconnecting it to the POS network did not yield a POS display.
- The installer later reported that the POS provider had misconfigured its system; after correction, caller ID worked on the order-entry screen.

## Think it through

What does the evidence establish? What remains uncertain? What would you verify before acting?

### 1. Which boundary does a populated device log but empty POS screen localize?

**A.** Carrier encryption alone

**B.** The power supply only

**C.** Device output/receiving POS integration

**D.** The customer's telephone dial tone

Selected letter: _____ Why? _____

### 2. What confirms the outcome?

**A.** The installer's report of a corrected POS setup and working order-entry display

**B.** The ticket was renamed

**C.** The phone switch had lights

**D.** A setup PDF was promised

Selected letter: _____ Why? _____

## Verification plan

## Cautions

- Do not prescribe an undocumented exact POS setting.

Practice source references: Technical helpdesk case A20