PUBLIC SAFETY LTE

A HOW-TO GUIDE – FIRSTNET EDITION

Alcatel·Lucent

For additional copies or to download this document, please visit:
www.alcatel-lucent.com/publicsafety

TABLE OF CONTENTS

NEW CAPABILITIES FOR PUBLIC SAFETY

We live in a changing world, where public safety agencies must address new threats and challenges, both natural and man-made. It's no longer enough for first responders to rely on a push-to-talk (PTT) network for situational awareness.

Police, fire and emergency medical services (EMS) play the central roles in emergency response. Mobile technology capable of sending and receiving bandwidth-intensive information can help first responders do their jobs much more effectively and safely. These emergency response organizations need mobile broadband networks that let them share streaming real-time video, detailed maps and blueprints, high-resolution photographs and other files that today's public safety wireless networks can't handle. The same is true when served by commercial wireless networks during major events or catastrophes.

Mobile carriers in many countries now have commercially available LTE networks. The Global mobile Suppliers Association (GSA) reported in June 2012 that 80 LTE operators have launched commercial services, and another 144 commercial networks are expected to be operational by the end of 2012. Altogether, the GSA found that 327 operators in 99 countries have committed to commercial LTE network deployments or are engaged in trials, technology testing or studies.

Source: http://www.gsacom.com/news/gsa_352.php

Currently deployed by many of the world's largest mobile carriers, Long Term Evolution (LTE), the new standard for mobile wireless technologies, will satisfy the growing need for broadband for emergency response organizations. The speed and power of LTE will enable sharing of incident data like never before — in real time, securely, and in line with mission-critical needs for the 21st century — and it will do so in a manner not typically possible with third-generation (3G) technologies available in today's commercial networks.

As the name implies, LTE encompasses the evolutionary path from today's networks to tomorrow's all-IP based, ultra-fast converged networks. It enables real-time video transmission from a firefighter at an incident scene to the emergency operations center, transmission of high-definition video (some of which may be received through next-generation 911 systems), distribution of high-resolution photos and detailed maps to police cars, and much more.

LTE provides unprecedented capabilities for mobile broadband networks and has been declared by public safety and communications experts to be the technology of choice for mobile broadband communications for years to come. As important, LTE is the mandated technology by the Federal Communications Commission (FCC) for use over the public safety broadband spectrum.

MAJOR PUBLIC SAFETY ORGANIZATIONS ENDORSE LTE

LTE has been endorsed by major public safety organizations as the technology of choice for the public safety broadband network. Proponents include:

- Association of Public-Safety Communications Officials (APCO)
- International Association of Chiefs of Police (IACP)
- International Association of Fire Chiefs (IAFC)
- National Emergency Number Association (NENA)
- Major Cities Chiefs Association
- National Public Safety Telecommunications Council (NPSTC)

Limitations of public safety communications today: No interoperability and no mission-critical broadband

Current Land Mobile Radio (LMR) networks rely on narrowband systems that are optimized for voice, and they lack the capacity to support rich, multimedia content needed to improve response and cooperation among agencies. While efforts are underway to standardize LMR networks using APCO Project 25 (P25) open standards, many LMR systems rely on outdated proprietary technology and hence do not interoperate. This hampers interagency response because LMR systems used by neighboring cities or counties can't communicate with each other. The problem is further compounded when a multi-agency response is required. Furthermore, these LMR systems have limited capacity, which forces first responders to use commercial cellular service — or the congested unlicensed spectrum — for non-mission-critical communication, resulting in additional expenses.

While some public safety agencies have low-rate wideband data capabilities, most do not. With most public safety mobile data networks, video and bulk file transfers are impossible and support for remote access to databases and Internet is limited. Some agencies have broadband through commercial providers, which allows them to have access to the Web and e-mail, for example. But these networks get congested during catastrophes, emergencies or other public safety events, just when public safety communication is most critical.

A typical agency may operate multiple dedicated networks to cater to its voice and data needs. With these separate networks, costs for deploying and managing them are multiplied, as every time a change is made to one of these separate networks, there are new costs for equipment, testing, operations and devices.

Unprecedented opportunities

Interoperability has always been an issue because most public safety agencies' radio systems leverage proprietary technologies, thereby inhibiting connectivity between systems. As a standards-based technology LTE provides a giant leap forward and, as a global mobile technology, it inherently supports roaming. It leverages a large competitive ecosystem of equipment, applications and devices made for the private (commercial) sector, bringing the development and equipment costs down.

LTE BENEFITS FOR PUBLIC SAFETY – AN OVERVIEW

LTE is a powerful new technology that will benefit public safety in numerous ways:

Greater interoperability and enhanced interagency cooperation

- Standardized protocols and interfaces
- Built-in roaming capabilities
- Sophisticated quality of service (QoS) toolbox, including priority access mechanisms that authorize and prioritize communication and provide guaranteed and differentiated QoS to applications

Unprecedented broadband capabilities

- High capacity, allowing a wide variety of applications that have rich, multimedia content
- Low latency, enabling real-time services (VoIP, video)
- Much faster than 3G, employing advanced technologies

Cost effective

- Simplified all-IP architecture lowers operating costs
- Leverages a rich, open ecosystem from commercial networks
- Complements existing narrowband radio networks
- Makes private networks more economically feasible

High reliability and security

- Supports a geographically redundant, IP-based architecture, reducing single points of failure
- Supports encryption/ciphering on both control and user planes, enabling secure communications

THE SOLUTION: FIRSTNET

In light of public safety's continued lack of interoperability and the critical need for 21st century broadband capabilities, the U.S. Congress and the Obama Administration took action in early 2012 to ensure that in the future public safety communications does not repeat the mistakes of the past.

On February 22, 2012 President Obama signed into law the Middle Class Tax Relief and Job Creation Act of 2012 (MCTRJC Act). This legislation includes critical changes to public safety broadband communications policy that will drive public safety needs for the next decade and beyond. The new law includes the following:

- Spectrum: Provides up to 34 MHz of 700 MHz spectrum for public safety broadband use
  - ¬ Dedicates 20 MHz of 700 MHz spectrum to public safety broadband use, pairing 10 MHz of 700 MHz public safety broadband spectrum already licensed to public safety with the 700 MHz D-block for a total of 20 MHz of dedicated broadband spectrum.

- ¬ Provides public safety with flexibility to use the remaining 14 MHz; that is, the 12 MHz narrowband block plus the 2 MHz guard bands for broadband.

- Governance
  - ¬ Creates a new public safety broadband licensee, the First Responder Network Authority (FirstNet), a 15-member board to include federal, state, local, and tribal representatives, public safety representatives, as well as financial, networking, and technology experts.
  - ¬ FirstNet will architect, deploy, operate, and maintain a public safety broadband network utilizing public safety spectrum, providing a priority access service to the nation's first responders.
  - ¬ FirstNet is empowered to establish first responder priority over its network, and to negotiate with commercial operators for similar treatment on their networks.
  - ¬ FirstNet is required to coordinate with state and local first responders; to aid coordination, the State and Local Implementation Grant (SLIG) Program includes $134 million in assistance to states to promote cooperation and coordination with FirstNet.
  - ¬ Governors in each state are provided an opportunity to "opt out" of the FirstNet network in favor of their own state-lead deployment, if they determine the FirstNet approach in their state does not meet local needs.

- Economics:
  - ¬ $7 billion in seed money is provided to FirstNet: $2 billion in short-term funding, with an additional $5 billion to be created through new commercial spectrum auctions.
  - ¬ FirstNet directed to utilize commercially standardized LTE technology and competitive procurement practices.

WHAT IS FIRSTNET?

FirstNet is not just another federal grant program that will feed money into states to be spent on public safety communications equipment. FirstNet is best thought of as a new national carrier created, first and foremost, to provide mission-critical broadband service to our nation's first responders.

- FirstNet is required by law to be economically self-sustaining, and as a result is authorized to charge network user fees and utilize public-private partnerships to generate the additional resources required to deploy a nationwide mobile broadband network with urban and rural coverage.
- National Institute of Standards and Technology (NIST) is provided up to $300 million for R&D into mission-critical voice communications, including push-to-talk over broadband.

FIRSTNET AND PUBLIC-PRIVATE PARTNERSHIPS

In the National Broadband Plan, the FCC estimated a total required investment of $16 billion to deploy a nationwide public safety LTE network (see FCC National Broadband Plan, p. 319). The MCTRJC Act doesn't come close on the funding front. Instead, Congress required FirstNet to look to partnerships to make up the $9 billion in additional resources needed to deploy a nationwide network. In practice, this means partnerships that create cash. It also means partnerships that reduce the deployment costs of the network. Fortunately, the new law provides FirstNet with some powerful tools to produce both through spectrum and network infrastructure sharing.

In today's commercial mobile marketplace, operators are spectrum starved (see FCC National Broadband Plan, pp. 76-78). With hundreds of millions of users, and

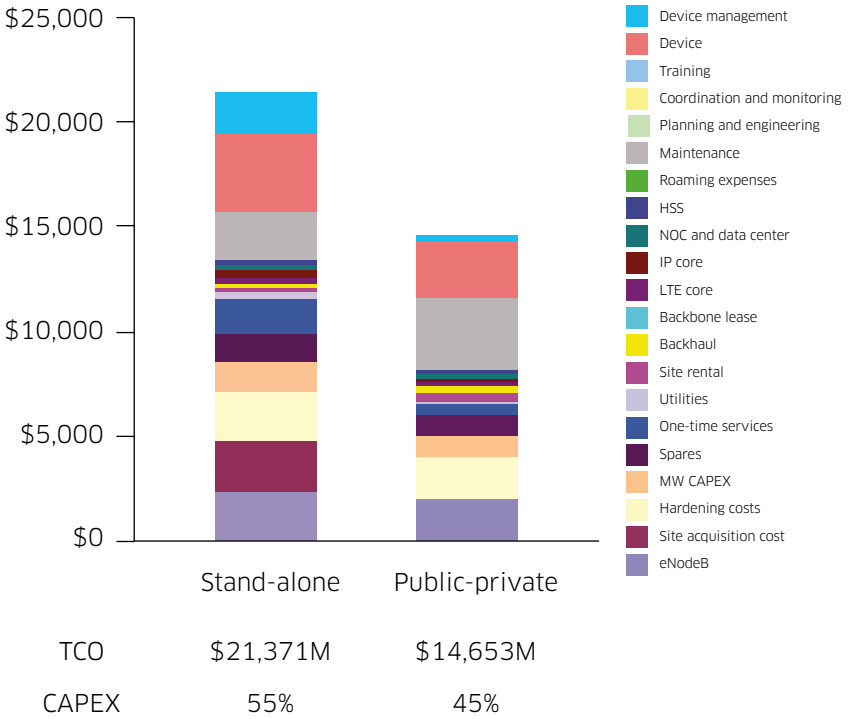
CONSIDERATIONS FOR PARTNERSHIPS

It may be the case that public-private partnerships are created at the state or regional level, not solely by FirstNet. In its recent Request for Information in Development of the State and Local Implementation Grant Program, the National Telecommunications and Information Administration (NTIA) specifically requested input on the role states might play in forming public-private partnerships. This actually makes a lot of sense. Utilities, for example, don't have a nationwide footprint like the four national carriers do, which may make it difficult for FirstNet to create nationwide partnerships with utilities. But if states take the lead, they are likely in a much better position to coordinate partnerships on a more granular level – sub-state, statewide, and partnerships matching regional coalitions of states.

multiples of that with the emergence of connected devices (for example, "machine-to-machine" communication), operators are desperate for access to new airwaves to help them address the crush of traffic on their networks.

Similarly, the nation's utilities are also desperate for spectrum. Unlike public safety, there is no dedicated allotment of spectrum to address utility needs, not only during emergency response to keep their networks up and running, but also for day-to-day utilization of spectrum for the smart grid, the deployment of which is critical for enhanced efficiency and security of the utility network. Figure 1 shows a 10-year total cost of ownership (TCO) comparison, based on Bell Labs research, indicating it is dramatically more cost effective to build a network as part of a public-private partnership rather than on a standalone basis.

Figure 1. Bell Labs comparison of a U.S. standalone public safety network versus public-private partnership



TCO	$21,371M	$14,653M
CAPEX	55%	45%

10-year TCO savings 46 % = $6718M

- Site acquisition cost is the biggest contributor to the standalone network TCO
- The other major contributors are hardening costs, maintenance costs, eNodeB, device management and one-time services are major contributors

- Maintenance is the biggest contributor to the public-private partnership TCO
- Other major contributors include eNodeB, hardening costs, devices

(as submitted on June 15, 2012 to the National Telecommunications and Information Administration in its Request for Information on the Development of the State and Local Implementation Grant Program)

FirstNet should leverage existing infrastructure to reduce its own cost of deployment and achieve its goal of a nationwide network serving first responders. For example, partnering with utilities could provide FirstNet with affordable access to utility-owned infrastructure in rural geographies — towers, rights-of-way, and network backbone — all of which can save considerable time and resources compared to a greenfield deployment. FirstNet-built infrastructure — backbone, towers — could also be leased to partners. The MCTRJC Act recognizes a broader set of eligible users for the network, which is critical to supporting public-private partnerships. Instead of limiting use of the spectrum to only public safety first responders, now FirstNet can work with partners to facilitate a much broader set of so-called "secondary users." And that can mean anybody, from a commercial carrier's subscribers, to utility employees, to any governmental users, depending on how partnerships are structured. It all means one thing at the end of the day: Access to more cash, more existing infrastructure, and a more robust ecosystem that can turn FirstNet's $7 billion into many billions more.

The utilities advantage

In many public safety emergency situations, utilities have a key role to play along with fire, police and EMS, and as such they maintain their own emergency response workforce. If a power line is involved in a fire, accident or other emergency, other responders may have to wait for the utility's staff to address the issue before other rescue activities can begin. Another example is a gas leak; it won't be safe for the fire and EMS responders until the leak has been contained by utility personnel.

Utilities are in an excellent position to partner with FirstNet for the deployment of LTE because they have a lot of infrastructure in place — such as power and transmission poles — to which they can add other equipment. They have a particularly strong presence in rural areas and are already focused on end-to-end coverage. For example, unlike commercial communications providers, utilities reach 100 percent coverage of a geographic area, rather than perhaps only 97 percent of the population, which is consistent with the coverage public safety is expected to provide.
Many utilities have been investing in IP-based communications for years, which in turn can provide the high bandwidth backhaul that will be required for LTE, and they already have fiber optics and microwave systems in place. There are already many successful shared LMR systems with utilities and public safety, demonstrating the value of cooperation. Also, utility organizations are well equipped and experienced at responding quickly to emergencies.

A WORD ABOUT UTILITIES

When the public safety community thinks of an ideal partner for the deployment and use of a mission-critical network, who do they think of? They think of a partner who has the same mission-critical needs as public safety – life and death, not revenues and profit. Utilities fit the bill: They are public safety, and they also need a five-9s network that is hardened and built for mission-critical needs so it won't go offline when the network is needed the most. They also have an existing revenue base that can support sensible investments in the utility business. Investing in the smart grid is sensible. Why else do you think the Obama Administration included $5 billion for smart grid investments in the American Recovery and Reinvestment Act, which is just about the same amount the Administration included for broadband?

LTE: WHAT IT IS, WHAT IT DOES

LTE is a relatively new cellular technology that greatly increases the speed, reliability and capacity of mobile phone networks. LTE standards were first described in Release 8 of the 3rd Generation Partnership Project (3GPP). Both 3GPP and 3GPP2 have declared LTE to be the next-generation global standard for mobile communications.

Why LTE

LTE is faster, simpler and more economically feasible than any other mobile communication technology. Working together, the following features and benefits make LTE much more powerful and reliable than 3G, and provide unprecedented capabilities for public safety, as well as utilities.

Better performance – The numerous technological advances of LTE bring better overall performance. End users will certainly notice an improved experience, and the technology itself will be more reliable.

Multiple-input multiple-output (MIMO) technology, for example, is used with LTE. MIMO puts several antennas — rather than one — on a single tower. With more antennas working for the same communication, performance is significantly improved. MIMO can employ multiple antennas on both ends — transmitter and receiver. MIMO increases data throughput without the need for additional bandwidth or increased transmitting power.

Orthogonal frequency division multiple access (OFDMA) is another technology that is used with LTE, which provides improved spectral efficiency — LTE is better than previous technologies at maximizing the use of available spectrum. This is a key attribute because there is a finite amount of spectrum anyone can use. The improved spectral efficiency of LTE lets the system maximize bandwidth data capacity, number of users and user experience.

- **What it means for public safety and utilities:** Improved situational awareness
  - ¬ Two-way voice, real-time high-definition video, and large data file distribution integrated with incident management databases, including Geographic Information Systems (GIS), provide for immediate, dependable communications during incident response. With LTE, voluminous amounts of information can be exchanged from anywhere, instantly, in many ways. Collaboration utilizing these tools ensures effective sharing of information in task force operations.

Simplified, IP-based architecture – LTE is based on a simplified all-IP architecture. An LTE network requires fewer elements, which results in lower CAPEX and OPEX as well as greater efficiency and lower latency. LTE is also extremely scalable, which makes it easy to accommodate a significant number of users. All-IP architecture is also more flexible, making it easy to connect nodes, build pathways between nodes for increased redundancy, and to change the logical paths between nodes if needed.

In today's commercial marketplace, fixed and mobile operators are reducing network complexity and cost by leveraging a common IP architecture for their fixed and mobile needs. In fact, today commercial mobile networks are typically relying on some of the largest fixed networks deployed. Leveraging the best of breed technologies and solutions from the commercial sector along with public safety specific

features, such as ruggedized devices for first responders, will in turn provide the very same efficiencies — reduced cost, reduced complexity, superior service — for the public safety market.

- **What it means for public safety:** Unified communications and enhanced day-to-day operations
  - ¬ Voice, video, and data on one end-to-end IP network means reduced complexity and lower costs through greater efficiency. Efficiency can also be greatly increased when people have instant remote access to databases, for example, to access vehicle records or suspect files, or to submit reports electronically. Public safety personnel are more effective when there is less paperwork to do, and when they're not waiting for information. Similarly, LTE enables telemetry and remote diagnostics, where LTE allows more data to be sent automatically from mobile devices so the data can be analyzed elsewhere, ensuring maximum information availability in the most efficient amount of time possible.
- **What it means for utilities:** Manage distributed field assets with a single network
  - ¬ LTE provides a single network to enable meter collectors, substations, pole-mounted and remote intelligent devices, field personnel, distributed energy resources, enterprise voice and data, as well as video surveillance.

Low latency – With LTE, users typically experience a one-way latency of 10-15 ms, which is very important when it comes to demanding applications such as push-to-talk or streaming video, and for applications that require very fast access setup, which is often the case with public safety applications. Too much latency degrades the signal and can frustrate the end user.

- **What it means for public safety:** Unprecedented video and digital imaging
  - ¬ LTE gives new meaning to the phrase "a picture is worth a thousand words." Seeing what's happening at an incident scene — while the situation is unfolding — is much more helpful than hearing about it. LTE provides near-real-time transmission of high-definition video, as well as detailed images of crime and disaster scenes, suspects, and more. If an officer isn't responding by radio, a dispatcher can instruct the squad car to activate and/or remotely control a camera and autonomously transmit video to the dispatcher.
- **What it means for utilities:** Realize the benefits of a "smart grid"
  - ¬ Utilities are looking for opportunities to leverage intelligent and proactive monitoring of their infrastructures to be smarter about how they manage their resources. With LTE, the ability to access extremely demanding applications will open the door to many functions that are not possible with current networks. For example, a utility may opt to use a drone to fly over transmission lines and check for faults before they occur. This kind of application is made possible through the ability of LTE to support high-definition video in real time. National energy, environmental and other policies are demanding a more efficient, clean and reliable electric grid. Smart technologies allow utilities to keep energy flowing as cost effectively as possible.

Greater interoperability – Commercially standardized protocols and interfaces of LTE mean that more public safety personnel can talk to one another. LTE can put agencies and individuals on the same communications platform. LTE supports an open device ecosystem. And the all-IP nature of LTE helps with interoperability because more and more public safety agencies are moving to IP-based systems.

- **What it means for public safety and utilities:**
  - ¬ Move away from "special" or proprietary and expensive technologies.
  - ¬ Allow roaming onto commercial networks when necessary, facilitating broad partnerships between FirstNet and commercial carriers.

- Communicate seamlessly with other emergency responders. When utilities join other first responders on a public safety LTE network, interagency communications is greatly enhanced.
- After next-generation 911 is a reality, leverage growing amounts of information — text, images, video — received by Public Service Answering Points (PSAPs) from the public through mobile devices.

Security – LTE makes use of some of the most advanced security mechanisms available and consists of two main components — air interface security and network security. Air interface security consists of all the security features and capabilities designed to protect the device, the network elements in the LTE system and the LTE traffic against attacks originated over the air interface. Network security consists of all the security features and capabilities that protect the LTE network elements and LTE traffic against security attacks generated in the wireline transport network and external devices connected to the evolved Radio Access Network (eRAN) and the Evolved Packet Core (EPC) network. End-to-end security is achieved with strong

data encryption, in devices and the network, including in base stations. Mutual authentication between the network and devices ensures system integrity.

- **What it means for public safety and utilities:**
  - ¬ Enables secure communication
  - ¬ Over the air information will not be tampered with
  - ¬ If needed, because of the throughput capability, additional security layers can be implemented
  - ¬ Because of mutual authentication, rogue devices will not jeopardize operations
  - ¬ Provides the basis for a secure and reliable communication between devices and data centers

Network sharing – The concurrent use of the network by multiple entities with distinct functions and roles will call for sharing assets in a reasonable manner. Standard network sharing methods are available to ensure multiple entities have access to their fair share of resources without hindering each other's operations. For example, an architecture based on the Multiple Operator Core Network (MOCN) concept is a possibility if utilities have access to their network identity.

- **What it means for public safety and utilities:**
  - ¬ Spectrum resources can be concurrently used
  - ¬ Spectrum sharing can be tailored on the basis of mutual agreements
  - ¬ Distinct encryption levels can be provided
  - ¬ Traffic can be segregated

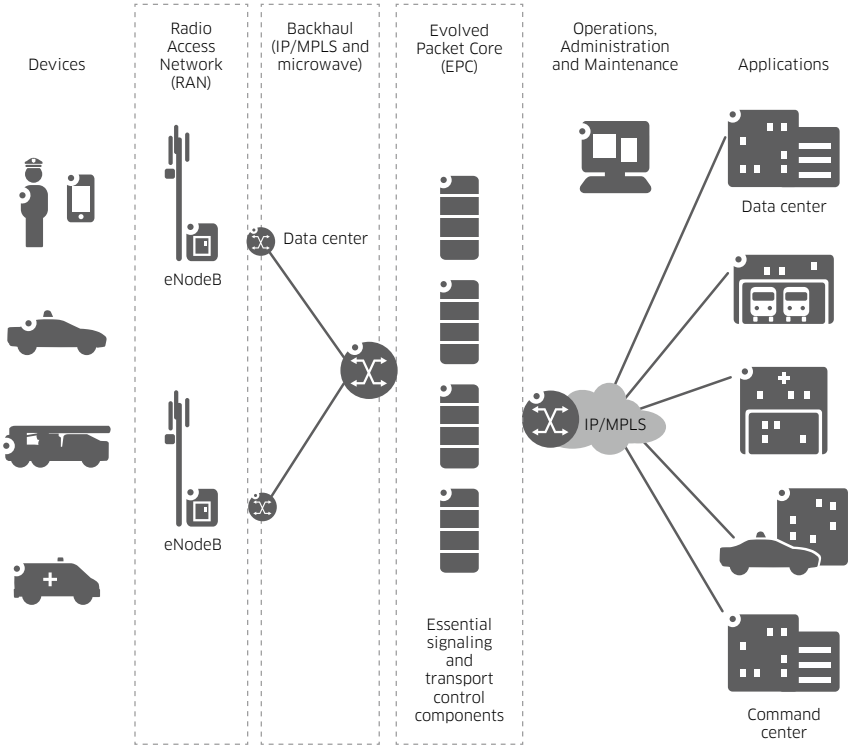
Quality of service and prioritization – With its flat-IP architecture the LTE network must rely on QoS controls to serve the different types of services and prevent congestion. In that regard, QoS functions are spread across the whole LTE network domain, including the UE and IP/Multiprotocol Label Switching (MPLS) backhaul segments. QoS continuity when roaming is ensured subject to local policies. Further, LTE introduces priority mechanisms, including pre-emption, to distinguish between higher and lower priority sessions and UEs.

- **What it means for public safety and utilities:**
  - ¬ Intelligent sharing of air resources and network capacity
  - ¬ Prioritization of traffic, for example, during incidents
  - ¬ Enabler of quality of experience

The LTE solution

LMR has been the workhorse for years, but it simply can't give public sector agencies everything they need today. Things have changed, and a narrowband technology is no longer sufficient. With LTE, emergency response agencies are afforded new applications to help them keep public and critical infrastructure safe — high-definition video, digital imaging, geographic information systems (GIS), Web access, automatic vehicle location (AVL), and much more. Voice over IP (VoIP) is enabled too, including interoperability with LMR systems with the use of appropriate gateways. LTE brings improved interoperability, providing the basis for the nationwide interoperability of the future. LTE provides multiple benefits related to situational awareness, decision making, response times and safety for first responders themselves.

Figure 2. Public safety LTE solution – high level



Seeing what is going on at an incident or what happened in the area prior to the incident helps improve situational awareness and decision making by first responders and command center personnel. This includes video surveillance feeds from fixed cameras, video from camera-equipped vehicles, first responders with tablets, and helmet cameras. All of these enable command/dispatch centers and other responders to see what's going on in real time. In the future, video will also be available from citizens through NG911 and can be rapidly shared with first responders. With LTE, because of the growth in frequency and volume of video content, several factors need to be addressed upfront including equipping command/dispatch centers and first responders to effectively manage video.

Within the dispatch and/or command center, an important element to implement as part of the initial solution deployment is a capability to effectively manage the video selection, distribution and storage. For many agencies this will require the integration of information from multiple applications including license plate recognition and access control systems in a police command center to deliver a more comprehensive situational view. Using remote camera management capabilities, the center can select the appropriate feed(s) and push them to the first responder(s) and agencies with whom they are collaborating at an incident. First responders need the capability to quickly and easily move between different live video feeds streamed to their device to effectively aid in increasing situational awareness and decision making. For example, they should be able to easily move a video from their vehicle laptop to a ruggedized tablet or smartphone when leaving their vehicle. The flexibility to view multiple video streams and then select the relevant one is also needed and is not always readily available on every device.

First responder needs associated with utilizing real-time video with LTE are a focus area for Bell Labs. The Bell Labs First Responder Video innovation addresses these needs with a solution that enables a first responder to easily manage, select and share relevant video with others and integrates with command centers applications while using a broad range of devices. Unique Bell Labs processing reduces the cost of ownership by squeezing seven video streams into one over the LTE network.

Supporting voice on the LTE network

A broadband public safety network is primarily deployed to provide additional capabilities to first responders that will improve operational effectiveness. Initially, these capabilities will likely be available to a subset of first responders, and then to an increasing number over time as budgets and applications become available. Although voice (and especially group voice calls) on existing LMR networks will continue to be an essential mode of communications for all first responders, the support of voice over broadband is very important. LTE can provide VoIP services today and a new set of standard parameters has already been defined for voice over LTE (VoLTE), which provides VoIP interoperability among service providers. Providing VoLTE on a public safety network initially enables agencies to replace commercial wireless devices with devices that leverage the public safety network, thus reducing the total cost of ownership for public safety.

But the requirements for support of voice go well beyond the standard voice over LTE service. In fact, in the public safety context it is most important for the LTE

network to interwork with LMR voice (and low data-rate services like short message). To achieve interoperability, a gateway that interconnects the narrowband systems with the LTE system will enable the extension of the LMR push-to-talk application to the LTE network. The same gateway may also provide the function of a full-blown PTT server for LTE. The current interworking protocol is based on the IP-based P25 ISSI interface, which is defined to interconnect multiple LMR systems and being extended to standardize the protocols between an LTE client and the PTT server. This will enable full interoperability between jurisdictions and solutions from different suppliers. In parallel, through the addition of talk-around and evolved Multimedia Broadcast Multicast Service (eMBMS), LTE public safety networks will be able to more efficiently handle large-scale group communications.

This will pave the way toward complete migration to a mission-critical LTE network. Preliminary implementations are available that enable a first level of interworking.

Supporting roaming out of jurisdiction

Public safety users generally collaborate with other jurisdictions, for example, to provide mutual aid. The LTE network enables this through seamless roaming from one part of the service area to another, using mechanisms defined in the 3GPP standards.

In addition to having access to the public safety networks of visiting jurisdictions, roaming to commercial networks is also required for those areas where the public safety network is not yet deployed. When visiting a commercial LTE network, the visiting network interfaces with the Home Subscriber Server (HSS) in the public safety network to retrieve the specific subscriber information. It is expected that FirstNet will select an Internet Packet Exchange (IPX) provider to handle the connectivity between the public safety network and the various commercial networks with whom FirstNet creates roaming agreements. In addition to roaming to commercial LTE networks, roaming to commercial networks with different radio technologies such as HSPA, GERAN, 1xEV-Do, or eHRPD is also supported, subject to device capabilities.

MISSION-CRITICAL VOICE: U.S. R&D

In the same legislative act that created FirstNet, the U.S. Congress also provided up to $300 million to the National Institute of Standards and Technology to pursue research and development of public safety communications needs, including mission-critical voice over broadband. This R&D program can ensure a speedy, cost-saving transition from LMR to mission-critical voice over broadband. The U.S. Congress directives include:

- Document public safety requirements
- Accelerate deployment of capability for communications between narrowband and broadband networks
- Research plan addressing wireless communications needs of public safety beyond that provided by the current generation of technology
- Accelerate deployment of mission-critical voice, including “talk-around,” over broadband networks, prioritization, authentication, and standard APIs for the nationwide broadband network
- Accelerate deployment of technology and equipment that eventually facilitates migration from narrowband to broadband network


Life Flight

PREPARING FOR LTE AND FIRSTNET: THE STATE AND LOCAL IMPLEMENTATION GRANT PROGRAM

Getting ready for the FirstNet LTE network will take some work, but the effort will be well worth it. As noted above, one of the key elements of the FirstNet success will be utilizing as much existing infrastructure as possible to reduce its network deployment costs. A critical source of infrastructure is the communications assets deployed by state and local governments. This makes a lot of sense as the FirstNet network is intended to benefit state and local first responders, so part of the trade-off is the intent for state and local networks to be made available for use by FirstNet. Before FirstNet can architect a network to take into account all of those existing resources and deploy a nationwide network, a number of steps must be taken locally first.

In the MCTRJC Act, FirstNet is required to coordinate with state and local public safety to ensure the nationwide network meets the public safety community's needs. The coordination mandate includes themes such as local views on the construction of the network core and Radio Access Network; where towers should be placed to maximize population and geographic coverage; and adequacy of hardening, security, reliability and resiliency. In fact, many of the coordination themes are the same things any entity deploying an LTE network should take into consideration before actually deploying a network. So it's critically helpful that in addition to requiring FirstNet to coordinate with state and local stakeholders, the legislation also includes the SLIG to fund state and local efforts to consider all of these inputs.

But what does a successful state and local engagement look like per the coordination requirement as supported by the SLIG? Here's an overview:

Governance

- **Select a coordinator.** Governors in each state are required in the legislation to identify one individual who will own the state's engagement with FirstNet. This individual should have authority to bring state and local authorities together to ensure the state's full range of interests are represented with one voice.
- **State and local coordination.** How will state and local jurisdictions work together and in the context of a nationwide network? With respect to infrastructure referenced above, who actually owns it and is authorized to make it available for use by FirstNet? Does the state need to create a new interjurisdictional agreement everyone can support? How will priority be established between jurisdictions within the state, between states working together in regional coalitions, and what happens when one region's users roam into another region and vice versa? "Jurisdictional priority" can be one way to address the issue. This gives each agency control of a portion of the network; for example, base stations within its jurisdiction. Thus each jurisdiction is truly part of the solution, while still retaining control. This can be scaled to the state and regional level as well.

State and local service needs

- **Determine user requirements.** Think ahead about what users will actually want to do after LTE is in place. What are their requirements? They could be different for each public safety agency. Will your users need high-definition video all the time? Will your agency want to do a lot of administrative or office work from

a mobile environment? What will you use text messages for and how often? Which databases will people need access to while out in the field? This type of application and user analysis is an important step in preparing for LTE. Be sure to talk with actual users — police officers, firefighters and EMS personnel, for example — and understand how they will use the LTE system. Which users should have priority access to the network? In which situations? You'll want to think about policies that spell out the priorities within the state. Even if within a single jurisdiction, you'll need agreement between police, firefighters and EMS, as well as agreement on what priority arrangements might look like between public safety and potential public-private partners such as utilities and commercial carriers.

- **Determine which applications you need.** After you really know what your users need, you'll know which kinds of applications you'll want on the FirstNet network. Look into the throughput requirements for those applications. How much capacity will be required to fulfill user needs? Think ahead: Public safety agencies always want more and more applications that require broadband. Consider applications that improve situational awareness. Also look at those that improve communications across different agencies and jurisdictions and increase the day-to-day productivity of your mobile workforce.

ng Connect POINTS TO THE FUTURE

A program called ng Connect (ng for "next generation") brings together companies that create infrastructure (including Alcatel-Lucent), devices, applications and content for broadband, to help develop the best possible uses of LTE and other broadband technologies. The goal is to share knowledge, work together and help create tomorrow's end-to-end broadband ecosystem. For more information, visit www.ngconnect.org.

- **Delivering quality of service.** The last key element relates to QoS and the specific management of QoS for public safety operations to deliver the required performance. LTE is an all-IP radio network where all applications share the same radio channel and IP infrastructure. The LTE standard defines a comprehensive toolbox that enables a differentiated QoS for specific applications (such as voice, data and video) and users. Rules can be defined for each application and

user to determine exactly how that particular traffic flow should be handled from end to end. The parameters that can be set include such things as data rate (guaranteed or not), latency, packet loss and priority. Every single packet that enters the LTE network is inspected and mapped to the appropriate bearer channel. Hence, it is of utmost importance to choose a solution with a high performance Packet Data Network Gateway (PGW) that is able to efficiently handle the deep packet inspection (DPI) and mapping process for all incoming packets. During deployment, the QoS parameters for each application/user are provisioned so that each user experiences the appropriate performance under any radio circumstances. It is also possible to control and modify the QoS parameters of a particular (group of) user(s) or applications dynamically. This means that in an emergency situation, for example, the situation commander could temporarily provide higher priority to the team assigned to respond to the incident.

Infrastructure and solution requirements

Now that you've looked at user requirements and which applications you'll need, consider the overall solution. You can now start to think about users, capacity, coverage, existing infrastructure, device ecosystem and other factors as you continue to prepare for LTE.

- **Assess what you have.** Early on, look at what you have, and how you're using it. Then you can determine how much of it you can make available to FirstNet to leverage in its network deployment. You may have extensive facilities you can make available, which will save a lot of money for FirstNet and ultimately save you money when it comes to service fees. Conduct an in-depth assessment of your existing network infrastructure and backhaul. What can you use from your LMR infrastructure? Do you have microwave? Fiber? IP/MPLS? How is everything connected to the network? What do you own? What do you lease?
- **Look at your physical infrastructure.** If you have existing tower sites for voice communications, it's likely you can reuse most of them for your LTE network. But you have to look closely. How many towers do you have? Can they bear more weight? Hold more antennas? Can you add an LTE base station (eNodeB)? Is there enough primary and backup power at the base of each tower to run more equipment? You also need to know how you're currently connecting to all those sites, including the capacity of those connections.
- **Maximize communications reach and coverage.** First, the public safety LTE radio coverage must span both densely populated areas as well as remote and

sparsely populated areas (for example, in mountains/forest areas to fight forest fires) where first responder operations are also needed. A common requirement is 95 percent to 98 percent outdoor coverage of the area an agency serves.

- **Identify system strengths and weaknesses.** With LTE, there will be more data traffic — and it needs enough network capacity to get from place to place. Where does your system have room to grow? How can you achieve greater capacity? Are there bottlenecks in your network where you simply can't add capacity? You need to identify strengths and weaknesses, whether you have your own network or are leasing from a commercial carrier. If you're leasing, can your carrier handle an increase in data traffic after LTE is here? If it's your own network, can the equipment and infrastructure grow to meet future demands? Will you need more backhaul? Sometimes, additional technologies can bridge the gaps. MPLS, for example, can help your current backhaul run more efficiently so you can expand capacity that way rather than building more backhaul.
- **Ensure non-stop communications.** Another aspect of the reliability and availability of an LTE public safety network relies on the way the nodes of an end-to-end LTE network are deployed and interconnected. The LTE core network can be deployed in a geo-redundant configuration to enhance

BELL LABS SUPPORT

During the SLIG phase states will need to ensure things are done right the first time. With its expertise in both telecommunications and economic analyses, Bell Labs Advisory Services can be the right partner to support the planning activities and make recommendations on the way to proceed. Examples of support may include:

- Assess the viability and capacity of backhaul/backbone facilities
- Traffic modeling
- Study of multiple RF coverage scenarios
- Reliability assessment of particular architectures based on potential site locations
- Total cost of ownership analyses; for example, to help spread costs with secondary partners

solution resiliency in the event of a disaster at a core site. On top of this, LTE offers the inherent capability to connect each base station (eNodeB) to multiple core network elements. This enables the load balancing of traffic to maximize performance and use of network capacity under normal operating conditions. But more importantly, it provides services continuity to the first responders if there is a failure of a core network element. Also, LTE is an all-IP technology and all nodes can be interconnected with a redundant/meshed packet-based backhaul network.

When IP/MPLS is used on the backhaul network, it can be designed so that any transmission link or transmission equipment failure can automatically be resolved in less than 50 ms by selecting an alternative transmission path using the Fast Reroute (FRR) feature.

The battery backup design also has a key role in the overall availability and resiliency of the solution. In the event of a major electricity blackout (caused, for example, by a tornado knocking down electrical poles), public safety communications must continue to operate to support the rescue of citizens and to maintain security in the disaster area. Consequently, the battery backup systems must be oversized compared to commercial network practices, and may include backup generators to handle prolonged power outages.

In the event the local communications infrastructure is destroyed by a major disaster (such as flooding or fire), it is always possible to deploy a Cell on Wheels (COW) equipped with a backup generator to provide emergency communications.

- **Local core or hosted core.** Per the MCTRJC Act, FirstNet is authorized to deploy a centralized core supporting the nationwide network. With respect to LTE architecture, this makes perfect sense. In one national network, you need a handful of geographically redundant cores to provide service across the country. To help reduce initial capital costs, operations costs and risk, states would essentially rely on a hosted or "cloud"-based LTE core solution provided by FirstNet. This will ensure the precious resources and infrastructure available for the nationwide network can be devoted toward the Radio Access Network, the density of which determines true throughput, geographic coverage, and

hardening — the real-world service parameters of the network that will be used in life and death scenarios. This is proven in national carrier networks that support hundreds of millions of subscribers and will represent a tremendous cost savings in deploying a new nationwide network for first responders.

Building up the backbone network to support broadband traffic

Historically, organizations have built networks for a single purpose. This has resulted in the operation and management of multiple siloed networks. Today, increasing numbers of state and local jurisdictions are breaking away from the siloed model in favor of end-to-end IP networks upon which multiple public applications can be layered. The result is increased efficiency, greatly reduced costs, and superior services. As state and local jurisdictions prepare for and coordinate with FirstNet, they must be mindful that these same investments — needed for statewide operations independent of LTE — have the added benefit of creating a ready-made backhaul environment for LTE when it is deployed.

IP/MPLS networks are perfectly suited for providing backhaul (transport) in LTE networks. IP/MPLS can handle high bandwidth, media-rich services that require end-to-end QoS. And while IP/MPLS can evolve with future needs and LTE, it also integrates with multigenerational networks that need to incorporate legacy technologies. The use of both IP and MPLS has been growing consistently in recent years, and that growth is expected to continue. Many public safety agencies have already transitioned to IP/MPLS networks to converge multiple services — voice, data and video — onto a single platform. Other agencies have at least started on this by moving their LMR communications to IP. With IP/MPLS, multiple types of data from numerous agencies can be sent over the network while keeping traffic separate and secure. MPLS also provides better flexibility and performance than previous technologies. MPLS can carry both mobile and fixed services simultaneously. It's a mature technology that provides many options for the future.

To the extent state and local jurisdictions are making such investments today, it pays to take the long view and determine how investments today may facilitate FirstNet deployment locally. To meet the stringent QoS requirements of real-time traffic, for example, a mobile backhaul network must integrate many of the qualities and attributes of switched networks including predictability, reliability and manageability. Rather than using multiple overlay backhaul networks, the solution should accommodate legacy access needs and be optimized for next-generation broadband services using Ethernet and MPLS, based on multiservice routing and switching platforms.

The use of Ethernet/ATM/TDM-based pseudowires will bring mature and efficient functionality to the RAN and enable the transition of the legacy RAN to packet.

When making the transformation to packet, there are some important requirements to keep in mind related to LTE. A mobile backhaul network must:

- Support current LMR services while providing the scalability and flexibility to support new LTE mobile services
- Enable scalable bandwidth at lower cost (leveraging Ethernet/IP over multiple media: copper, fiber, microwave)
- Provide service assurance across all services (using carrier-grade Ethernet/MPLS)
- Deliver accurate clock synchronization mechanisms to converge rapidly across the packet RAN
- Lower operational costs (through integrated management)
- Provide QoS support for all mobile services, efficiently allocating scarce network resources in real time
- Increase network optimization and capacity, improving cost per bit transported as leased lines are replaced
- Address infrastructure diversity using flexible backhaul alternatives, each providing an evolution to all-IP

RETURN ON INVESTMENT

State and local public safety jurisdictions must be mindful that the $7 billion appropriated to support FirstNet will need to be supplemented in order to build the nationwide public safety broadband network. Organizations that have invested in upgrading their networks – for example, states that have already deployed IP/MPLS networks – may be more likely to be leveraged by FirstNet to more quickly deploy the nationwide LTE network. The takeaway is this: State and local jurisdictions have present day needs for up-to-date, IP-based backbone networks for their existing communications needs. This means that those investments today may also have the added benefit of delivering LTE to public safety users in the future faster and at lower cost.

Opting out of FirstNet: What it means, how it works, and why it's not a near-term concern

As noted above in the outline of the MCTRJC Act, states will have an opportunity to decide whether to participate in the FirstNet network or to opt out in favor of their own. Some states may be tempted to default toward an opt-out expectation right from the start, but such a premature decision would be a mistake. For the time being, regardless of whether a state "opts in" (that is, decides from the start to robustly coordinate and cooperate with FirstNet to ensure its success) or opts out, all of the same work must be done. States still need to address governance and coordination internally. States still need to understand the parameters of the service they feel best meets local needs. States still must inventory existing infrastructure that may facilitate LTE deployment. In short, all of the work that must be done by a state coordinating with FirstNet must be done by a state that opts out, so why not set aside the ultimate question and make the best effort possible for FirstNet to be successful? Besides, it remains to be seen just how simple the opt-out mechanism will be after it is available to states, and that's likely a few years down the road.

To cover off the facts, here are the parameters of the state opt-out process:

- After FirstNet finishes its nationwide architecture and RFP process, NTIA will inform each governor about FirstNet deployment plans for that state, including how much of the $7 billion FirstNet intends to spend there. It's only at this point — one, two, or even more years down the road — before a state has to make the decision whether or not to opt out.
- After a state decides to opt out, it then has 180 days to conduct its own state-level RFPs for network deployment.
- After a state completes its RFPs and puts its final plan together, it must then send its plan to the FCC. The commission will then assess the state plan for compliance with FCC interoperability guidelines, as established by the Interoperability Technical Advisory Board. If the FCC rejects the state's plan, then the state opt out is eliminated and FirstNet will deploy. If the FCC approves the state's plan, then the plan gets referred to NTIA.
- The role of NTIA in a state opt out addresses two key ingredients — access to funding and access to spectrum.
    - ¬ **Funding:** States that attempt to opt out and pass the FCC interoperability assessment then have the opportunity to "request" their share of the $7 billion for deployment. Nothing in the MCTRJC Act actually requires NTIA to give states money, so it's not clear whether they will get any.
    - ¬ **Spectrum:** States that attempt to opt out and pass the FCC interoperability assessment then must request permission from NTIA to lease spectrum from FirstNet. That means opting out states must have money to pay for a lease, and we cannot confirm at this early date how much that lease payment will be.

In a nutshell, there's plenty of uncertainty surrounding the opt-out process. But more importantly, a state that decides to opt out is likely not going to have any chance to be successful if it waits until the 180-day RFP process tolls to start doing all the work that is required to plan an LTE deployment. In other words, a state that successfully opts out is likely going to have been working on its plan for a couple of years prior to the decision actually being made, just like a state that opts in to make FirstNet a success. That just underscores the value of not worrying about whether to opt out today, but instead focusing on all the work that must be done for the purposes of coordinating with FirstNet and participating in the State and Local Implementation Grant Program.

Alcatel-Lucent is a leading LTE provider globally and a trusted partner in building public safety networks for state, regional and local governments. Alcatel-Lucent delivers complete, best-in-class communications solutions aligned with the most challenging mission imperatives of public safety networks, and tailored to meet the needs and requirements of governments.

For more information, visit **www.alcatel-lucent.com/publicsafety** or call **1-877-425-8822**.

For additional copies or to download this document, please visit: **www.alcatel-lucent.com/publicsafety**