Broadband Revolution: Roadmap for Safety and Security Mobile Communication Services

Contents

What You Will Learn

With the convergence of Internet technologies and broadband wireless communications, mission-critical services for public safety emergency communications are undergoing tremendous change and growth. However, challenges and requirements are increasing for public safety and those organizations responsible for providing network services to address the increasing complexity across mission-critical voice, data, and video communications. The Cisco vision for emergency service provider organizations addresses the critical communications requirements public safety organizations have to prevent, prepare for, respond to, and recover from emergency incidents.

This paper is intended for organizations that provide mission-critical network communications services for national security, defense, and public safety organizations including systems integrations, service providers, and managed service providers. It explains the rationale and vision including:

- Public safety challenges and requirements for communication, collaboration, and operations
- Emergency response use case scenarios
- Key trends impacting requirements for emergency service providers
- Roadmap to evolve existing a mission-critical network to support mobile broadband (3G, 4G/LTE, Wi-Fi)

Executive Summary

For the last 15 years, the safety communication market has seen a consolidation in terms of technologies (TETRA and P25) and vendors to deploy private networks and provide dedicated mission-critical voice services. This consolidation has led to limitations in developing the communication services capabilities at the same pace as the commercial mobile communication systems. For instance, mobile broadband has become widely available while public safety networks remain focused on voice services.

With the availability of LTE, specific markets (US, Middle East) have decided to embrace this new technology to disrupt the critical communication services and deploy new capabiities using private radio with dedicated spectrum as well as commercial networks.

Cisco considers this evolution an opportunity to rethink the balance between what needs to be specific and what can rely on commercial technologies and resources in the safety world.

In this paper, a smooth migration scenario is described, allowing the public safety ecosystem composed of vendors, system integrators, and safety service providers to enhance the communication capabilities (e.g., providing advanced mobile data services such as video) while meeting safety requirements and constraints.

Overview

Public safety and emergency response organizations face challenges and increasing demands for critical communications across a growing sprectrum of voice, data, and video. In a crisis situation, every second counts. Potentially life-threatening situations change in a heartbeat, and decisions must be made in seconds.

Table 1. Emergency Response Spectrum

Safety and Security	Examples
Natural disaster	Earthquake, fire, hurricane, tsunami
Crisis management	Tunnel disaster, medical emergency
Urban security	Citizen protest, bank robbery
National security	Civil unrest, terrorist attack
Border control	Illegal immigration, smuggling
Mass venues and events	Crowd violence at sporting event, Olympic security, national convention security
Transportation	Train crash
Critical infrastructure	Nuclear power plant, refinery

Public safety and security is a complex discipline with many stakeholders under growing pressure to increase the speed and precision of decision-making processes as well as address the increasing levels and complexity of threats and crisis events—all with the realities of reduced budgets and limited resources.

To be effective, public safety and emergency response organizations need strategies and capabilities to communicate, collaborate, and operate efficiently and effectively:

- **Communicate:** Support multiple devices (e.g., radios, smartphones, BYOD) and modes of communications (e.g., real-time video). In addition, map user roles and profiles to devices to support the mission with mobile applications, video communications, and surveillance for real-time incidence communications.
- **Collaborate:** Provide shared services for local public safety and national security and defense organizations, including multi-agency and multidisciplinary collaboration to support effective decision making.
- **Operate:** Deliver intelligence and knowledge-based tools to facilitate sitatuational awareness and increase coordination of response.

Table 2. Requirements to Communicate, Collaborate, and Operate

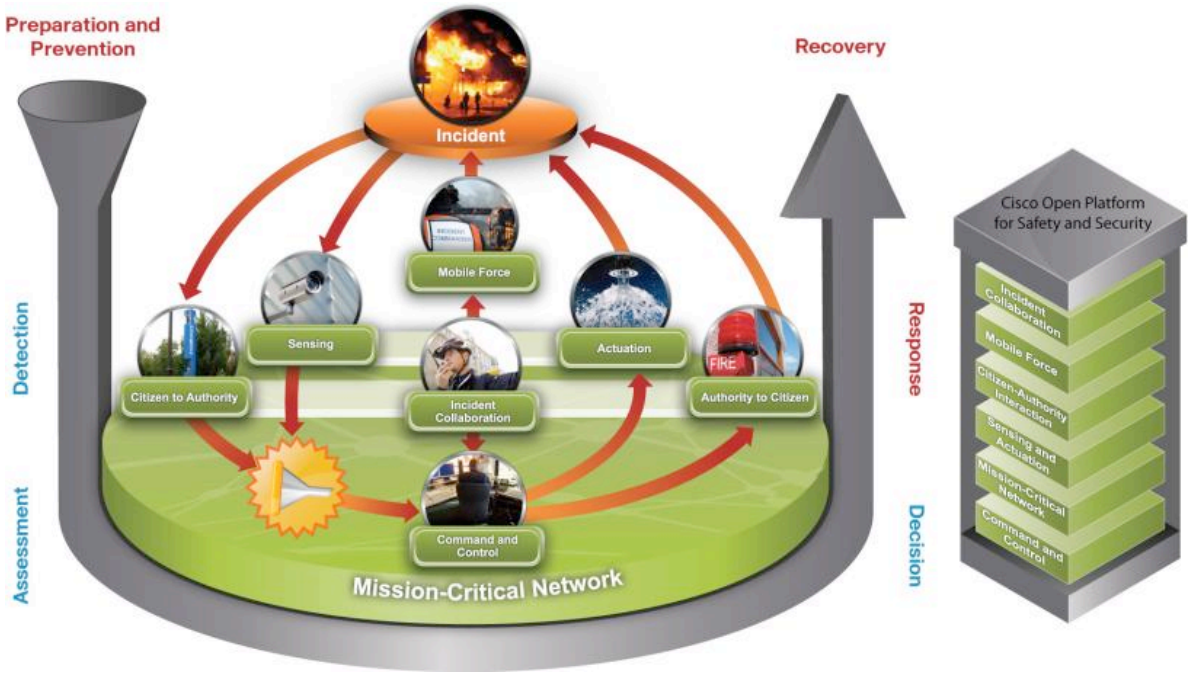
Requirement	Voice, Data, Video, Mobility, Security
Communicate	Multiple devices and modes (radios, smartphones, tablets, real-time video, text, social media)
Collaborate	Shared services across departments, agencies, and jurisdictions
Operate	Intelligence, tools, and applications

To deal with the increasing frequency and complexity of safety and security incidents (natural and man-made), forward-looking emergency agencies want to share more transparent and detailed information about the situation in the public open area to increase operational excellence. To better confront these challenges, public safety organizations have to connect emergency responders to the critical information, applications, and human resources they require. They must provide efficient dispatch, problem resolution, automated incident reports, and emergency communications.

The Cisco® Open Platform for Safety and Security framework describes how the mission-critical network provides the foundation for preparation and prevention, detection, assessment, decision, response, and recovery processes to address incident scenarios with integrated capabilities.

Government organizations, network operators, and service providers can now fully enable mission-critical broadband services with full IP LTE architecture together with a flexible Mobile Packet Core environment. This provides organizations with the capability for IP LTE networks to deliver secure, mission-critical voice, video, and data at a net bit-rate capacity of 100 Mbps for the downlink stream and 50 Mbps for the uplink stream per 20Mhz channel, and higher levels in the future. Safety and security organizations, both public and private, can also use the LTE and evolved packet core (EPC) capabilities while using commercial off-the-shelf technology (COTS) for critical infrastructure and services setup and support. They can use LTE network infrastructure, yet support secure services delivery and interwork with existing public safety radio and voice networks.

Figure 1. Cisco Open Platform for Safety and Security



Emergency Response Use Cases

1. Command and control capabilities improved with increased efficiency and important information flow (authority to authority and citizen to authority) and provides:

   - Actionable intelligence
   - Decision support tools
   - Real-time situational awareness

2. Situational awareness for the mobile first responder in the field with geographical information about activities and threats shared to provide an optimal view to:

   - Adopt early warning tools and response plans
   - Safeguard people, property, and assets
   - Provide instant notification of security breaches and threats
   - Determine the scope of the incident and next actions
   - Coordinate real-time communication

3. Collaborative incident communications: During a crisis situation, emergency responders need to collect and disseminate real-time information to all participants. Collaborative incident response helps:

   - Increase interagency collaboration and productivity while cutting costs
   - Speed identification of threats and decision making
   - Unify incident command
   - Rapidly disseminate critical information and interagency communication

4. Citizen to authority interactions: The explosion of mobile devices (smartphones, tablets, etc.) and social media tools has transformed how information is communicated during emergencies and drives the need for integration between commercial and security communications:

   - Scan social media for incident information
   - Integrate citizen to authority communications (information, photos, videos)
   - Support for bring your own device (BYOD) capabilities for off-duty responders

Key Trends Impacting Requirements for Emergency Service Provider Networks

Two key trends are impacting the requirements for emergency service provider (ESP) networks:

1. Mission-critical information capabilities

Emergency and public safety organization require capabilities not only for mission-critical voice, but also mobile data communication to deliver more accurate information and applications to mobile responders in the field, to off-load dispatch, and to improve efficiency through applications hosted via a secure network to the data center. In addition to basic information sharing, new sources of rich information and media are available via sensors (video cameras) and mobile devices (mobile cameras in vehicles) to provide more complehensive, timely, and accurate information to make effective decisions.

Understanding the need for both mission-critical voice and data capabilites, Cisco strategizes that both services will evolve into one holistic system which will deliver mission-critical information to emergency responders and ecosystem partner agencies.

To support this transition, Cisco is focused on a flexible architecture to help emergency service provider organizations and public safety agencies smoothly evolve from existing mission-critical voice environments to the mobile mission-critical information framework.

2. Mobile broadband technology innovation

The technology landscape is undergoing rapid change with the increasing availability of mobile broadband through the deployment of commercial 3G, 4G/LTE, and Wi-Fi networks. Public safety and ESPOs are evolving to create an environment that will support hybrid solutions mixing private radio network, but also using other access technologies as available. A layer of separation between the networks and the applications will allow organizations to match both user and operational requirements.

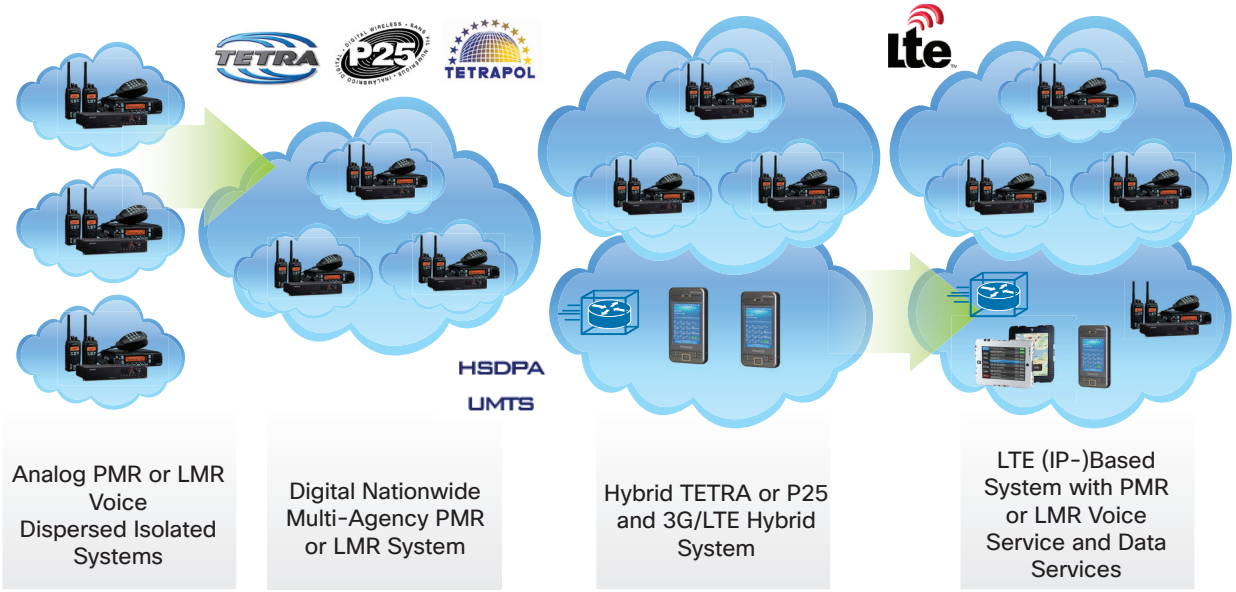
Two significant disruptions are impacting the current model for providing emergency mobile communications and are driven by the need to meet the growing demand for mobile data applications. The expected benefit is to have better alignment with the mobile network industry, minimizing the specifities of the public safety networks. These disruptions are:

- Use of commercial access technologies such as 3G and LTE access technologies that are already widely adopted around the world as well as others such as Wi-Fi
- Integration with commercial network as an access to purpose-built public safety network infrastructure and services

Emergency Service Provider Evolution

Emergency Service Providers are shifting from traditional legacy systems to hybrid environments as the first step in the transition to LTE broadband transformation.

Figure 2. Emergency Service Provider Network Evolution



The Cisco vision for the evolution to the next-generation public safety access network is based on an architecture composed of mobile clients, mobile transport, and mobile core networks, allowing for support of multiradio access technologies (3G, LTE, and SP Wi-Fi). Thanks to the breadth of products and expertise acquired from the development and deployment of commercial networks for mobile service providers, Cisco can offer an end-to-end architecture for public safety networks.

This approach uses all available access media for the most effective communication. Compared to a full private LTE network, the model offers transitional steps. Indeed, it enables phased and/or regional deployments and allows organizations to develop the purpose-built elements of the networks on top of an array of collaborative opportunities with commercial and existing deployed technologies.

Compared to a full dedicated network approach, this approach offers the capability to develop specific designs and applications required by individual user organizations, without the need for a complete nationwide deployment of those designs and applications.

Security and safety system integrators will be able to bring the expertise acquired from standards-based digital radio network systems such as P25 and TETRA-based mission-critical voice networks and apply it to LTE for mission-critical voice and data services. With flexible, robust IP technologies, the platform provides a framework to position traditional emergency requirements (such as secured and open to pre-emption PTT and group calls together with critical data) with future-proof technology.

Cisco offers safety and security system integrators, end users, and ESPOs the fundamental building blocks part of Cisco Mobile Internet products and solutions.[1] In particular, these include:

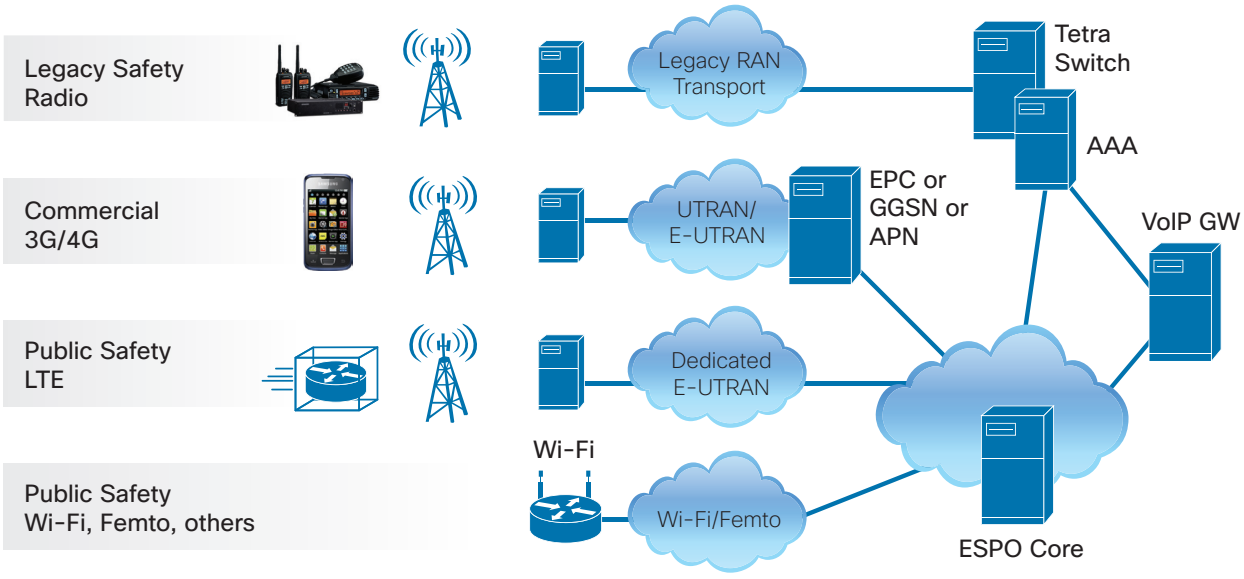
- Mobile Packet Core consisting of the flexibile EPC supporting private and dedicated LTE-based network as well as providing the necessary interfaces to integrate with commercial network (in that case, the ESPO would be acting as a Mobile Virtual Network Operator [MVNO])

- Broadband mobile CPE routers that offer extended mobile connectivity (3G, LTE, Wi-Fi) and integrate into different environments including vehicles

The proposed architecture relies on having the ESPOs deploy a centralized core infrastructure and services. This allows organizations to support both the existing (or upcoming) private radio networks and the the commercially deployed networks. Due to Cisco's core network flexibility, the core infrastructure can be deployed either at the national or regional level. The difference between the two models lies in the details of the specific services requirements as well as the specific interconnection agreements with the commercial network providers.

The following diagrams depict the overall architecture with options to support the existing environment and other access technologies.

Figure 3. Proposed Broadband Emergency Services Framework



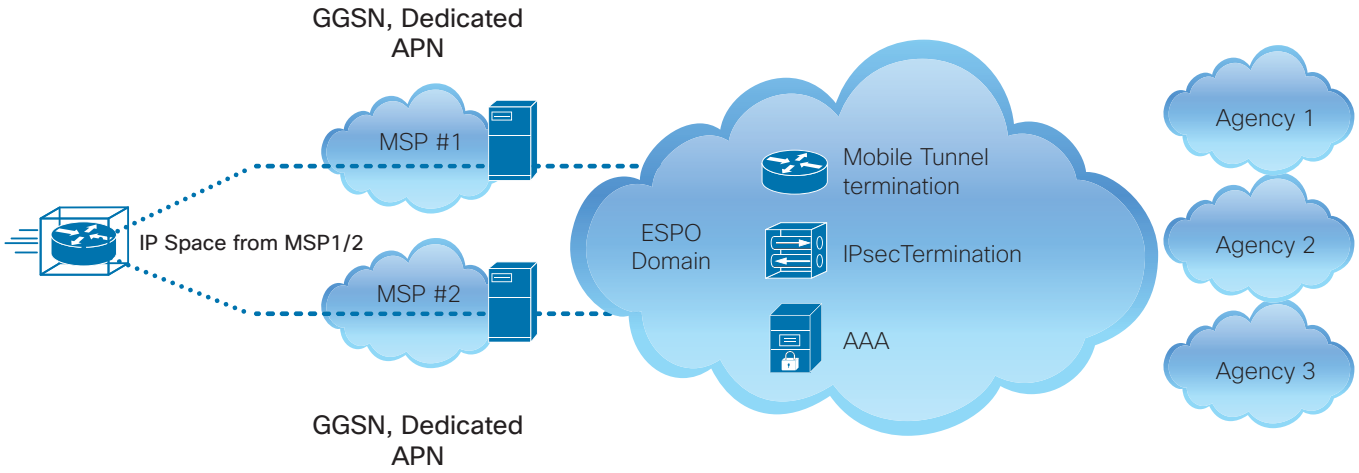
[1]Refer to the Cisco Mobile Internet solution page: http://www.cisco.com/go/mobile

The following sections describe possible phases for the public safety network to integrate with a commercially available network. The phases are ordered in terms of breadth or partnership with the mobile service provider, ranging from the simpler approach (mobile data access integration) to the more complex (full MVNO model).

Initial Phase: Public Safety Access Point Name (APN)

Mobile data services are supported on commercially available 3G/4G networks. Through the centralized aggregation solution offered by Cisco, provisioning, control, shared billing, or other security mechanisms can be implemented in a consistent manner. For instance, using a Cisco ISG (IP Services Gateway), the ESPO can provision, secure, bill, and manage on a per user, per organization, or per application basis. The end-user equipment could be commercially available user handsets as well as broadband CPE fleet with 3G/4G mobile routers enabling connectivity. Other technologies such as service provider Wi-Fi, as they are getting deployed today, can also be integrated.

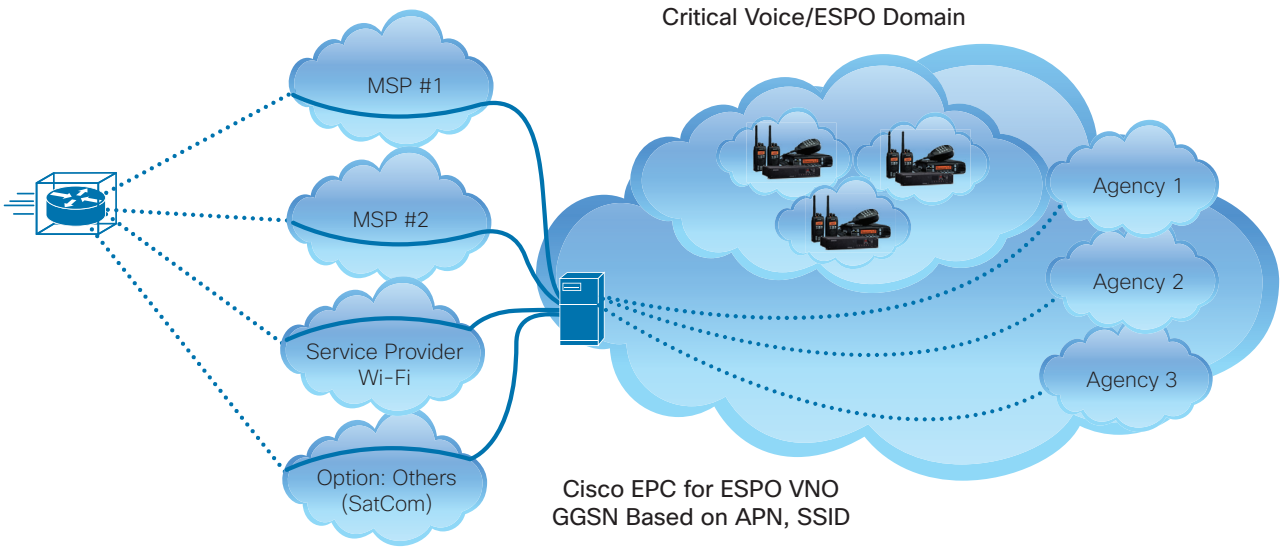
Figure 4. Public Safety Access Point Name (APN)



Transformation Phase: Public Safety MVNO Model

This phase can be considered an evolution of the APN phase with the traffic delivered over a commercially available mobile network. The difference lies in the fact that the traffic would not be terminated on the service provider infrastructure, but rather within a central platform managed by, or on behalf of, the ESPO. This way, the ESPO would, in effect, become a Mobile Virtual Network Operator (MVNO). There are different levels of MVNO deployments, and these will depend on the specific agreement being negotiated with the service provider and the architectural depth of the infrastructure.

Figure 5. Lightweight MVNO



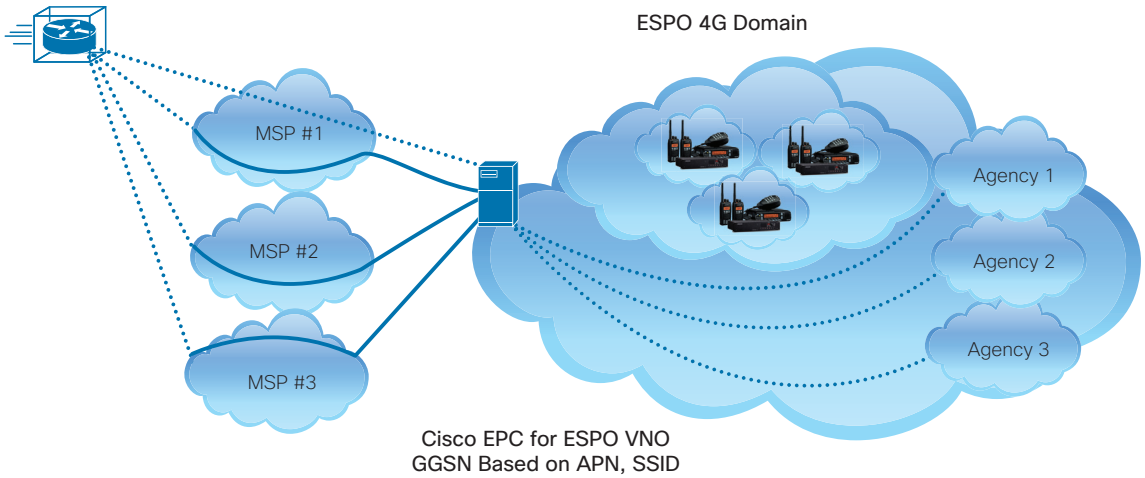
In the lightweight MVNO model, the ESPO infrastructure would be enhanced to include a mobile data gateway (e.g., GGSN for 3G and EPC PGW for LTE). The mobile data APN would not be terminated within the service provider network, but all traffic related to that APN would be handled by the ESPO network directly. A standard set of capabilities would be available including authentication, aggregation, and security. The main difference is the capability to control the quality of service (QoS) associated with the mobile data traffic. A mobile gateway can be used to control and change the QoS policy enforced within the access network. The specific QoS and preemption (assuming preemption capabilities become available) policies will have to be negotiated with the mobile service providers as part of the MVNO agreements. In addition, the ESPO infrastructure offers the capability to manage private Wi-Fi deployments that can be properties of end-user emergency organizations.

Maturity Phase: Dedicated Access and Full MVNO

IIn the full MVNO phase, the virtual operator can take a broader role to provide the mobile infrastructure and services. This can include delivering the actual SIM cards to the set of subscribers, which would be authenticated against a dedicated HLR to make it possible for the emergency services network to have its own mobile network identifier and national roaming with agreements commercial networks.

In addition, the ESPO would deploy additional network infrastructure and services that could allow organizations to eventually deploy its dedicated radio access network in dedicated places through a specific deployment phasing and use a common core environment.

Figure 6. Target Phase: Full Public Safety Service Provider Including private LTE



After the maturity phase is reached, the ESPO is positioned to deploy its own purpose-built LTE for safety network islands. The model requires that access to the LTE spectrum be offered to safety and security organizations in a direct or indirect manner through traditional service providers.

Combining the full IP LTE architecture together with a flexible Mobile Packet Core environment would provide safety and security experts, system integrators, and end users the capability to use a COTS technology for critical infrastructure and services setup.

Summary

In summary, the emergence of mobile broadband and Internet technologies and services provides the opportunity to transition mission-critical network services for emergency and public safety organizations. The architecture presented above provides a flexible approach to complement and transition the legacy and hybrid environments today to a next generation of heterogeneous technology networks, including current TETRA, P25 to upcoming LTE.

To help this transition, Cisco can offer to the public safety ecosystem its experience and broad portfolio of products and solutions that supported the commercial service provider journey into mobile broadband. To make sure the safety experts will be able to implement the relevant architectures and applications for the safety world, Cisco continues to enhance its products and solutions to meet specific requirements, offer flexibility, and provide state-of-the-art capabilities.

For More Information

To read more about Cisco resources for public safety, national security, and defense, visit: www.cisco.com/go/government

For more information about how Cisco can help migrate to an LTE mobile network, visit: www.cisco.com/go/mobileinternet

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**