Alcatel·Lucent

STRATEGIC WHITE PAPER

# Long Term Evolution (LTE) for Public Safety

## Enabling Flexible Business Models

To provide seamless data communication during emergencies, public safety practitioners endorse 4G Long Term Evolution (LTE) technology as the foundation for new wireless networks. LTE offers nationwide interoperability in the 700 MHz band, and it can support key broadband applications that accelerate response times, improve situational awareness — and increase the safety of the public and all personnel. However, LTE requires a move to all-IP networks and presents some operational challenges, including the need to minimize costs in today's difficult economic environment. This paper explains operational business models that public safety entities can use to manage LTE networks more efficiently and cost effectively. For organizations considering outsourcing, it explores key factors, such as funding requirements, operational costs, tolerance for shared control, and solution expertise.

## Table of contents

# 1. Introduction

Public safety entities rely heavily on telecommunications networks to ensure the success of mission-critical operations. In North America, digital and analog Land Mobile Radio (LMR) networks are used for mission-critical voice communications. These networks are often shared across agencies, combining multiple disparate radio networks that are interconnected by a transport network. The networks are difficult to manage and operate, because they often link to a complex infrastructure based on diverse technologies, vendors and domains. For most public safety emergency service personnel, telecommunications is not their core mission — which adds to the challenge of operating and managing these networks.

Furthermore, LMR is a narrowband technology, which is good for voice and low bandwidth data services. But it simply cannot handle the advanced data applications that frontline officers and first responders require. Wireless broadband is essential for delivering these applications, which may include video surveillance, automated vehicle license plate recognition, biometric identification, mobile crime scene units, mobile incident command, geospatial information systems, medical telemetry and automated vehicle location.

To implement these broadband capabilities, public safety organizations in North America are considering 4G LTE networks deployed as an overlay to existing LMR networks. This approach will support broadband data in the short term, and in the longer term, the networks can evolve to support mission-critical voice.

Because LTE is proposed for commercial 700 MHz spectrum deployments in North America, its adoption for public safety deployments presents an unprecedented opportunity for mission-critical communications to become interoperable across the United States. Public safety users and first responders will have access to critical communications services wherever they go, while leveraging common user equipment.

To implement an LTE public safety network without disrupting existing day-to-day operations, public safety agencies must consider a number of key issues, including multivendor interoperability, network reliability, scalability and interworking with existing LMR systems. A successful transformation involves the following considerations:

- Optimizing the total cost of ownership (TCO) of the LTE network
- Selecting the correct technological solution
- Minimizing implementation and technical risk
- Securing migration from present mode of operation (PMO) to future mode of operation (FMO)
- Setting up network operations efficiently to reduce OPEX

The following section describes operational business models that address these considerations.

### Deployment options

The following three deployment options each have positive and negative factors. For all options, it is important to understand the requirements, resources and risks.

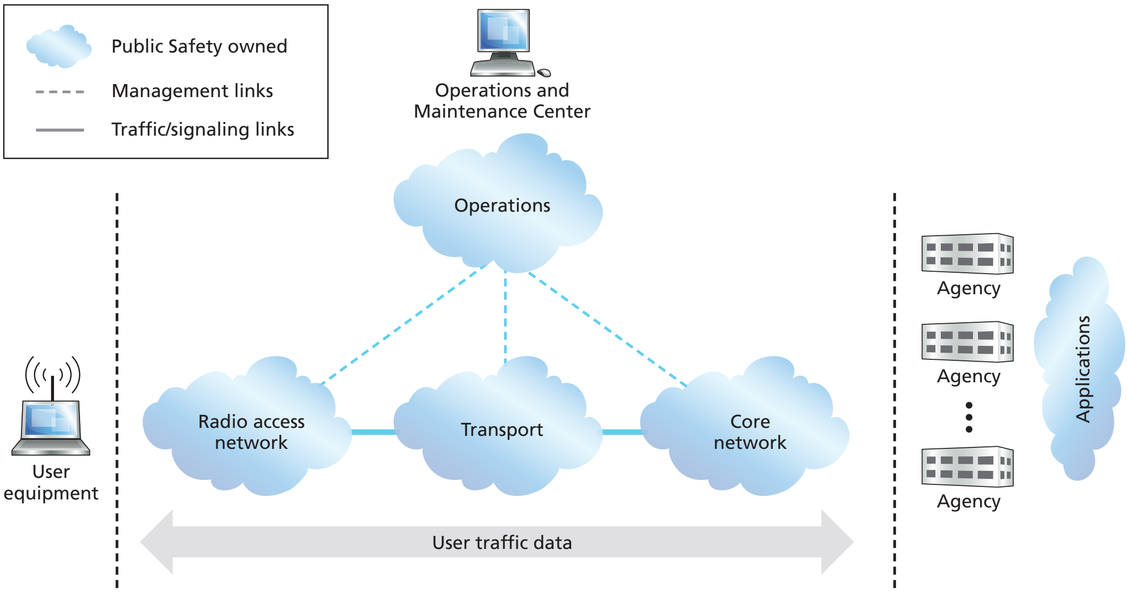
- *CAPEX model* – All equipment and software is purchased, and ongoing support is provided through in-house personnel.
- *Managed model* – All equipment and software is purchased, but the ongoing support is either wholly provided by another party, or the support is shared by another party and in-house personnel.
- *Hosted model* – Network access is provided by another party and leased to a public safety entity for a monthly fee.

In addition, a public safety provider could lease spectrum to a commercial provider, but this option will not be addressed in this paper. It has multiple criteria to evaluate — and is contingent on the Federal Communications Commission's (FCC) pending decision regarding the additional 2x5 MHz spectrum band, known as the D block, which is adjacent to the Public Safety Broadband spectrum.

### 2.1 CAPEX model

In the CAPEX model, the overall network is owned and managed by one or more public safety entities, as shown in Figure 1. These entities take full responsibility for purchasing all network elements and software, and they employ in-house personnel to build, manage, operate and maintain the network. Individual agencies may be able to remotely monitor network health.

**Figure 1. CAPEX model architecture**



Mission-critical networks are built with complete geographic redundancy to eliminate any single point of failure. This approach increases costs for core network equipment, beyond what is usually required for commercial networks. Initial upfront costs can be offset — and ongoing OPEX costs can be reduced — through government grants and incentives, along with any reallocated monthly per-subscriber fees (which may currently be paid to commercial broadband wireless service providers).

The extent of upfront costs depends on: the scale of deployment (local or regional), whether the core network is shared among multiple areas or entities and how deployment is scheduled (gradually over years or within a shorter time period). With the CAPEX model, the public safety entity must also employ skilled personnel for network design, operations, maintenance, security and technical support, as well as program and project management. For a small deployment, these expenditures might not be economically viable.

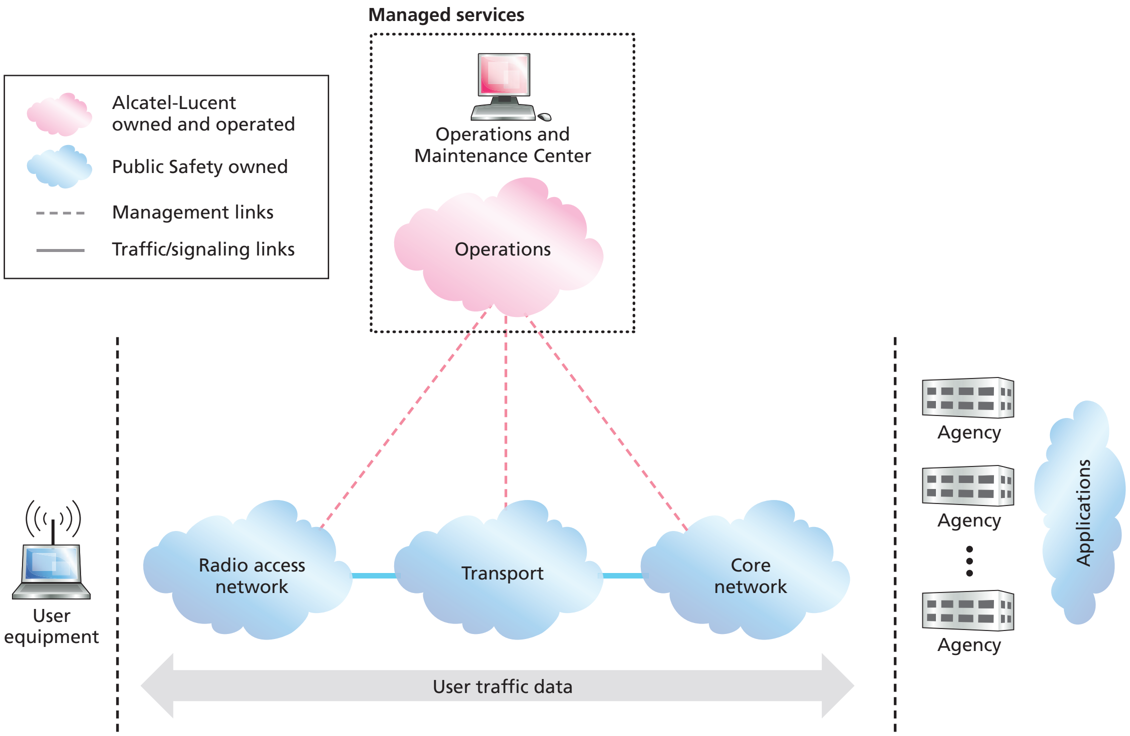
The public safety entity has full control over the network. A dedicated network in the 700 MHz band provides operational benefits, along with potential savings on margins imposed by service providers. With the proper know-how in place, a self-managed network can also offer an "a-la-carte" selection of applications and services customized to user needs in the target area, which could be local, county or another public sector. On the other hand, smaller networks would not benefit from the economies of scale a commercial operator might be able to realize. For example, commercial operators could gain efficiencies by leveraging their existing commercial resources to manage — and possibly build — the public safety network.

The CAPEX model can be a good option for public safety entities that deploy their own network as long as they have "critical size." Critical size is determined by comparing the total allocated costs with the cost of an equivalent outsourced or managed service.

## 2.2 Managed model

The managed model is a hybrid, combining elements of the CAPEX and hosted models. With the managed model, the public safety entity is responsible for ensuring that network elements are appropriately owned and deployed. But it contracts with another party to manage and/or operate the network, as illustrated in Figure 2. Leased lines connect the network to the Operations, Administration and Maintenance (OA&M) center. Individual agencies may be able to remotely monitor the health of the network.

Figure 2. Managed model architecture



Similar to the CAPEX model, this model requires each public safety entity to purchase all the equipment and software and contract for the required deployment services. Depending on the network architecture, these costs can vary significantly. Though in this model, cost savings are possible by contracting management functions with another party. For the highest Quality of Service (QoS), management services should go beyond traditional network monitoring and provide a performance management platform that proactively monitors for predetermined thresholds, along with preventive maintenance to ensure all network elements are running at peak efficiency. In doing so, the network is managed proactively to maintain network availability while ensuring a high degree of service uptime.

The managed model offers flexibility in terms of the management functions contracted. For example, a public safety entity could have another party provide end-to-end operational support, using a service-centric approach. This approach provides operational support from the core through the network to the end user. Contracting one party to provide full operational support eliminates finger pointing and the need to address multivendor management requirements.

The managed model provides a degree of control to each public safety entity. Network elements are deployed at a site chosen (and often owned) by the public safety entity. Owning the assets allows each public safety entity to decide when to upgrade the network and implement its own security platform. By contracting with another party to provide management services, the public safety entity will have a predictable monthly fee with lower IT and administrative headcount. It will also require less investment in network management tools and training.

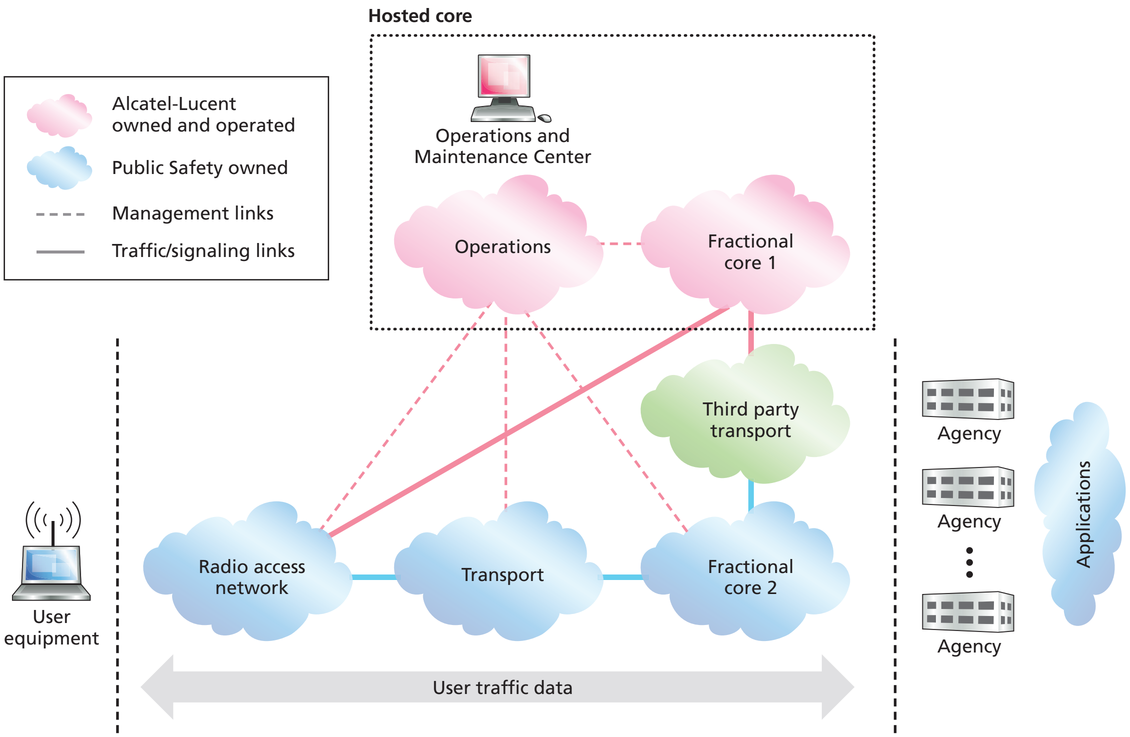
## 2.3 Hosted model

The hosted model allows each public safety entity to use network assets that are owned and managed by another party. These assets are usually shared among several similar types of customers with similar needs, creating economies of scale for both capital and operational expenses. While core infrastructure is shared, Radio Access Networks (RANs) are usually owned — and may be unique to — each individual public safety entity. The shared core provides the benefits of the platform while reducing startup costs and ongoing operations costs.

With a hosted model, the public safety entity pays a consistent, predictable periodic fee for network access. The fee is usually a function of some known factor, such as the number of end users, devices or usage. This model also eliminates the need to plan and allocate funding for network upgrades, maintenance contracts and ongoing training for operations. These expenses are all handled by the hosting provider, who is responsible for keeping the platform current, resolving all technical issues and ensuring the appropriate level of service.

Figure 3 shows a hosted model architecture, where a non-public safety entity, such as Alcatel-Lucent, is the host — thereby owning a portion of the core and handling OA&M activities. The hosted core (fractional core 1) may include all functions related to mobility control, bearer management, gateway selection and authentication, messaging center, device management center, subscriber databases and Quality of Service control. The public safety portion of the core (fractional core 2) consists primarily of gateways to provide external connectivity and IP addressing. Both fractional cores could be physically separate. This approach accommodates large implementations and can eventually serve multiple jurisdictions. Transport is split between public safety-owned backhaul — for example, within a given jurisdiction — and a third-party transport cloud that carries traffic (mainly signaling) toward the hosted core. Individual agencies may be able to remotely monitor the health of the network.

Figure 3. Hosted model architecture

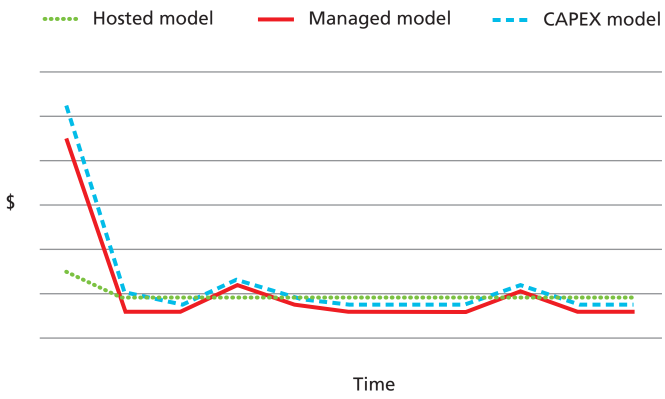


## 2.4 Which model to choose?

Regardless of which model is chosen, it is important for each public safety entity to ensure the network is managed using an end to end service-centric approach. Moving beyond the traditional network management approach of ensuring connections are up and traffic flows properly to one where end-to-end QoS and quality of experience (QoE) is upheld. Delivering advanced applications and services anytime, where needed, requires a shift from traditional network-centric monitoring and management to services-centric management. This end to end service centric approach provides for proactive detection, diagnosis and resolution of services-related problems before it impacts the end user.[1]

Figure 4 shows the cost profiles for the three deployment options. Startup costs are greatest for the CAPEX model, because it requires equipment purchases, software licensing, employees and training, management tools, facilities and circuits. The managed model also requires initial capital purchases, but headcount and training needs are lower. Startup costs for the hosted model are substantially lower.

Figure 4. Deployment options cost profile



[1] Services Quality Management Beyond the Network, Improving competitiveness with Services-Centric Managed End-to-end Service Operations for a Managed Quality of Experience – Jack L. Zatz, Director Carrier Network Operations Managed Services Offer Management, Managed Services Division, Alcatel-Lucent, December, 2009.

Over time, the CAPEX and managed models may have a periodic lower cost, but they will see spikes as upgrades and training are incurred, and as the platforms are kept up to date. After initial startup, the hosted model will provide a consistent, known cost. All network upgrades and training are absorbed by the hosting provider.

To determine which model provides the best financial view, a full lifecycle analysis needs to be completed. For the CAPEX and managed models, a number of assumptions would be required, while the hosted model has known costs for comparison.

Aside from costs, each model has its own pluses and minuses, based on each public safety entity's individual needs, resources and capabilities.

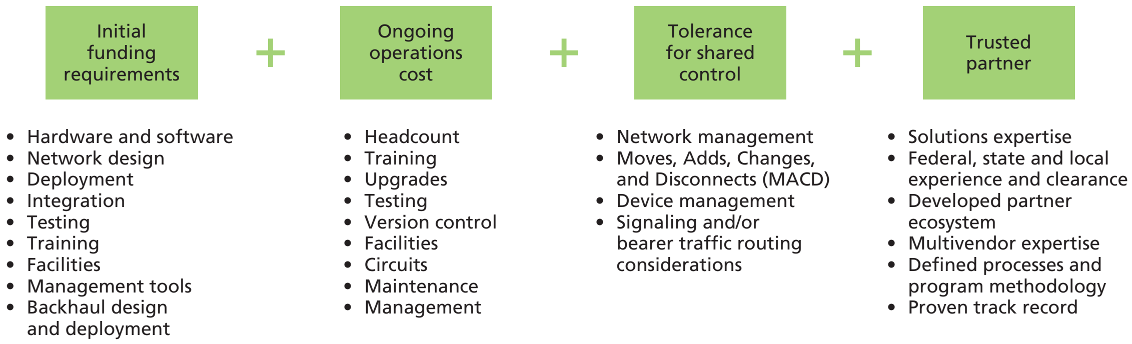
- The CAPEX model provides the greatest level of internal control but also requires the highest funding and skilled headcount.
- The managed model helps to level out ongoing operational costs but still requires a significant initial capital outlay.
- The hosted model provides the most predictability — helping each public safety entity manage and control costs, while offering a platform that will stay more up to date than a locally deployed infrastructure. However, it does require public safety entities to be comfortable with a greater amount of third-party control.

With both the managed and hosted models, degrees of control can be shared between the public safety entities and the service provider. While complete control and operations can be contracted, public safety entities can also maintain a level of management they are comfortable with and have the resources to support. This shared control could be as simple as setting up alarm conditions that both parties can see. Or it could be more operational, allowing public safety entities to manage end-user devices for adds, changes and deletes.

With a managed or hosted service, public safety entities do not have to give up total control. Mechanisms and processes can be implemented to address any concerns regarding security or control.

The choice of model can only be made after considering the benefits and considerations of each option. But they all require a trusted partner with highly qualified personnel, fully defined support processes, experience in the types of services required and a well defined security posture. Figure 5 details the aspects to consider. The end result must meet the needs of the departments, municipalities and residences being served.

**Figure 5. Business model considerations**



- Hardware and software
- Network design
- Deployment
- Integration
- Testing
- Training
- Facilities
- Management tools
- Backhaul design and deployment

- Headcount
- Training
- Upgrades
- Testing
- Version control
- Facilities
- Circuits
- Maintenance
- Management

- Network management
- Moves, Adds, Changes, and Disconnects (MACD)
- Device management
- Signaling and/or bearer traffic routing considerations

- Solutions expertise
- Federal, state and local experience and clearance
- Developed partner ecosystem
- Multivendor expertise
- Defined processes and program methodology
- Proven track record

# 3. Conclusion

To implement broadband capabilities, public safety organizations in North America are evaluating 4G LTE networks. LTE offers improved communications and breakthrough service capabilities, along with national interoperability through the use of a common technology for 700 MHz. LTE brings fundamental changes to how public safety networks are owned and operated. A variety of operational business models are available, and the ultimate choice depends on how well the model suits the public safety entity's needs, resources and capabilities.

Regardless of the model chosen, the network must be managed using an end-to-end service-centric approach. This allows operational support to be maintained from the core through the network to the end user — and includes capabilities such as proactive setup and monitoring of services. As a result, advanced applications can be delivered with the highest possible Quality of Experience.

A full cycle analysis can provide insight into which model is best financially for the public safety entity. Ideally, this analysis will be conducted by a trusted partner with highly qualified personnel, fully defined support processes, a well developed partner eco-system and solutions expertise. The end result should be a solution and operational model focused on meeting the needs of the jurisdictions being served.

Alcatel·Lucent