

# **City of Charlotte**

## **Interoperability Showing Technical and Operational Response**

Original Date: July 19, 2010

## **Interoperability Showing Response: Executive Summary**

---

On behalf of the City of Charlotte, this document responds to the Commission's May 12, 2010 Order, FCC 10-79 (Waiver Order) granting conditional waivers to twenty-one public safety entities for early deployment of public safety broadband networks in the 700 MHz public safety broadband spectrum (PSBB Block) and its subsequent Public Notice, DA 10923 (May 21, 2010). Charlotte is a waiver recipient. The Waiver Order established technical, operational and governance conditions for early deployment and requires each Waiver Recipient to submit to the Public Safety and Homeland Security Bureau a detailed plan for achieving interoperability with other public safety broadband networks. The plan is referred to as an Interoperability Showing.

In presenting this Interoperability Showing, Charlotte has consulted and been assisted by technology and equipment providers, other agencies, representatives of the Public Safety Spectrum Trust (PSST) and other parties. It has also drawn on its own internal resources and expertise. The objective has been to demonstrate Charlotte's serious commitment to a broadband network that embraces pervasive interoperability. Recognizing that there will likely be submissions of a similar nature, our purpose is to promote analysis and discussion rather than a definitive recitation of the ultimate network. It is not intended to portray the system's final design and deployment requirements for acquisition purposes. Charlotte by necessity must reserve these decisions. It is presented to invite examination by the Emergency Response Interoperability Center (ERIC) and its technical advisory committee, the Commission and interested parties so that a nationwide interoperable broadband network can emerge.

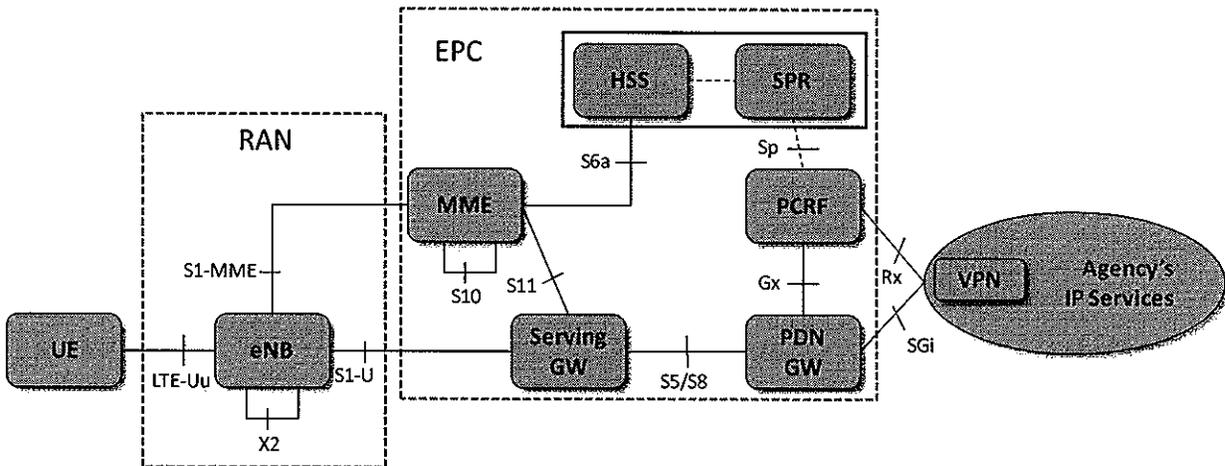
Charlotte's is commitment to deploy an Interoperable Public Safety 700 MHz Network to provide ubiquitous Broadband connectivity evolves from its experience in r the Charlotte Urban Area Security Initiative (UASI) region. The partners to Phase 1 of the Regional Public Safety Broadband Network (CharMeck Connect) are – the City of Charlotte, County of Mecklenburg, and the communities of Cornelius, Huntersville, Davidson, Mathews, Mint Hill and Pineville. An enormous contribution will be made to the Charlotte UASI Region. The CharMeck Connect project will be capable of providing true interoperability in emergencies requiring a multi-jurisdictional and multi-disciplinary response. The CharMeck Connect Broadband Network will deploy Long Term Evolution (LTE) technology operating at 758-763 MHz and 788-793 MHz. The R8 LTE standards based system will allow CharMeck to be interoperable with other public safety agencies on LTE networks and also for the planned National Public Safety Broadband Network. The Interoperability Showing Response submitted by the City herewith addresses each interoperability component in the Broadband Public Safety solution, demonstrating how the City of Charlotte network will achieve interoperability. The plans to deploy multiple applications like CAD, Live Incident Video, Automated Vehicle Location, High resolution images of suspects/vehicles, building plans, and examine patient details on the Broadband network that will help improve Officer Safety as well as Operational Efficiency of the Public Safety and Emergency responders. This citywide 700 MHz public safety LTE network will enable multiple provide interoperable communications, and data exchange among the fire, police, EMS, and Emergency responders.

This Executive Summary serves to provide an overview of the content in the formal Interoperability Showing Response. It is highly recommended the reader refer to the Interoperability Showing Technical and Operational Response for additional information on each of these topics. Sections below provide a high level overview of the System Architecture, key components and questions on Interoperability that the City has for FCC/ERIC.

The City of Charlotte appreciates the Commission’s commitment to advancing public safety communications and looks forward to moving a broadband network to reality.

## System Architecture

The Broadband Public Safety solution is based on the 3GPP R8 standards, and consists of the Radio Access Network (RAN), the Evolved Packet Core (EPC), Devices, and the key interfaces exposed by these components. The solution includes the ability to roam between systems, provide priority access and QoS to ensure the most critical public safety users receive the highest priority, and ensure the Broadband Public Safety solution is secure.



### Radio Access Network (RAN) Architecture

The eNodeB (eNB) is the only 3GPP defined network element within the Evolved Universal Terrestrial Radio Access Network (EUTRAN) for 3GPP R8. The eNB provides the user plane and control plane protocol terminations toward the UE. The eNB consists of the inter-working function between the backhaul interface and the base band interface, the base band processing elements for the air interface, and the radios. The eNB in this system is built based on the 3GPP R8 standards. The eNB is designed for compatibility with 3GPP compliant UE’s and utilizes 3GPP compliant network interfaces.

### Core Network Architecture

The core network is based on the 3GPP R8 defined EPC (Evolved Packet Core) as mainly defined in 3GPP TS 23.401. The solution supports the MME, SGW, PGW, HSS and PCRF/SPR functions using standards defined network interfaces. A VPN element is also shown. This element supports a secure public safety VPN and can be used with alternate access technologies (WiFi, 3G).

### Interfaces

The RAN/EPC solution supports the following interfaces based on 3GPP R8 compliance: LTE-Uu, Gx, Gz, Rf/Ga, Rx, S1-MME, S1-U, S5, S6a, S8, S9, S10, S11, SGI, SP, X2.

### Mobility and Handoff (Handover)

The mobility solution is fully compliant with 3GPP standards. It supports high-speed mobility and seamless handoffs between eNBs within the Broadband Network. Radio frequency phase shift acquisition up to 300 Hz Doppler is supported, which accommodates handoffs above 75 mph in a properly-engineered and functioning network.

The mobility solution will support inter-network handover between regional public safety networks. The approach taken to support inter-network handover between regional networks is dependent on several factors. These factors include:

- Frequency bands assigned to and shared between the regional networks
- PLMN ID's assigned to and shared between the regional networks
- Administrative relationships between the regional networks

In order to support inter-PLMN handover with 3GPP R8 specifications, coordinated network planning and operations across the PLMN ID domains is required. In order to support inter-PLMN handover across operational domains without operational coordination, 3GPP standards enhancements are required. MVPNs provide an alternative solution approach to inter-PLMN handover; the MVPN provides IP layer mobility and intelligent route selection which is independent of handover in the radio access layer.

### ***Roaming***

Intra-system roaming will be supported as needed by operational scenarios which require service across regional network boundaries. In addition to intra-system roaming, adjacent regional networks will also raise the need for inter-PLMN handover.

Inter-system roaming will be supported as needed by operational scenarios which cross regional network boundaries, and as allowed by roaming agreements with commercial carriers. Inter-system roaming may also require addition of Border Gateway routers to interconnect with a Roaming Service provider. The same 3GPP standards constraints apply to inter-PLMN handover across operational domains for inter-system roaming as for intra-system roaming. However, inter-system and inter-PLMN handover is more challenging due to the additional interfaces and operational dependencies between commercial carrier networks and the Shared Wireless Broadband Network (SWBN).

### ***Priority Access and QoS***

LTE offers the most advanced QoS capabilities of any commercial cellular technology; however the technology must be properly configured to meet the needs of public safety usage and to support roaming to carriers and other public safety regional systems. The Interoperability Showing Response describes how advanced priority access and QoS capabilities should be configured in order to maximize the interoperability benefits to public safety. These LTE configurations should be standardized across all public safety regional systems in order to facilitate nationwide interoperability.

A flexible priority access and QoS framework must be established which provides:

- **Regional Flexibility**  
Each public safety region should have flexibility to choose an LTE prioritization model to suit its need. For example, region 1 may prioritize responders based on role and region 2 may prioritize responders based on application. The region should have some latitude to choose how to prioritize devices and applications on the regional system.
- **Roaming Support**  
Whether roaming between regional systems or roaming to a commercial LTE system, the prioritization framework should support a consistent and fair policy of mapping priority between systems.

The realization of the priority access/QoS framework is based on standardization of LTE configuration parameters for public safety use, such as ARP, QCI, GBR, and MBR. The Interoperability Showing Response outlines the specific configuration required for the solution.

### **Security**

3GPP standards have defined a suite of security related specifications for LTE systems. From an interoperability perspective, of particular interest are the specifications 33.401 (“3GPP System Architecture Evolution (SAE); Security architecture”), 33.210 (“3G security; Network Domain Security (NDS); IP network layer security”), and 33.310 (“Network Domain Security/Authentication Framework (NDS/AF)”). We will fully support the requirements stated in these specifications to ensure secure inter-system interoperability. The City is also planning to use MVPN to provide end-to-end secure data tunnels between the UE and the backend application servers.

### **Devices**

Delivery of user devices for Public Safety broadband agencies will be driven by the availability of an LTE chipset that supports standard 3GPP baseband protocols and RF operation in the 10 MHz of Public Safety spectrum (763 MHz to 768 MHz lower and 793MHz to 798 MHz upper). All devices will adhere to the 3GPP Release 8 air interface specification and the recommended out of band emissions (OOBE) as specified in the waiver order, as well as existing OOBE requirements to protect Public Safety narrowband voice services in the 700MHz spectrum. The user devices intended for early deployment Public Safety LTE networks are USB-Dongles, Vehicle Modems, and Smartphones.

### **Applications**

The FCC has identified in the 10-79 order a list of minimum waiver applications potential waiver grantees must support. These applications provide the foundation for meaningful nationwide interoperability, and are explained in the Interoperability Showing Response.

Two key application technology areas for broadband public safety are internet access and a Status/Information Homepage (SIH)

The LTE system must be configured to provide Internet Access by first accessing the responder’s home system (i.e. Internet/Intranet traffic is home-routed). Serving the Internet from a home APN lessens the need for additional APNs on the device. Each additional APN may imply the device connects to more and more network segments (and subsequently has multiple IP addresses); increasing security risks at the device. Therefore, home-routed Internet Access reduces the need for a “local APN” while roaming and improves security on the device.

Another key technology for LTE public safety will be the Status/Information Homepage (SIH). The SIH is envisioned to provide home and roaming responders with incident-specific information, alerts, system status, weather, traffic, and other information. This information may come from Computer-Aided Dispatch (CAD) terminals, responders, or in the future the NG911 ESInet.

### **Reliability and Availability**

The CharMeck Connect Broadband Network reliability and availability is focused but not limited to following areas:

- Regional Data Center and NOC
- LTE Enhanced Packet Core (EPC)
- Transport and Backhaul network.
- Radio Access Network (RAN)
- Mobile and portable User Equipment

In order to maintain service availability, the network has been designed with multiple layers of redundancy and resiliency. The network can be deployed such that module failures, node failures, and even failure of an entire data center site will not degrade network service availability. The Regional Data Center and NOC can be deployed in a fully-redundant configuration, such that a catastrophic failure of a data center location will not result in the loss of critical functionality, since all operations and traffic can be served by an alternate data center.

The mobile and portable User Equipment (UE) devices are hardened in accordance with Public Safety best-practices. Generally, the eco-system for LTE 700 MHz broadband Public Safety UE's is still emerging. However, we expect that as the eco-system matures, a wide range of device capabilities will be available to Public Safety markets, spanning low-end commercial grade devices to high-end devices compliant with military-specifications.

The Interoperability Showing Response provides additional information on the reliability and availability aspects of the solution.

## **Radio Frequency (RF) Engineering**

RF system performance factors such as coverage footprint, throughput, and capacity depend upon many different variables in RF design, including but not limited to the number of users, desired site density, system cost, traffic model, interference, etc. As such, these variables are interrelated, so that changes in one variable inevitably impact the others. The CharMeck Connect Broadband Network is designed to support current users and applications in the most cost effective manner and the design is scalable for future expansion.

LTE system capacity and coverage performance depend on interference levels; therefore, interference mitigation is a primary objective of the LTE RF system design. Several measures are taken during the system design phase to mitigate interference including selecting appropriate antenna patterns, adjusting the individual sector antenna tilts, and selecting optimal site locations and site separation distances. Site separation, antenna down-tilt, along with eNB features like static and semi-static inter-cell interference coordination (ICIC) are key elements towards minimizing intra-band interference levels. OFDM systems like LTE can also take advantage of frequency diversity and frequency selectivity gain via scheduler algorithms to further minimize intra-band interference.

## **Testing**

Testing validates key functionality, performance and interoperability requirements of the PS LTE solution. This interoperability testing is in addition to the extensive testing performed by the solution provider in their internal laboratories to ensure conformance of their LTE solution to 3GPP standards. An outline of this testing can be provided by our solutions provider. We as a Waiver Recipient are also planning to participate in the PSCR/DC demonstration network, starting in 2010. In order to meet the requirement of the Waiver Order, a trial activity will be planned using our selected PS LTE solution. This trial activity will constitute and form the basis for initial testing of the system. The Interoperability Showing Response provides an overview of the trial activities (initial testing), and descriptions of the tests to be performed.

## **Deployment**

The CharMeck Connect Broadband Network will deploy thirty radio sites and EPC core. The City will leverage its existing towers, and other infrastructure to complete this project. The City also plans to deploy multiple handheld devices and also provide connectivity to Vehicles on street. The current plan is to complete the Deployment of the Core, one-third of sites and devices in year 1, one-third of the sites, and devices in year 2, and rest of the sites in year 3. The detail deployment plan can be found in the Deployment section of the submitted document.

## **Operations, Administration and Maintenance**

The City's OA&M solution is comprehensive and standards-based. It encompasses the entire lifecycle, including system design, assembly and staging, installation and commissioning, operations, optimization, and billing. The operations solution includes Fault Management, Configuration Management, Accounting Management, and Performance Management (FCAPS) support for the system infrastructure and devices, as well as the advanced capabilities such as NMS, Over the Air Device Management, Self Organizing Network, Integrated Subscriber Provisioning, and an Integrated Billing solution. The full paper describes the OA&M capabilities. The OA&M solution requires interoperability coordination of vendor SON algorithms, subscriber provisioning, and device management.

**Table Of Contents**

Introduction.....	95
A. System Architecture .....	95
A.1 Radio Access Network (RAN) Architecture .....	95
A.2 Core Network Architecture.....	106
A.3 Interfaces .....	128
A.4 Mobility and Handoff (Handover).....	128
A.4.1 3GPP Compliant Handover.....	128
A.4.2 Adjacent Network Handover .....	139
A.4.3 Mobile VPN .....	139
A.5 Roaming.....	1410
A.5.1 Terminology and Scope .....	1410
A.5.2 PLMN ID Assignment.....	1410
A.5.3 Intra-system Roaming .....	1511
A.5.4 Inter-system Roaming .....	1511
A.5.5 Commercial Network Roaming .....	1511
A.5.6 Roaming Interoperability .....	1511
A.5.7 Roaming Configurations.....	1512
A.6 Priority Access and QoS .....	1612
A.7 Security .....	1613
A.8 Devices .....	1815
B. Applications .....	1916
B.1 Internet Access .....	2016
B.2 VPN Access to Any Authorized Site and to Home Networks .....	2017
B.3 Status/Information “Homepage”.....	2017
B.4 Access to Responders under the Incident Command System .....	2118
B.5 Field-Based Server Applications.....	2218
C. Reliability and Availability .....	2219
C.1 Regional Data Center and Network Operations Center .....	2219
C.2 Enhanced Packet Core .....	2319
C.3 Transport Network.....	2320
C.4 Radio Access Network.....	2320
C.5 Mobile and Portable User Equipment.....	2420
D. Radio Frequency (RF) Engineering.....	2420
D.1 Radio Access Network Planning .....	2421
D.1.1 RF Propagation analysis.....	2421
D.1.2 Network Capacity and Throughput Analysis.....	2521
D.1.3 Scalability, expandability, and cost effective design .....	2521
D.1.4 Modeling Assumptions .....	2522
D.2 Interference Coordination .....	2522
D.2.1 Network Planning .....	2622
D.2.2 eNB Features .....	2723
E. Testing.....	2724
F. Deployment.....	3026
G. Operations, Administration and Maintenance .....	3128
Appendices.....	3330
Appendix A. Definitions and Acronyms.....	3330
Appendix B. LTE/EPC Functions and Interfaces.....	3532
Appendix C. Priority Access and QoS Configurations.....	3937
G.1.1 General Priority Access and QoS Configurations.....	3937
G.1.2 Roaming to Commercial Public LTE Systems .....	4038
G.1.3 Roaming to Other Regional Public Safety LTE Systems.....	4139
Appendix D. LTE Test Tools .....	4240

## Introduction

This Interoperability Showing Technical and Operational Response is intended to demonstrate the technical and operational proficiency of the City of Charlotte (“City”), necessary to achieve operability and interoperability of public safety broadband networks in accordance with FCC Waiver Order 10-79.

## A. System Architecture

The Broadband Public Safety solution is based on the 3GPP LTE network solution, and consists of the Radio Access Network (RAN), the Evolved Packet Core (EPC), Devices, and the key interfaces exposed by these components. The solution includes the ability to roam between systems, provide priority access and QoS to ensure the most critical public safety users receive the highest priority, and ensure the Broadband Public Safety solution is secure.

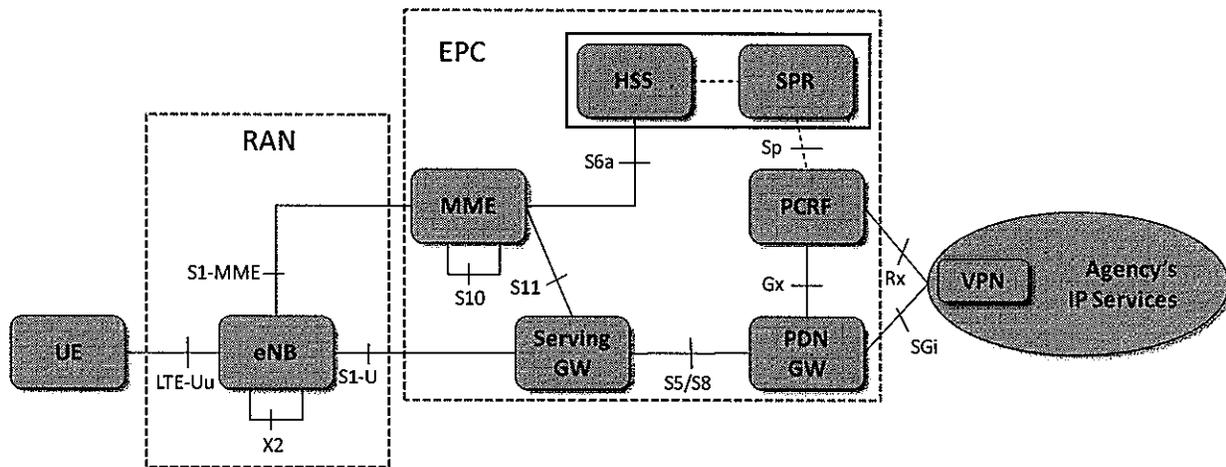


Figure 1 - Logical Architecture

The LTE standard is the right standard for Public Safety broadband use. As with any commercial technology, there are elements in the LTE standard that are not defined based on public safety operations. Issues around inter-PLMN HO support and improvements to access class barring are best dealt with in standards. Issues around priority and pre-emption, especially at the agency, incident or role level are handled by the implementation of this system. Consistent policy enforcement across commercial and regional Public Safety networks requires the correct amount of Public Safety specific standardization that still allows for some regional and agency control.

The LTE RAN and EPC architecture and interfaces are shown in Figure 1 and described in the following sections. A more detailed description of the LTE/EPC infrastructure elements and interfaces is contained in [H. Appendix B](#).

### A.1 Radio Access Network (RAN) Architecture

The eNodeB (eNB) is the only 3GPP defined network element within the EUTRAN for 3GPP R8. The eNB provides the user plane and control plane protocol terminations toward the UE. The eNB consists of the inter-working function between the backhaul interface and the base band interface, the base band processing elements for the air interface, and the radios. The eNB in this system is compliant with the 3GPP R8 standards. The eNB is designed for compatibility with 3GPP compliant UE's and utilizes 3GPP compliant network interfaces.

Functions supported by an eNB are defined mainly in 3GPP TS 36.300. The RAN solution for this system is compliant with the R8 version of 36.211, 36.212, 36.213, 36.214, 36.300, 36.321, 36.322, 36.323, 36.331, 36.413, 36.423 and other referenced specifications. Compliance of devices and the RAN continues to evolve from Dec 2008 to Dec 2009 specification versions and beyond. The eNB is designed to support upgrade to support modifications of the air-interface and network interfaces in accordance with evolution of the LTE standards.

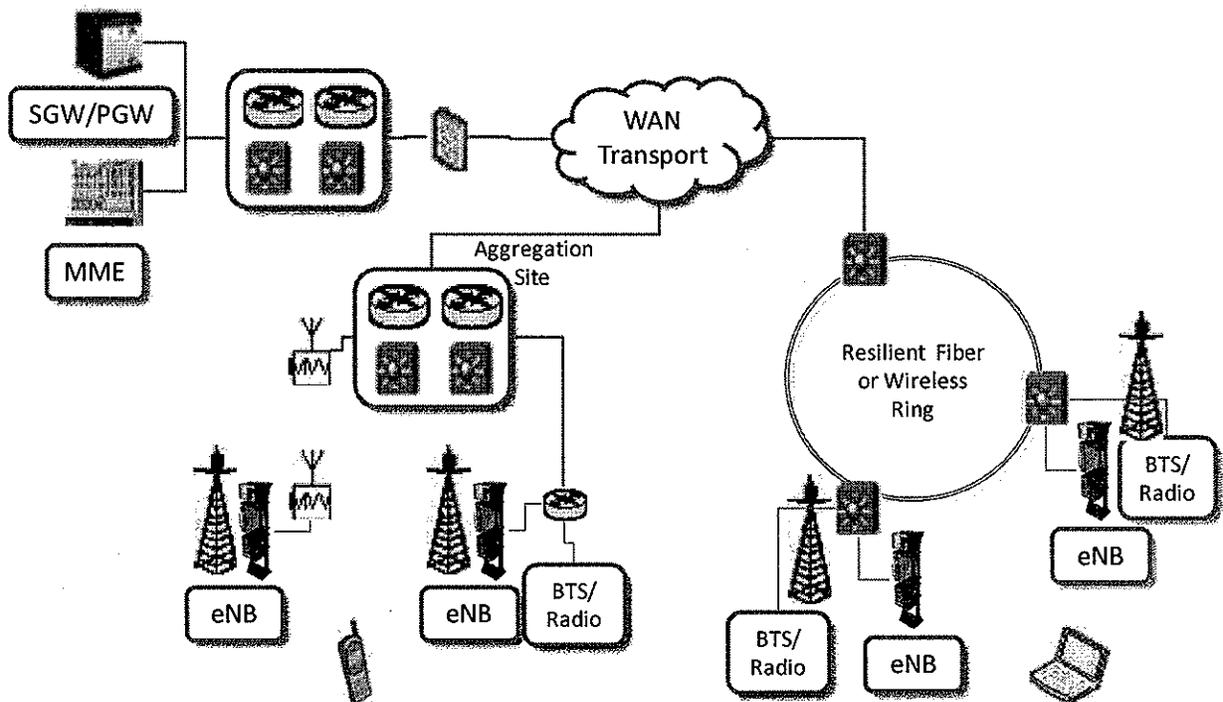


Figure 2 – RAN Physical Architecture

The RAN solution is based on IP transport. The solution supports collocation with existing narrowband or commercial sites and supports shared backhaul of various types. The eNB hardware supports 5+5 MHz PSST band or 10+10 MHz D/PSST 5MHz bands simultaneously. The solution will support optical and electrical Ethernet interfaces and can support external L2 or L3 equipment to fit within a number of transport scenarios. Backhaul redundancy is supported when required. The equipment supports the logical User Plane, Control Plane and OAM&P interfaces on the same physical interfaces and supports VLAN separation when required. The eNB is built with Self Organizing Network (SON) functions to automate deployment and optimization functions. The solution will support both GPS and IEEE 1588v2 timing solutions as needed (e.g. for ICIC (Inter-Cell Interference Coordination) or MBMS).

## A.2 Core Network Architecture

The core network is based on the 3GPP R8 defined EPC (Evolved Packet Core) as mainly defined in 3GPP TS 23.401. The solution will support the MME, SGW, PGW, HSS and PCRF/SPR functions using standards defined network interfaces. A VPN element is also shown. This element supports a secure public safety VPN and can be used with alternate access technologies (WiFi, 3G).

The EPC solution is based on the GTP-based S5 and S8 interfaces. The EPC solution is compliant with the R8 version of 23.203, 23.401, 23.402, 24.301, 29.212, 29.214, 29.272, 29.274, 32.240, 32.251, 32.295 and other referenced specifications. Compliance of devices and

infrastructure continues to evolve from Dec 2008 to Dec 2009 specification versions and beyond.

Additional interfaces supporting charging are provided but not shown for simplicity. The PGW and SGW support offline charging interfaces (Gz/Rf/Ga). These interfaces may be valuable in a system supporting multiple agencies and user affiliations.

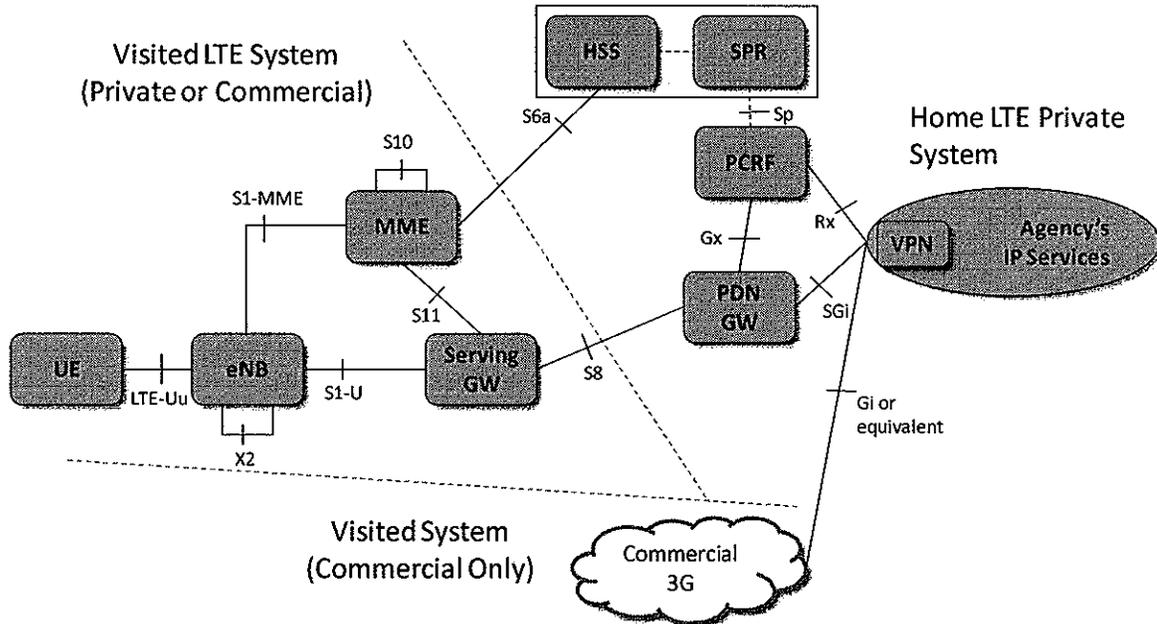


Figure 3 – EPC Roaming Architecture

The system is capable of supporting roaming with other regional PS LTE systems or with a commercial LTE system (if supported by the device capabilities). Note that local breakout is not currently shown (although can be supported). Further study is needed around the impact of supporting a secure VPN and multiple APN's simultaneously. Support for roaming on a commercial 3G network is shown using a VPN solution and a unique subscription on the 3G network. Use of standard EPC interfaces for 3G inter-connectivity between a regional PS network and an existing commercial 3G network run by a different entity are for further study and subject to potential operational complications.

The EPC physical architecture is shown in Figure 4. The EPC solution is based on IP transport and pooling of network elements. The solution supports IPv4 and IPv6 UE's and additional IPv6 network interfaces as a future software upgrade. The solution will support a platform that hosts the SGW and PGW on one platform instance and the PCRF/SPR/HSS functions on another platform instance. Redundancy is supported at several levels including geographical distributed elements to mitigate disaster scenarios.

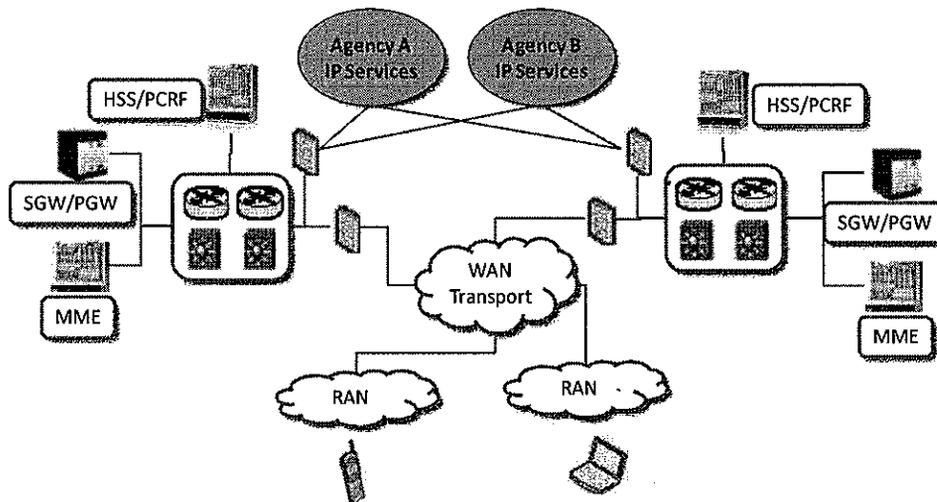


Figure 4 – EPC Physical Architecture

### A.3 Interfaces

The RAN/EPC solution will support the following interfaces based on 3GPP R8 compliance:

**LTE-Uu, Gx, Gz, Rf/Ga, Rx, S1-MME, S1-U, S5, S6a, S8, S9, S10, S11, SGi, SP, X2.**

These interfaces support inter-operability of the LTE network with 3GPP R8 compliant UE devices, as well as inter-operability with other PS regional LTE networks. Details on handoff and mobility inter-operability are addressed in Section A.4 including mobility across regional PS LTE networks. Details on supporting a VPN service are also covered in Section A.4.

### A.4 Mobility and Handoff (Handover)

Regional wireless mobile broadband systems, in conjunction with the Shared Wireless Broadband Network (SWBN), present unique mobility requirements, including mobility while maintaining a secure VPN session connection. These requirements are met by leveraging robust and efficient handover algorithms and inter-eNB handover coordination via 3GPP standardized interfaces. The mobility solution accommodates both active and idle mode handovers within LTE networks.

#### A.4.1 3GPP Compliant Handover

The mobility solution is fully compliant with 3GPP standards. It supports high-speed mobility and seamless handoffs between eNBs within the Broadband Network. Radio frequency phase shift acquisition up to 300 Hz Doppler is supported, which accommodates handoffs above 75 mph in a properly-engineered and functioning network.

The mobility solution will support UE physical layer measurements, as specified in TS 36.214, to determine cell signal strengths and actions specified by the RRC L3 protocol in TS 36.331. The UE receives measurement control information from the eNodeB (eNB) via the following System Information Blocks (SIB):

- SIB3 information block contains common information for both intra-frequency and inter-frequency cell reselection
- SIB4 information block contains neighboring cell related information for intra-frequency cell re-selection including specific re-selection parameters
- SIB5 information block contains neighboring cell related information for inter-frequency cell re-selection including specific re-selection parameters

The MME and eNB utilize UE receiver measurement reports for controlling UE handover behaviors. When making a decision to handover a UE to another cell and/or carrier frequency the following factors or parameters are considered:

- UE measurement reports of its serving and neighbor cell signal strengths
- UE's current signal to interference ratio
- UE's serving cell and neighbor cell loading conditions
- UE's QoS/application profile and the UEs mobility level

#### **A.4.2 Adjacent Network Handover**

---

The mobility solution will support inter-network handover between regional public safety networks. The approach taken to support inter-network handover between regional networks is dependent on several factors. These factors include:

- Frequency bands assigned to and shared between the regional networks
- PLMN ID's assigned to and shared between the regional networks
- Administrative relationships between the regional networks

If the regional networks are allocated a common frequency band, then issues associated with inter-band management are not required. However, if separate frequency bands are allocated to the regional networks, then inter-band handover management functions, such as neighbor band advertisement and frequency selection priority must be supported.

Assuming that regional networks are allocated unique PLMN ID's (see section A.5) then inter-PLMN handover capabilities will be required as regional networks expand and become adjacent. In commercial carrier networks, inter-PLMN handover across operators is not typical. This is because commercial carriers deploy near-ubiquitous coverage in their service areas. Commercial carrier networks may also be comprised of multiple PLMN ID's. However, in these cases, the administrative functions of network planning and operations are managed by the carrier. Thus the carrier is able to coordinate cell identifiers, neighbor lists, and handover configurations across their PLMN ID domains. Since network planning and operations are typically not coordinated across commercial carriers, inter-PLMN handover is typically not supported across commercial carrier networks.

Further, 3GPP R8 standards do not identify the inter-MME S10 interface as a roaming interface. If MME's are deployed in the regional networks (i.e., not shared), then inter-PLMN handover would cross MME domains and the S10 interface would be needed to support inter-PLMN handover across MME domains. Since 3GPP R8 standards do not identify S10 as a roaming interface, inter-PLMN handover across operational domains is not yet supported in the standard. Therefore, in order to support inter-PLMN handover, coordinated network planning and operations across the PLMN ID domains is required. In order to support inter-PLMN handover across operational domains without operational coordination, 3GPP standards enhancements are required.

Similarly, 3GPP R8 specifications do not support LTE<->3G inter-PLMN handover across operational domains. Therefore, handoff across home and visited networks when a visited network is using 3G networks will be gated by availability of 3GPP standards.

#### **A.4.3 Mobile VPN**

---

In addition to handover, the solution also supports Mobile VPN's. MVPN solutions, which are already in wide use by public safety agencies, provide application-level session continuity across disparate radio access networks, as well as security all the way back to the mobile user's home domain. Session continuity is supported at the application IP layer, which is above the radio access layer. Thus, the MVPN solutions can provide session continuity across various radio access technologies, such as LTE, 3G packet data, and Enterprise WiFi. Each radio access technology comprises an independent link between the MVPN server and the MVPN

client in the UE. As such, each radio link is independently monitored and the MVPN selects the optimum radio link to support the application sessions. If a radio link becomes disconnected or impaired, the MVPN can switch to an alternate available radio link. Thus, the MVPN can provide IP layer mobility and intelligent route selection which is independent of handover in the radio access layer. The MVPN can provide an alternative solution to inter-PLMN handover across regional networks, as well as across 3G networks.

In addition to providing IP layer mobility, the MVPN can provide secured connections between the server and client. The secured connection provides authentication, confidentiality, and integrity protection. Cryptographic modules which support the MVPN are compliant with FIPS 140-2 standards. The use of MVPN's with these security capabilities is critical, since current Criminal Justice Information Services (CJIS) security policy requires the use of highly secure VPNs for mobile device access.

## **A.5 Roaming**

---

Regional wireless mobile broadband systems, in conjunction with the Shared Wireless Broadband Network (SWBN), present unique roaming requirements, including support in initial operations, as well as roaming among regional networks. These requirements are supported by leveraging 3GPP standardized interfaces, as well as adoption of a roaming service tailored to the SWBN.

### **A.5.1 Terminology and Scope**

---

Using terminology from the NPSTC BBTF report, intra-system roaming refers to roaming across regional networks: *"9.4 Intra-system Roaming - The regional networks will be stand alone systems, part of a single national system, so public safety users roaming from their home regional systems to another regional system are considered to be roaming within (intra) the system."* Also from the NPSTC BBTF report, inter-system roaming refers to roaming between the national system of regional networks and commercial carrier networks: *"9.5 Inter-system Roaming - Public safety users that are part of a regional system may roam off of the national system and commercial users may roam onto the national system. This roaming is defined as inter-system roaming"*

According to 3GPP standards, home and visited network domains are delineated by PLMN ID. Roaming is the ability for a user to obtain service in a visited network. Note that roaming pertains to obtaining service, whereas handover pertains to the transfer of a user's connection from one eNB or cell to another.

### **A.5.2 PLMN ID Assignment**

---

The NPSTC BBTF report also recommends that the number of PLMN ID's allocated for the SWBN should be less than 100 IDs, and may be as few as 1 ID. The solution aligns with this recommendation. A unique PLMN ID should be assigned to each region in the US, such as each State or UASI region, and one common virtual PLMN ID should be reserved for the entire SWBN. This scheme allows flexibility and autonomy for regional network operations, yet also provides a single identifier which represents all regional networks in the SWBN.

With a unique PLMN ID assigned to each State or region, roaming as defined in the 3GPP standards will not occur within the regional network. Rather, roaming will occur if a Public Safety user obtains service from a commercial carrier, or obtains service from another regional network. Similarly, mobility within regional networks only requires intra-PLMN (as opposed to inter-PLMN) handover to support session continuity as users move between eNB's or cells within the regional network. Therefore, mobility within a regional network does not constitute roaming. The solution will support mobility via intra-PLMN handover within regional networks as described in section A.4.

### **A.5.3 Intra-system Roaming**

---

Inter-system roaming occurs when users obtain service from a commercial carrier network, which is not part of the SWBN. Intra-system roaming will be supported as needed by operational scenarios which require service across regional network boundaries. Intra-system handover capability can be added as an incremental software upgrade as standards mature. In addition to intra-system roaming, adjacent regional networks will also raise the need for inter-PLMN handover. See section A.4.2 for the solution approach to inter-PLMN handover.

### **A.5.4 Inter-system Roaming**

---

Inter-system roaming occurs when users obtain service from a commercial carrier network, which is not part of the SWBN. Inter-system roaming will be supported as needed by operational scenarios which cross regional network boundaries, and as allowed by roaming agreements with commercial carriers. As with intra-system handover, inter-system handover can be added as an incremental software upgrade. Inter-system roaming may also require addition of Border Gateway routers to interconnect with a Roaming Service provider. The same 3GPP standards constraints apply to inter-PLMN handover across operational domains for inter-system roaming as for intra-system roaming. However, inter-system and inter-PLMN handover is more challenging due to the additional interfaces and operational dependencies between commercial carrier networks and the SWBN.

### **A.5.5 Commercial Network Roaming**

---

Commercial carriers typically leverage roaming service providers to provide inter-network connectivity, security, and charging remediation functions. Roaming standards, such as IPX, are evolving to support QoS-enabled IP transport services, and therefore should support the services required for roaming with commercial carriers. However, inter-system roaming may have unique requirements as compared to commercial carrier roaming services, such as the support for the large number of regional network entities comprising the SWBN. Therefore, it will be beneficial to establish an SWBN roaming service to minimally support intra-system roaming. In order to support inter-system roaming, the SWBN roaming service could then interface to commercial roaming service providers, representing a single point-of-presence for the SWBN.

### **A.5.6 Roaming Interoperability**

---

UE's conforming to 3GPP standards will be able to roam across regionally deployed networks. However, it is essential for the UEs to be configured with appropriate frequency bands, PLMN lists, and access parameters corresponding to associated roaming agreements. 3GPP compliant UE's will minimally support the following roaming-related behaviors:

- Scan supported/configured bands,
- Perform network and cell selection,
- Authenticate on a visited network.

After authentication on a visited network, an IP address is assigned, and the UE then has the ability to access IP services. If home routed session is initiated, then the home network assigns an associated IP address to the UE. If a local breakout session is initiated, then the visited network assigns an associated IP address to the UE.

### **A.5.7 Roaming Configurations**

---

The solution will support home routed roaming configuration. Home routed configuration is when a user's traffic is routed back to the home network to enable the use of home applications and Internet access. The home routed case can support the majority of Public Safety applications and use cases. Home routed bearer flows benefit from QoS policies controlled in the home network. In addition, home routed provides many operational and security benefits, such as:

- Single point of authentication for applications
- Single point for firewall, intrusion detection/prevention, and anti-virus protection
- Activity logging and Internet access policy control

The solution will also support local breakout roaming configuration as needed for Public Safety applications. Local breakout configuration is when a user's traffic is routed within the visited network, and therefore is not routed back to the user's home network. Local breakout provides for optimization of bearer routing and access to visited network services. It should be noted that roamers may be subject to QoS policies of the local (i.e., visited) network. This is because 3GPP R8 standards allow the visited network to override QoS parameters from the home network. For this reason, the local services provided in the visited network are likely to be limited to IP services with static QoS and priority (e.g., best effort) for roaming users. It should be noted that the S9 interface is only applicable to local breakout scenarios. The S9 interface is used to provide dynamic charging and QoS policies from the home network to the visited network. Since use of local breakout scenarios are expected to be limited to static QoS policy, use of the S9 interface may not be required to support Public Safety applications. See section B for additional information regarding configurations used to support Public Safety applications.

## **A.6 Priority Access and QoS**

---

LTE offers the most advanced QoS capabilities of any commercial cellular technology; however the technology must be properly configured for optimal public safety implementation and to support roaming (with carriers and other public safety regional systems). This section provides an overview of the solution while highlighting the interoperability configurations for public safety. These LTE configurations should be standardized across all public safety regional systems in order to facilitate nationwide interoperability. The system defined in this section is compliant with 3GPP TS 23.203.

A flexible priority access and QoS framework is provided by the solution:

- **Regional Flexibility**  
Each public safety region has the flexibility to choose an LTE prioritization model to suit its need. For example, region 1 may prioritize responders based on role and region 2 may prioritize responders based on application. The region should have some latitude to choose how to prioritize devices and applications on the regional system.
- **Roaming Support**  
Whether roaming between regional systems or roaming to a commercial LTE system, the prioritization framework can support a consistent and fair policy of mapping priority between systems.

The realization of this framework is standardization of LTE configuration parameters for public safety use, such as ARP, QCI, GBR, and MBR. ~~H.Appendix C~~ Appendix G lists the specific LTE system configuration necessary to achieve interoperable priority and QoS between two systems that are involved when roaming is utilized. The reader will appreciate that these recommendations must be consistently applied to all 700MHz commercial and public safety LTE systems in order to achieve meaningful interoperability.

## **A.7 Security**

---

Security is a critical aspect of the public safety broadband network solution. This section describes the comprehensive and interoperable security solution included in the offering.

### **Overall security architecture**

3GPP standards have defined a suite of security related specifications for LTE systems. The 33 series of 3GPP specifications contains several documents defining various aspects of LTE and broadband application security architectures. From an interoperability perspective, of particular

interest are the specifications 33.401 (“3GPP System Architecture Evolution (SAE); Security architecture”), 33.210 (“3G security; Network Domain Security (NDS); IP network layer security”), and 33.310 (“Network Domain Security/Authentication Framework (NDS/AF)”). The solution will fully support the requirements stated in these specifications to ensure secure inter-system interoperability.

The solution will support both the mandatory and certain optional aspects of the 3GPP SAE security architecture specification, as defined in 33.401. The optional aspects the solution considers mandatory align with recommendations given by the NPSTC Broadband Task Force. Specifically:

- Both control plane and bearer plane traffic will be encrypted over-the-air. This includes RRC signaling, NAS signaling, and user plane traffic.
- 33.401 requires the support of both the SNOW 3G and AES encryption algorithms. AES will be default choice in the solution, since it is a NIST/FIPS recommended algorithm for securing public safety communications.

The solution will utilize secure O&M protocols and methods to distribute software and configuration information to the network elements.

### ***Network Domain Security***

The solution will implement the 3GPP defined mechanisms for Network Domain Security, as defined in the 3GPP spec 33.210, “Network Domain Security, IP Network Layer Security”. Per 33.210, the interfaces between the network entities in the network are to be secured using IPsec security associations. The security associations will be established and maintained using either IKE (Internet Key Exchange)v1 or IKEv2. Per 33.210, the Za interface is used to interface between two security domains and the Zb interface is used to interface between the various network entities within a single security domain. Specifically:

- NDS/IP inter-domain interface (Za) cryptographic protection via Security Gateways (SEGs) will be provided. The Za interface security associations will be established using IKEv1 or IKEv2. X.509 digital certificate based authentication will be utilized between SEGs in different security domains.
- NDS/IP intra-domain interfaces (Zb) as specified in 33.210 will be cryptographically protected unless within physically secure and/or fully trusted environments.

### ***Inter-Domain Trust Establishment***

In order to facilitate interoperability for establishment of trust across potentially large numbers of public safety security domains, a scalable mechanism is needed for establishing security associations, whether at the network domain level or applications/services level. Digital certificates and Public Key Infrastructure (PKI) based trust management are the methods defined in 3GPP specification 33.310 for achieving these goals.

The solution supports the methods defined in 33.310 for creating, exchanging, and validating digital certificates across security domains. These mechanisms ensure that regional broadband networks have policies and protocols in place to establish a basic, interoperable authentication framework. As discussed in 33.310, the selection and design of the appropriate PKI based trust models will need to be made (e.g. the use of cross-signed certificates between the security domains vs. the use of a trust bridge model via Bridge CAs). In addition, work will be needed to define public safety specific certificate policies that further enable interoperability.

Coordinated certificate policies can help interoperability by defining common rules for the usage of digital certificates in a system. Some examples of policy parameters that are important to interoperability include:

- consistent rules on certificate issuance vetting and authentication
- agreed upon methods of safeguarding Certificate Authorities

- personnel security controls
- selection of public key crypto key sizes and algorithms

By having such policy elements consistent across systems, the difficult task of policy mapping between security domains can be minimized.

### ***MVPN Access to Home***

The Waiver requirements specify that petitioners' systems allow the use of network layer MVPN access to any authorized site and to home networks on the deployed network. This requirement is designed to ensure the ability of first responders to securely connect back to their home systems when attaching to foreign wireless networks. Without this requirement, there is the risk some deployments may have their wireless networks configured to discard any traffic that is encrypted and destined to an external domain. This would be very problematic, as there are security compliance policies by CJIS, and NCIC (National Crime Information Center) that require the use of VPNs for remote user access.

CJIS (Criminal Justice Information System) requirements mandate the use of FIPS 140-2 validated encryption. Thus any user of a deployment utilizing a broadband waiver must use FIPS 140 validated solutions to be compliant with CJIS security policy and to access CJIS related services. The solution will use FIPS 140-2 compliant MVPN solutions for remote user access.

### ***Application Security***

Application security is first provided by limiting access to authenticated users through the use of MVPN access to the home system. Once access has been authorized and secured, user authentication to specific applications such as the local status page will be required per local policy.

The specific authentication framework has not been specified by 3GPP or PSCR. The following represent the desired capabilities of the application authentication method ultimately selected.

- The security framework should provide authentication and authorization information between security domains (e.g. between Waiver Recipients)
- The security framework should provide single sign-on solutions that are compatible with existing commercial web browser user agents.

The use of a federated identity management solution enables portability of identity information across different agencies. This is essential to enabling many application security interoperability use cases. The creation of such a federated identity management solution is a work in progress. As such, the final solution should be specified with input from the public safety and vendor communities, with objective of identifying and deploying the appropriate solutions to meet Interoperability requirements.

## **A.8 Devices**

---

Delivery of user devices for Public Safety broadband agencies will be driven by the availability of an LTE chipset that supports standard 3GPP baseband protocols and RF operation in the 10 MHz of Public Safety spectrum (763 MHz to 768 MHz lower and 793MHz to 798 MHz upper). All devices will adhere to the 3GPP Release 8 air interface specification and the recommended out of band emissions (OOBE) as specified in the waiver order, as well as existing OOBE requirements to protect Public Safety narrowband voice services in the 700MHz spectrum. The following are the user devices intended for early deployment Public Safety LTE networks:

### ***USB-Dongle***

Initial trial and early deployment networks will be supported by a USB-dongle device suitable for external connection to a host personal computer. A broad range of Public Safety legacy IP data applications including Internet, Mobile VPN, CAD, mobile office, text messaging, location,

lookups, and records will be supported as well as uplink and downlink streaming video. The form factor of this device will follow commercial industry norms and be conducive to nomadic PC use both in and out of the vehicle.

The USB-dongle will support the 3GPP Release 8 standard interface to the LTE RAN, and operate as a 3GPP Power Class 3 device. The USB-dongle will be able to roam to other regional Public Safety LTE. Due to the physical size of the USB-dongle devices, the benefits due to 2X2 MIMO downlink will be limited.

#### ***Vehicle Modem***

The vehicle modem is an essential component for vehicle-based first responders and law enforcement officers in either urban/suburban or rural environments. It will support the 3GPP Release 8 standard interface to the LTE RAN, nominally as a 3GPP Power Class 3 device, and potentially at higher power levels, depending on final FCC rules relating to interference protection, and ERIC's endorsement. The vehicle modem, equipped with a set of external high gain omni-directional MIMO antennas, offers improved link budget and throughput performance compared to embedded PC or dongle solutions and is key to extending per site coverage range, particularly in rural environments. The vehicle modem will be able to roam to other regional Public Safety LTE networks.

The vehicle modem will be suitably rugged for cab or trunk vehicle mounting and support Ethernet-based wired computers and peripherals, as well as internal GPS capability. A broad range of Public Safety legacy IP data applications including Internet, Mobile VPN, CAD, mobile office, text messaging, location, lookups, and records will be supported as well as uplink and downlink streaming video from the vehicle.

The vehicle modem is intended to be managed remotely and upgradable over the air via standard means such as OMA-DM.

#### ***Smartphone***

A handheld device that operates on the PSST spectrum and serves as both a data and phone device is important to early Public Safety LTE deployments, particularly in urban/suburban environments where on-street or in-building portable coverage is provided. It will support the 3GPP Release 8 standard interface to the LTE RAN as a 3GPP Power Class 3 device, with internal MIMO antennas. The smartphone will be able to roam to other regional Public Safety LTE networks. The smartphone will have the capability of also roaming to a commercial network for data and telephony services as a backup to Public Safety LTE services.

A broad range of Public Safety legacy IP data applications including Internet, Mobile VPN, CAD, mobile office, text messaging, location, lookups, and records will be supported as well as uplink and downlink streaming video. The smartphone will be able to support VoIP services such as commercial PTT and telephony on the PS LTE network, as well as legacy circuit switched telephony. The device will be of a form factor suitable for belt or pocket, with user ergonomics as driven by the commercial market, but suitable for Public Safety use in a range of indoor and outdoor environments. Standard commercial capabilities such as a high resolution camera, GPS, Bluetooth, and WLAN will be supported.

The smartphone is intended to be managed remotely and upgradable over the air via standard means such as OMA-DM.

## **B. Applications**

---

The FCC has identified in their 10-79 order a list of minimum waiver applications potential waiver grantees must support. These applications provide the foundation for meaningful nationwide interoperability. This section will demonstrate how the waiver system will support these applications.

## B.1 Internet Access

---

Today, responders typically utilize their vehicle-docked Mobile Data Terminal (i.e. ruggedized laptop) to access the Internet over a secure VPN to their home agency Intranet. The responder's vehicle typically contains a 3G commercial cellular modem. In this usage model, a public safety responder "looks" like a mobile enterprise employee. An IT administrator from the agency facilitates the (M)VPN solution used in the vehicle and provides an agency Intranet. Like corporations, the agency Intranet contains valuable data and resources necessary for responders to do their job (as does the greater Internet). Also, the IT administrator:

- establishes policies as to which Internet sites may and may not be accessed
- logs responder activities on the Internet
- provides virus/firewall protection

As a technology, LTE provides 2 methods to access the Internet: (1) by the responder's home system (i.e. home routed traffic) and (2) by the roamed-to (visited) system (i.e. local breakout). The UE selects an access point name (APN) identifier and the EPC determines whether the APN is for home routed or local breakout traffic. **The system is configured to provide Internet Access by first accessing the responder's home system** (i.e. Internet/Intranet traffic is home-routed). This will allow the home agency to continue to support the above enterprise bullet points. This is accomplished by either adjusting the default APN in the responder's HSS record or by requiring the responder's home APN to be programmed into the device (and used during attachment).

Serving the Internet from a home APN lessens the need for additional APNs on the device. Each additional APN may imply the device connects to more and more network segments (and subsequently has multiple IP addresses); increasing complexity and security risks at the device. Therefore, home-routed Internet Access reduces the need for a "local APN" while roaming and improves security on the device.

If the responder's device is allowed to directly access the Internet from the visited system, it bypasses home agency logging, web-site policy, and firewall protections. This would be very harmful to public safety.

## B.2 VPN Access to Any Authorized Site and to Home Networks

---

The FCC has identified roaming onto commercial networks as an essential component for public safety to obtain the bandwidth it needs in a crisis. Further, connection to the commercial operator may likely traverse a roaming clearinghouse. In some cases, even the Internet may be used to carry public safety responder traffic whilst roaming. For these reasons, public safety should not expose control or media traffic to these untrusted networks. **A secure VPN or MVPN is provided for confidentiality and integrity of the responder's UE traffic.** If utilized, a matching device client may be necessary. A dedicated (M)VPN server may also be required and may be deployed with the EPC or agency, as the regional system dictates.

In addition to the description provided in the previous Internet Access section, it is important to note NPSTC's recommendation for VPN access cited secure access to public safety databases and agency reporting by way of the responder's home system.

## B.3 Status/Information "Homepage"

---

The Status/Information Homepage (SIH) builds upon the two previous features. **Access to the local SIH will be provided by way of Internet Access from the home system** (see reasoning in section B.1). Because the content of this web page is sensitive, it must be protected as it traverses un-trusted networks (see reasoning in section B.2).

The SIH is envisioned to provide home and roaming responders with incident-specific information, alerts, system status, weather, traffic, and other information. This information may

come from Computer-Aided Dispatch (CAD) terminals, responders, or in the future the NG911 ESInet.

Because routing to the UE's home system is assumed for Internet access the following techniques may be utilized to obtain access to a visited system's SIH:

- **Explicit Addressing**

The responder explicitly enters the URL (e.g. <https://publicsafety.charlotte.nc.us>) of the region they wish to connect with into their web-browser or selects from a pre-populated list of URLs in the browser. Although this requires responders to know the URLs, or the correct URL to choose, for the systems they wish to obtain information from, it is the most straight-forward approach. Additionally, a well-known national URL could be provided which contains links to all regional SIHs.

- **Location Mapping**

Responders attempt to access a well known URL and the home system uses location services to redirect the request to the serving region's SIH. This method would require some form of user location information, such as GPS coordinates or serving cell ID, to be provided to the home system. This also requires a supporting directory service which maps user location to status home page address.

**For initial deployments, the Explicit Addressing method is utilized until further standardization or policy definition is provided.**

Because the SIH will contain sensitive information and be accessed by many different responders (and roaming responders), **role-based authorizations are necessary to protect SIH content.** Because it is impractical for every SIH to contain subscription and authorization information for every public safety device in the U.S., a method is necessary to provide federated identity management to a SIH server in a visited system. The visiting responder's authenticated role must be known by the visited SIH and only information the responder is authorized for (based on role) should be presented. One such widely-adopted technique for providing federated identity management is the Security Association Markup Language (SAML) framework.

## **B.4 Access to Responders under the Incident Command System**

---

The National Incident Command System (NIMS) has defined the Incident Command System (ICS) to help quickly coordinate and organize mutual aid situations for typically large incidents. ICS offers many benefits including a command and control structure, common vocabulary, staging, incident action plan, and integrated communications.

Application servers used for Mutual Aid may be deployed in a variety of ways:

- by the region requesting mutual aid assistance
- by a hosting entity
- on the Internet
- by an on-scene command vehicle (see section 4.5)

Regardless of deployment, applications used for ICS access (such as an ICS server or mutual aid communications service) must be accessible by both home and roaming UEs in the public safety region where the incident is taking place. It may also be necessary for responders outside the incident region to access the Mutual Aid application(s). This requires the public safety region to support an IP plan with route-ability between these different application deployments and home/roaming devices. Techniques that will be required to support this include:

- Static IP addresses
- NAT/NAPT
- DNS
- IPv4v6 translation

## **B.5 Field-Based Server Applications**

---

Public safety today will deploy “command vans” and other tactical mobile vehicles to address specialized incidents, such as hurricanes. Typically, these vehicles use cellular technology as the “last mile” for an application server co-resident in the command van. Similarly, the LTE air interface will serve as “last mile” for field-based application servers (both fixed and mobile applications).

These application servers must be accessible by:

- responders homed to the same public safety region as deploying the application
- roamers in the same public safety region as deploying the application
- responders homed in other public safety regions or carriers
- Internet users with authorization

In order to achieve this, it is anticipated one or more LTE modems will exist in the command van. From LTE’s perspective, each modem will be treated as a UE (i.e. will have an IMSI, be authenticated, etc.), however HSS configuration will allocate the LTE modem a static IP address (part of a well-known local APN in the region). In order to be Internet-visible, this static IP address will have to be NATed to the larger Internet and Internet-visible DNS records must be created. In lieu of providing a static IP address for the command van modem, it is also possible to provide a dynamic IP address and utilize a dynamic DNS service (whereby the dynamic address is directly or indirectly Internet-routable). Such an approach may be more suitable for a command van that serves multiple regional systems. Finally, proper PCC configuration will be necessary to provide suitable “last mile” QoS resources using the LTE air interface.

## **C. Reliability and Availability**

---

The solution provides for high reliability and high availability for the following network components:

- Data Center and NOC
- LTE Enhanced Packet Core (EPC)
- Transport network
- Radio Access Network (RAN)
- Mobile and portable User Equipment

In addition, the solution also includes support for a MVPN which enables multiple access technologies, such as WLAN, 3G, and commercial carrier 4G networks. Please refer to section A.4 for additional information on the MVPN. The MVPN provides an additional level of disaster resilience by virtue of access to those networks, in that if a network becomes congested or goes down, Public Safety users will be able to obtain service on alternate surviving networks.

### **C.1 Regional Data Center and Network Operations Center**

---

In order to maintain service availability, the network has been designed with multiple layers of redundancy and resiliency. The network can be deployed such that module failures, node failures, and even failure of an entire data center site will not degrade network service availability. The Regional Data Center and NOC can be deployed in a fully-redundant configuration, such that a catastrophic failure of a data center location will not result in the loss of critical functionality, since all operations and traffic can be served by an alternate data center.

Network elements are modular and fault tolerant, providing advanced high availability features. The high availability elements contain internally redundant components which include:

- Redundant data path switch fabrics
- Redundant control path switch fabrics
- Multiple power supplies using separate power feeds and buses

- Redundant network processing modules
- Redundant application processor modules

Server redundancy is supported. In the event of a server failure, redundant server nodes are invoked. High availability network elements include load balancing for application processing modules. In the event of a failure of a module, traffic will be distributed over the remaining active modules. Modules are hot swappable, with repair and replacement taking place without disruption of normal operations. The re-initiation of the configuration and software takes place upon replacement of the module prior to being placed into service.

## **C.2 Enhanced Packet Core**

---

The EPC is comprised of the following standards-compliant network elements:

- Home Subscriber System (HSS)
- Policy and Charging Rules Function (PCRF)
- Serving Gateway (SGW)
- Packet Data Gateway (PGW)
- Mobility Management Entity (MME)
- Element Manager System (EMS)

These components are internally redundant and designed to provide robust hardware reliability and service assurance. The solution is able to support EPC component pooling to achieve a highly available and resilient system with disaster recovery capabilities. Operation and maintenance components can similarly be deployed independently in redundant and geographically diverse locations.

## **C.3 Transport Network**

---

Transport network resiliency is accomplished by enabling an IP mesh backbone network. As an analogy, the public Internet is highly available due to inherent mesh and/or ring connection of core routers. Additional resilience in the “last mile” links can be supported by deploying redundant links between the backbone and the network sites. Ethernet switches which comprise the transport nodes also use redundant hardware with dual homed switch ports. Failure of a switch or optical interface module will not result in the loss of traffic flow through the mission critical core. If any failures of switches, links or modules occur, traffic will be switched to a backup module or port. Interface redundancy allows backup links and ports. In addition, Metro fiber rings can be leveraged to connect the cell sites and data centers. Agency networks are equipped with redundant links to each of the data centers.

## **C.4 Radio Access Network**

---

The network site civil facilities are constructed according to industry best practice standards for:

- Building construction
- Seismic robustness
- Fire suppression
- Lightning and power surge protection
- Electromagnetic energy safety and interference management
- Power Utility service interconnect and backup power sources

The solution includes site hardening standards which cover the design, construction, and maintenance aspects for each of these disciplines.

The solution also leverages state-of-the-art system-on-chip (SoC) processors. These processors enable an exponential reduction of the number of chips and power consumption of electronic modules as compared to previous generation technologies. As a result, the Mean Time to Failure (MTTF) of electronic modules has increased significantly as compared to

previous generation technologies. This has enabled a reduction in the number of redundant modules while maintaining required levels of service availability.

In addition, the solution will include support for Cells on Wheels (COWS) provide coverage replacement and/or additional site capacity. This approach requires manual transport of the COWS to the target area. Therefore, this capability is targeted at planned events and large-scale incidents.

## **C.5 Mobile and Portable User Equipment**

---

The mobile and portable User Equipment (UE) are hardened in accordance with Public Safety best-practices. Generally, the eco-system for LTE 700 MHz broadband Public Safety UE's is still emerging. However, we expect that as the eco-system matures, a wide range of device capabilities will be available to Public Safety markets, spanning low-end commercial grade devices to high-end devices compliant with military-specifications.

## **D. Radio Frequency (RF) Engineering**

---

RF system performance factors such as coverage footprint, throughput, and capacity depend upon many different variables in RF design, including but not limited to the number of users, desired site density, system cost, traffic model, etc. As such, these variables are interrelated, so that changes in one variable inevitably impact the others. The City's system is designed to support current users and application in the most cost effective manner and the design is scalable for future expansion. The following paragraphs describe the tools and methodology used in designing this network.

### **D.1 Radio Access Network Planning**

---

The City's RAN design leverages extensive experience in modeling and designing wireless packet data networks, as well as extensive experience in RF propagation analysis.

The coverage prediction tools used in this analysis follow a two step process. First, an initial RF propagation analysis of the service area is performed using known models such as Okumura with shadow loss and TSB-88 statistical methods to provide a highly reliable prediction of coverage performance. Second, the tool performs a discrete event Monte Carlo simulation to model the LTE system based on current and future requirements. This detailed simulation characterizes the system performance and interference analysis based on a particular number of users and a traffic model. Coverage maps are based on these simulation results, which depict coverage at certain performance levels. Coverage maps for the City are provided in addendum of this document. Section D.1.4 of this document provides details of the traffic model used in our simulations.

#### **D.1.1 RF Propagation analysis**

---

The system is designed with coverage prediction tools, which were developed to provide an accurate prediction of radio coverage for a particular system by applying proven models to detailed system and environmental data across large geographical areas.

The system factors analyzed in the coverage modeling include: frequency, distance, transmitter power, receiver sensitivity, antenna height, and antenna gain. Environmental factors such as terrain variations, obstructions, vegetation, buildings, ambient noise, interference, and land-use in general are also taken into consideration for the analysis, using the data provided by environmental and topographical databases. Employing the knowledge gained from Motorola's many years of practical experience and coverage testing, these coverage designs are performed by computing coverage, and throughput on every tile in a defined service area, thus providing the most accurate coverage prediction and reliability results.

### **D.1.2 Network Capacity and Throughput Analysis**

---

The design methodology for the network was intended to meet, at a minimum, the current requirements of the City's member agencies. However, it is recognized that over time City's member agencies will require a more bandwidth intensive traffic model. Further, some member agencies may choose to limit use of commercial carrier networks thus changing the traffic model of the City's LTE network. With these goals in mind, the LTE network is designed to carry a certain amount of load per user per busy hour as explained in the "Modeling Assumptions" section below. This approach gives different member agencies the flexibility to vary the mix of application types that constitute this network load per user. It also allows the agencies to create a prioritization scheme and standard operating procedures that govern the use of fixed and shared resources in the network under normal and emergency conditions.

### **D.1.3 Scalability, expandability, and cost effective design**

---

In any wireless network, the goals of coverage and capacity are intertwined and inversely proportional. Keeping in mind the conflicting needs of a cost effective design and high capacity, the network design methodology allows City's member agencies the use of 4G type broadband applications while at the same time maximizing coverage from the available sites to ensure a cost effective solution. This approach anticipates the current capacity requirements and ensures the ability to add further capacity with the addition of sites in the future. The City anticipates the need for a larger number of sites over time to support extensive use of streaming video. Our design offers a flexible approach starting with an affordable network deployment optimized for coverage with a plan to build capacity as additional funding and capacity needs are identified.

### **D.1.4 Modeling Assumptions**

---

To date much of Public Safety wireless data usage has been limited to narrowband networks and few data points are available to shed light on Public Safety usage on 4th generation broadband networks. While commercial wireless data usage has been increasing significantly in recent years, the more recent widespread use of smart phones has provided some insights into potential data consumption on 4th generation broadband networks.

In order to arrive at a suitable broadband network profile for Public Safety, the City made certain assumption for traffic usage in the Charlotte area.

The following parameters were also used for this design:

- 95% area reliability.
- Coverage based on up to 4 retries.
- Mobile on street coverage using 23 dBm (200 mw) subscribers.
- 4050 concurrent users.
- Average cell edge data rates of 768 Kbps downlink and 256 Kbps uplink.
- 14.9 dB antenna gain at the eNodeB.
- Antennas heights ranging from 80 – 200 feet
- Single Frequency Reuse of the 10 MHz PSST spectrum in a 5+5 MHz configuration.

A list of initial planned sites and coverage maps is provided in addendum of this document.

## **D.2 Interference Coordination**

---

The solution will employ several techniques and features to mitigate interference among Band 14 eNB's within a region and with adjacent regions. These fall into two general categories: Network Planning and eNB Features. Note that Network Planning techniques may be applied to equipment from any vendor, and thus should be the first line of defense from an interoperability point of view. However, in a multi-vendor environment, eNB Features are dependent on vendor support for specific features and compatibility of the vendor implementations in terms of

strategies and optimizations as applied to intra-band interference mitigation. Thus it is possible that vendors of adjacent regions will be required to optimize and/or adapt their eNB feature implementations for interference mitigation compatibility. Below are techniques and features which may be employed in the system:

## **D.2.1 Network Planning**

---

LTE system capacity and coverage performance depend on interference levels; therefore, interference mitigation is a primary objective of LTE RF system design. Several measures are taken during the system design phase to mitigate interference including selecting appropriate antenna patterns, adjusting the individual sector antenna tilts, and selecting optimal site locations and site separation distances.

### **D.2.1.1 Site Separation**

An LTE system can be designed as noise limited or interference limited, depending on the separation distance between sites. In the case of a noise limited design, the coverage boundary is reached when the desired signal level is within a given threshold of the thermal noise floor. In contrast, when sites are deployed close together in a geographically contiguous manner, performance becomes limited by the co-channel interference as opposed to the thermal noise floor. The site separation distance also depends on the propagation environment and is selected to ensure that all coverage and interference requirements are met. Interference is attenuated more readily in environments where the propagation path loss slope is high and less readily in environments where the propagation path loss slope is low. The proposed vendor's LTE design procedure and tools account for these differences in propagation environment as well as the noise limited versus interference limited considerations when determining the optimal site locations and separation distances.

### **D.2.1.2 Antenna Down-tilt**

Down-tilting is the method of effectively adjusting the vertical radiation pattern of the antenna of the base station to direct the main energy downwards and reduce the energy directed towards the horizon. Down-tilting can be used to improve the level of coverage close to the site where "nulls" (e.g. coverage holes) may exist due to the effective height of the antenna. Down-tilting can also be used to reduce interference caused by reflections or undesired RF propagation beyond a predetermined footprint.

The final phase of the design process incorporates further detail into the design. This phase may include such items as collecting drive data to be used to tune or calibrate the propagation prediction model, and fine tuning of parameter settings, such as antenna down-tilting. This final design process is required in the deployment of a system. The main benefits of down tilting are:

- Control range of site
- Reduce energy at the horizon
- Maximize effective coverage closer to the site
- Reduce co-channel interference in adjacent sectors

The amount of down-tilt depends on the height of the antenna above the ground, the characteristics of the terrain, and the vertical beam-width of the antenna. The horizontal antenna beam width is selected to be narrow enough to limit interference between sectors yet wide enough to ensure reliable coverage. The vertical antenna beam width is selected to balance good coverage within the serving sector and interference mitigation to distant sectors. Antenna tilts are adjusted for each sector to optimize coverage within the serving sector while attenuating interference to distant sectors.

## **D.2.2 eNB Features**

---

### **D.2.2.1 Static ICIC:**

Inter-cell Interference Coordination (ICIC) is part of the 3GPP standards. It is recognized as a means to improve coverage and edge of cell performance. This feature is intended to minimize inter-cell interference by providing a fixed, static method of allocating resource blocks between cells within the system. This method relies exclusively on information contained in each eNB, and as such does not require the use of messaging across the X2 interface between eNBs nor does it require any kind of dynamic coordination between eNB scheduler processes. Another aspect of this static ICIC method is support for wideband and narrowband services by allowing the independent scheduler processes to allocate the entire channel bandwidth (all resource blocks) to a single user if needed. An important realization of the use of static ICIC methods is that the real-world traffic distributions are highly non-uniform spatially and temporally. The static ICIC method takes advantage of this non-uniform, time variant traffic to provide maximum coverage and performance for most scheduling opportunities by in essence providing frequency reuse in those situations. This static ICIC method may also be known as Preferred Frequency Reuse. The concept behind this method is to provide each cell with a list of preferred resource blocks for allocations and to make each cell's list unique to avoid interference with adjacent cells.

### **D.2.2.2 Semi-static ICIC:**

Semi-static ICIC is also part of the 3GPP standards. This feature is intended to minimize inter-cell interference by making use of 3GPP standardized messaging across the X2 interface between eNBs. Measurement reports exchanged between eNBs over the X2 interface can be used to support interference coordination in both the downlink and uplink. Semi-static ICIC relies on three types of measurement reports between eNBs. Reporting of Relative Narrowband Transmit Power (RNTP) between neighbor cells enables downlink ICIC. In the uplink, the standard supports reporting of a reactive Overload Indicator (OI), which indicates the level of uplink interference and noise. The standard also supports a second uplink indicator, High Interference Indicator (HII), which allows an eNB to report to neighboring eNBs that it will soon be scheduling uplink traffic by one or more cell-edge UEs in certain parts of the bandwidth. These three measurements can be exchanged on a periodic basis between neighboring eNBs to allow the eNBs to reconfigure their usage of Resource Blocks.

### **D.2.2.3 Frequency Selective Scheduling:**

OFDM systems can take advantage of frequency diversity and frequency selectivity gain via scheduler algorithms. Frequency diversity gain is achieved by allocating a UE in subcarriers spread across the entire carrier bandwidth. Frequency selectivity gain is achieved by allocating an UE a contiguous set of sub-bands within some fraction of the carrier bandwidth that is favorable to that UE based on narrowband fading conditions and/or interference. Frequency diversity scheduling may be preferred for users with high mobility while frequency selective scheduling is preferred for users with low mobility.

## **E. Testing**

---

This section of the document describes the activities associated with testing which validates key functionality, performance and interoperability requirements of the PS LTE solution. This is in addition to the extensive testing performed by the solution provider in their internal laboratories to ensure conformance of their LTE solution to 3GPP standards. An outline of this testing can be provided by our solutions provider. We as a Waiver Recipient are also planning to participate in the PSCR/DC demonstration network, starting in 2010. In order to meet the requirement of the Waiver Order, a trial activity will be planned using our selected PSLTE

solution. This trial activity will constitute and form the basis for initial testing of the system. This section provides an overview of the trial activities (initial testing).

The trial lifecycle is broken into four stages: Site readiness, installation activities, interoperability testing, and test execution for specific functionality and applications.

**Site Readiness:** This includes all activities related to preparing the chosen site(s) for equipment installation. Site readiness begins after the sites have been identified for the trial.

**Installation:** This includes all activities related to installing the trial equipment. This stage is started once site readiness has completed and ends when all the equipment associated with the trial network has been installed. This stage also includes any testing to verify that the equipment was installed correctly (ref Health Check).

**IOT:** This stage specifies the interoperability tests executed as part of the trial network. It includes all activities related to validating that other supplier components of the trial network are functioning correctly with our solutions provider’s components of the trial network prior to initiating trial testing.

There are two aspects of interoperability testing that must be addressed: 1) The Network, and 2) Devices. The network component validates that the other suppliers’ network elements are sufficiently functional with our selected supplier’s network components to initiate trial testing. The devices component validates that the devices used in the trial are sufficiently functional with our network components to initiate trial testing. The signaling procedures for the different interfaces will be tested using system level use cases as defined in the table below.

**Figure 1.0 Interface Procedure to System Use Case Mapping – S1**

Interface	Interface Specification Procedure	System Level Use Case
S1-MME	Reset	Link Management
	S1 Setup	
	Handover	S1 Based Handover
	E-RAB Setup, Modify, and Release	Dedicated Bearers
	Initial UE/Context	Attach, Detach, Authentication, TAU
	UE Context Request, Release Modification	Attach, Detach, Dedicated Bearers
	Uplink/Downlink NAS Transport, NAS Delivery/Error Indication	Attach, Detach, Authentication, TAU, Dedicated Bearers
S1-U	GTP Procedures	Link Management
	Bearer w/o Fragmentation	Uplink/Downlink Bearer Traffic
	Bearer with Fragmentation	Uplink/Downlink Bearer Traffic

The system level use cases that will be used to trigger and drive messaging for the IOT interfaces are detailed below:

S1-MME

- Link Management
- Attach
- Release
- Service Request
- Tracking Area Updates
- Detach
- Authentication
- Dedicated Bearers
- Handovers

S1-U

- Link Management
- Non-fragmented IP over GTP-U
- Fragmented IP over GTP-U

Uu-LTE: This is demonstrated using the devices. This will also have been demonstrated through device vendor specific IOT testing in the lab.

Test Execution: This stage specifies the functional and performance tests executed as part of the trial. This stage is started once interoperability testing has completed. The following aspects will be tested:

- Inter-Node Communication Verification
- Operations and Maintenance (OAM)
- Single User Stationary Calls
- Multiple Users Stationary Calls
- Single User Throughput vs. Mobility
- Single User with QoS
- Multiple Users with QoS
- Multiple Users Mobility with QoS

As part of the goal to achieve nationwide interoperability, the following applications and interfaces will be tested as part of the trial activities, with testing distributed over time and as the technology matures (features are added) and the standards evolve. The applications and interfaces to be tested in the initial trial timeframe (2010) are noted. The interfaces that are in support of the required roaming model will be tested in two ways. Those interfaces that are part of the roaming feature will be tested in our supplier's internal laboratory environment. As systems are deployed in the field, and as we encounter other vendors' equipment outside of our home network, we will actively work to conduct the proper IOT testing with that agency (local or regional) and their supplier to verify the implemented solution. In this way we will address the fundamental roaming requirement and in testing the interfaces (visited to home) listed below.

**Applications**

- Internet access (Initial Trial)
- VPN access to any authorized site and to home networks
- Status or information homepage
- Access to responders under the Incident Command System
- Field-based server applications (Initial Trail)

**Interfaces**

- Uu-LTE air interface (Initial Trial)
- S6a-Visited MME to Home HSS
- S8-Visited SGW to Home PGW
- S9-Visited PCRF to Home PCRF for dynamic policy arbitration
- S10-MME to MME support for Category 1 handover support
- X2-eNB to eNB (Initial Trial)

For the trial network, a configuration consisting of the following elements (in addition to tools and transport elements) will be used as the test bed: eNB, UE (USB dongle, VSM, and/or Handheld Portable, availability to be specified in our Roadmap over time), MME, S/P GW, and HSS/PCRF. The software used in the test bed and as part of the verification trial is compliant to 3GPP Release 8 of the LTE standard.

A listing of LTE test tools utilized by the solution is included in H.Appendix DAppendix-D.

## F. Deployment

The implementation plan involves several technical tasks directly related to the LTE system such as equipment installation, integration, optimization, and training. And in addition to those, there is also a civil work/site development component which includes site improvement at selected P25 sites (in order for those to sustain the added equipment), as well as construction of new monopoles at a number of Fire Stations. The timeline developed reflects a three (3) year schedule. This plan and schedule are subject to change pending FCC approval, NTIA grant, and final system design.

The exact phases and tasks are shown in the Gantt chart that is attached as an appendix to this document. The critical path is also depicted in the chart by the tasks shown in red.

The milestones for the main phases are planned as follows:

Contract Award	Year 1
Design Review Approval complete	Year 1
A&E (Architecture and Engineering) complete for Core Site	Year 1
Site Development complete for Core Site	Year 1
A&E (Architecture and Engineering) complete for eNodeB Sites	Year 1
Site Development complete for each eNodeB at existing Sites	Year 2
Equipment Factory Staging complete	Year 2
Ship Equipment to Field	Year 2
Site Development complete for each eNodeB at New Sites	Year 2
LTE Core Installation complete	Year 2
eNodeB Installation complete	Year 3
LTE Antenna System Complete	Year 3
Backhaul PTP Installation Complete	Year 3
Integration Complete	Year 3
Optimization Complete	Year 3
Training Complete	Year 3
VSM Installation Complete	Year 3
Final System Acceptance	Year 3

The proposed LTE system is designed to support 4,050 concurrent Public Safety users (distributed evenly across the network) and is capable of future expansion. The design utilizes 30 total sites; 24 Fire Station sites and 6 sites in the P25 Overlay. The design reuses existing sites to keep costs low. All Fire Station sites have 80' monopole towers. The existing P25 sites will use 100' at a minimum except the North site which will use antenna heights of 200' (assuming tower loading is not an issue at any of the sites). Site surveys will be performed to determine final heights in the system design. The system provides on-street coverage for users with edge data

rates at a minimum of 256 Kbps uplink and 768 Kbps downlink. The painted areas on the coverage maps (found as an appendix to this document) indicate 95% reliability (30 sites) modeling a 200mW in vehicle modem with external antenna. These system parameters are derived using a generic traffic model which is considered representative of typical Public Safety usage with 1 Mbytes of data transferred in the uplink per user and 3 Mbytes of data transferred in the downlink per user during the busiest hour of a shift. The Internet Peering Point for this LTE project will be the Meyers Site in Charlotte, NC. This location will provide all access to the City's network in addition to the connections to the internet. The backhaul requirement will need to be evaluated based on the required capacity needed to accommodate the 30 LTE sites. If capacity is exceeded a fiber connection may be necessary to meet the bandwidth needs. The Meyer's site will also be the location of any interfaces into Third Party Commercial service providers and/or local exchange/Central offices but details still need to be worked out with the various providers.

## **G. Operations, Administration and Maintenance**

---

The OAM&P solution is comprehensive and standards-based. It encompasses the entire lifecycle, including system design, assembly and staging, installation and commissioning, operations, optimization, and billing. The operations solution includes Fault Management, Configuration Management, Accounting Management, and Performance Management (FCAPS) support for the system infrastructure and devices, as well as the following advanced capabilities: **Network Management System (NMS)**. The NMS provides an integrated point of control for the system. It includes network monitoring and recovery, security monitoring, performance management analysis and reporting, integrated configuration management, and infrastructure software upgrade.

**Over The Air (OTA) Device Management**. The device management solution is an industry standard solution that works with any Open Management Alliance (OMA) client device. The solution Device Manager provides an easy-to-use interface to perform software upgrade, configuration and provisioning of a variety of public safety devices, including portables, vehicular modems, dongles, and mobile data terminals.

**Self Organizing Network (SON)**. The system SON solution, fully based on 3GPP standards, provides a self-configuring, self-healing, and self-optimizing RAN solution. System planning requirements are significantly reduced, as cell neighbors and LTE physical cell identifiers are automatically determined by the RAN infrastructure. Infrastructure equipment is automatically discovered and provisioned. The SON solution should simplify emergency coverage such as Cell On Wheels (COW). Key features of the SON offering include:

Automatic Neighbor Relations (ANR), which automatically determines the neighbors for each cell in the network, and continuously optimizes the neighbour lists.

Automatic Physical Cell ID (PCI), which automatically computes the LTE physical cell identifier for each cell in the network.

Automatic Load Balancing, which biases the handoff decisions based on the load presented in a particular cell.

Automatic Handover Optimization, which optimizes the handovers between cells to eliminate too-late and too-early handovers.

**Integrated Subscriber Provisioning**. The solution provides an integrated subscriber provisioning solution that simplifies the process of adding new broadband subscribers to the Regional Public Safety System and the Agency.

**Integrated Billing**. The system provides an integrated billing solution that supplies charging information, including the ability to support complex roaming and usage-based accounting. The billing solution provides robust data analysis, reporting, invoicing and data warehousing.

OAM&P exhibits the following points of interoperability:

- The self-organizing network (SON) consists of use cases and interfaces defined by 3GPP and algorithmic processing to be defined by each vendor. SON algorithm compatibility must be verified between vendors. Automatic Neighbor Relations (ANR) and Automatic Physical Cell ID (PCI) are two examples of SON algorithms that need to be verified for interoperability between LTE vendors. This interoperability must be demonstrated within a multi-vendor regional network as well as across regional boundaries.
- From a security perspective, the OA&M authentication and authorization framework utilizes industry standard secure protocols to enable operational access within the system. The interoperability solution leverages SSH , HTTPS and SNMPv3 to maintain confidentiality and integrity of management related information. User authentication and authorization is enabled through the use of LDAP and TACACS+. In addition, where web based UIs are provided, the Security Assertion Markup Language (SAML) is supported enabling single sign-on authorization across different administrative user interfaces within the system.
- Subscriber provisioning use cases and interfaces between the Public Safety Agency, Regional Public Safety Network and the Commercial Carrier Network must be formalized.
- Devices should be OMA-compliant in order to support standards-based device management.

## Appendices

---

### Appendix A. Definitions and Acronyms

---

ARP	Allocation and Retention Priority
BBTF	Broadband Task Force
CAD	Computer Aided Dispatch
CJIS	Criminal Justice Information System
DNS	Domain Name Service
EPC	Enhanced Packet Core
E-RAB	EUTRAN Radio Access Bearer
FIPS	Federal Information Protection Standards
GPS	Global Positioning System
GTP	Generic Tunneling Protocol
HAAT	Height Above Average Terrain
HO	Handover
HSS	Home Subscriber Server
ICIC	Inter-Cell Interference Coordination
IKE	Internet Key Exchange
IOT	Inter-Operability Testing
IP	Internet Protocol
IPX	IP Exchange (see <a href="http://www.gsmworld.com/our-work/programmes-and-initiatives/ip-networking/ipi_documents.htm">http://www.gsmworld.com/our-work/programmes-and-initiatives/ip-networking/ipi_documents.htm</a> )
LTE	Long Term Evolution
MBMS	Multimedia Broadcast Multicast Service
MME	Mobility Management Entity
MVPN	Mobile Virtual Private Network
NAPT	Network Address and Port Translation
NAS	Non-Access Stratum
NAT	Network Address Translation
NCIC	National Crime Information Center
NOC	Network Operations Center
NPSTC	National Public Safety Telecommunications Council
OAM&P	Operations, Administration, Maintenance, and Provisioning
OMA-DM	Open Mobile Alliance – Device Management
OOBE	Out of Band Emissions

PC	Personal Computer
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PGW	PDN Gateway
PKI	Public Key Infrastructure
PLMN ID	Public Land Mobile Network Identifier
PMIP	Proxy Mobile IP
PSST	Public Safety Spectrum Trust
PTT	Push To Talk
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RFI	Request for Information
RICS	Regional Interoperable Communications System
SGW	Serving Gateway
SIB	System Information Block
SON	Self Organizing Network
TAU	Tracking Area Update
TS	Technical Specification
TSB	Telecommunications System Bulletin
UASI	Urban Area Security Initiative
UE	User Equipment
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

## Appendix B. LTE/EPC Functions and Interfaces

---

This section provides a detailed description of the LTE RAN and EPC infrastructure elements, as well as their corresponding interfaces, and is provided as a supplement to sections A.1, A.2 and A.3.

**eNB** - The eNodeB (eNB) provides the user plane and control plane protocol terminations toward the UE. The eNB consists of the inter-working function between the backhaul interface and the base band interface, the base band processing elements for the air interface, and the radios.

- Radio Resource Management - Assignment, Re-assignment, and Release of radio resources
  - Radio Bearer Control (RBC) - Responsible for the Establishment, Maintenance, and Release of radio resources associated with specific radio bearers. The RBC function must maintain the quality of existing sessions when conditions change due to environmental and mobility activity.
  - Radio Admission Control (RAC) - Responsible for maximizing the radio resource utilization by intelligent admission or rejection of new radio bearer requests.
  - Connection Mobility Control (CMC) - Responsible for the management of radio resources during active or idle mode mobility of the UEs.
  - Dynamic Resource Allocation (DRA) - Packet Scheduler (PS) - Responsible for the scheduling of both user plane and control plane packets over the air interface. Scheduling takes into account QoS requirements of users, radio conditions, available resources, etc. to efficiently utilize the radio resources for all active users.
- MME Selection when UE initially attaches - A single eNB may have communication links to multiple MMEs. The controlling MME for each session must be selected if the UE does not indicate a specific MME to be used, or if the MME specified by the UE is unreachable.
- Routing user plane data to the SGW - A single eNB may have communication links to multiple SGWs. The data stream for each UE must be routed to the appropriate SGW.
- Scheduling and transmission of paging messages received from the MME.
- Scheduling and transmission of broadcast information received from the MME or configured from the Element Manager - The scheduling on the appropriate radio resource block and periodic broadcasting is performed by the eNB.
- Measurement gathering for use in scheduling and mobility decisions - Scheduling and handover decisions are performed based on uplink related measurement data from the eNB and downlink related measurement data from the UE. The eNB configures the measuring and reporting criteria and collects the data for input to the scheduling and handover functions.
- Radio Protocol Support
  - Radio Protocol Support
  - Physical Layer (Control and Bearer)
  - MAC (Control and Bearer)
  - RLC (Control and Bearer)
  - PDCP (Control and Bearer)
  - RRC (Control)
  - Session trace

- Inter-eNB handover preparation, Context & Buffer forwarding, Inter-cell interference coordination over X2 interface.
- eNB also forwards buffered downlink data during the Inter eNB handovers using non guaranteed delivery of user plane PDUs.

**MME** - The MME (Mobility Management Entity) manages authenticating users on the EPC and tracks active and idle users in the RAN. The MME pages users when triggered by new data arriving for an idle user at the assigned SGW. When a user attaches to an eNB, the eNB selects a serving MME. The serving MME selects a SGW and a PGW to handle the users bearer packets. The MME provides the following functions:

- Non-Access Stratum (NAS) Signaling. The MME is the termination point in the network for ciphering/integrity protection for NAS signaling and handles the security key management.
- Authentication: The MME is responsible for authenticating the UE by interacting with the HSS and is also responsible for the generation and allocation of temporary identities to UEs.
- Idle State Mobility Handling. The MME is responsible for idle mode UE tracking and paging procedure including retransmissions. The MME handles page request to its associated eNBs that contained the tracking area list last registered by the UE.
- EPC Bearer Control. The MME is involved in the bearer activation/deactivation process and is also responsible for selecting the SGW and PDN-GW for a UE at the initial attach, dedicated bearer activation, service request, and handover involving MME or SGW relocation.

**SGW** - The Serving Gateway terminates the S1-U interface towards EUTRAN and is also the local mobility anchor for the UE. The mobility anchor function applies to a mobile in the EUTRAN. In a commercial network, the mobility anchor also applies to a mobile transitioning from a non-3GPP network to a 3GPP network owned by the same operator. For each UE associated with the Evolved Packet System (EPS), at a given point of time, there is a single serving SGW. The SGW maintains a packet buffer for each idle UE and holds the packets until the UE is paged and an RF channel is re-established. The SGW maintains a connection to a PGW for each UE. The SGW provides the following functions:

- Local Mobility Anchor point for inter-eNB handover
- Packet routing and forwarding
- Assist the eNB reordering function during inter-eNB handover by sending one or more “end marker” packets to the source eNB immediately after switching the path
- E-UTRAN idle mode downlink packet buffering and initiation of network triggered service request procedure

**PGW** - The Packet Data Network Gateway (PGW) is the gateway which terminates the SGI interface towards the PDN (e.g. agencies network). The PGW is a macro mobility anchor and is responsible for UE address assignment. The PGW provides the following functions:

- The Packet Data Network Gateway terminates the SGI interface towards the PDN. The PGW supports connectivity of UE's traffic to specified interfaces based on APN (Access Point Name). The APN determines which PDN a UE is connected to.
- UE IP address allocation, DHCPv4 (server and client) and DHCPv6 (client, relay and server) functions
- The PGW is the source of service data flow based charging records for the UE.
- The PGW acts as the macro mobility anchor for the UE across EUTRAN.
- UL and DL bearer binding and UL bearer binding verification.

- Transfer of (QoS) policy and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the PGW. Policing and shaping the traffic rate of the user's downlink EPS bearers.
- Transport level packet marking in the uplink and downlink, e.g. setting the DiffServ Code Point, based on the QCI of the associated EPS bearer.

**HSS** – The HSS stores UE subscription and authentication data for authenticating/authorizing UE access. The HSS provides the following functions:

- Authentication and authorization data for the UE
- Location information of the UE (MME and PGW serving the UE)
- Lawful intercept support
- The HSS in the solution shares the UE subscriber database with the PCRF

**PCRF** - The PCRF provides network control regarding the service data flow detection, gating, QoS authorization and flow based charging (except credit management) towards the network element. The PCRF supports dynamic interfaces towards applications and a rule based engine that allows policy rules to be executed and the resulting policy passed to the PGW. The PCRF can pass both QoS and charging rules to the PGW. The PCRF uses the **SPR** (Subscriber Profile Repository) to store subscription profile records. The PCRF provides the following functions:

- PCRF decides how service data flows will be treated in the PGW, and ensures that the PGW user plane traffic mapping and treatment is in accordance with the user's subscription profile.
- PCRF will check that the service information is consistent with both the operator defined policy rules and the related subscription information. Service information will be used to derive the authorized QoS for the service.
- PCRF authorizes QoS resources. The PCRF uses the service information and/or the subscription information to calculate the proper QoS authorization (QoS class identifier, bit rates, etc.).
- PCRF can use the subscription information as basis for the policy and charging control decisions.
- PCRF supports different bearer establishment modes (UE-only, UE/Network or Network-only).

**Supported Interfaces:**

- **LTE-Uu** - This interface carries control and user (bearer) signaling between the eNB and the UE to facilitate the delivery of high speed data services to the end user. The associated control plane signaling supports mobility management, session management, admission control, QoS management, radio resource/connection management and all other functions that are necessary to enable the transfer of application data across the user plane.
- **Gx** - Provides transfer of (QoS) policy and charging rules from PCRF to the PGW.
- **Gz** - This interface is based on the GTP prime protocol. It is used to transfer Charging Detail Records (CDRs) from a PGW and/or SGW to a Charging Gateway in support of offline charging.
- **Rf/Ga** - This interface based on the DIAMETER protocol. It is used to transfer Charging Detail Records (CDRs) from a PGW and/or SGW to a Charging Gateway in support of offline charging.

- **Rx** – This reference point enables transport of application level session information from application to PCRF. Such information includes IP filter information to identify the service data flow and Media/application bandwidth requirements for QoS control.
- **S1-MME** - Control plane signaling between the eNB and the MME
- **S1-U** - Bearer plane support between the eNB and the SGW. In general, procedures for the S1-MME interface may affect the setup or teardown of a bearer link; however, the standards do not indicate specific procedures between the eNB and SGW. This path interface is for uplink and downlink data only.
- **S5** - The S5 interface provides user plane tunneling and tunnel management between SGW and PGW. It is used for SGW relocation due to UE mobility and if the SGW needs to connect to a non-collocated PGW for the required PDN connectivity.
- **S6a** - This interface enables the transfer of subscription and authentication data used for UE access to the LTE system. It carries control messages between the MME and the HSS over DIAMETER.
- **S8** – Roaming version of S5 for communication between a visited SGW and a home PGW.
- **S9** – The S9 interface is between a home PCRF and a visited PCRF in the case of local breakout.
- **S10** - This interface carries control messages between MMEs.
- **S11** - This interface carries control messages between the MME and the SGW.
- **SGi** - This interface carries bearer traffic between the UE and the agencies PDN. This interface optionally carries control traffic between the PGW and the agencies PDN to facilitate IP address allocation, IP parameter configuration and AAA services associated with UE activity.
- **SP** – This is a named interface between the PCRF and its subscriber database, the SPR. This interface is not standardized
- **X2** - The X2 interface provides a control plane and bearer plane connection between eNBs to support load management and handover procedures.

## **Appendix C. Priority Access and QoS Configurations**

---

### **G.1.1 General Priority Access and QoS Configurations**

---

When a responder roams from one regional system to the next regional system (or to commercial carrier network), there are certain parameters that should be standardized so that roaming QoS can be more easily facilitated. While it is possible for a for a home LTE system to map QoS policy for every unique roamed-to network, this is difficult to manage, and cumbersome at best. The need for standardized QoS parameters becomes especially needed for LTE “home routed traffic” (i.e. the use of the S8 roaming interface, which the FCC has required).

#### **Configuration – Implement the PCRF**

Inclusion of a Policy and Charging Rules Function (PCRF) is optional in LTE, however because of public safety’s desire to support session-oriented, QoS-enabled traffic, home routed traffic, and roaming to both public safety and commercial carrier network, a PCRF is essential. Complex policy rules that vary between PLMNs may also be needed, requiring a PCRF. For these reasons, all public safety LTE deployments should include a PCRF.

#### **Configuration – Public Safety First Responders Use Reserved Access Class 14**

LTE includes “Access Class Barring”, a method to prevent congestion of the control channel at busy eNBs. While assigning access class 14 to devices operating on a public safety system isn’t expected to offer a significant benefit (because most devices will be the same access class), access class 14 can be of significant benefit when public safety roams to commercial carrier networks because commercial users will typically be of lower access class(es). In order for this to be effective, access class 14 must be reserved for public safety usage. This configuration matches recommendations made by the NGN/GETS effort.

#### **Configuration – Standardize QCI Values across Public Safety Regional Systems and Commercial Systems**

The QoS Class Identifier is a scalar parameter that maps to QoS scheduling characteristics at the eNB (such as scheduling priority, packet delay budget, packet error loss rate, etc.) 3GPP TS 23.203 includes a table that maps standard QCI values to QoS attributes. When a UE roams, the QCI scalar is passed from the home to visited system. If the QoS attributes that map to the QCI scalar are different than the home system, this could result in poor (or no) application performance. It is key to require 3GPP standardized QCI scalars (and the QoS characteristics they map to) for public safety and commercial LTE systems. A “reserved for future use” QCI range is also established with all public safety and commercial LTE systems. This will allow future specialized public safety applications to be added.

The remaining configurations in this section focus on LTE’s Allocation and Retention Priority (ARP). The ARP includes 3 attributes:

- a. the priority a bearer will have for admission control at the eNB (and subsequently if it should be pre-empted at a future time)
- b. whether or not the bearer can be preempted
- c. whether when admitting the new bearer the eNB should attempt to preempt other bearers to make room for the new bearer

The remainder of this section focuses on ARP configurations. Figure 3.6.1-1 as a framework for how ARP can work between systems.

#### **Configuration – The Highest ARP Priority Should Be Reserved for Responder Emergency**

For both commercial carrier and Public Safety systems, standardization of this value insures the health and well-being of public safety and insures LTE resources are available under life-threatening conditions.

#### **Configuration – Standardize Number of ARP Priority Buckets**

Figure 5 suggests the possibility of four PS priority buckets (Responder Emergency, High, Medium, Low). The actual number of buckets is open to debate, however, the important point is once the number of buckets is chosen, the buckets must be available on both commercial and regional public safety systems. Defining a consistent set of ARP priority buckets facilitates inter-system QoS, which is essential to a consistent roaming experience.

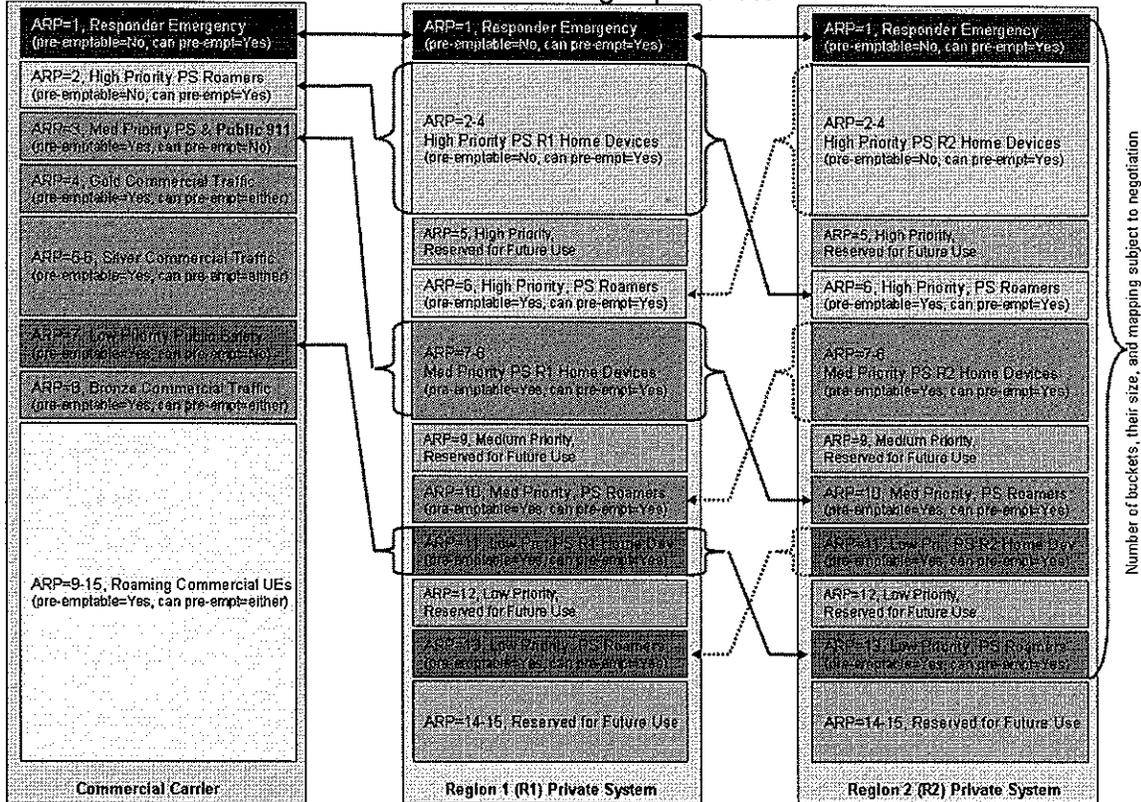


Figure 5: ARP Mapping Between Public Safety and Commercial Carrier Networks

### G.1.2 Roaming to Commercial Public LTE Systems

Configurations in this section apply to the case when a public safety device (home to a specific public safety regional system) attempts to roam to a commercial carrier network.

#### Configuration – Carriers Support All ARP Priority Buckets

After the number of ARP priority buckets is selected for use on regional public safety networks, then the same number of buckets should be available on carrier systems. When mapping ARP from a public safety regional system to a commercial carrier system, it is envisioned only 1 ARP priority will represent an entire ARP priority bucket on a public safety regional system because the carrier has additional constraints on ARP usage. For example, the LTE standard recommends ARP priority values 9-15 be reserved for public roamers onto public spectrum.

#### Configuration – Public Safety Bearers Associated with the Responder Emergency and High Priority ARP Values Should Not Be Preempted

Because public safety will require the use of carrier spectrum in many circumstances (i.e. because the PSST 5+5MHz capacity can be insufficient), bearers in these categories should be allowed to be established onto the commercial system and the bearers should be able to continue until de-activated by the responder.

#### Configuration – Public Safety Bearers Associated with the Responder Emergency and High Priority ARP Values Should Be Able to Preempt Other Lower Priority Bearers

Public safety using these higher priority ARP values must be allowed to instantly obtain resources as needed from lower priority commercial traffic (and even lower priority public safety traffic).

### **G.1.3 Roaming to Other Regional Public Safety LTE Systems**

---

Configurations in this section apply to the case when a public safety device (homed to a specific regional system) attempts to roam to an EPC serving another public safety region.

#### **Configuration – Allow Each Region to Use the ARP Priority Buckets to Fit Their Needs**

Within the confines of each priority bucket in the public safety regional network, public safety should be free to assign what UEs, applications, etc. map to each priority bucket. Today, some public safety systems prioritize based on application, and others based on responder role. Many agencies have expressed a desire for incident-based priority on LTE. This configuration gives public safety an excellent balance between regional flexibility (whether for incident, application, device, or other priority scheme) and inter-system roaming compatibility.

#### **Configuration – Public Safety Roamers Can Be Assigned to Each Priority Bucket**

In order to facilitate relatively consistent prioritization between public safety regions, it is expected that roamers between regional public safety systems be allowed to utilize each of the ARP buckets. For LTE home routed traffic, the home PCRF assigns the ARP priority of the bearer established in the visited system's eNB. For this reason, a consistent treatment of roamers is essential in the prioritization hierarchy.

#### **Configuration – A Roaming UE's Bearers may be preempted**

When a public safety UE roams to another public safety LTE system, the visited system should have ultimate control over its resources. For this reason, all bearers for roamers (other than the Responder Emergency bucket) may be preempted.

#### **Configuration - Public Safety Bearers Associated with the Responder Emergency and High Priority ARP Values Should Be Able to Preempt Other Lower Priority Bearers**

As with roaming to public systems, the use of higher priority ARP ranges must be allowed to instantly obtain resources as needed from lower priority public safety bearers.

## Appendix D. LTE Test Tools

LTE Test Tools		
Function	Tool (specified or equivalent)	Description
Spectrum Analyzer	Agilent SA	Cell coverage, characteristics
Air Interface Monitor	UE Tool Sanjole WaveJudge	Synchronization, system broadcast information, registration, DL/UL transfers
Network Monitor	Wireshark – Windows PC	Protocol dissectors to analyze L1/L2/L3, per segment
Service Simulator	Iperf – Windows PC	Service emulator using TCP and UDP pseudo packets and setting up bearer types and QoS over the air
Service Evaluator	Wireshark – Windows PC	Transport Quality (Loss, Latency, Jitter, Throughput), Handover Latency
UE	Available UE	Will be provided