SPECS SURVEY: Base Stations and Repeaters | WHAT'S NEW: P25 and LTE

RadioResource

March 2020 | MCCmag.com

MissionCritical™

COMMUNICATIONS

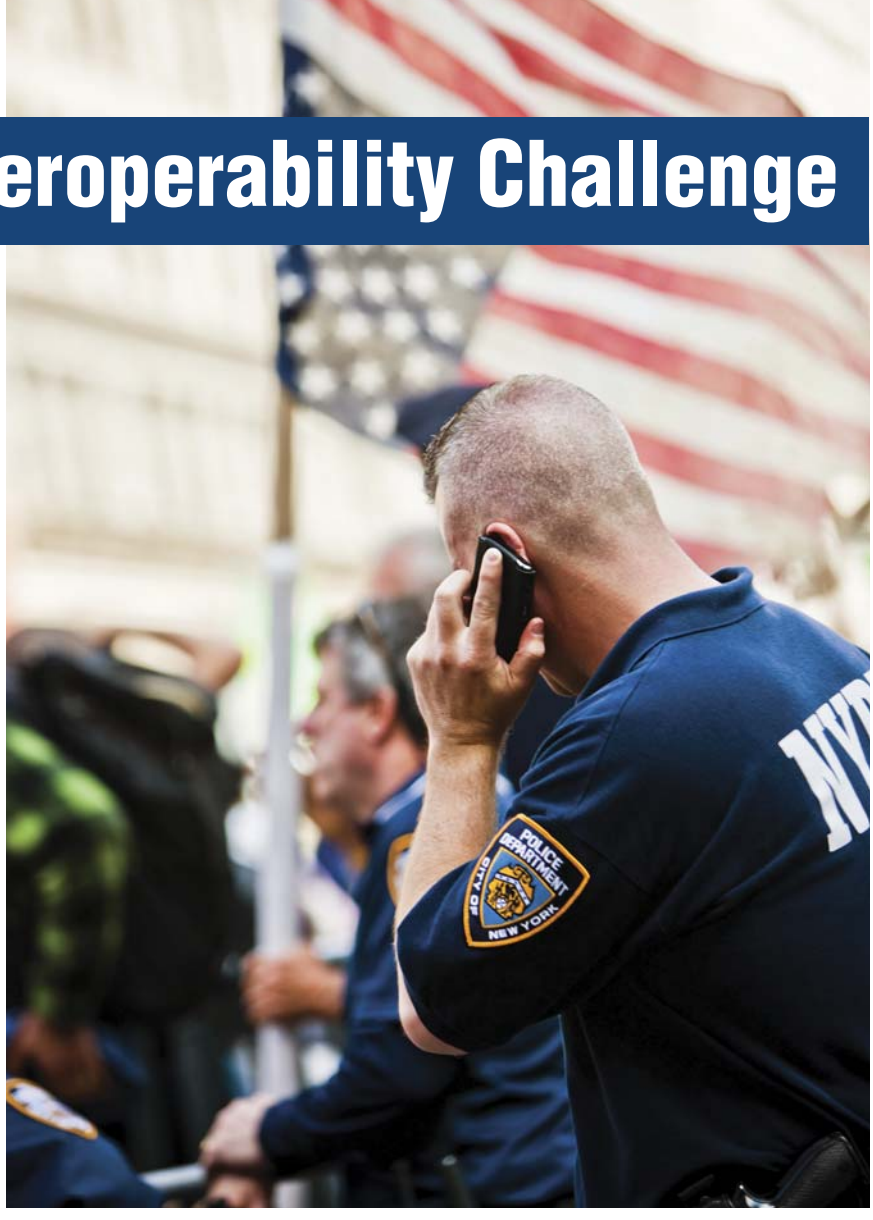
Industry Insight Report

The PTT Challenge

The PTT Interoperability Challenge

Industry's mission for public safety includes hybrid LMR and broadband PTT systems that create a ubiquitous communications network.

By Josh Lober



During the past 10 years, broadband push-to-talk (PTT) solutions have experienced widespread adoption throughout government and commercial markets. The availability of broadband data rates and the open application distribution platforms for smartphone and tablet devices have fueled this growth. Some believe that broadband PTT solutions are now positioned to replace traditional LMR solutions entirely. However, there are vast architectural differences between LMR network infrastructure and the commercial wireless carrier network infrastructure that hosts most broadband PTT solutions.

LMR and broadband PTT technologies each include features that the other does not. Perhaps the question of using broadband PTT as an LMR replacement is the wrong question. Why not leverage both technologies, integrating the two into a hybrid network that allows users to communicate across networks while taking advantage of the features that allow public-safety users to best meet their mission? This hybrid model is rapidly gaining traction in the public-safety market.

The viability of broadband PTT for mission-critical public-safety users depends on the mission itself. Certain disciplines within the public-safety sector are best served by LMR technologies, while other disciplines are better served by broadband PTT solutions. For example, undercover and investigative units within military, as well as federal, state and local law enforcement agencies, have adopted broadband PTT service. These typically include narcotics, robbery, anti-crime, vice, gangs and auto-theft units, whose mission is better served by discreet smartphone devices rather than LMR radios, which are better suited for officers performing patrol and traffic duties and firefighters. Some benefits of the broadband offerings include smaller handset size, enhanced coverage area, improved voice quality, and integrated features such as real-time location services and multimedia messaging that provide an enhanced common operational picture for improved situational awareness. When public safety uses broadband PTT on a hybrid network, officials can still communicate directly with LMR users and dispatch.

In the public-safety space, hybrid Project 25 (P25) and broadband PTT solutions are being deployed using the P25 Inter Subsystem Interface (ISSI) for integration. The ISSI was designed to connect multiple P25 systems; however, it can also be used to connect P25 and non-P25 systems. In this model, broadband PTT users are assigned P25 unit IDs, and while the users talk on P25 channels, the P25 system manages floor control, priority and pre-emption. ISSI-integrated hybrid networks also support passing unit IDs, private calls, group calls and emergency calls, as

well as transparent integration with Console Subsystem Interface (CSSI)-connected dispatch consoles and call-logging systems. End-to-end encryption between smartphones, radios and consoles is also supported, including key management via the P25 key management facility (KMF).

For public safety, interagency, intersystem, intervendor and intercarrier interoperability must all be supported.

A Little History

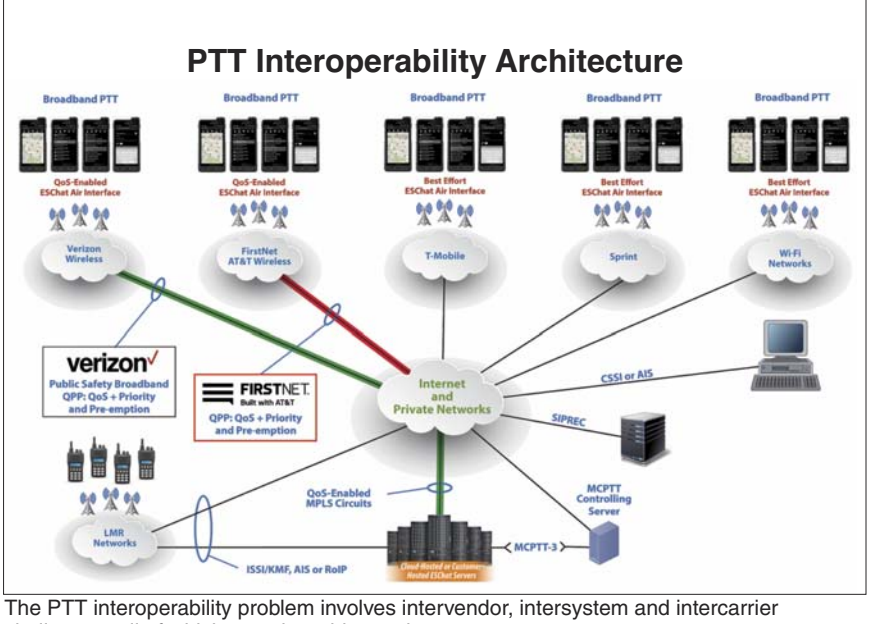
The success of cellular-based PTT goes back to iDEN products, deployed in the United States by Nextel. iDEN's PTT feature was successful, mainly because the network was built more like an LMR network than a cellular network. The architecture established iDEN's PTT performance as the benchmark for future cellular PTT offerings. This was also the downfall of iDEN because it was feature limited compared with traditional cellular services, particularly as cellular data rates increased with the 3G upgrades of the day.

Commercial wireless network architectures are different from LMR networks, regardless of LMR technology. Each LMR network is designed to meet specific requirements for its user base. LMR networks have a more limited feature set than commercial wireless networks but provide efficient and reliable channelized communications over a limited but dedicated regional block of spectrum. Commercial cellular networks, which began as narrowband and evolved into broadband, are designed to provide non-channelized voice and data services to customers who use a wide variety of handset devices over a nationwide coverage area. Commercial wireless networks are continually evolving to provide improved throughput and capacity to support an increasing user base and an expanding set of data-intensive applications.

PTT Connectivity

The 9/11 Commission report, which identified LMR challenges, recognized that a lack of interoperability between public-safety agencies impacted responders' abilities to effectively communicate during a major multiagency response. Today's challenges are even more complicated with the widespread adoption of broadband PTT. We must ensure that all PTT technologies, whether LMR or broadband, regardless of agency, technology, frequency band and vendor, all work together. To enable ubiquitous cross-agency communications, we must focus our efforts on two critical categories: connectivity and interoperability.

All PTT systems, whether broadband PTT or LMR, require wireless connectivity. LMR networks are engineered to provide connectivity across a limited coverage area. Broadband PTT solutions leverage commercial and private networks for their connectivity. The connectivity problem can be distilled into two key elements:



The PTT interoperability problem involves intervendor, intersystem and intercarrier challenges, all of which must be addressed.

coverage and capacity.

Coverage is a function of the quantity, location and radiated output power of the LMR or broadband radio access networks (RAN). LMR networks are engineered to provide coverage in a specific area or region, while broadband PTT solutions take advantage of commercial wireless networks that are engineered to provide a nationwide coverage footprint.

Because coverage is determined by a fixed set of parameters, it is consistent and reliable unless the wireless infrastructure has been impacted by technical or environmental factors. Users generally learn where they do and don't have sufficient wireless coverage.

Capacity is a function of data throughput, which requires RF channel availability and sufficient backhaul between the RAN and site controllers or the network's core. Unlike coverage, capacity will vary based on usage patterns.

At its core, the challenge of operating public-safety PTT voice communications over a commercial wireless network is bandwidth. It seems intuitive that broadband networks would have sufficient bandwidth available to carry narrowband voice traffic, which is true more than 99% of the time. However, during planned public events and unplanned emergencies, when commercial users are live-streaming video and using other data-intensive applications, bandwidth becomes the limiting factor for real-time PTT voice communications.

For a number of years, to resolve both coverage and capacity limitations, Verizon and AT&T have offered their commercial and public-safety customers enhancements including quality of service (QoS) and priority on their RANs. Verizon's Private Network Traffic Management (PNTM) and AT&T's Dynamic Traffic Management (DTM) enhancements help customers access and communicate over their networks during bandwidth-limited times, as well as when users are at the edge of the wireless coverage area.

As part of its First Responder Network Authority (FirstNet) offering, AT&T added a dedicated core specific to public-safety users. FirstNet also added pre-emption to its DTM offering, allowing the network to "move" noncritical users during times of extreme capacity limitation. Verizon's public-safety offering includes a host of options that also include pre-emption and a dedicated virtual core network.

As agencies look to migrate more users to broadband-enabled PTT solutions, the largest factor that affects the capacity problem goes back to the wireless network architecture itself. Commercial wireless networks use unicast transmissions between cell sites and phones, whereas LMR networks use multicast transmissions. Therefore, if you have 100 broadband PTT users on the same channel (group) all within the range of a single cell site, you are bridging 100 individual data calls using 100 broadband channel resources. In the multicast LMR architecture, the same scenario will only use a single LMR channel resource. The Third Generation Partnership Project (3GPP) MCPTT architecture specifies support for multicast, but this feature is years away from availability on commercial wireless networks and smartphone devices. Setting aside all other differences between broadband and LMR systems, a full rollout of broadband PTT as a complete replacement for LMR would not be practical until multicast and a direct mode option are available throughout the coverage region.

Another major factor that makes MCPTT over broadband a challenge is the device landscape. LMR handsets, whether portable or mobile, are deployed as a tested set of hardware, operating system (OS), application software and accessories. Broadband PTT handsets operate on a wide range of commercial handsets, with multiple OSs, near unlimited range of apps and a broad range of accessories. This makes broadband PTT solutions prone to failure if the agency's device ecosystem is not carefully managed using a mobile device management (MDM) platform. This became an issue in mid-2019, when Apple's 12.4 OS update broke background operations for iOS users across all commercial broadband PTT solutions.

In California, during the third and fourth quarters of 2019, a new issue threatened broadband PTT service. As a pre-emptive measure to avoid starting wildfires during windstorms, power utility PG&E cut electricity to large areas of the state. This meant all cell sites in those areas, many with no or limited access to backup power, went off the air for potentially weeks at a time. If public safety is to rely on commercial broadband infrastructure, wireless networks must be capable of operating in the absence of power for the duration of any planned outages.

All that said, the commercial

cellular networks generally provide better wide-area coverage than LMR networks, and they have sufficient bandwidth available for broadband PTT service most of the time. However, during critical moments when public safety needs it most, broadband service may be impaired.

PTT Interoperability

The original interoperability problem can be broken down into two groups: intervendor interoperability and intersystem interoperability. The widespread adoption of broadband PTT technologies has introduced a third interoperability problem, intercarrier interoperability.

Intervendor interoperability has mostly been solved by third-party interoperability products and standards-based protocols or interfaces between various system components. Some examples of standards-based protocols from P25 include the Common Air Interface (CAI), the ISSI and the CSSI. The CAI allows agencies to use radios from any vendor with infrastructure from any other vendor, while the ISSI supports communications between multiple P25 systems regardless of infrastructure manufacturer. Some broadband PTT solutions, including Motorola Solutions' WAVE and ESChat, have implemented the ISSI to provide advanced interoperability between broadband PTT users and P25 LMR users. CSSI ensures that compliant console solutions can connect to any compliant P25 network, enabling communications with P25 radios and ISSI-connected broadband PTT devices.

Intersystem interoperability issues require connecting disparate LMR technologies, including analog trunked, P25 and other digital LMR technologies including Digital Mobile Radio (DMR), TETRA and NXDN. This also includes connecting across multiple frequency bands, such as VHF low and high, UHF, and 700 and 800 MHz. Intersystem interoperability issues have mainly been solved using appliance-based third-party solutions. These solutions, from companies such as JPS Interoperability Solutions, are effective at providing communications across LMR networks, regardless of LMR technology and frequency band.

Intercarrier interoperability problems are the result of the widespread adoption of broadband PTT technologies in the commercial and government marketplace. Carrier integrated and over-the-top (OTT) technology are the two basic categories of broadband PTT solutions.

Carrier-integrated solutions use an architecture where the broadband PTT server is tightly integrated with the wireless carrier's core network. However, in North America, the wireless carriers that offer a carrier-integrated PTT solution, including AT&T, Verizon, Sprint and Bell Mobility, block the ability of their PTT users to communicate with PTT users on other carriers. The remaining wireless carriers, T-Mobile USA, TELUS Canada and Rogers Wireless, offer broadband PTT service based on the OTT architecture, which supports cross-carrier

interoperability between all wireless carriers and Wi-Fi throughout the world. The MCPTT architecture previously discussed falls in the carrier-integrated model, and as such, will not provide PTT communications across wireless carriers.

In an October 2019 filing with the FCC, AT&T said its upcoming FirstNet MCPTT offering is not required to provide intercarrier interoperability per its contract with FirstNet. This position is troublesome because one reason that FirstNet was created was to provide a nationwide, fully interoperable network available to all public-safety agencies. With the status quo, the only viable option for intercarrier broadband PTT communications are from the OTT solutions. FirstNet has granted FirstNet Certified status to five OTT PTT solutions, including AT&T Enhanced PTT (EPTT), ESChat, Tango Tango, Orion and MODULO, which are available to FirstNet subscribers in the FirstNet App Catalog.

The intervendor interoperability problem between infrastructure and handsets is a non-issue on commercial broadband networks. Smartphone and tablet devices purchased for wireless carrier use are guaranteed to work on the carrier, regardless of device vendor.

While this article focused on public safety, commercial markets are also seeing widespread success with hybrid networks. In January 2019, Tait Communications announced its hybrid broadband PTT and DMR network built for Transport for London, connecting more than 9,500 buses, was operational. The Tait broadband PTT solution uses DMR's Application Interface Specification (AIS) interface to provide intersystem interoperability. AIS is an IP-based interface, akin to P25's ISSI interface.

Leveraging all the available technologies, public safety has a broad set of tools available to facilitate cross-system, cross-carrier communications to support mission-critical users. The hybrid broadband PTT and LMR networks can solve issues that have plagued public safety for decades. Interoperability on this level is no small task, but most of the pieces exist. Advanced broadband to LMR interoperability must be coordinated at the mutual-aid level, extending the efforts for ISSI interoperability between P25 networks. The broadband PTT intervendor interoperability problem is the newest and needs to be addressed, and perhaps the ISSI is the answer here too. Either way, the community that provides communications solutions to public safety must be willing to work together for the benefit of those who risk their lives for us. ■

Josh Lober is president and CEO of SLA, parent company of ESChat. Since 1991, SLA has developed numerous wireless solutions for government, commercial and military applications. Prior to founding SLA, Lober held positions at 3dbm and Biocom, where he worked on the company's orange paramedic radio made famous in the TV show "Emergency." Email feedback to editor@RRMediaGroup.com.