



# Tech Support Real-World Answer Key

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.

### Answers and reasoning

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

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

The supplied observations support: OPUS is audio, while caller identity is in SIP; readable TCP signaling is not a dependable legacy Vertex UDP feed. They do not establish the competing explanations without additional evidence.

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

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

The bulletin's evidence supports this sequence: Preserve an inbound capture and ask the provider about an authorized compatible UDP signaling path; test repeated calls. Do not treat an untested recommendation as a confirmed repair.

### Documented guidance / next steps

1. Separate SIP signaling from RTP/audio.
2. Check actual TCP/UDP headers on the inbound INVITE.
3. Escalate transport changes to provider and validate at the observation point.

### Verification

- Repeat inbound calls and confirm every number and matching POS event.

### Cautions

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

---

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

#### Answers and reasoning

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

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

The supplied observations support: The URI's 5060 does not override the observed wire transport/port; the documented Vertex path is not receiving the expected UDP/5060. They do not establish the competing explanations without additional evidence.

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

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

The bulletin's evidence supports this sequence: Confirm live packet transport/port and device compatibility with support, then request an authorized provider change and retest. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Filter for the actual inbound INVITEs and inspect UDP/TCP source and destination ports.
2. Confirm device firmware/model expectations; arrange provider-side correction if supported.
3. Retest inbound identification and POS receipt.

#### Verification

- Capture compatible inbound INVITEs at the Vertex and matching caller-ID output for multiple calls.

#### Cautions

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

## 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.

#### Answers and reasoning

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

Correct: D. The URI's 5060 is a logical SIP address, not proof of an inbound packet sourced from 5060. The supplied observations support: The URI's 5060 is a logical SIP address, not proof of an inbound packet sourced from 5060. They do not establish the competing explanations without additional evidence.

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

Correct: D. Inspect both packet header ports on a timed inbound call and consult product/provider support before altering transport or NAT. The bulletin's evidence supports this sequence: Inspect both packet header ports on a timed inbound call and consult product/provider support before altering transport or NAT. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Match REGISTER and inbound INVITE directions.
2. Compare the actual source and destination UDP headers with the reader's documented requirement.
3. If an authorized correction is proposed, preserve rollback and re-test every call leg.

#### Verification

- Correct identities reach the reader and POS without affecting phone registration or audio.

#### 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.

Practice source references: Technical bulletin B014

## 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.

#### Answers and reasoning

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

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

The supplied observations support: A SIP display filter hides encrypted TLS; lack of readable SIP alone does not establish a cable or hardware fault. They do not establish the competing explanations without additional evidence.

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

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

The bulletin's evidence supports this sequence: Capture unfiltered traffic at the actual observation point and correlate a timed inbound call before deciding topology versus encryption. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Export VCT decoded call records first.
2. Capture a consented timed inbound test at the bridge/appropriate mirror.
3. Inspect unfiltered transport and SIP/TLS and compare with VCT output.

#### Verification

- Show a matching inbound INVITE or TLS flow at the intended port; establish whether identity is readable.

#### 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.

#### Answers and reasoning

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

Correct: C. Opening ports or enabling SIP ALG does not expose protected INVITE identity to a passive listener. The supplied observations support: Opening ports or enabling SIP ALG does not expose protected INVITE identity to a passive listener. They do not establish the competing explanations without additional evidence.

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

Correct: D. Consult provider and qualified network engineer about an explicitly supported TLS-terminating SBC/B2BUA with a compatible, authorized local signaling leg. The bulletin's evidence supports this sequence: Consult provider and qualified network engineer about an explicitly supported TLS-terminating SBC/B2BUA with a compatible, authorized local signaling leg. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Confirm phone mode and actual signaling at capture point.
2. Document provider-supported SBC topology, certificates and security boundary.
3. Pilot an authorized clear compatible signaling leg at Vertex's real interface.

#### Verification

- Repeated calls reveal expected caller headers on the intended local leg and POS records without degrading service.

#### 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.

## 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.

#### Answers and reasoning

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

Correct: D. SIP gateway identification and POS output delivery are distinct settings and failure domains. The supplied observations support: SIP gateway identification and POS output delivery are distinct settings and failure domains. They do not establish the competing explanations without additional evidence.

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

Correct: C. Discover the inbound gateway MAC on a test call; inspect configured output destination, format and receiver before changing either. The bulletin's evidence supports this sequence: Discover the inbound gateway MAC on a test call; inspect configured output destination, format and receiver before changing either. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Record current configuration.
2. Use VCT discovery or inspect Ethernet source of a real inbound INVITE.
3. Verify programmed output IP/MAC/port with the POS administrator and observe receiver traffic.

#### Verification

- Matched inbound call is classified and matching POS record arrives at configured receiver.

#### 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.

### Answers and reasoning

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

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

The supplied observations support: Multiple downstream gates can block the POS independently of readable SIP; no single fleet-wide port, IP or firmware assumption is safe. They do not establish the competing explanations without additional evidence.

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

Correct: 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.

The bulletin's evidence supports this sequence: Ask the authorized POS/network owner to identify the site-specific allowed port, firmware requirement, listener format and destination; isolate them with captured output. Do not treat an untested recommendation as a confirmed repair.

### Documented guidance / next steps

1. Preserve current settings and confirm device/POS compatibility.
2. Capture output on both sides of the approved switch path and check listener state.
3. Have the POS owner authorize required port, format, firmware and destination changes one at a time.

### Verification

- Test ringing popup and caller identity after each change and after reboot.

### 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.

## 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.

#### Answers and reasoning

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

Correct: D. The failure is on the relay-to-POS HTTP delivery leg, not evidence of simultaneous device failures. The supplied observations support: The failure is on the relay-to-POS HTTP delivery leg, not evidence of simultaneous device failures. They do not establish the competing explanations without additional evidence.

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

Correct: A. Escalate sanitized HTTP response/request characteristics to the POS vendor for endpoint/WAF review and confirm an approved resolution. The bulletin's evidence supports this sequence: Escalate sanitized HTTP response/request characteristics to the POS vendor for endpoint/WAF review and confirm an approved resolution. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Correlate relay inbound events with outbound HTTP errors.
2. Provide vendor minimal redacted response and timing.
3. Retest authorized GET and fallback POST after vendor change.

#### Verification

- Application acknowledgement and corresponding popup observed across representative sites, not just HTTP 202.

#### 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.

## 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.

#### Answers and reasoning

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

Correct: C. Working one-touch entry does not establish that the independent live-popup feature is enabled. The supplied observations support: Working one-touch entry does not establish that the independent live-popup feature is enabled. They do not establish the competing explanations without additional evidence.

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

Correct: B. Confirm requested feature and per-device portal state, then test a ringing call outside an active order. The bulletin's evidence supports this sequence: Confirm requested feature and per-device portal state, then test a ringing call outside an active order. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Identify analog versus IP line and appropriate device.
2. Check device-specific prompt setting and tablet screen state.
3. Enable with POS authorization and test both workflows.

#### Verification

- One-touch and live popup independently show expected results on each intended tablet.

#### 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.

#### Answers and reasoning

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

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

The supplied observations support: A per-line service or physical monitoring gap is plausible; intermittent caller display alone does not prove rollover is the root cause. They do not establish the competing explanations without additional evidence.

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

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

The bulletin's evidence supports this sequence: Place controlled calls to each configured line, including simultaneous calls, then compare provider routing, monitored ports and received POS records. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Map active line numbers to physical monitored inputs.
2. Verify caller-ID and hunt configuration with the provider.
3. Correlate each concurrent test call with the device event and POS list.

#### Verification

- Every intended active line produces the correct caller event during simultaneous tests.

#### 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.

#### Answers and reasoning

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

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

The supplied observations support: A model suffix cannot prove cellular-only operation, and one LAN TLS flow cannot establish both lines' modes. They do not establish the competing explanations without additional evidence.

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

Correct: 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.

The bulletin's evidence supports this sequence: Confirm the configured mode and observe a timed call on each line before selecting an approved analog, provider event, or authorized clear-SIP path. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Record non-secret line mode and physical path.
2. Correlate each inbound line with its LAN or analog signaling.
3. Pilot only a provider-supported integration on the identified path.

#### Verification

- Each required line's caller identity reaches the POS on repeated controlled calls.

#### 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.

#### Answers and reasoning

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

Correct: C. The receiver can begin parsing inside the header; a header delimiter search is not safe. The supplied observations support: The receiver can begin parsing inside the header; a header delimiter search is not safe. They do not establish the competing explanations without additional evidence.

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

Correct: A. Have the POS integrator parse the documented fixed header boundary and validate with sanitized records. The bulletin's evidence supports this sequence: Have the POS integrator parse the documented fixed header boundary and validate with sanitized records. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Compare raw payload offsets with receiver field extraction.
2. Skip the first 21 payload bytes, not Ethernet/UDP headers; accept only recognized call records and reject setup acknowledgements or unrelated datagrams.
3. Regression-test header values containing punctuation and ordinary records.

#### Verification

- Phone/name fields decode correctly for header values with and without punctuation; non-call traffic is rejected.

#### 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.

#### Answers and reasoning

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

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

The supplied observations support: The device cannot emit an analog hang-up event it never observes; POS clear policy needs separate evaluation. They do not establish the competing explanations without additional evidence.

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

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

The bulletin's evidence supports this sequence: Ask the POS integrator to review timer/answered-event dismissal against actual line behavior and test call states. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Observe analog line before and after park.
2. Correlate device Start/End with POS popup lifecycle.
3. Design and test POS-owned dismissal rule with the integrator.

#### Verification

- Popup closes appropriately for parked, answered and hung-up calls without prematurely clearing active calls.

#### 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.

#### Answers and reasoning

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

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

The supplied observations support: CANCEL closes the losing branch, not the answered dialog; an early device End versus POS clearing remains unproven. They do not establish the competing explanations without additional evidence.

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

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

The bulletin's evidence supports this sequence: Capture synchronized SIP, configured device output and POS popup timestamps for a success and failure. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Match Call-ID and branch tags, excluding the prior call's BYE.
2. Verify output destination/port and avoid competing diagnostic listeners.
3. Compare early End, POS clear and actual answered-leg BYE; assign review to device or POS owner based on evidence.

#### Verification

- Observe one matched working and failing call with synchronized output and POS records.

#### Cautions

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

## 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.

#### Answers and reasoning

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

Correct: A. The SIP side is readable; POS delivery must be measured on its separate interface. The supplied observations support: The SIP side is readable; POS delivery must be measured on its separate interface. They do not establish the competing explanations without additional evidence.

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

Correct: D. Capture at the Management-port receiver and verify local listener ownership, programmed format and destination. The bulletin's evidence supports this sequence: Capture at the Management-port receiver and verify local listener ownership, programmed format and destination. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Identify the capture interface and actual output settings.
2. Close conflicting listener on the same machine for a controlled test.
3. Trace sample event to POS receiver and application.

#### Verification

- Observe matching output packet and accepted POS event.

#### 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.

### Answers and reasoning

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

Correct: C. Sample failure isolates an output/receiver path; the capture cannot classify live inbound signaling. The supplied observations support: Sample failure isolates an output/receiver path; the capture cannot classify live inbound signaling. They do not establish the competing explanations without additional evidence.

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

Correct: B. Trace sample UDP output at the POS server and test port ownership, interface and format before a separate live-call capture. The bulletin's evidence supports this sequence: Trace sample UDP output at the POS server and test port ownership, interface and format before a separate live-call capture. Do not treat an untested recommendation as a confirmed repair.

### Documented guidance / next steps

1. Record VCT host and server locations.
2. Capture at the POS server with its actual listener state.
3. After sample works, capture a real inbound call and diagnose live signaling independently.

### Verification

- Sample appears in the POS; then repeat actual inbound calls and verify caller identity.

### 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.

#### Answers and reasoning

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

Correct: A. A receiver's expected field spacing can cause a parse failure even when identity was extracted. The supplied observations support: A receiver's expected field spacing can cause a parse failure even when identity was extracted. They do not establish the competing explanations without additional evidence.

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

Correct: C. With the POS vendor's format requirement verified, select the matching software format in VCT and test a raw sample. The bulletin's evidence supports this sequence: With the POS vendor's format requirement verified, select the matching software format in VCT and test a raw sample. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Record current output settings and expected vendor format.
2. Choose matching Known Formats entry via VCT.
3. Compare received bytes and POS interpretation.

#### Verification

- Receiver accepts number/name and call lifecycle records with documented spacing.

#### 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.

## 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.

#### Answers and reasoning

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

Correct: B. First distinguish analog call-waiting service and second-call signaling from a VoIP SIP-leg issue. The supplied observations support: First distinguish analog call-waiting service and second-call signaling from a VoIP SIP-leg issue. They do not establish the competing explanations without additional evidence.

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

Correct: C. Confirm carrier Caller ID plus Call Waiting service and capture second-call event and receiver behavior while line is occupied. The bulletin's evidence supports this sequence: Confirm carrier Caller ID plus Call Waiting service and capture second-call event and receiver behavior while line is occupied. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Identify analog versus SIP topology.
2. Make a controlled second inbound call during active conversation.
3. Compare line signaling, device event and POS display.

#### Verification

- Second caller's identity reaches intended receiver during a live first call.

#### 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.

#### Answers and reasoning

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

Correct: B. Ring detection alone does not establish that the test call included usable caller ID. The supplied observations support: Ring detection alone does not establish that the test call included usable caller ID. They do not establish the competing explanations without additional evidence.

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

Correct: B. Repeat with a known outside line whose caller ID is enabled; inspect identity if the warning persists. The bulletin's evidence supports this sequence: Repeat with a known outside line whose caller ID is enabled; inspect identity if the warning persists. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Record test call source and ring observation.
2. Use a known unblocked external calling line.
3. If repeated failure, capture actual signaling and VCT output.

#### Verification

- Wizard recognizes a valid number and subsequent real calls display correctly.

#### 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.

#### Answers and reasoning

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

Correct: A. The first record validates output to POS, but absence of update leaves dial capture/signaling unverified. The supplied observations support: The first record validates output to POS, but absence of update leaves dial capture/signaling unverified. They do not establish the competing explanations without additional evidence.

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

Correct: D. Stop repeated blind programming; check whether the Vertex can observe this site's VoIP signaling and escalate if it is encrypted.  
The bulletin's evidence supports this sequence: Stop repeated blind programming; check whether the Vertex can observe this site's VoIP signaling and escalate if it is encrypted. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Confirm setup record first.
2. Place prescribed setup call from site VoIP handset and look for Setup Updated.
3. Restore original DIP positions and reboot only after validated procedure; escalate missing record.

#### Verification

- Setup Updated appears and normal post-restart incoming calls display in the intended time zone.

#### 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.

#### Answers and reasoning

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

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

The supplied observations support: Investigate ATA account registration/proxy and the ATA-to-PBX path first. They do not establish the competing explanations without additional evidence.

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

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

The bulletin's evidence supports this sequence: Preserve settings without copying secrets into tickets; inspect account status, proxy and provider record one line at a time with provider support. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Test one FXS line directly and inspect registration status.
2. Coordinate provider-approved reprovisioning or correction from secure record.
3. Reconnect PBX only after independent line tests.

#### Verification

- Each required line Registered; inbound and outbound calls pass before and after PBX reconnection.

#### 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.

### Answers and reasoning

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

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

The supplied observations support: Competing registration or provider forking is plausible, but false answer or LAN interference also remains possible. They do not establish the competing explanations without additional evidence.

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

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

The bulletin's evidence supports this sequence: Request provider binding and per-leg SIP traces, then pilot distinct extensions with explicit simultaneous ringing if shared registration is verified. Do not treat an untested recommendation as a confirmed repair.

### Documented guidance / next steps

1. Preserve non-secret configuration.
2. Determine whether AOR Contacts replace or coexist and inspect INVITE/200 OK/CANCEL.
3. Pilot at one site with provider-approved parallel routing; check for false answer and LAN faults if needed.

### Verification

- Both handset rings and POS receives identity on repeated calls after reboot and reprovisioning.

### 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.

### Answers and reasoning

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

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

The supplied observations support: An intact series diode does not exclude damage to the separate SCR gate network upstream of the starved regulators. They do not establish the competing explanations without additional evidence.

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

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

The bulletin's evidence supports this sequence: Quarantine power, confirm correct center-negative supply and refer board-level testing/replacement to qualified repair personnel. Do not treat an untested recommendation as a confirmed repair.

### Step-by-step solution

1. Remove wrong supply and verify adapter polarity.
2. Inspect diode, SCR branch and downstream components safely.
3. Replace verified damaged component through authorized repair and run full test.

### Verification

- Correct rails and complete device performance tests with approved adapter.

### 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.

### Answers and reasoning

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

Correct: B. The software database/write path is implicated; a reboot alone does not prove corruption. The supplied observations support: The software database/write path is implicated; a reboot alone does not prove corruption. They do not establish the competing explanations without additional evidence.

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

Correct: D. Preserve error and version, close clients normally, identify data path and backup, then let product support choose repair. The bulletin's evidence supports this sequence: Preserve error and version, close clients normally, identify data path and backup, then let product support choose repair. Do not treat an untested recommendation as a confirmed repair.

### Documented guidance / next steps

1. Collect application/version and affected workstation scope.
2. Identify verified database location and good backup.
3. Have support select documented repair, restore or duplicate-source correction.

### Verification

- Original records preserved and repeated calls write successfully without duplicate-key error.

### 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.

#### Answers and reasoning

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

Correct: A. Operational availability does not prove security and all services survived the move. The supplied observations support: Operational availability does not prove security and all services survived the move. They do not establish the competing explanations without additional evidence.

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

Correct: C. Do not reuse the recorded procedure; perform named-user credential cleanup and dashboard-only service/security review with rollback gates. The bulletin's evidence supports this sequence: Do not reuse the recorded procedure; perform named-user credential cleanup and dashboard-only service/security review with rollback gates. Do not treat an untested recommendation as a confirmed repair.

#### Documented guidance / next steps

1. Inventory DNS, email, certificate and Cloudflare settings.
2. Verify authorized named-user access and revoke temporary remote/root exposure.
3. Sign off mail and dashboard-only tests plus rollback readiness.

#### Verification

- Service tests and access/audit review are recorded before closure.

#### 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.

#### Answers and reasoning

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

Correct: B. Compare the device's data output port against the POS listener  
The follow-up isolated a separate port mismatch; hardware recovery alone did not configure the receiving application.

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

Correct: A. The port was changed and the installation was reported working  
A recorded working result after the port change is stronger than stage or LED status.

#### Step-by-step solution

1. Distinguish the earlier no-link hardware fault from the later application-layer failure.
2. Check the receiving port on both ends rather than repeating the RMA diagnosis.
3. Retest the actual POS display after making the documented port correction.

#### Verification

- Case notes explicitly report working operation after the port change.

#### 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.

#### Answers and reasoning

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

Correct: A. A capture of signaling on the relevant link  
The capture directly tests whether signaling is readable; an application error label is not a protocol decode.

##### 2. What ultimately resolved the symptom?

Correct: B. Correcting the POS configuration  
The support thread attributes restored operation to the POS provider's setup correction.

#### Step-by-step solution

1. Separate raw signaling from the POS interpretation of that signaling.
2. Use packet evidence to test the encryption hypothesis.
3. Engage the receiving POS vendor once the upstream signal is shown to be readable.

#### Verification

- POS provider reported the setup corrected and working.

#### 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.

#### Answers and reasoning

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

Correct: B. The SIP gateway configuration after the router swap  
A router change can change the gateway the device must recognize.

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

Correct: A. No, firmware and gateway configuration were changed together  
The notes record both interventions before success and do not independently test them.

#### Step-by-step solution

1. Anchor the diagnosis on the recent network change.
2. Review gateway detection/configuration and firmware compatibility.
3. Verify caller ID in Toast after changes.

#### Verification

- Support explicitly documented working Toast operation.

#### 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.

#### Answers and reasoning

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

Correct: B. The device-to-POS management path should be checked  
A locally generated test failing to reach POS points to the output/network path, irrespective of live SIP.

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

Correct: B. Move the receiving switch port back onto the POS network  
The affected switch port's POS-LAN assignment was corrected, after which the system worked.

#### Step-by-step solution

1. Check bridge lights, then test the data path separately.
2. Trace the management cable to its switch port and network membership.
3. Repeat the POS test after port reconfiguration.

#### Verification

- The note explicitly says the system worked after the port was reconfigured.

#### Cautions

- Link lights do not establish VLAN or subnet reachability.

Practice source references: Technical helpdesk case A04

## 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.

#### Answers and reasoning

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

Correct: B. Stabilize and test the management path, then capture a real call and set gateway/protocol options  
Changing one variable at a time preserves diagnostic evidence; this thread used a capture to configure the gateway.

##### 2. What supports a working outcome?

Correct: B. The user's report of data in the Pulse terminal  
The receiving application's observed data is the documented end-to-end check.

#### Step-by-step solution

1. Stop simultaneous changes to both sides of the installation.
2. Capture a real call and identify the gateway without publishing its address.
3. Apply the documented protocol option and test the receiving POS.

#### Verification

- Caller ID was reported visible in the Pulse terminal.

#### Cautions

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

Practice source references: Technical helpdesk case A05

## 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.

#### Answers and reasoning

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

Correct: D. UDP allowance on the new POS equipment's device-facing port  
The receiver-side Pulse port policy was the documented blocker.

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

Correct: C. An application/network policy can block otherwise valid pushes  
The working result after UDP permission shows that missing output does not imply faulty hardware.

#### Step-by-step solution

1. Confirm the management path after the upgrade.
2. Have the POS provider inspect whether the required UDP traffic is permitted on the relevant port.
3. Test a live popup after the policy correction.

#### Verification

- The notes report pop-ups starting after the port allowance.

#### 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.

#### Answers and reasoning

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

Correct: D. It restored physical/network link only  
Correct link lights did not remove the separate encrypted-signaling barrier.

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

Correct: C. Adding a carrier-side device with usable signaling and completing setup  
The thread records working Toast operation only after the Edgewater installation and setup.

#### Step-by-step solution

1. Resolve layer-one link problems without conflating them with SIP readability.
2. Use capture/carrier confirmation before proposing a signaling workaround.
3. Perform phone setup and observe the POS after the carrier-side change.

#### Verification

- The final note explicitly reports working Toast operation.

#### 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.

#### Answers and reasoning

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

Correct: B. The modified installer still failed; the exact restriction remained a suspicion  
The thread explicitly frames the locked-down OS as a suspicion, not a confirmed cause.

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

Correct: B. So the relay can run while the host is powered without an interactive login  
That operational behavior was the reason documented for service-mode configuration.

#### Step-by-step solution

1. Differentiate application-launch failure from phone capture and POS delivery.
2. Avoid claiming an unproved OS root cause.
3. Set up the working host, location and service mode; validate actual relay operation.

#### Verification

- The mini-host service-mode configuration was explicitly reported working.

#### 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.

### Answers and reasoning

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

Correct: B. Phone service, device monitor and POS receiver separately  
The voice path worked while the POS-side service remained broken.

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

Correct: D. Documented guidance with POS-side work outstanding  
There is no final report of the POS service working.

### Documented guidance / next steps

1. Restore phone service before continuing any experiments.
2. Confirm the device detects calls and isolate the receiving service.
3. Hand off the remaining POS-service failure with observed evidence.

### Verification

- Phone service and call detection were verified; POS pop-ups were not verified.

### Cautions

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

Practice source references: Technical helpdesk case A09

## 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.

#### Answers and reasoning

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

Correct: B. The phone routing and receiving POS data path can fail independently  
SIP visibility and correct POS delivery were separately established in this case.

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

Correct: D. Four simultaneous calls appearing on screen  
The simultaneous calls supplied explicit receiving-screen verification.

#### Step-by-step solution

1. Check live SIP after the phone-routing change.
2. Inspect POS switch membership and the broadcast target.
3. Test concurrent calls at the receiving screens.

#### Verification

- Four simultaneous calls were documented as appearing on screen.

#### Cautions

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

Practice source references: Technical helpdesk case A10

## 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.

#### Answers and reasoning

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

Correct: B. Forwarding can keep the inbound call out of the local signaling path  
The team noted that cloud voicemail forwarding meant calls were not reaching the site for a meaningful capture.

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

Correct: B. The new port arrangement worked and survived a reboot  
The thread documents working operation and persistence after reboot.

#### Step-by-step solution

1. Disable or account for call forwarding while testing.
2. Trace the provider router, gateway-facing bridge port, phones and Toast management paths.
3. Reboot and repeat a real inbound POS test.

#### Verification

- The support note reports working operation and settings surviving the restart.

#### 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.

#### Answers and reasoning

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

Correct: C. The original hardware or its power supply merits bench diagnosis  
The comparison controls much of the site setup while changing the hardware.

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

Correct: C. Bench testing after component replacement  
The repair note says tested and ready to return, but does not document customer-site reinstall.

#### Step-by-step solution

1. Use the working substitute to narrow the fault.
2. Submit the suspect device for evaluation rather than asserting a specific chip fault in the field.
3. Record bench test separately from any subsequent site-level acceptance.

#### Verification

- Bench testing after component replacement was reported successful; on-site acceptance is not in this thread.

#### Cautions

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

Practice source references: Technical helpdesk case A12

## 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.

#### Answers and reasoning

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

Correct: B. It also failed discovery in a separate environment  
Reproducing a symptom off the original LAN supports bench evaluation rather than only local router investigation.

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

Correct: C. No; reprogramming and power-supply replacement were performed, but cause was not isolated  
The notes describe a state and combined corrective actions, not a proven original trigger.

#### Step-by-step solution

1. Recheck discovery with a controlled direct/network connection.
2. Escalate to hardware evaluation when it remains unreachable.
3. Differentiate successful bench repair from unrecorded field reinstallation.

#### Verification

- The final bench comment says the reprogrammed unit worked.

#### Cautions

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

Practice source references: Technical helpdesk case A13

## 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.

#### Answers and reasoning

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

Correct: D. Direct connection still failed and the phone source proved to be VoIP  
Correct-looking RJ11 ports do not prove the source provides analog caller-ID signaling.

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

Correct: D. Verify the provider's SIP transport and encryption and the proposed bridge wiring  
The notes explicitly request confirmation of usable UDP and unencrypted SIP before deploying the VoIP product.

#### Documented guidance / next steps

1. Identify the actual telephone signaling source, not just connector shape.
2. Determine whether analog line caller ID exists on the proposed input.
3. Validate VoIP transport before an exchange; do not mark the new installation resolved prematurely.

#### Verification

- The analog mismatch was identified; no replacement-site operation is documented.

#### 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.

#### Answers and reasoning

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

Correct: B. The symptom was not reproduced under the tested conditions  
Three successful reproductions refute a consistently broken line under those conditions, not all intermittent possibilities.

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

Correct: A. A timed real-call example with station/line and device-versus-POS observations  
Correlating line, time and receiving station can expose a condition absent from the controlled test.

#### Documented guidance / next steps

1. Arrange an on-site simultaneous-call test.
2. Compare device records with each POS station.
3. Document successful tested behavior without claiming an intermittent complaint can never recur.

#### Verification

- Both calls were observed at the device and POS on three attempts.

#### 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.

### Answers and reasoning

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

Correct: D. A shared upstream POS/API policy change  
A common endpoint challenge is more consistent with multiple independent sites failing together.

#### 2. What status should be communicated?

Correct: D. Vendor-side remediation recommended, but no successful follow-up recorded  
The thread documents diagnosis and proposed mitigations but not vendor deployment or recovered requests.

### Documented guidance / next steps

1. Compare failures across sites to find the common boundary.
2. Inspect API response behavior and whether the client can complete browser challenges.
3. Provide the POS vendor specific machine-client exemption or token options and retest after their change.

### Verification

- No post-remediation success is recorded in the ticket.

### Cautions

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

Practice source references: Technical helpdesk case A16

## 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.

### Answers and reasoning

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

Correct: D. The popup appears first and clears at pickup  
The initial display establishes some upstream and POS communication; investigate the termination event.

#### 2. What should support do next?

Correct: C. Correlate the CANCEL event with device output and POS dismissal; ask the provider/POS vendor about the reason  
The capture supplies a concrete hypothesis, but the exact behavior change and recovery remain unverified.

### Documented guidance / next steps

1. Reproduce the call while capturing signaling and POS behavior.
2. Correlate pickup timing with the CANCEL reason.
3. Escalate the signal/receiver policy to the responsible provider or vendor.

### Verification

- The reason in the capture is documented; no resolution test is documented.

### 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.

#### Answers and reasoning

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

Correct: B. Capture actual serial output at the configured baud rate with the POS service released from the COM port  
A direct serial test distinguishes device output from the application's COM-port configuration.

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

Correct: B. Unresolved serial-to-POS path with a suspected device issue and pending bench test  
An authorized exchange is not a bench-confirmed root cause or observed POS recovery.

#### Documented guidance / next steps

1. Prove capture in a mode that has an appropriate monitor.
2. Check baud, cabling, COM-port ownership and the actual serial stream.
3. Keep the suspected hardware issue provisional until bench and replacement tests.

#### Verification

- Capture was demonstrated in network mode; serial-to-POS success was not documented.

#### Cautions

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

Practice source references: Technical helpdesk case A18

## 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.

### Answers and reasoning

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

Correct: A. Calls are bypassing the intended inline monitoring path  
If phones stay online with the bridge disconnected, another path feeds them.

#### 2. Was the entire installation verified?

Correct: B. No; test numbers reached POS but real-call output remained incomplete  
The last note still describes incomplete data from a real call and pending diagnostics.

### Documented guidance / next steps

1. Prove phones actually depend on the inline path before analyzing SIP.
2. Correct the bypass and run phone setup.
3. Compare simulated data with real-call contents and keep the remaining symptom open.

### Verification

- Simulated numbers reached POS; full real-call caller ID was not verified.

### 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.

#### Answers and reasoning

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

Correct: C. Device output/receiving POS integration  
The device had caller data, so the next investigation is delivery and the POS receiver.

##### 2. What confirms the outcome?

Correct: A. The installer's report of a corrected POS setup and working order-entry display  
This thread has direct post-correction confirmation from the installer.

#### Step-by-step solution

1. Compare device call log and receiving POS display.
2. Involve the POS provider with evidence that calls reach the device.
3. Retest in the actual order-entry screen after their configuration correction.

#### Verification

- Installer explicitly reported working POS caller ID after correction.

#### Cautions

- Do not prescribe an undocumented exact POS setting.

Practice source references: Technical helpdesk case A20