Modernizing the Network. Protecting the Mission.

Legacy network assurance during the FAA telecommunications transition

A technical perspective by Onyx Spectrum Technology, Inc. | November 17, 2026

Executive perspective

Modernizing mission-critical communications is necessary. But while legacy services remain in operation, modernization success also depends on understanding how the existing network behaves when components, interfaces, transport paths, and configurations change.

The Federal Aviation Administration (FAA)'s November 13, 2026 nationwide ground stop illustrates the operational consequences of instability in a highly interconnected telecommunications environment. The FAA and L3Harris are investigating the event. A disciplined response should examine the full end-to-end service environment—including any legacy dependencies that are actually present—without assuming the cause in advance. [1, 4]

Onyx Spectrum Technology (OST) brings specialized experience with legacy NET Promina networks and the FAA Bandwidth Manager (BWM) environment. OST offers that knowledge to complement the FAA's and L3Harris's engineering, sustainment, and modernization teams.

What the FAA has publicly established

In its November 15, 2026 Q&A, the FAA reported that legacy equipment became unstable when the FAA Telecommunications Infrastructure (FTI) network received approximately 1,000 connection attempts every four to five seconds. The agency reported communications and radar-feed instability affecting 17 of 22 Air Route Traffic Control Centers and some terminal facilities. [1]

The FAA identified a radar site in Amarillo, Texas, and a radio communications site in El Dorado, Arkansas, as initial areas of investigation. L3Harris, the network service provider, had been working at El Dorado, including deploying a router. According to the FAA, isolating the two locations helped stabilize the network, and broadcasting functionality on new routers was disabled as a precaution. [1]

Those are important observations—not a complete root-cause analysis. The public Q&A does not establish that BWM, NET Promina, or any particular legacy node caused the event. Nor does it identify a definitive hardware, software, configuration, or installation failure. [1]

Why legacy-network knowledge still matters

The FAA's May 2025 NAS Enterprise Architecture Communications Roadmap lists Bandwidth Manager (BWM), System 246, as “In-Service” and depicts it within the longer telecommunications transition planning horizon. The roadmap is a planning baseline, not a real-time inventory of active BWM devices in November 2026. [2]

FAA Order NG 6100.6, issued in July 2019 and listed as active, addresses the transition from Time Division Multiplexing (TDM) to Internet Protocol (IP) and directs FAA system owners and program offices to undertake TDM-to-IP assessments. [3]

In parallel, L3Harris said on November 14, 2026 that, together with the FAA and telecommunications partners, it had completed more than 70% of its planned copper-to-fiber communications conversion. That progress underscores the importance of supporting legacy and modern capabilities simultaneously until individual services can be safely retired. [4]

Technical questions worth investigating—not assumed causes

Legacy node and service dependencies. Which BWM / NET Promina nodes and services remain active? Are network maps, node relationships, service assignments, and retirement records aligned with the operational environment?

Configuration integrity after changes. Could a removed node, changed interface, or outdated service definition cause retries, timeouts, reroute attempts, or unintended traffic under particular conditions? OST's existing NET Promina health-check methodology flags these as general legacy-network failure modes, not findings about the November 13 event. [5]

Behavior at transition boundaries. When a new IP transport or router is introduced, have traffic patterns, interface assumptions, routing/discovery behavior, and fallback paths been assessed against the legacy system's expected behavior?

Operational visibility and isolation. Can engineering teams distinguish normal events from unusual connection volume, trace service impact across dependencies, and isolate an affected segment without introducing further instability?

Institutional knowledge and change readiness. Do current technicians and contractors have the BWM / NET Promina configuration history, troubleshooting guidance, test criteria, and rollback procedures needed to manage remaining legacy assets?

A practical legacy-network assurance approach

1. **Establish the baseline.** Reconcile available BWM / NET Promina inventory, active services, network diagrams, node configurations, software/hardware status, and known dependencies with authorized operational records.

2. **Assess transition exposure.** Review planned retirement and IP-interface changes for configuration consistency, expected traffic behavior, routing/reroute interactions, resilience, monitoring coverage, and fallback requirements.

3. **Validate before and after change.** Support engineering-approved test plans, baseline measurements, documented acceptance criteria, maintenance windows, post-change checks, and controlled rollback criteria. Any live testing should be authorized and coordinated with FAA and incumbent operational teams.

4. **Sustain and transfer knowledge.** Deliver an actionable health-check report, prioritized corrective recommendations, updated service documentation, and targeted technical training for the personnel responsible for the remaining legacy environment.

Evidence-led assessment and decision-ready outputs

A rigorous review should begin by asking whether the suspected legacy components are on the affected service paths. That determination requires authorized architecture records, node and service inventories, change histories, operational telemetry, and interface information. If BWM or NET Promina is not implicated by those records, the investigation should follow the evidence elsewhere rather than force a legacy-system explanation.

Where legacy dependencies are present, useful deliverables include a verified current-state inventory; a configuration and service-dependency baseline; a change-impact and compatibility review; observable pre-change and post-change performance measures; a prioritized risk register; and a concise set of operational checklists and knowledge-transfer materials. Recommendations should be ranked by operational impact, evidence strength, and feasibility, with corrective actions authorized by the responsible FAA and L3Harris teams.

The intended outcome is practical: better visibility into the remaining legacy estate, clearer control of changes at transition boundaries, faster diagnosis when unusual behavior occurs, and stronger confidence that critical communications services are protected during each cutover.

What OST can contribute

OST's relevant experience includes maintenance of NET Promina nodes supporting Defense Information Systems Agency (DISA) environments; historical training of FAA technicians on BWM maintenance; and support for the Bay Area Rapid Transit (BART) NET Promina network as BART plans and executes modernization. These experience statements are provided by OST; the company's public capabilities page also describes its BART sustainment and training work. [5, 6]

OST's published NET Promina Network and Node Health Check covers performance evaluation, security review, infrastructure and compatibility assessment, configuration audit, monitoring and logging, documentation, and prioritized recommendations. The methodology is intended to identify service risks while legacy systems continue to operate. [5]

OST is not proposing to replace the FAA's or L3Harris's incident-investigation teams. Its value is to bring concentrated legacy-platform expertise into the existing technical process, subject to access controls, engineering authorization, and the findings of the ongoing investigation.

A focused next step

An initial joint scoping session with FAA FTI infrastructure/Technical Operations personnel and L3Harris network engineering could determine whether BWM/NET Promina components or related dependencies are within the relevant service paths. If so, OST could help define a bounded legacy-network health and transition-risk review with clearly documented evidence, deliverables, roles, and acceptance criteria.

The goal is not to prejudge the cause of the November 13 disruption. It is to strengthen confidence in the systems still carrying critical traffic—and reduce avoidable operational risk as the next generation is introduced.

Publication note

This paper distinguishes publicly reported facts from OST technical hypotheses and proposed assessments. It does not claim BWM or NET Promina caused the November 13 incident, and it is not an FAA or L3Harris investigative finding. BWM status referenced here comes from a May 2025 planning baseline; actual November 2026 component status requires confirmation with authorized personnel. Onyx Spectrum Technology, Inc acquired the NET Promina assets, intellectual property and SME support from Sonus (now Ribbon Communications) in 2017.

References and source notes

[1] FAA, “Nationwide Ground Stop: Questions and Answers,” November 15, 2026 [View source]

[2] FAA, NAS Enterprise Architecture Infrastructure Roadmaps v19.1, Communication Roadmap (May 2025), p. 4 [View source]

[3] FAA, Order NG 6100.6, “TDM-to-IP Transition Requirements for FAA Systems” (issued July 2, 2019) [View source]

[4] L3Harris, “Statement on the Nov. 13 Ground Stop,” November 14, 2026 [View source]

[5] Onyx Spectrum Technology, “Onyx NET Promina Network and Node Health Check,” OST capabilities statement supplied for this paper

[6] Onyx Spectrum Technology, “Capabilities” (BART NET Promina sustainment and training) [View source]