ULTRA-BROADBAND PMR: FIVE BUSINESS MODELS FOR ENHANCED MISSION-CRITICAL OPERATIONS

STRATEGIC WHITE PAPER

Public safety professionals require the highest level of reliable mobile communications, including broadband data services that deliver real-time imagery, video, geo-localization and always-on connectivity to private cloud-based applications and databases. Long Term Evolution (LTE) provides the most cost-effective and secure way to support these services. The transition to LTE will entail a complex technical, operational and business evolution for the public safety community (end users and industry). This white paper examines the features, benefits and future of LTE mobile broadband networks for public safety, with specific guidance on moving forward with five business models: MNO (contracting services through an existing mobile network operator), G-MVNO (operating or getting service from a government mobile virtual network operator), PPP (deploying dedicated network services through a public-private partnership project), Private (building a dedicated network), and Hybrid (combining a G-MVNO with a private network).

Alcatel·Lucent

TABLE OF CONTENTS

THE MOBILE BROADBAND IMPERATIVE

Public safety communications are at a turning point. The most urgent planned and unplanned events now require the highest level of reliable, integrated mobile communications. In today's world, this means not only mission-critical voice, but also real-time imagery, video, geo-localization, and high-speed access to private cloud-based information and applications. These demands must also be matched with dependable, real-time coordination between multiple government agencies.

Existing private mobile radio (PMR) systems, based on APCO Project 25 (P25), Terrestrial Trunked Radio (TETRA) and TETRAPOL standards, cannot deliver this set of capabilities, because they were designed primarily to support mission-critical voice. However, standards-based Long Term Evolution (LTE) – the global mobile broadband technology – can complement existing PMR networks to dramatically enhance operational effectiveness and coordination within a secure infrastructure shared by cooperating agencies. The operational benefits include:

- **Enhanced Situational Awareness**: When a broadband mobile data network is added to a legacy PMR system, all public safety agencies gain 360° situational awareness. Command and control officers can obtain and immediately share essential data with officers in the field. This includes high-definition video, social media, advanced analytics and accurate multimedia information such as object and person identification, gunshot detection and crime scene views. Additionally, vital signs from first responders and injured people can be transmitted to the appropriate command and control centers to improve personal safety and save lives.
- **Enhanced Interoperability and Collaboration**: As a technology based on open standards, LTE offers inherent interoperability and roaming capabilities between public safety organizations using LTE. By means of gateways, it is also possible to enable communication interworking with the legacy PMR systems. The collaboration capabilities are then enhanced, strengthening a key aspect for successfully conducting life-critical operations.
- **Affordable flexibility and evolution**: LTE is based on commercial off-the-shelf systems, which means it offers significant economies of scale in the global marketplace by leveraging the broad ecosystem nurtured by commercial deployments worldwide. This translates to lower costs for the equipment, along with unprecedented flexibility for easily deploying new IP-based application and sensors. Additionally, LTE provides the capability for network sharing with other agencies and strategic sectors such as utilities and transportation, which can further optimize the cost of deployment.

When evolving to mobile broadband, a public safety agency may choose from numerous business models that will support its specific needs, taking into account existing PMR network operations, available spectrum, regulatory environment and financial resources. It may contract services provided by a mobile network operator (MNO), operate or use a service from a dedicated virtual network over a mobile operator's infrastructure (G-MVNO), build a wholly owned and operated dedicated network, or use a mix of different approaches.

One size doesn't fit all. Adding LTE mobile broadband capabilities to existing PMR networks in a nondisruptive and cost-effective way can be complex, with many factors to consider. Fortunately, proven roadmaps exist for a smooth migration that leverages existing infrastructure and investments.

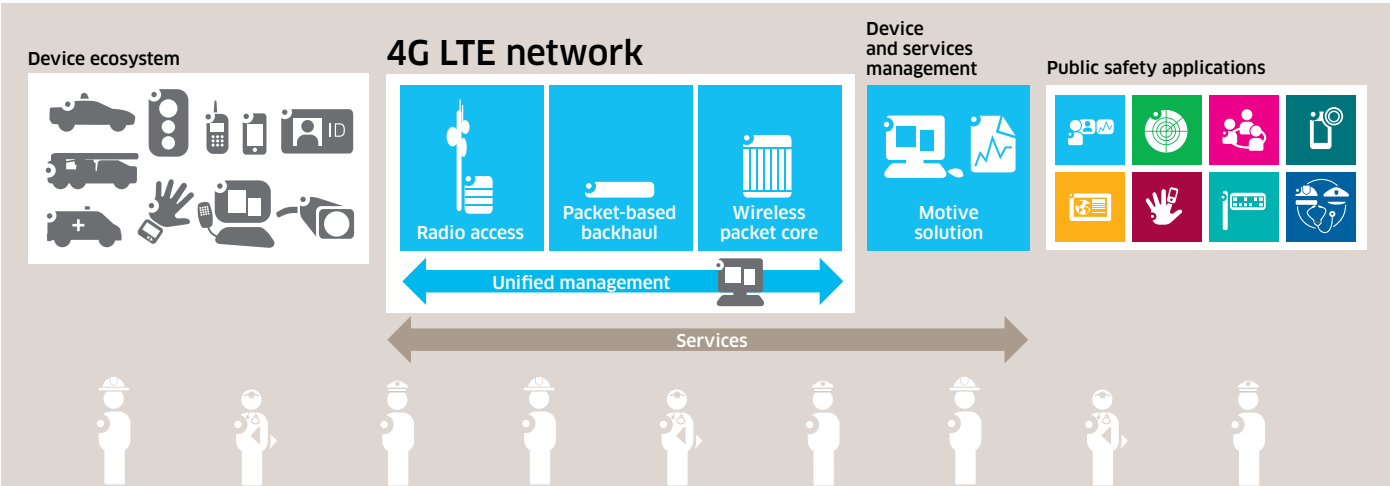
LTE: THE NEW STANDARD FOR BROADBAND PMR

LTE is the global standard for the fourth generation (4G) of mobile multimedia broadband communications (data, video and voice). Defined by the global 3GPP organization, it has been massively deployed worldwide by many commercial operators and is available now to the public safety community.

LTE offers interoperability, scalability and high reliability for broadband PMR networks. It also provides low latency (<10 ms) and high data throughput (up to several hundred Mb/s, depending upon available spectrum, radio conditions and network load). As such, it provides a highly efficient and effective platform for advanced multimedia services, innumerable mission-critical applications and a broad range of devices. Its advanced processing and spectral efficiency provide optimal support for day-to-day operations as well as large-scale events and emergencies.

Major mission-critical users and industry associations, such as APCO and the TETRA and Critical Communications Association (TCCA), have defined LTE as the successor technology for legacy PMR systems. As a consequence, beginning with 3GPP Release 12, LTE standards are being upgraded to make it a mission-critical-grade system. This capability is reflected in estimated worldwide spending on private public safety LTE eNodeB deployments, which is projected to expand from $256 million in 2013 to $1,711 billion in 2018, according to the "Critical Communications Broadband – World – 2014" report from IHS Technology.

Figure 1. Mobile Broadband Network Architecture



However, PMR operators wishing to migrate to LTE may need to address some challenges. The maturity level of legacy PMR systems varies from country to country, and some regions may not have the available spectrum for deploying a dedicated LTE network. Additionally, LTE technology is still a few years away from attaining the full set of mission-critical features that would enable a 100 percent migration of all PMR communications. Public safety organizations therefore must balance the necessary investment to maintain their current level of operations with preparation for the enhanced benefits of LTE. The different business models proposed by this white paper provide guidelines to support these decisions.

LTE spectrum for public safety

Commercial LTE is available in a wide spectrum, ranging today from 450 MHz to 3.5 GHz, and can accommodate different channel bandwidths (from 1.4 MHz to 20 MHz) and duplex modes (FDD and TDD). The spectrum considered for dedicated broadband public safety networks is usually below 1 GHz (400 MHz, 700 MHz band 14 or 700 MHz band 28), and the bandwidth is usually 5 + 5 MHz or 10 + 10 MHz. Aware of the strategic advantages, several countries are already allocating spectrum specifically for public safety LTE (for example, the United States, Canada, South Korea, Spain, the Middle East, Brazil, Chile, Australia and China). In Europe, major decisions are expected from the ITU World Radiocommunication Conference to be held in November 2015. The United States has allocated 10 + 10 MHz of spectrum to broadband public safety at 700 MHz. This allocation provides an unprecedented opportunity for mission-critical communications to become interoperable across the country – a main driver behind its national FirstNet interoperable broadband initiative.

Secure, mission-critical architecture

LTE-based solutions use an all-IP architecture that, combined with geographic redundancy, reduces potential points of failure and provides the high availability required by public safety users. LTE technology is perfectly suited for efficiently handling any mix of applications. It boasts guaranteed and differentiated end-to-end Quality of Service (QoS) and priority/preemption mechanisms to ensure that the most critical applications and users always get serviced. LTE systems also offer extensive self-optimizing network capabilities for simplified network operations, maintenance and self-healing. These capabilities make it easier to rearrange networks when needed, such as when adding deployable units for disaster scenarios.

LTE network management can be integrated easily with an existing PMR network umbrella management system to provide a comprehensive single view for managing all network resources and enabling full control of end-to-end availability.

LTE continues to evolve

LTE Release 10, approved in 2011, and subsequent specifications planned for the long term, have been designated as LTE Advanced, or LTE-A. These enhancements are already producing major benefits, including the potential for ultra-wide bandwidth – up to 100 MHz of spectrum, if available – with ultra-high data rates and greater capacity to support more sophisticated applications.

LTE-A includes additional advanced multiple input multiple output (MIMO) capabilities, enhanced support for heterogeneous networks and machine-type communications. More importantly, starting from 3GPP Release 12, LTE integrates public safety features mimicking the most demanding mission-critical capabilities of existing PMR systems. These include support of efficient group communications, including Push to Talk (PTT), direct communications between terminals and fallback mode for the base stations.

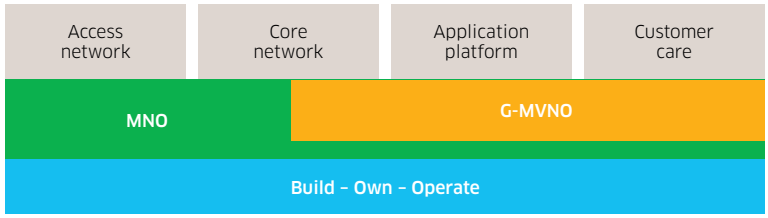
The essential set of mission-critical communication functionality previously developed for TETRA and other PMR technologies is projected to be available in LTE standards early in 2016 (3GPP Release 13). A fully developed ecosystem of standards-compliant devices and infrastructure is therefore not expected to develop much before 2018. Nevertheless, existing LTE standards and solutions already meet first-responder requirements for augmenting and complementing legacy PMR systems with broadband data-based capabilities. First responders can therefore enjoy the additional capabilities delivered by LTE now.

BUSINESS MODELS FOR MOBILE BROADBAND LTE

Public safety agencies migrating to LTE broadband networks must consider many factors. These include startup costs, operating and capital expenditures (OPEX and CAPEX), expected revenues, available spectrum, existing network equipment, commercial wireless services and the political environment. Several emerging business models match the tradeoff between objectives (short-, mid- and long-term) and constraints. The following are five possible business models:

- **MNO**: Contract services through an existing mobile network operator
- **G-MVNO**: Operate or use services through a government mobile virtual network operator
- **PPP**: Deploy dedicated network services through a public-private partnership project
- **Private**: Build, own and operate a dedicated network for dedicated services
- **Hybrid**: Combine a G-MVNO with a private network

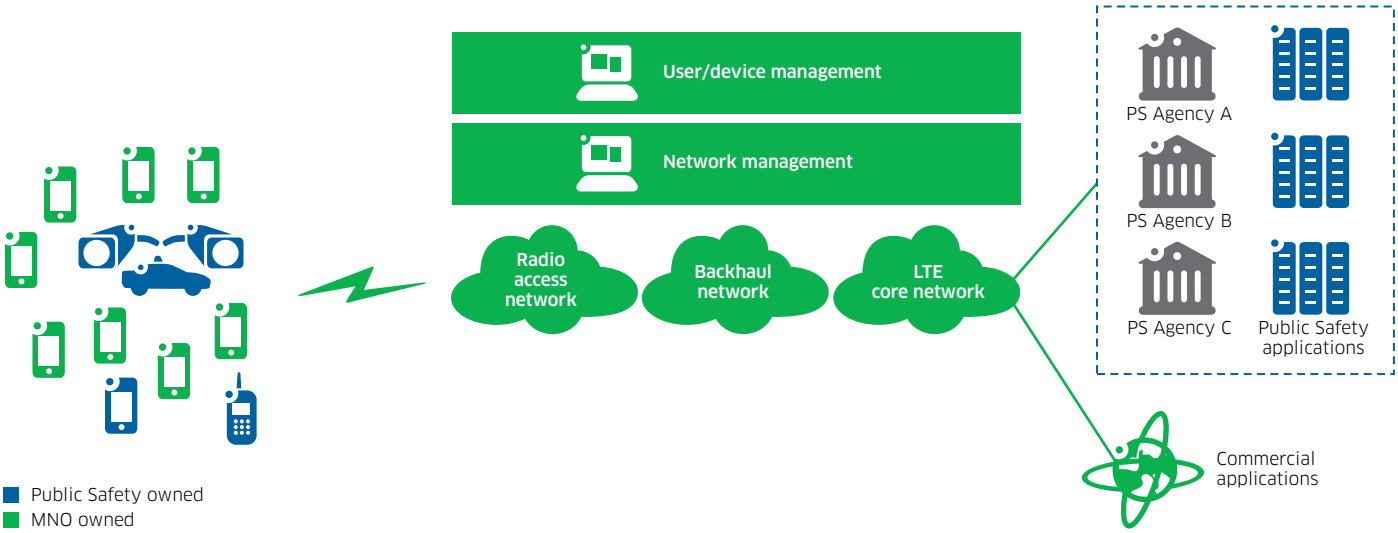
Figure 2. Responsibility of mobile network operators



Contract services through an existing Mobile Network Operator

In this model, the public safety agency simply contracts data subscriptions with an MNO to provide mobile broadband services. Public safety users and consumers share the same spectrum and network. The public safety entity pays a consistent, predictable periodic fee for network access, usually a function of some known factor, such as the number of end users, devices or usage. Note that public safety traffic profiles differ greatly from those for commercial users. Services such as mobile video protection may consume large volumes of uplink data. For example, a daily uplink transmission of two hours of an HD video stream will consume more than 50 gigabits monthly.

Figure 3. Contract services through an existing Mobile Network Operator



Advantages

This arrangement is relatively inexpensive if traffic, the number of users and subscription fees can be low, and fast if MNO LTE service already is available, and if standard and/or rugged devices within an assigned commercial spectrum can be used. CAPEX concerns only applications and terminals, which could remain significant if a large number is required. OPEX consists mainly of monthly fees for using the MNO service, and is proportional to the number of users and usage volume.

This model eliminates the need to plan and allocate funding for network upgrades, maintenance contracts and training for network operations. These expenses are all handled by the MNO, which is responsible for keeping the platform current, resolving all technical issues and ensuring the appropriate level of service. An MNO network can become available almost immediately, usually with good population coverage, helping the public service agency to quickly meet the capacity demands of increased data traffic.

Challenges

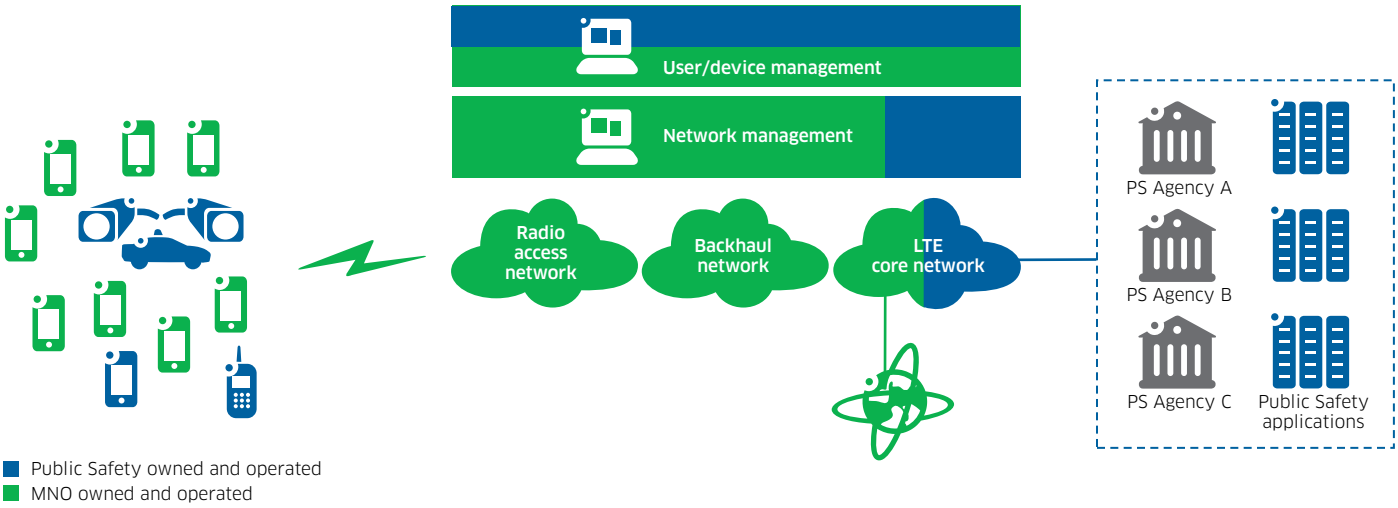
Challenges for the MNO model include no control over four critical requirements: coverage (usually very poor in sparsely populated areas), availability, prioritization and resilience. Typically, little or no support exists for mission-critical features, and gaps in coverage can occur where the population density is low, such as in rural and isolated areas. For mission-critical needs, these issues might be addressed through stringent service level agreements (SLAs) to assure such features as priority access or network redundancy in case of an outage, which may significantly increase the subscription fee. Also, most MNOs have a monthly data cap and additional fees for excess usage, which can significantly impact OPEX.

Operate or obtain service from a Government Mobile Virtual Network Operator

The MVNO approach has become prevalent in the commercial sector, where branded operators resell bulk-purchased wireless services to consumers while providing their own usage plans, billing and customer support. The MVNO approach can be extended to the support of public safety users. In that case, the MVNO, called a G-MVNO (Government MVNO) provides added-value services (such as user and device management, customer care, end-to-end security, billing and so on) to the public safety users that in turn get access to secure broadband data services when the G-MVNO leverages the 4G access network from the MNO.

Different G-MVNO business models may apply. G-MVNO services can be operated by the public safety entity itself or by a public or private organization. Additionally, different technical G-MVNO implementations may be considered from light to full G-MVNO, which provides the highest level of control on end-to-end services, and consequently is recommended. Figure 4 depicts a full G-MVNO model operated by a public safety organization itself.

Figure 4. G-MVNO



Advantages

The G-MVNO model offers more control over services and security than the MNO approach, providing a ready-made network for basic public safety needs. It keeps CAPEX moderate (mainly terminals and a few LTE core network nodes). A G-MVNO can manage services and management over a mix of 4G, 3G and PMR platforms for the best possible availability in routine situations and major crisis. It can be configured to combine security, availability, ease of use and economics tailored for public safety, while keeping the effective management of end-to-end data service a first priority. Key benefits include:

- **Security**: End-to-end service control and encryption, multi-network coverage and availability across multiple operators. Diverse radio technology support to integrate legacy systems with LTE.
- **A cost-effective solution**: Scalability, with the capability to serve thousands to hundreds of thousands of public safety professionals on a network designed for millions of commercial users.
- **An evolutionary roadmap toward dedicated broadband needs**: Existing investments in older radio technologies and broadband systems (core network and terminals) can be fully leveraged.

Challenges

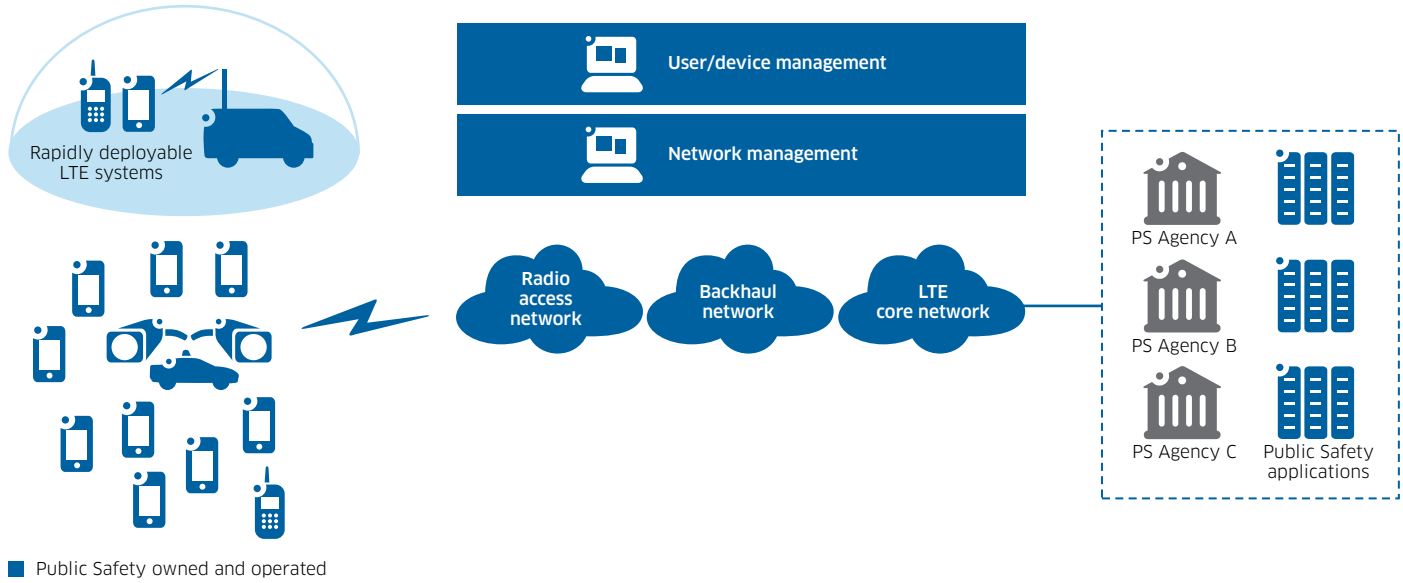
As with the MNO model, a G-MVNO provides no absolute control over coverage (especially in rural areas), availability and assured resilience. Depending on the MNO, it may offer limited support of some critical public safety features, such as direct mode or group calling. Because it may offer less flexibility for mission priorities, an SLA should be negotiated with the host operator(s) to include a definition of scope, services, performance measurement, problem management, customer duties, warranties, disaster recovery and termination. The SLA should also guarantee such services as priority access and network redundancy in case of outages. These guarantees may significantly impact the bulk fees for using the MNO network.

Deploy dedicated network services through a Public-Private Partnership Project

The PPP business model features a dedicated and standalone LTE network, which is deployed, operated and maintained by an MNO and/or another independent operator. This type of network is typically owned by a telecom operator, which provides the service to the public safety agencies while usually assuming the financial, technical and operational risk of the service offer. As with the other MNO and G-MVNO models, the public safety organizations are responsible for purchasing the applications and the terminals that will operate over the dedicated network.

The infrastructure can be complemented by rapidly deployable LTE systems to produce the extra capacity or coverage required to cope with major planned or unplanned events.

Figure 5. Owned dedicated private network or PPP



Advantages

One of the key benefits of the PPP model is that the public safety agency is the only entity using the network. CAPEX and OPEX can be reduced through synergies in the reuse of antenna sites, backhaul and technical skills contributed by the private partner. Public safety communications requirements are assured and customized, with full control over such critical specifications as latency, coverage and resilience.

Organizational advantages stem from the fact that the public safety agency can concentrate on its mission, with the network operator role (including network operations and upgrades) handled by the PPP operator. Additionally, excess capacity and infrastructure elements can be sold to commercial users and/or shared with other critical infrastructure operators such as utilities and transportation.

Challenges

This model requires having access to a dedicated broadband public safety spectrum and negotiating with a partner to invest the upfront CAPEX to build the network. However, many synergies can exist to minimize this upfront investment as mentioned previously.

Build, own and operate a Dedicated Private Network

In this model the public safety agency finances, procures, builds and manages its own network, setting technical requirements for capacity, security, reliability, redundancy and robustness. It takes full responsibility for all network elements and software, and employs in-house personnel to build, manage, operate and maintain the network. The extent of upfront costs depends on the scale of deployment (local, regional or national), whether the network is shared among several entities and/or whether the deployment is scheduled gradually over years or within a shorter time period. In an alternative scenario, network operations can be outsourced to a specialized company (managed services).

Advantages

The clear advantage with a dedicated LTE network is that it can be designed to match all mission-critical requirements, with the agency having full control over the procurement process. Specifications (such as site hardening, extended coverage and resilience to multiple faults and extreme events) can be tailored to missions, as well as to the agency's future evolution strategy. As with the PPP model, a dedicated network can offset CAPEX and OPEX by operating as a wholesaler where regulations permit, or sharing with other critical users of the public sector such as defense, utilities and transportation agencies.

The infrastructure can be complemented by rapidly deployable LTE systems to provide the extra capacity or coverage required to cope with major planned or unplanned events.

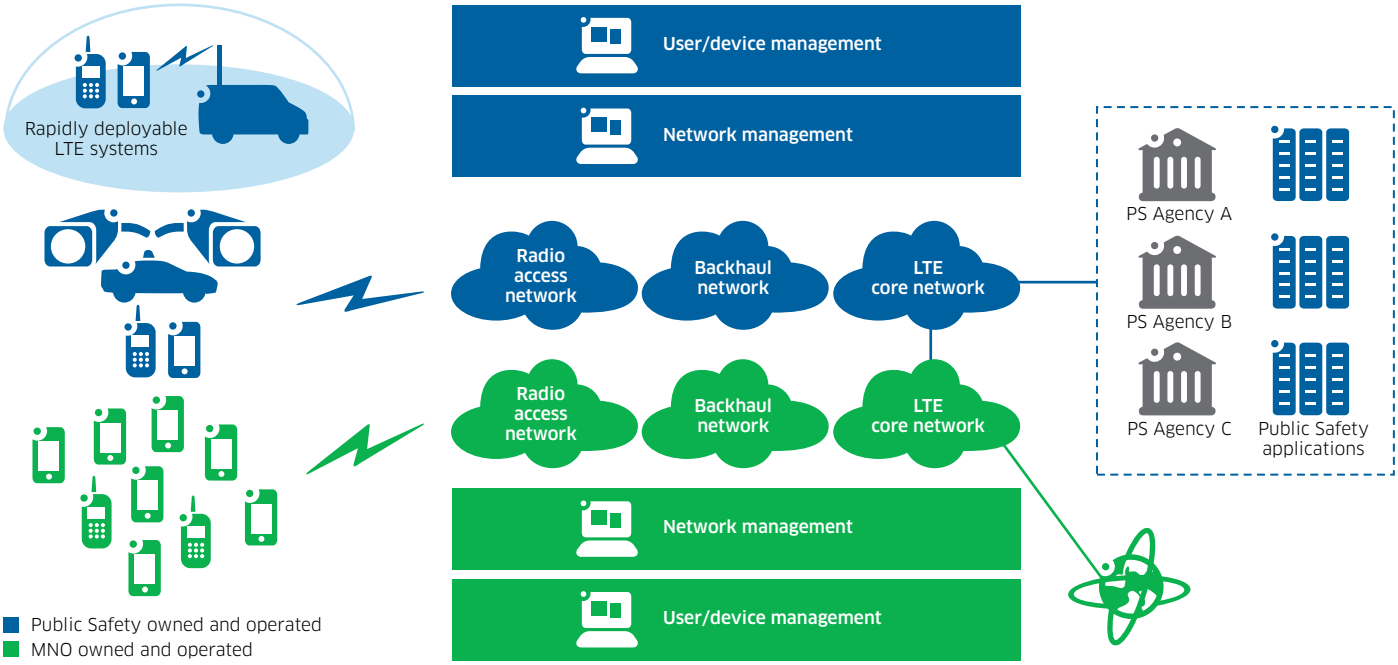
Challenges

Specifying, building and maintaining a dedicated network requires significant upfront investments and technically skilled professionals for network operations. Acquiring dedicated LTE spectrum may require an initial investment or an annual fee. Dedicated spectrum must be cleared of any previous service – usually a slow process in countries where no dedicated spectrum currently exists. Terminals for dedicated spectrum may also be slightly more expensive than those for commercial users (depending on the band). Both CAPEX and OPEX typically could be higher in this model. However, CAPEX depends significantly on the spectrum of operations (the lower the spectrum, the lower the number of sites to deploy) and can be planned over multiple years to deploy in critical areas first.

Combine a G-MVNO with a private network (Hybrid Model)

Given that spectrum is a scarce resource in many regions, some agencies may elect to build a custom communications network dedicated exclusively to mission-critical services, while conducting less critical back-office operations through commercial operators using the G-MVNO model. This approach can be implemented relatively easily, since LTE is both a technology for commercial carriers as well as the new-generation platform for PMR. In time, when desired dedicated spectrum becomes available, an agency will then be well positioned to transition to a fully owned and operated network.

Figure 6. Hybrid



Advantages

This model has the advantage of rapid deployment without having to wait for dedicated broadband spectrum to become available. It enables an agency to handle very high volumes of everyday data traffic while preserving a fully controlled, mission-critical core for emergency situations. It is flexible and positions the agency for future evolution to a fully dedicated network. It allows agencies to make investment efficient by combining a mix of commercial and dedicated spectrum terminals. Also, when both options are available, the MNO network can be used to offload traffic from the private network that is not mission-critical, preserving key resources for mission-critical traffic and applications.

Challenges

Following this strategy means less than full control over the entire network and its coverage area, and may require mobile transmitters or antennas on some occasions. Developing a hybrid approach also introduces slightly greater complexity to design, operations and financial models, requiring critical consideration and coordination of these elements. Assuring optimal outcomes requires a carefully negotiated SLA and spectrum coordination with MNO partners.

ASKING THE RIGHT QUESTIONS FOR LTE NETWORK DEPLOYMENT

Public safety agencies embarking on an LTE deployment project must consider factors such as budget, regulatory issues, internal resource constraints, coverage and reliability targets, available spectrum (frequency band and bandwidth) and number of end users when choosing the best overall design and business model (See the accompanying table.) Agencies should also have a plan for doctrine change management, because the wealth of robust data will offer new ways of conducting operations. Regardless of the model chosen, the network must be defined through an end-to-end service-centric approach. This approach enables operational support to be maintained from the core through the network to the end user.

Figure 7. Merits of the different models

	CAPEX	OPEX	Timing	Coverage	Capacity	High availability	Control	PS features	Security
Hybrid	Depends on spectrum								
Private	Depends on spectrum								
PPP									
G-MVNO	High number of users	High number of users	Populated areas	Populated areas	Populated areas	Populated areas			
	Low number of users	Low number of users	Rural areas	Rural areas	Rural areas	Rural areas			
MNO	High number of users	High number of users	Populated areas	Populated areas	Populated areas	Populated areas			
	Low number of users	Low number of users	Rural areas	Rural areas	Rural areas	Rural areas			

A full-cycle analysis by a trusted partner can provide deep and actionable insight into which model and variation is the best choice, both financially and operationally, for each public safety entity. A consulting service is key to defining the dashboard and ensuring success.

Ideally, this partner should offer highly qualified personnel, fully defined support processes and solutions expertise. The partner should also do the following:

- Assist agencies in testing and ensuring that the new LTE system meets the requirements of its public safety users
- Make sure that all devices, applications and individual components within the system are working properly
- Internally test the end-to-end LTE solution and provide expertise and experience during design and implementation stages

The result should be an operational model that fully meets the needs of the public safety organizations being served.

MOBILE BROADBAND FOR IMPROVED PUBLIC SAFETY

Public safety agencies charged with protecting lives and property cannot compromise on emergency response capabilities and the latest intelligent communications technologies to support them. Fortunately, public safety agencies can now tightly integrate LTE mobile broadband technology with existing LMR/PMR networks, providing a scalable, secure and cost-effective way to add mobile streaming video, high-speed Internet access, multi-media messaging and VPN to home agency applications and incident command systems, all under a unified infrastructure that can be securely shared by cooperating agencies.

Alcatel-Lucent has provided mission-critical network-based solutions to the public safety industry for more than 20 years, with extensive experience in deploying LTE networks for a wide range of applications, from small or private infrastructures to the largest and densest LTE networks existing today. Operations and maintenance services extend value further, providing a full range of support, including site acquisition, preparation, installation and commissioning.

Alcatel-Lucent Bell Labs can support planning activities and make recommendations for any public safety broadband network, providing such services as assessing the viability and capacity of backhaul/backbone facilities, traffic modeling, studying multiple radio frequency coverage scenarios, assessing the reliability of particular architectures based on potential site locations, total cost of ownership analyses and business modeling. As a market leader in LTE, Alcatel-Lucent offers a comprehensive wireless broadband solution for public safety that is designed for interoperability, scalability and high reliability, and supports public safety agencies in every step of their communications transformation.

ACRONYMS

3G	The third generation of mobile telecommunications technology, based on a set of standards used for mobile devices and infrastructure
3GPP	3rd Generation Partnership Project made up of several international telecommunications standard development organizations
4G	The fourth generation of mobile telecommunications technology, based on a set of standards used for mobile devices and infrastructure
CAPEX	Capital expenditures
EPC	Evolved Packet Core, the core network architecture of the LTE communication standard
FDD	Frequency Division Duplexing
GCF	Global Certification Forum.
GSM	Global System for Mobile Communications, a 2G standard developed by the European Telecommunications Standards Institute (ETSI).
IP-MPLS	Internet Protocol-Multiprotocol Label Switching, a scheme that directs packet-based data from one network node to the next based on short path labels.
IMSI	International Mobile Subscriber Identity, a unique number that describes a network operator and subscriber.MIMOMultiple-input and multiple-output, referring to the use of multiple antennas at both the transmitter and receiver to improve communication performance
LMR	Land Mobile Radio
LTE	Long Term Evolution, a standard for high-speed mobile data and voice services

LTE-A	LTE Advanced
MIMO	Mulitple-input and multiple-output, referring to use of multiple antennas at both the transmitter and receiver to improve communication performance.
MNO	Mobile Network Operator
MVNO/G-MVNO	Mobile Virtual Network Operator or Government Mobile Virtual Network Operator
OPEX	Operating expenditures
PMR	Private Mobile Radio
PPP	Public-Private Partnership
Project 25/P25	A suite of standards for public safety digital radio communications mainly used in North America
QoS	Quality of Service
SLA	Service Level Agreement
TCCA	TETRA and Critical Communications Association
TDD	Time Division Duplexing
TETRA	Terrestrial Trunked Radio, a suite of standards for mission-critical digital radio communications
TETRAPOL	A standard for public safety digital radio communications used throughout the world
VPN	Virtual Private Network

CONTACTS

Jerôme Brouet
Public Safety Solution Director
Alcatel-Lucent
Email: jerome.brouet@alcatel-lucent.com

Alcatel·Lucent