State of Texas

Public Safety LTE
Interoperability Showing
Technical and Operational Response

September 2, 2011

Table Of Contents

A. Executive Summary

A.1 Introduction

This Interoperability Showing Technical and Operational Response is intended to demonstrate the technical and operational proficiency of the State of Texas (the “State”) necessary to achieve operability and interoperability of public safety broadband networks in accordance with FCC Waiver Orders adopted on May 12, 2010, December 10, 2010, and January 25, 2011, docket number PS 06-229. This document will also outline, to the extent they are understood at this juncture, the strategies, methods and processes the State of Texas intends to implement in order to achieve a statewide Public Safety Interoperable Long Term Evolution (LTE) network. Such a network would be realized through a fair and competitive procurement environment created by Public Safety agencies desiring to build-out in Texas. Approved agencies would be granted authority by the State of Texas through the Texas Department of Public Safety to construct and operate LTE layers under the broadband waiver granted to Texas by the Federal Communications Commission on May 12, 2011, and the FCC approved spectrum lease to Texas by the Public Safety Spectrum Trust (PSST), the nationwide licensee for the public safety broadband frequencies of 763-768/793-798 MHz.

As the state which has historically led the nation in annual federally-declared disasters, Texas is dedicated and committed to statewide cooperation and a collaborative effort in building and operating public safety LTE infrastructure to provide the highest level of prevention, protection, response, and recovery from acts of terrorism and other catastrophic events in the State and nation[1]. The State of Texas also commits in this showing, that it will ensure that early deployments within its borders will be consistent with current and future FCC orders relating to nationwide interoperability, serve as the state-level interface with the PSST and the FCC’s Emergency Response Interoperability Center (ERIC), and facilitate coordinated equipment development and purchases throughout the State.[2]

The State of Texas will deploy a 700 MHz interoperable public safety wireless broadband network which complies with FCC orders, and will implement the statewide network in phases, beginning with the BIG-Net[3] project as the first phase being implemented for the Houston metropolitan and coastal region. As such, implementation details of the BIG-Net project are included herein. Additional interoperability showings will be presented to the FCC in advance of construction of future infrastructure phases. The State of Texas will continue to promote a competitive multi-vendor environment for future phases of network implementation. The State of Texas will work closely with the Commission to ensure that compliance is maintained throughout each phase of the deployment and will submit interoperability showing updates and quarterly reports to the Commission. Indeed, the FCC acknowledged that “to the extent that

---

[1] *See Petition by the State of Texas For Waiver of the Commission’s Rules to allow Establishment of a 700 MHz Interoperable Mobile Public Safety Broadband Network*, filed by the State of Texas, Mike Simpson, September 10, 2010, page 4.

[2] *Ibid,* page 5.

[3] BIG-Net is the network name for the Broadband Interoperability Gateway Network.

Texas plans to deploy its network in phases, we expect that each phase would carry independent obligations to submit an interoperability showing under this Order".[4]

In summary, the State of Texas agrees and commits to remain subject to existing technical rules, the requirements of the *Texas Waiver Order* (11-863), the *Interoperability Order* (10-2342), the January 2011 *Third Report and Order, 4th NPRM* (11-6), the May 2010 *Waiver Order* (10-79) and any future rules which may be adopted in future proceedings.[5] A Commitment to Compliance summary is provided in Appendix F.

A.2 State of Texas Objectives for PS LTE

In recognition of the dramatic and potentially transformational benefit that Public Safety (PS) LTE broadband services will bring to its public safety users, the State of Texas has made the deliberate decision to pursue early deployments of PS LTE in Texas. This leadership is evidenced by the Texas Petition for 700 MHz waiver, the granting of such waiver by the Commission, the timely execution of a spectrum lease with the PSST, the FCC's approval of that lease, and the willingness on the part of a leading Public Safety wireless provider in the State, Harris County, to proceed with an early deployment once this interoperability showing receives Commission approval. In taking on the early deployment, the State understands this endeavor will result in additional risks, costs and burdens on State resources and projects. Other public safety agencies within Texas have indicated an eagerness to get started. The State is acutely aware of the critical need to guide and direct them toward a viable, interoperable solution. As a committed partner in the vision toward a National Public Safety Broadband Network, the State of Texas is willing to take on some of the initial burdens in order to put the technology into the hands of Texas' first responders sooner, and help pave the way for similar deployments across the nation.

The State of Texas recently released[6] a clear set of high level objectives associated with the early deployment of PS LTE. Those objectives have been refined further to read:

To create an effective and interoperable 700 MHz Interoperable Mobile Public Safety Broadband Network, which, when fully deployed, will enable public safety users operating in Texas to be safer, more responsive, and more effective in the saving of lives and property.

- To enable early deployments of interoperable 700 MHz PS LTE network layers in Texas.
- To facilitate an open, standards-based 3rd Generation Partnership Project (3GPP) LTE environment which supports a healthy, competitive multi-vendor procurement environment for network infrastructure and terminal devices, while enabling LTE suppliers to innovate and produce sustainable products and services.
- To support the eventual deployment of a Nationwide Public Safety Broadband Network by working closely with agencies within Texas, other states and jurisdictions across the country, federal agency partners such as the Commission, Department of Commerce, Public Safety Communications Research program (PSCR), DHS-Office

---

[4] *See Texas Waiver Order*, *Requests for Waiver of Various Petitioners to Allow Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks*, DA 11-863, PS Docket 06-229, May 12, 2011, page 5, footnote 33.

[5] *See Third Report and Order*, 11-6, PS Docket 06-229, January 26, 2011, ¶14. See also Waiver Order, Recommended Requirements, ¶ A.

[6] Released in documents related to the Region VI Public Safety LTE Interoperability Forum

of Emergency Communications, and of course, the nationwide network governance entity (NNGE), if and when it is formed.

- To aggressively explore possibilities for Private/Public partnerships in order to leverage existing commercial capabilities and associated economies of scale.

A.3 Multi-Vendor System Architecture Summary

The State of Texas is embarking upon a focused effort to determine an effective and manageable approach to incorporate multi-sourcing into the State of Texas PS LTE environment. The State will be gathering information from key industry players regarding which interoperability interfaces are most critical, where the risks are, and how these choices impact interoperability. Multi-source designs will be pursued at the Evolved Packet Core (EPC) core layer, and examined regarding the Home Subscriber Server (HSS) and the eNodeB layers. Especially for LTE device certifications, the State plans to lean heavily on the carriers and the PCS Type Certification Review Board (PTCRB) process also in development.[7]

The applications planned for the network are in their formative stages, and will be further refined as the needs and requirements of the end users are examined. For the first phase of BIG-Net, the initial LTE system roll-out will support: internet access, authorized VPN access, status/information homepage, ICS access, and field base data and server applications.

As the network expands and evolves, the State is looking toward a full range of potential applications, including: streaming video, video transfer, silent dispatch by CAD/MDT, location services, SMS/MMS, federal database access, fingerprint identification, automatic license plate reader, intelligent transportation systems, medical telemetry and access to hazmat, building plans and critical infrastructure information.

Implementing a network with the level of reliability and availability required by mission critical public safety networks requires a variety of approaches at all stages of network planning and maintenance. The State of Texas PS LTE network will provide high reliability and high availability components for all layers of the network: HSS, network operations center, EPC, WAN/transport, and the RAN/eNodeBs. The specifics of this design as it relates to the overarching multi-vendor architecture will be developed as part of the broader network design and requirements process.

All other aspects of the network design, including security services, authentication, encryption, RF design, RF coverage, and interference, will be approached per the guidance and recommendations of the Commission, PSST, ERIC, National Public Safety Telecommunications Council (NPSTC), PSCR, and DHS-OEC among others.

More technical details on these and other topics are provided in the sections below.

[7] *See Interoperability Order*, 10-2342, ¶18.

A.4 Summary

In summary, it should be emphasized that the State is in an early stage of project planning. As directed by the original Waiver Order[8], the State of Texas will submit quarterly reports to provide progress on the planning, funding, deployment and interoperability testing. The following sections provide more detail on the programs we have undertaken to begin the network design, demonstrations, trial network, and planning efforts.

The State would like to once again emphasize the deep commitment toward developing the strategies, programs, and processes needed to ensure that the State of Texas Public Safety LTE network is compliant with 3GPP LTE standards, that it is fully interoperable with a nationwide network, and that it be deployed and managed in a way that allows the State to sustain and evolve its interoperable capabilities.

B. Processes for Establishing and Sustaining Interoperability for PS LTE

The most central questions posed by the request for an Interoperability Showing involve precisely how the State of Texas will develop the multiple processes needed to design, procure, implement, and sustain an interoperable network, all while maintaining the appropriate autonomy and specific needs of public safety partners and users. Especially during early deployment phases with the greatest uncertainty, the State will be working closely with all of its deployment partners to ensure they meet the requirements and policies set forth by the State and the Commission. Without such compliance, as the designated 700 MHz waiver recipient and PSST spectrum lease holder, the State would have the right to withhold approval to constituent jurisdictions to operate on the broadband frequencies of 763-768/793-798 MHz.

B.1 Intra-State Processes

Thus far, the State of Texas has identified the following process development initiatives for establishing and sustaining interoperability among agencies within the State ("intra-state"). Associated milestones are shown in the State of Texas Milestone chart in Appendix B.

- **Individual Jurisdiction Application to Texas Department of Public Safety (TxDPS) to Host a Public Safety LTE Broadband Layer in a Given Geographic Area of Texas** – A jurisdiction wishing to host a public safety LTE broadband layer in a given geographic area of Texas shall make application to TxDPS. Applicant shall, at a minimum, provide: 1) A summary of major elements of the applicant's LTE broadband plan, identification of the proposed geographic area to be covered, and an explanation of how all eligible entities within the proposed LTE broadband geographic footprint were given an opportunity to participate in the planning process and to have their positions heard and considered fairly, and whether such entities endorse the application to TxDPS; 2) Records of open meetings held by applicant with eligible entities, including dates, times, and locations of meetings, meeting agendas, meeting notes, names of individuals invited and individuals in attendance,

[8] *See Waiver Order, Requests for Waiver of Various Petitioners to Allow Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks*, May 12, 2010, PS Docket 06-229, ¶64.

individual titles, agency names, agency addresses, phone numbers, and individual email addresses; 3) Details of applicant's proposed funding and construction plan with identified timeline and milestones and 4) Technical information necessary to support Home Routing and Local Breakout access. TxDPS will work in close coordination and constant consultation with the Harris County BIG-Net leadership and management team, for both the development of the detailed processes as well as the implementation of any connectivity and roaming programs. The State of Texas will submit an updated *Texas Interoperability Showing* to cover any new proposed additions to the State network under the *Texas Waiver Order*.[9]

- **Texas DPS has notified representatives of the 24 Texas Councils of Governments, and the major metropolitan areas, concerning the FCC broadband waiver to Texas and what it means.** Broadband presentations were made by TxDPS at the annual Texas Homeland Security Conference in April, 2011, and to two FEMA Region VI Regional Emergency Communications Coordination Working Group meetings. Additional outreach regarding the above-mentioned application process will be made to Texas public safety jurisdictions at future conferences and meetings across the state, and through regular electronic message updates.
- **Participation in the PSCR Demonstration Network** – Any manufacturer wishing to sell infrastructure equipment to the State of Texas (or a local Texas jurisdiction) to become a part of the Texas PS LTE network must have sufficient proof or certification that the manufacturer is "participating" in the PSCR demonstration network program.
- **State of Texas PS LTE Architectural Requirements & Guidelines Process** – The State of Texas will develop design guidelines by December 1, 2011 for public safety entities wishing to consider procurement of a Public Safety LTE infrastructure layer.
- **Conformance, IOT, and End-to-End Validation Plan** – As described in the Testing section below, the State will support all aspects of conformance and IOT on all operational devices as required ensuring compliance with applicable standards. The State will also perform End-to-End Validation testing. No device model will be allowed on the network without passing the required tests, performed by an authorized or accredited entity.
- **Interoperability Monitoring, Issue Tracking, and Escalation Service Plan** – Once the systems are deployed, the State will establish within a consolidated customer service center, the ability to handle complaints or problems experienced by users accessing the Texas PS LTE network. This special "help desk" program will ensure that these issues are properly diagnosed and resolved. A process of escalation to upper management of the Texas Department of Public Safety will also be set forth.
- **Special-Handling for the City of San Antonio** – The State is in direct discussions with the City of San Antonio, the only other FCC broadband waiver recipients within the State, as to how a potential future City of San Antonio LTE layer would integrate into the LTE infrastructure to be constructed under the Texas waiver authority. Such an arrangement would be consummated with an "inter-government agreement."

[9] *See Texas Waiver Order*, *Requests for Waiver of Various Petitioners to Allow Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks*, DA 11-863, PS Docket 06-229, May 12, 2011, page 5, footnote 33.

These discussions are slow-moving at present, as the City of San Antonio has not yet identified sufficient funding for build-out.

B.2 Inter-State Processes

This section outlines a high level process for how to establish and sustain interoperability with entities which are outside Texas and therefore require an inter-state process.

The State of Texas realizes that the facilitation of effective Inter-State interoperability processes demands a full commitment to interoperability by the State of Texas. As described in this document, the State of Texas remains fully committed to complying with interoperability requirements expected, so that the State not only stays symmetrical with other interoperating entities, but also continues to support the nationwide goals and objectives.

- **Requirements on Other FCC 700 MHz Broadband Waiverees to Connect to the Texas PS LTE Network** – Out-of-state FCC 700 MHz public safety broadband waiverees wishing to connect to the Texas PS LTE network shall make a request to TxDPS, in which the requester shall include, at a minimum, documentation proving that requester: 1) Has been granted an FCC 700 MHz public safety broadband waiver for a specific geographic area; 2) Has a valid spectrum lease with the PSST, which has been approved by the FCC; 3) Provides technical information necessary to support Home Routing and Local Breakout access and 4) Agrees to conform with all current and future FCC orders pertaining to 700 MHz public safety broadband interoperability. The State will directly inform current and future FCC broadband waiverees on how to make a request to the State of Texas through TxDPS, and provide regular feedback as to the status and progress of their request. TxDPS will work in close coordination and constant consultation with the Harris County BIG-Net leadership and management team, for both the development of the detailed processes as well as the implementation of any connectivity and roaming programs.

It shall be emphasized that while specific information is required to support interoperability from an external entity, per the Waiver Order and ERIC guidance, the State of Texas agrees and commits to honoring roaming and access requests from any qualified entity.[10] Additionally, the State agrees to refer the matter to the Bureau if an agreement with the outside entity cannot be reached within ninety days.

C. System Architecture Overview

The State commits to a uniform deployment of at least 3GPP standard Evolved Universal (or UMTS) Terrestrial Radio Access (E-UTRA) Release 8 and associated EPC, prior to the date of service availability.[11] Additionally, the State commits to deploying LTE such that backward compatibility between all subsequent releases from Release 8 and onwards is ensured.[12]

The Broadband Public Safety implementation is based on the 3GPP LTE standards, and consists of the Radio Access Network (RAN), the EPC, the LTE devices, and the key interfaces exposed by these components. The implementation includes the ability to roam between

---

[10] See *Interoperability Order*, DA 10-2342, PS Docket 06-229, Recommended Requirements, Public Safety Roaming on Petitioners' Networks, ¶ A.

[11] *See Third Report and Order*, 11-6, PS Docket 06-229, ¶10.

[12] *Ibid,* ¶11.

systems, provide priority access and quality of service (QoS) to ensure the most critical public safety users receive the highest priority, and ensure the Broadband Public Safety implementation is secure.

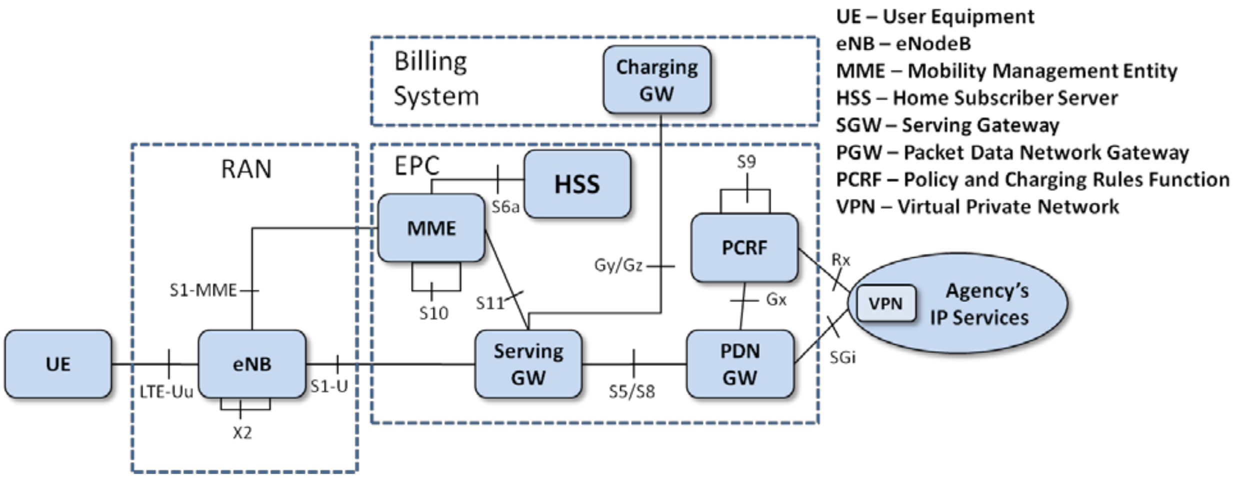


Figure 1 - Logical Architecture

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 Appendix C.

C.1 Radio Access Network (RAN) Architecture

The eNodeB (eNB) is the only 3GPP defined network element within the EUTRAN. The eNB provides the user plane and control plane protocol terminations toward the User Equipment (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 Release 8 and Release 9 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 Technical Specification (TS) 36.300. The RAN implementation for this system will be compliant with, at a minimum: 36.104, 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 3GPP Release 8 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.

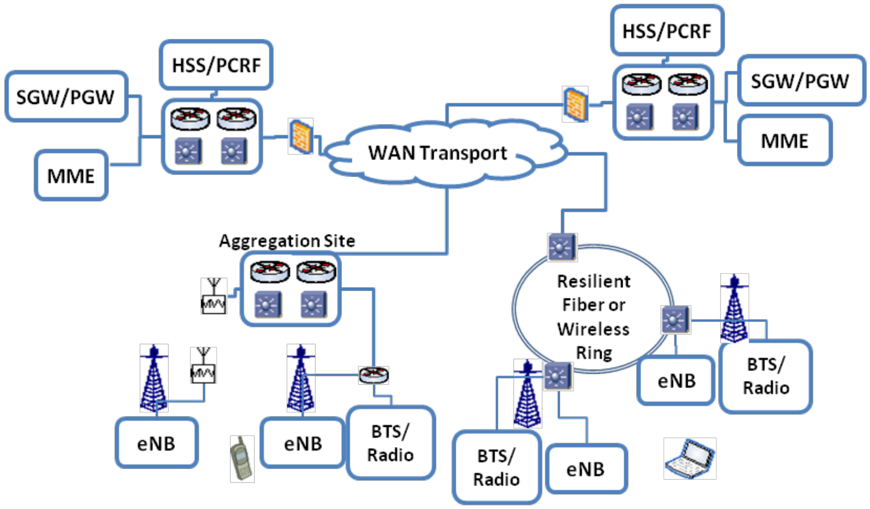


Figure 2 – RAN Physical Architecture

The RAN implementation is based on IP transport. The implementation supports collocation with existing narrowband or commercial sites and supports various types of backhaul transport mediums. The equipment supports the logical User Plane, Control Plane and Operations, Administration, Maintenance, and Provisioning (OAM&P) interfaces on the same physical interfaces and supports Virtual Local Area Network (VLAN) separation. The eNB hardware supports 5+5 MHz PSST band or 10+10 MHz D/PSST band or both D and PSST 5MHz bands simultaneously. The eNB is built with Self Organizing Network (SON) functions to automate deployment and optimization functions. The implementation will support both GPS and IEEE 1588v2 timing solutions as needed.

C.2 Core Network Architecture

The core network is based on the 3GPP R8 defined EPC as mainly defined in 3GPP TS 23.401. The solution will support the MME, SGW, PGW, HSS and PCRF 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 (e.g., WiFi and 3G).

The EPC implementation is based on the (Generic Tunneling Protocol) GTP-based S5 and S8 interfaces. The EPC implementation is compliant with specifications 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 3GPP Release 8 specification versions and beyond.

Additional interfaces supporting charging are supported. The PGW and SGW can support both online (Gy) and offline (Gz) charging interfaces.

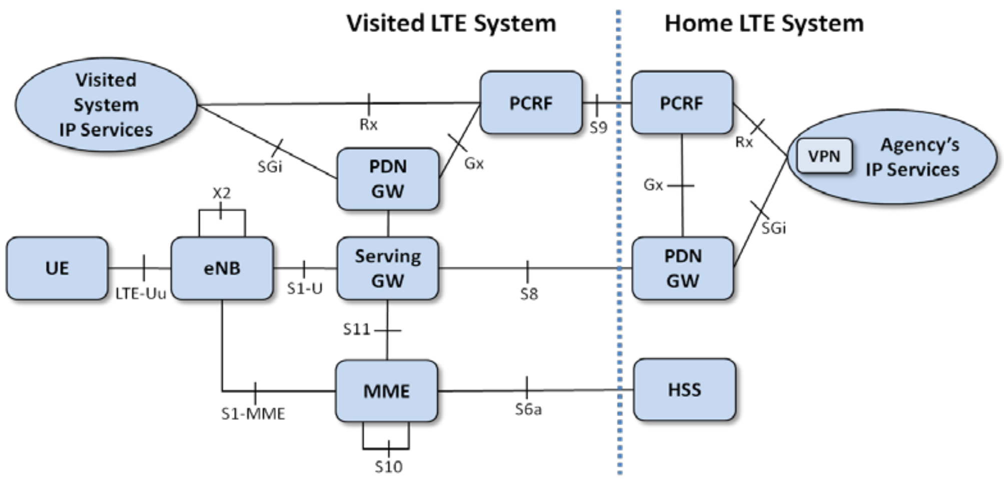


Figure 3 – EPC Roaming Architecture

The system is capable of supporting roaming with other regional PS LTE systems and with commercial LTE systems (if supported by the device capabilities).

The EPC physical architecture is shown in Figure 4. The EPC solution is based on IP transport and pooling of network elements. The EPC has been centrally located to help facilitate statewide deployment and minimize the risk of natural disasters. To minimize backhaul traffic an additional SGW/PGW has been deployed in the Harris County region for localized connection to the RAN. The solution supports IPv4 and IPv6 UE's and additional IPv6 network interfaces as a future software upgrade. Redundancy is supported at several levels including geographically distributed elements to mitigate disaster scenarios. The HSS and its associated subscriber database will be duplicated across geographic locations. The primary Network Operations Center functions (NOC) for the LTE System will be located in an existing Harris County facility. The redundant NOC will be located in the City of Austin in an existing Department of Public Safety facility.

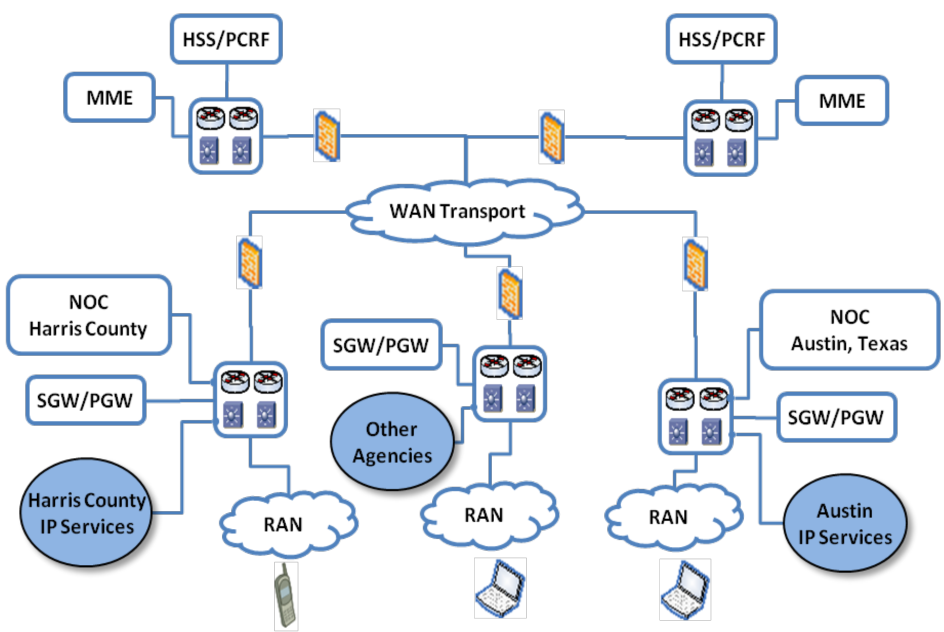


Figure 4 – EPC Physical Architecture

C.3 Interfaces

Prior to the Date of Service Availability, the State of Texas agrees to support the following interfaces as defined by the 3GPP Standard[13]:

Uu – LTE over the air interface

S1-MME – eNb and the MME

S1-u – eNb and the SGW

S5 – SGW and PGW

S6a – Visited MME and the Home HSS

S8 – Visited SGW and Home PGW

S9 – Visited PCRF and Home PCRF

S10 – MME to MME for Category 1 Handover

S11 – MME and SGW

SGi – PGW and external PDN

X2 – eNodeB to eNodeB

Gx – PGW and PCRF

Rx – PCRF and AF located in PDN

Gy/Gz – online/offline charging interfaces

These interfaces support interoperability of the LTE network with 3GPP R8 December 2009 freeze or R9 September 2010 freeze compliance. These standards apply to UE devices, as well as interoperability with other PS regional LTE networks. Details on handoff and mobility inter-operability are addressed in Section C.4 including mobility across regional PS LTE networks. Details on supporting a VPN service are also covered in Section C.4.

C.4 Mobility and Handover

The State of Texas commits to supporting mobility and handover, such that users have a smooth and seamless transition between eNode sites wherever possible. The handover functionality can be supported using one of the many options available in the LTE architecture.[14] These functions will be supported via 3GPP standardized interfaces. In addition, careful planning, configuration, optimization, and maintenance will be managed to achieve optimum handover performance. The mobility implementation accommodates both active and idle mode handovers within LTE networks. These aspects are discussed in more detail in the following paragraphs.

C.4.1 3GPP Compliant Handover

The mobility implementation is fully compliant with 3GPP standards. It supports high-speed mobility and seamless handoffs between eNBs within the Broadband Network. Radio frequency

[13] *See Third Report and Order*, 11-6, PS Docket 06-229, ¶12.

[14] *See 4th NPRM*, 11-6, PS Docket 06-229, ¶¶47-8.

phase shift acquisition up to 300 Hz Doppler can be supported, which accommodates handoffs above 75 mph in a properly-engineered and maintained network.

C.4.2 Adjacent Network Handover

The mobility implementation can support inter-network handover between regional public safety networks.

If all networks are allocated a common or single Private Land Mobile Network Identifier (PLMN ID), then issues associated with inter-PLMN handover are avoided. However, in this case there must be a nationwide network planning, operations, and maintenance authority. The authority would be required to coordinate cell identifiers, eNB neighbor lists, network interconnections, and handover configurations across the regional administrative domains.

If the regional networks are allocated different PLMN ID's (see Section C.5) then inter-PLMN handover capabilities will be required as regional networks expand and become adjacent. In this case, nationwide network planning, operations, and maintenance are avoided. Instead, network planning and coordination is limited to RF planning along geographic borders between regions. The network interconnections are minimized and can leverage industry standard roaming interfaces.

The State of Texas is working with the public safety and vendor communities to deploy an interoperable implementation supporting adjacent network handover.

C.4.3 Mobile VPN

In addition to handover, the implementation also supports Mobile VPN (MVPN). MVPN implementations provide application-level session continuity across disparate radio access networks, as well as security between the UE and the agency application domain. Session continuity is supported at the application IP layer, which is above the radio access layer. Thus, the MVPN implementations 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 optimum radio link is selected 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 a solution for mobility across disparate radio access 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 technologies 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.

C.5 Roaming

Roaming is the ability for a user to obtain service in a visited network. Roaming will be supported with other regional networks across the nationwide Shared Wireless Broadband Network (SWBN). These requirements are supported by leveraging 3GPP standardized interfaces, as well as adoption of a roaming services tailored to the SWBN.

C.5.1 PLMN ID Assignment

The NPSTC Broadband Task Force report[15] recommends that the number of PLMN ID's allocated for the SWBN should be less than 100 ID's, and may be as few as one ID. The implementation will support this recommendation, and can be adjusted to accommodate the PLMN ID allocation for the SWBN.

The State of Texas hereby commits that the implementations of the PLMN ID for the State of Texas can be and will be adjusted as necessary to accommodate the nationwide PLMN ID plan currently in development. As directed by the *Interoperability Order,* the State will submit notice to the FCC of the need for a PLMN ID at least 90 days prior to the planned date of service availability.[16]

C.5.2 Intra-system Roaming

Intra-system roaming occurs when users obtain service from a visited regional network within the SWBN which is not the user's home network. The implementation will support intra-system roaming.

C.5.3 Inter-system Roaming

Inter-system roaming occurs when users obtain service from a commercial carrier network, which is not part of the SWBN. The implementation will support inter-system roaming as enabled by roaming agreements with one or more commercial carriers.

Commercial carriers typically leverage roaming service providers to provide inter-network connectivity, security, and billing 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 a number of regional network entities comprising the SWBN. Therefore, it may 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.

C.5.4 Roaming Interoperability

UE's conforming to 3GPP standards will be able to roam across regionally deployed networks. However, it is essential for the UE's 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

[15] *See NPSTC Broadband Task Force Report*, September 2009, Section 6.3.1.

[16] *See Interoperability Order, 10-2342,* ¶16 and Appendix A, ¶C.

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.

C.5.5 Roaming Configurations

The State of Texas commits to supporting home-routed traffic, such that a "visiting" user's traffic is routed back to the home network to enable the use of visitors' home resources.[17]

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 State of Texas commits to supporting local breakout traffic, such that a "visiting" user is able to utilize the resources of the State of Texas PS LTE network.[18] 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.

C.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. The State of Texas is working with the public safety and vendor communities to contribute to the development of interoperable priority access and QoS requirements. The implementation will be compliant with 3GPP TS 23.203. All of the (QoS Class Identifier) QCI (1-9) and (Allocation and Retention Parameters) ARP (1-15) values defined in this specification will be supported in the deployed equipment. In addition, all of the Access Class (0-15) values as defined in TS 22.011 will be supported.

A flexible priority access and QoS framework is provided by the implementation. Principles of the framework are as follows:

- **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 includes adoption of LTE configuration parameters for public safety use, such as ARP, QCI, GBR (Guaranteed Bit Rate), and MBR (Maximum Bit Rate),

---

[17] *See Interop Order,*¶10 and Appendix A, ¶A

[18] *Ibid*, ¶9 and Appendix A, ¶A

Framework adoption must be consistent across all 700 MHz public safety LTE systems in order to achieve meaningful interoperability. Deployments in the State of Texas will be adjusted to comply and adapt with the eventual nationwide framework for Priority Access and QoS, once it is established.

C.7 Security

Security is a critical aspect of the public safety broadband network implementation. Therefore, the State of Texas commits to supporting the optional security features specified in 3GPP TS 33.401, which include integrity protection, verification of data and ciphering and deciphering of data. The State also commits to supporting network layer VPNs.[19] This section describes the comprehensive and interoperable security implementation in the State of Texas network.

C.8 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 implementation will fully support the requirements stated in these specifications to ensure secure inter-system interoperability.

The implementation will support both the mandatory and optional aspects of the 3GPP SAE security architecture specification, as defined in 33.401.The optional aspects 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 Radio Resource Control (RRC) signaling, Non Access Stratum (NAS) signaling, and user plane traffic.
- Both SNOW 3G and AES encryption algorithms will be supported. AES will be default choice in the implementation, since it is a NIST/FIPS recommended algorithm for securing public safety communications.

The implementation will utilize secure operations and management protocols and methods to distribute software and configuration information to the network elements.

C.9 Network Domain Security

The implementation will utilize 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:

---

[19] *See Interoperability Order, 10-2342,* ¶25 and Appendix A, ¶J. See also *Waiver Order*, ¶47.

- 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.

C.10 MVPN Access to Home

The Waiver Order requires petitioners' systems allow the use of network layer VPN 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 implementations to be compliant with CJIS security policy and to access CJIS related services. The implementation will use FIPS 140-2 compliant VPN solutions for remote user access.

C.11 Devices

Delivery of user devices for Public Safety broadband agencies will be driven by the availability of LTE chipsets supporting 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 or later 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.[20] In addition, all devices deployed after the system achieves service availability will be FCC Type approved. Frequency bands planned for the deployed devices are discussed in Appendix H. The following are examples of user devices intended for deployment in the State of Texas Public Safety LTE network:

C.11.1 USB-Modem

Initial trial and early deployment networks will be supported by a USB-modem 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.

[20] *See Waiver Order*, 10-79, ¶¶43-4.

C.11.2 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. 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 USB solutions and is key to extending per site coverage range, particularly in rural environments.

The vehicle modem will be suitably rugged for cab or trunk vehicle mounting and support Ethernet-based wired computers and peripherals. 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.

C.11.3 Smartphone

A handheld device that serves as both a data and phone device is important to Public Safety LTE operations, particularly in urban/suburban environments where on-street or in-building portable coverage is provided.

D. Applications

The FCC Waiver Order has identified a list of minimum applications that waiver networks must support. These applications provide the foundation for meaningful nationwide interoperability. Consistent with the *NPSTC Broadband Task Force* report, and to support a common set of applications for the nationwide network, the State of Texas commits to deploying, at a minimum, the following applications and services on the PS LTE network: authorized VPN access, Status Information Homepage, access to users under ICS and field-based server applications.[21]This section will explain how the State of Texas network will support these applications.

D.1 Internet Access

Initially, internet access will be hosted in Harris County. The implementation will support two 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 associated with the Internet Access host network and the MME determines whether the APN is for home routed or local breakout traffic. This is accomplished by either configuring a default APN in the subscribers HSS record or by requiring the Harris County APN to be programmed into the devices.

D.2 VPN Access to Any Authorized Site and to Home Networks

A secure VPN or MVPN may be implemented to support confidentiality and integrity of the responder's UE traffic. A corresponding device client may be necessary. A dedicated (M)VPN server may be deployed in an authorized site or in an agency home network, as the regional system dictates. An essential component of providing VPN access to any authorized site and to a home network is a network routing configuration which can support security, QoS, and network resiliency requirements. The State of Texas implementation will include support for

[21] See *Waiver Order*, 10-79, PS Docket 06-229, ¶46.

each of these aspects via NetMotion Wireless (www.netmotionwireless.com) mobility products with other qualified vendors being added as the program proceeds.

D.3 Status/Information Homepage

The State of Texas network will provide the necessary functions to support the Status/Information Homepage (SIH) application. 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.

The SIH builds upon the two previous (D.1, D.2) features. Access to the local SIH will be provided by way of Internet Access from the home system. All home and visiting users will obtain access to the SIH via the Internet access server. A well known URL (e.g., http://status.local.gov) will map to the Harris County SIH server.

In the future, the SIH may contain sensitive information and be accessed by many different responders (and roaming responders). Therefore, authorizations may be necessary to access certain 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 nationwide method will be eventually needed to provide federated identity management to a SIH server in a visited system. This capability can be layered onto the basic SIH access capability.

D.4 Access to Responders Under the Incident Command System

The National Incident Command System (NIMS) has defined an 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 D.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 UE's 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 operators to support IP connectivity for each of these different application deployments and home/roaming devices. IP networking tools that can be deployed to support this application include:

Static IP address assignments	DNS
NAT/NAPT	IPv4-v6 translation

The State of Texas network will provide the necessary functions to support the IP connectivity to application servers required to support the ICS application.

D.5 Field-Based Server Applications

Public safety agencies regularly use Mobile Command Vehicles to support specialized incidents, such as hurricanes. Typically, these vehicles use cellular technology as the last mile link 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. 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, HSS will be configured to allocate a static IP address to UE's serving as the modems for field-based servers. In order to be Internet-visible, this static IP address will use NAT/NAPT technology in the near term. Longer term, IPv6 technology may be used.

The State of Texas network will provide the necessary IP address allocation technologies to support the field-based server application.

E. Reliability and Availability

The implementation 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 implementation also includes support for a MVPN which enables use of diverse access technologies, such as WLAN and commercial carrier 3G networks. Please refer to section C.4.3 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.

The MTBF information is provided in Appendix I.[22]

E.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:

---

[22] *See Public Safety and Homeland Security Bureau Offers Further Guidance to Conditional Waiver Recipients on Completing the Interoperability Showing Required by the 700 MHz Waiver Order*, DA 10-923, PS Docket 06-229, May 21, 2010, ¶C, page 4.

- 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.

E.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 Management System (EMS)

These components are internally redundant and designed to provide robust hardware reliability and service assurance. The implementation is able to support EPC component pooling to achieve a highly available and resilient system with disaster recovery capabilities. The IP version supported by each network element is summarized in the table below:

Network Element	IP Version
HSS	IPv4, IPv6
PCRF	IPv4, IPv6
SGW	IPv4, IPv6
PGW	IPv4, IPv6
MME	IPv4, IPv6
EMS	IPv4

E.3 Transport Network

Transport network resiliency is accomplished by enabling a multi-path IP 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 core network. If any failure of switches, links or modules occurs, traffic will be switched to a backup module or port. Interface redundancy allows backup links and ports. In addition, fiber rings can be leveraged to connect the cell sites and data centers. Agency networks are equipped with redundant links to the data centers.

E.4 Radio Access Network

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

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

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

In addition, the implementation will include support for deployable units to provide coverage replacement and/or additional site capacity in support of large-scale incidents or planned events.

E.5 Mobile and Portable User Equipment

The mobile and portable User Equipment (UE) is 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 UE's will support both IPv4 and IPv6 via dual-stack capabilities. Initially, deployed UEs may need to be upgraded to support the dual-stack capability.

F. 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, and traffic model. These variables are interrelated, such that changes in one variable inevitably impact the others. The State of Texas system is designed to support users and applications 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.

Among the more critical RF engineering tasks is to prevent and manage out of band emissions (OOBE). The State of Texas commits to implementing the PS LTE network in Band Class 14, in a mutually agreeable manner which eliminates out of band emissions (OOBE) by attenuating transmission power outside the band by at least 43+10 log (P) dB below the transmitter power.[23]

[23] *See Waiver Order*, DA 10-79, PS Docket 06-229, ¶¶ 43-44.

F.1 Radio Access Network Planning

The State of Texas 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 operational 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 Harris County BIG-Net deployment are provided in Appendix E of this document. Section F.1.4 of this document provides traffic model parameters.

F.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 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.

F.1.2 Network Capacity and Throughput Analysis

The design methodology for the network was intended to meet, at a minimum, the current requirements of Harris County. However, it is recognized that over time State of Texas member agencies will require additional coverage. With these goals in mind, the Harris County BIG-Net is designed to carry a certain amount of load per user per busy hour as explained in the "Modeling Assumptions" section F.1.4 below. Sector utilization information is provided in Appendix J.

F.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 State of Texas 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 implementation. This approach anticipates the current capacity requirements and ensures the ability to add further capacity with the addition of sites in the future. State of Texas anticipates the need for a larger number of sites over time. The network design offers a flexible approach starting with an affordable network deployment with a plan to build coverage and capacity as additional funding becomes available.

F.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 LTE 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 LTE networks.

In order to arrive at a suitable broadband network profile for Public Safety, certain assumptions for traffic usage in the Harris County region has been made. The following parameters were also used for this design:

- 95% area reliability
- Coverage based on up to 4 HARQ retry attempts
- Mobile on street coverage using 23 dBm (200 mw) UE's
- 200 concurrent users per eNB
- Average cell edge data rates of 768 Kbps downlink and 256 Kbps uplink
- 11.8 dBd antenna gain at the eNodeB
- Antennas heights ranging from 100-155 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 Appendix E of this document.

F.2 Interference Mitigation

The implementation will employ several techniques and features to mitigate interference among Band 14 eNBs. Before deploying, the State commits to coordinating and addressing interference with bordering and adjacent jurisdictions.[24]

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 to some extent on compatibility of the vendor implementations. Thus it is possible that vendors of adjacent regions will be required to optimize and/or adapt their implementations for interference mitigation compatibility. The State of Texas will self-certify that interference coordination techniques are implemented by the date of service availability. Below are techniques and features which are planned to be employed in the system.

F.2.1 Network Planning for Interference Mitigation

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.

[24] *See Interop Order,* 10-2342*,* ¶26 and Appendix A, ¶K. See also *Waiver Order*, 10-79, ¶42.

F.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 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.

F.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 downtilting 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.

F.2.2 eNodeB Interference Mitigation Features

F.2.2.1 Inter-cell Interference Coordination (ICIC)

Inter-cell Interference Coordination (ICIC) is used as a means to improve coverage and edge of cell performance. Prior to the Date of Service Availability, the State of Texas commits to implementing Inter-Cell Interference Coordination on and among the eNodeBs to ensure the network operates without interference.[25] The goal is to achieve an evenly distributed utilization

[25] *See Interoperability Order, 10-2342,* ¶26 and Appendix A, ¶K.

of radio resources between neighboring cells in low-to-medium loading scenarios, while also enabling high utilization of radio resources in high load scenarios.

F.2.2.2 Frequency Selective Scheduling

OFDM systems can take advantage of the frequency selectivity of the uplink and downlink channels. Some frequency diversity gain may be achieved by varying subcarrier allocations over the entire carrier bandwidth. Additional diversity gain is possible by utilizing channel characteristics to allocate sub-band allocations that are favorable based on fading and/or interference conditions. The State of Texas may implement either or both of these Frequency Selective Scheduling techniques, depending on vendor-specific capabilities and deployment needs.

G. State of Texas PS LTE Testing

This section provides an overview of the testing commitments, strategies and high level program overviews for each type of testing envisioned.

G.1 Strategies for Effective PS LTE Testing

The State of Texas has embarked upon the development of fair, open, standards-based, multi-vendor Conformance, Interoperability and End-to-End Validation Testing plans by applying the following high level strategies to:

- Ensure an “even playing field” such that no manufacturer or supplier has an undue advantage do its relationships or deployment status in the State;
- Continue to mandate that all network infrastructure suppliers wishing to deploy equipment in the State of Texas needs verification that the vendor is a certified participant in the PSCR PS LTE laboratory project;
- Continue to look to PSCR for guidance on how to handle 3GPP standards conformance testing;
- Investigate all options for leveraging IOT activities, including but not limited to PSCR, NVIOT Forum[26], existing carrier labs, “pair-wise” vendor testing[27], third party certified test labs such as PTCRB[28] or Idaho National Labs and possibly self certification by the manufacturers under certain, stringent conditions;
- Minimize, as much as practical, selection of interface and equipment combinations not currently supported by any current or planned IOT activities;
- Determine the need for state or regional PS LTE interoperability Test Bed and/or how a jointly owned PS LTE test bed could be established; and to
- Allow manufacturers to self-certify, but only when other more open options are not available and only under certain constraints.

[26] National Vendor Interoperability Testing Forum (NVIOT Forum)

[27] Also recommended in *Comments from Alcatel Lucent*, 06-229, page 22

[28] PTCRB is a global organization created by the Mobile Network Operators to provide an independent evaluation process where GSM/UMTS Type certification can take place. See PTCRB, http://ptcrb.com/.

In summary, as directed by the December 10, 2010 *Interoperability Order*, the State of Texas will ensure, through a variety of programs and processes, that the suppliers selected by the State have met all of the Interoperability (IOT) and Conformance Testing objectives.[29] The State will validate that the selected suppliers' network components have received applicable certifications and have fully participated in available interoperability testing programs, such as the PSCR, the Multi Service Forum (MSF) or the NVIOT Forum. The State will also validate that the selected suppliers' device components have received applicable certifications from the PCS-Type Certification Review Board (PTCRB). Certifications from additional laboratories, such as the Global Certification Forum, may also be required.

G.1.1 Conformance Testing to 3GPP Standards

The State wholeheartedly agrees with the Commission's tentative conclusion[30] that all PS LTE devices should be subjected to rigorous conformance testing to verify compliance to 3GPP LTE Release 8 or higher standards. Therefore, the State of Texas agrees to comply will all future orders regarding LTE device conformance testing. This requirement will be extended to regional partners as well as part of the processes and regional agreements which will be developed.

G.1.2 Multi-Vendor Interoperability Testing (IOT)

An effective strategy and plan for Multi-Vendor Interoperability Testing (IOT) is among the more critical and powerful mechanisms to ensure sustainable interoperability and as importantly, a transparent "interchangeability" among devices and components in a PS LTE network. This entire program and plan will be an area of specific focus and planning, as noted, since the over-riding objective of achieving an open, fair and highly competitive procurement environment rests so heavily upon it.

As critical, if not more so, the mission critical operational environment demands even more care and investment than commercial cellular devices since in most cases much more is at stake than a consumer moving to another provider, for this reason the State of Texas agrees with the NTIA recommendation that no device or component will be allowed to go into operation until IOT is successfully completed using accredited laboratories.[31]

The State appreciates and agrees with Nokia Siemens in recent reply comments, "that all major vendors perform IOT in adherence to industry-wide principles," and also agrees that IOT policies and requirements need to be standardized under the oversight of a single body.[32]

Per the Third Report and Order[33] all of the LTE interfaces must be supported, while the following interoperability interfaces will receive particular scrutiny and attention for the IOT plans, procedures and compliance to 3GPP Release 8 or higher, these include:

- U_u – LTE over the air interface
- S6a – Visited MME to Home HSS

---

[29] *See Interoperability Order*, DA 10-2342, PS Docket 06-229, December 10, 2010, ¶D,E.

[30] *See 4th NPRM,* January 26, 2011, ¶106

[31] *See Comments of the NTIA*, June 10, 2011 section 5, page 21.

[32] *See Comments of Nokia Siemens Networks* PS 06-229, page 29.

[33] *See Third Report and Order*, January 26, 2011 ¶12.

- S8 – Visited SGW to Home PGW
- S9 – Visited PCRF to Home PCRF

An important interface for already identified as a high level interchangeability need, would add:

- S1-u – between eNodeB and SGW
- S1-MME – between eNodeB and MME

The list about is preliminary and not necessarily inclusive; additional interoperability and IOT needs may be identified in the multi-vendor architecture definition process.

This program, once developed, will be fully implemented in order to enable interconnection and interoperability with other LTE networks. The State will ensure that all required Interoperability and Conformance test validations have been performed by the proposed interoperability partner, prior to Texas establishing or offering interoperability services to end users. Specifically, the State of Texas will support, monitor and require that any new PS LTE operator, even of a "sub-core" based system within Texas, has submitted a certification to at least the IOT specified above.

G.1.3 End-to- End Functional Validation Testing

This stage specifies the functional and performance end to end validation tests will be executed as part of the Trial Network testing plan. 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 (e.g., features are added) and the standards evolve. The applications and interfaces to be tested in end to end validation are described 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)	S9-Visited PCRF to Home PCRF
S6a-Visited MME to Home HSS	S1-U-eNB to SGW
8-Visited SGW to Home PGW	S1-MME-eNB to MME

A listing of LTE test tools utilized by the implementation is included in Appendix D.

G.1.4 Summary of Testing Commitments

The State of Texas commits to complying with the following testing requirements as recommended and mandated:

- The State commits to deploying vendor equipment which has been subjected to rigorous Conformance Testing by certified laboratories. [34]Within six months of either the availability of PTCRB testing or the Date of Service Availability, whichever is later, the State of Texas commits to completing the PRCRB process and to submitting these certification as part of the quarterly reports.[35]
- The State of Texas commits to performing interoperability testing (IOT) on a minimum of Uu, S6a, S8 and S9 interfaces, recognizing a more comprehensive scope may be needed. The state also commits to testing on a regular basis as the network changes and evolves.[36]

H. Deployment

The following project plan reflects an 18site deployment which comprises the initial phase of deployment within the State of Texas. A .pdf format file has been included in this document in Appendix G.

Subsequent deployment phases will be planned in accordance with requirements of the associated funding sources.

The State of Texas will provide the Commission with documented results of the IOT described in Section G on or before the conclusion of the 18 site deployment which comprises the initial phase of deployment. Further, the State of Texas will provide results of future IOT on or before the conclusion of each subsequent phase of the network build-out.

I. Operations, Administration, Maintenance & Provisioning

The OAM&P implementation 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 implementation 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.

I.1.1 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.

[34] *See Interoperability Order*, 10-2342, Appendix A, ¶D.

[35] *Ibid*

[36] *Ibid* ¶E.

I.1.2 Over The Air (OTA) Device Management

The Device Management implementation provides an easy-to-use interface to perform software upgrade, configuration and provisioning of a variety of public safety devices, including portables, vehicular modems, USB modems, and mobile data terminals.

I.1.3 Self Organizing Network (SON)

The system SON implementation, fully based on 3GPP standards, provides a self-configuring, self-healing, and self-optimizing RAN implementation. 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 implementation 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.
- Base Station Integration Manager, which significantly simplifies planning, preparation, deployment and commissioning of eNBs.

I.1.4 Integrated Billing

The system provides an integrated billing implementation that supplies charging information, including the ability to support complex roaming and usage-based accounting. The billing implementation 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. If SON is utilized in LTE border cells, 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 will need to be verified for interoperability between LTE vendors if LTE border cells enable these SON capabilities. A simpler option is to not enable SON capabilities in LTE border cells.
- 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 able to support Open Mobile Alliance Device Management (OMA-DM) clients in order to support standards-based device management implementations.
- Billing reconciliation between public safety LTE networks requires the exchange of billing records. Billing records will be exported and imported between networks using TAP3 record formats.

Appendices

Appendix A. Definitions and Acronyms

ACB	Access Class Barring
AF	Application Function
ARP	Allocation and Retention Priority
BBTF	Broadband Task Force
CAD	Computer Aided Dispatch
CJIS	Criminal Justice Information System
DNS	Domain Name Service
EMS	Element Management System
EPC	Enhanced Packet Core
E-RAB	EUTRAN Radio Access Bearer
E-UTRA	Evolved Universal (or UMTS) Terrestrial Radio Access
FIPS	Federal Information Protection Standards
GBR	Guaranteed Bit Rate
GPS	Global Positioning System
GTP	Generic Tunneling Protocol
HAAT	Height Above Average Terrain
HO	Handover
HSS	Home Subscriber Server
ICIC	Inter-Cell Interference Coordination
IMSI	International Mobile Subscriber Identity
IKE	Internet Key Exchange
IOT	Inter-Operability Testing
IP	Internet Protocol
IPX	IP Exchange (see http://www.gsmworld.com/our-work/programmes-and-initiatives/ip-networking/ipi_documents.htm)
LTE	Long Term Evolution

MBMS	Multimedia Broadcast Multicast Service
MBR	Maximum Bit Rate
MME	Mobility Management Entity
MVPN	Mobile Virtual Private Network
NAPT	Network Address and Port Translation
NAS	Non-Access Stratum
NAT	Network Address Translation
NAPT	Network Address and Port 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
PSCR	Public Safety Communications Research (program)
PTCRB	PCS Type Certification Review Board
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
RRC	Radio Resource Control
SGW	Serving Gateway
SIB	System Information Block
SON	Self Organizing Network
SWBN	Shared Wireless Broadband Network
TAU	Tracking Area Update
TS	Technical Specification
TSB	Telecommunications System Bulletin
TxDPS	Texas Department of Public Safety
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. Key Milestone Chart

State of Texas PS LTE Program Milestones, 09012011, v7.2	Due Date (if applicable)	Target for Completion	ACTUAL
State of Texas Interop Showing filed with FCC (initial filing)	7/12/2011	7/11/2011	7/11/2011
State of Texas Interop Showing filed with FCC , revised filing		8/3/2011	8/3/2011
Launch State of Texas Vendor Demonstration Network Project		July 2011	TBD
Launch Region VI PS LTE Network Achitecture Working Group	July-11	7/8/2011	7/8/2011
Extend Official Invites to Participate in Multi-Vendor Demo Network		July 2011	July-11
BIG-Net OTA Test Deployment Phase 1.0 Site Deployment - 6 sites, total of 6 Complete		7/15/2011	7/22/2011
Quarterly Report #5	7/19/2011	7/19/2011	7/18/2011
Region VI Public Safety LTE Interoperability Forum II, Albuquerque, NM		7/21/2011	7/21/2011
Submit notice of need for PLMN ID to Bureau	5/1/2012	8/20/2011	8/19/2011
Begin Technical Working Teams to Implement Multi-Vendor Demos		Sept 2011	
Region VI Public Safety LTE Interoperability Forum III		Sept 2011	
Conformance, IOT and End-to-End Validation Plan		Oct 2011	
Quarterly Report #6	10/19/2011	10/19/2011	
State of Texas PS LTE Architectural Requirements & Guidelines, v1		Nov 2011	
Quarterly Report #7	1/19/2012	1/19/2012	
BIG-Net temporary PLMN ID change-over to permanent PLMN ID		2/1/2012	
Interoperability Monitoring, Issue Tracking and Escalation Service Plan		Feb 2012	
Quarterly Report #8	4/19/2012	4/19/2012	
BIG-Net OTA Test Deployment Phase 2.0 - Add 11 sites, total of 17 complete		6/27/2012	
Quarterly Report #9	7/19/2012	7/19/2012	
BIG-Net OTA Test Deployment Phase 2.1 - Add Cell-on-Wheels (CoW), Total of 18 complete		7/20/2012	
Complete Phase 1 Interoperability Testing		7/27/2012	
BIG-Net Date of Service Availability ("Go Live" Date)		**8/1/2012**	
Quarterly Report #10 - 1st Report after Date of Service Availability	10/19/2012	10/19/2012	
Qtrly #10- Plan for conducting IOT on Uu, S6a, S8 and S9; must also commit to testing on a regular basis with other PS LTE networks in service	10/19/2012	10/19/2012	
Qtrly #10- Submit certification of Public Safety Roaming on Petitioner Network	10/19/2012	10/19/2012	
Qtrly #10- 256K/768K UL/DL performance of "as-built" network,	10/19/2012	10/19/2012	
Quarterly Report #11	1/19/2013	1/19/2013	

Appendix C. 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 UE's.
    - 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
    - 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.
- 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 UE's.
- 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. For each UE associated with the Evolved Packet System (EPS), at any 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 "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 implementation 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 stores subscription profile records and 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. LTE-Uu provides 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.

Gy/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 online/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 – The S1-U provides 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.

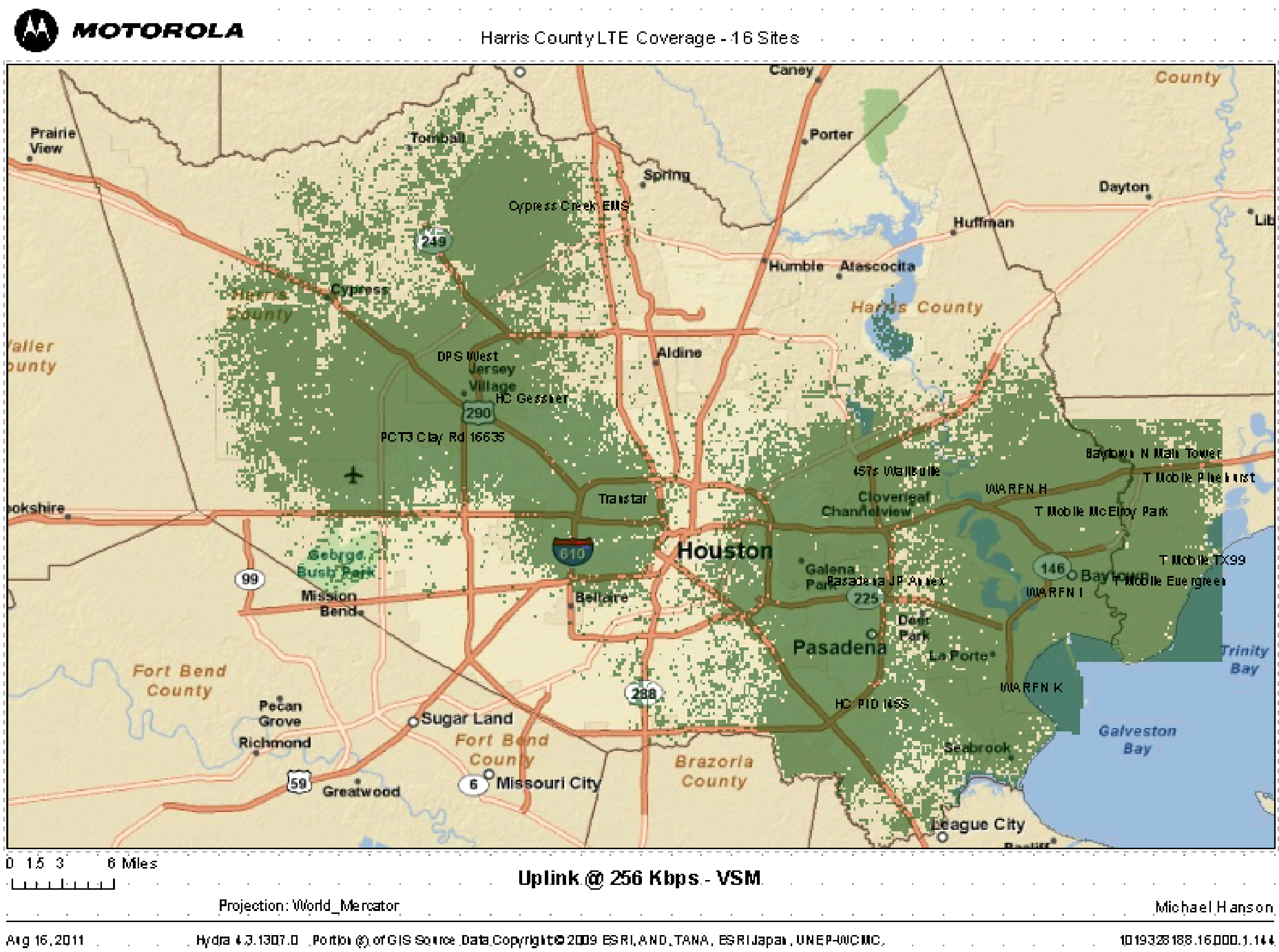
X2 - The X2 interface provides a control plane and bearer plane connection between eNBs to support load management and handover procedures.

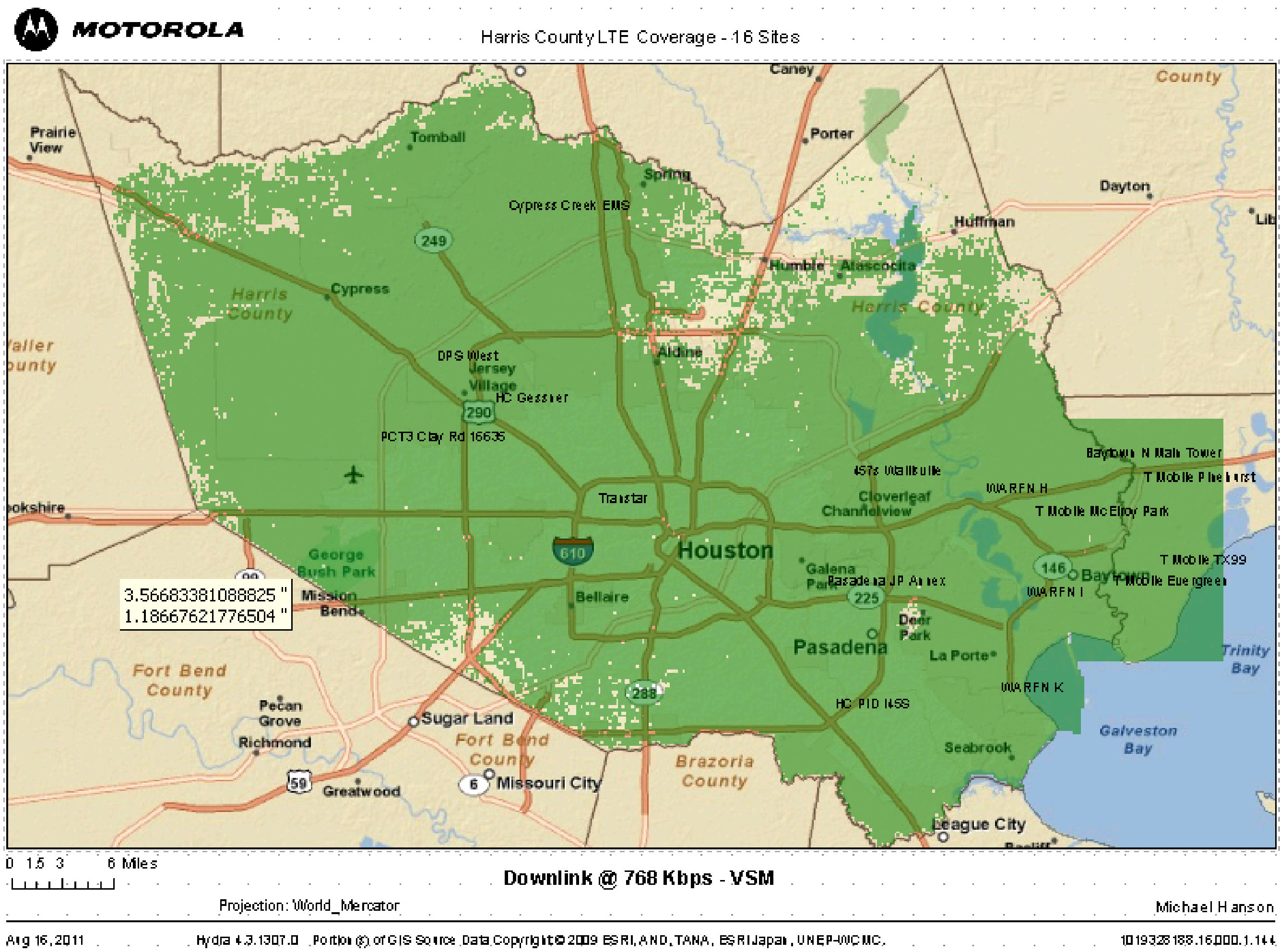
Appendix D. LTE Test Tools

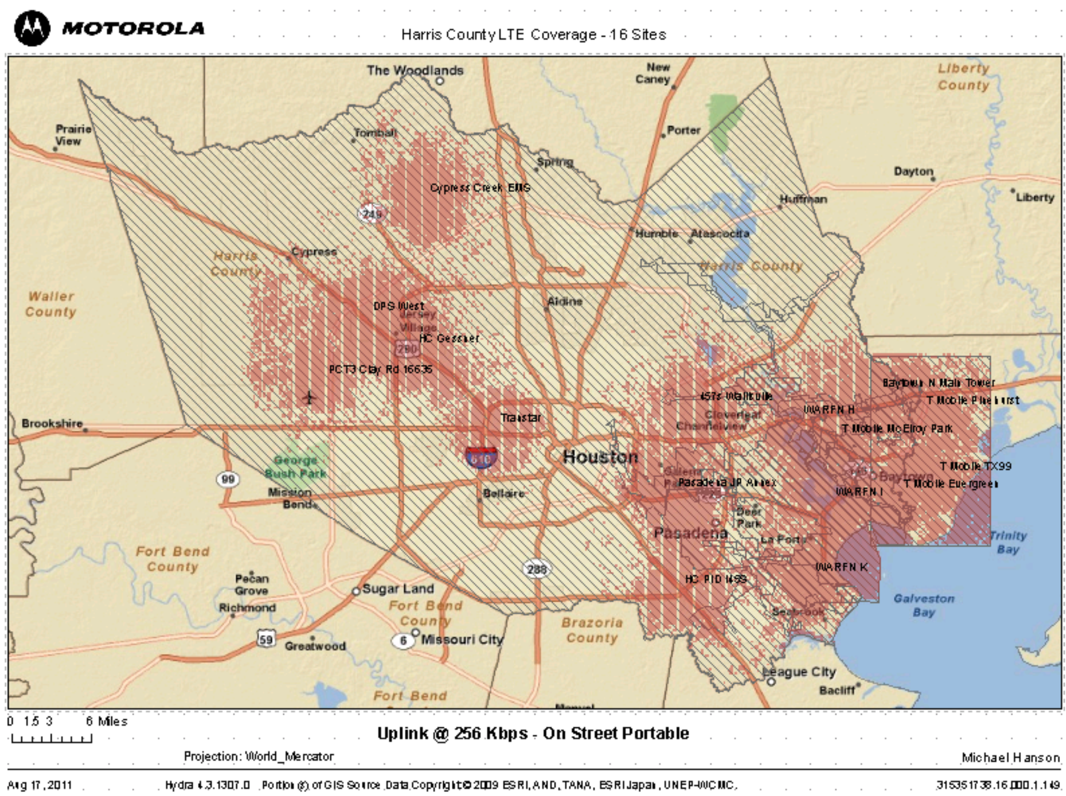
LTE Test Tools		
Function	**Tool (specified or equivalent)**	**Description**
Spectrum Analyzer	Agilent SA	Cell coverage, characteristics
Air Interface Monitor	UE Tool	Synchronization, system broadcast information, registration, DL/UL transfers
	Sanjole WaveJudge	
Network Monitor	Wireshark – Windows PC	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

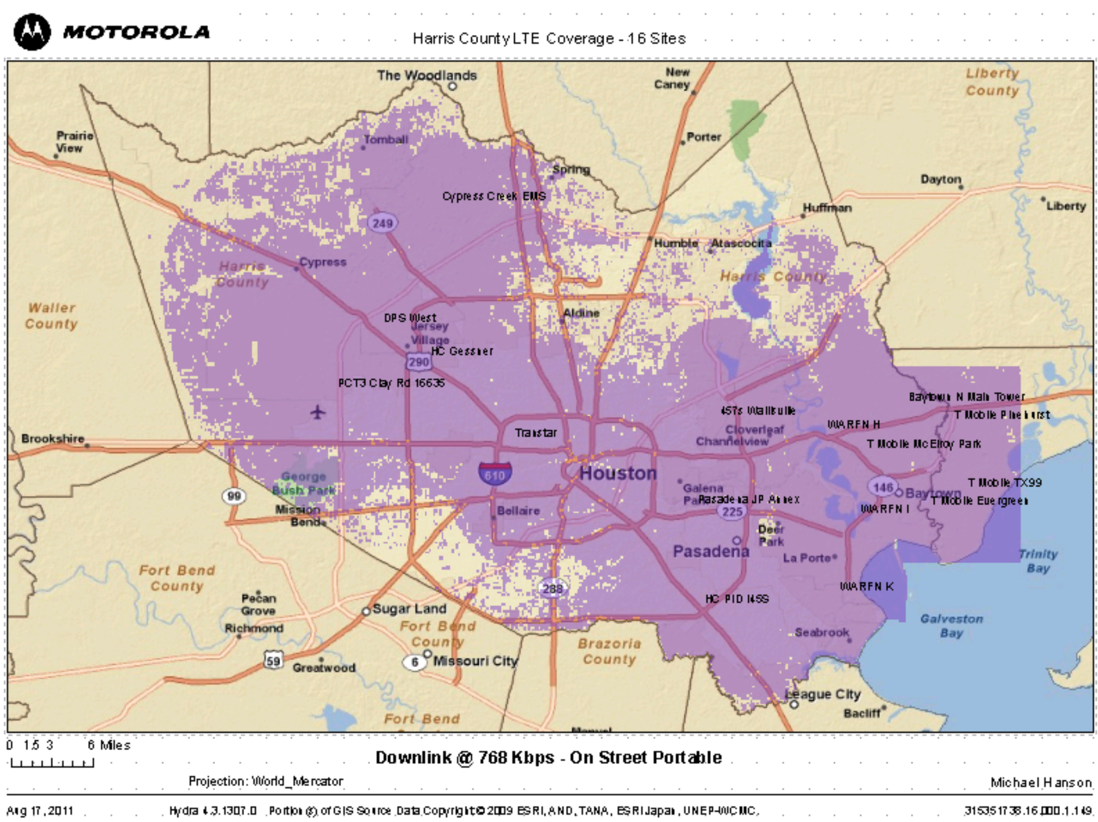
Appendix E. Harris County Initial Phase Coverage Maps

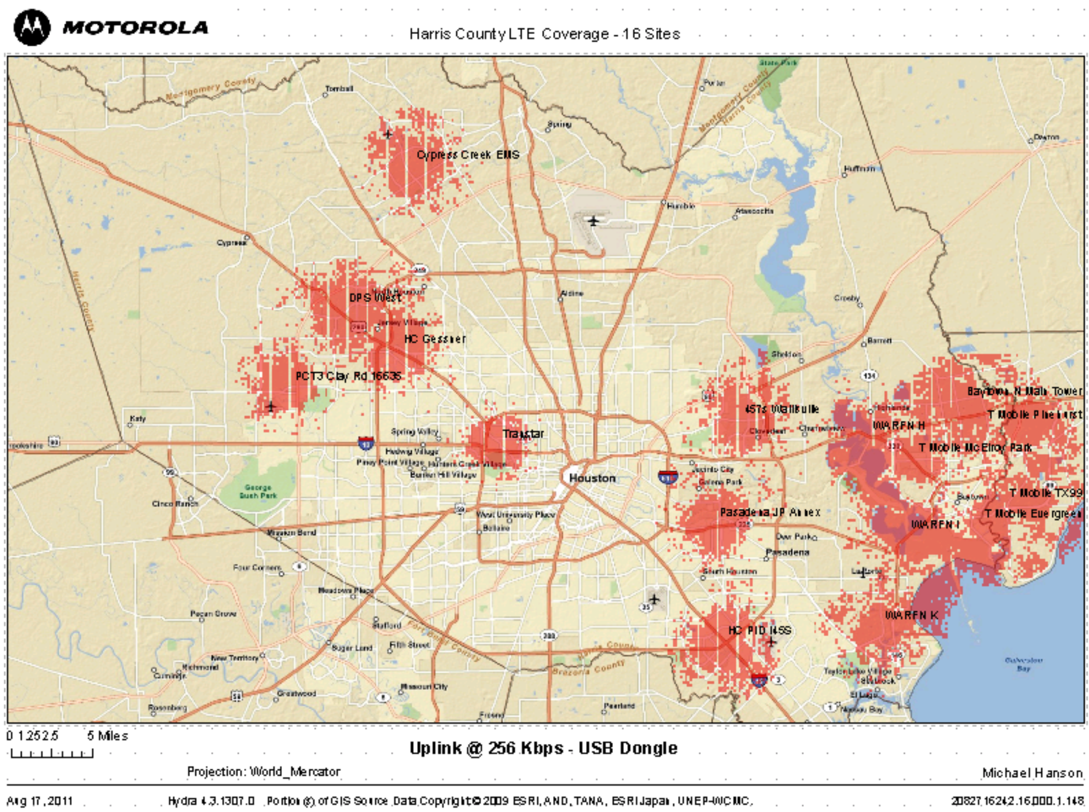
The coverage maps shown below comprise 16 sites using an approximation of the Application Load Model with 200 users per site with minimum application data rate of 256 Kbps uplink and 768 Kbps downlink. The initial deployment will be a total of 18 sites, with 16 deployed to cover the Houston area as shown in the coverage maps, one (1) which will be deployed at one of the core sites for testing only in College Station, Texas and another one (1) which is a mobile Cell-on-Wheels site.

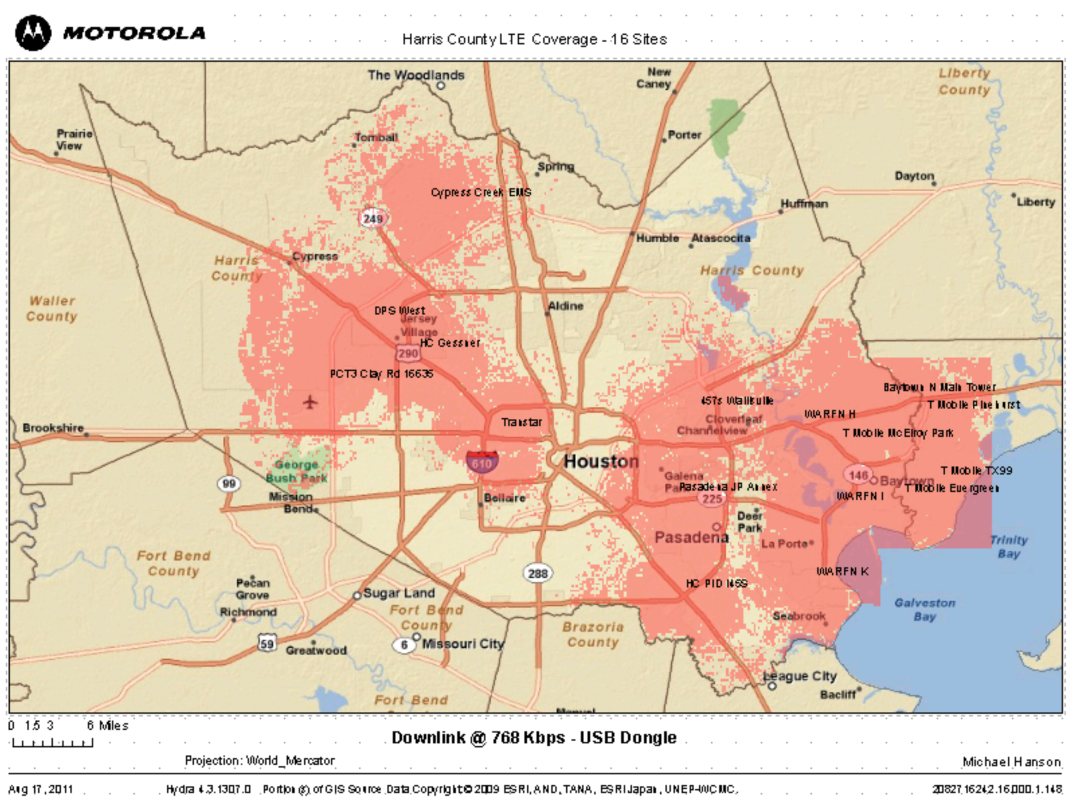



MOTOROLA
Harris County LTE Coverage - 16 Sites
Downlink @ 768 Kbps - VSM
0 1.5 3 6 Miles
Projection: World_Mercator
Michael Hanson
Aug 16, 2011
Hydra 4.3.1307.0 Portions (c) of GIS Source Data Copyright © 2009 ESRI, AND, TANA, ESRI Japan, UNEP-WCMC,
3.56683381088825 "
1.18667621776504 "
Cypress Creek EMS
DPS West
HC Gessner
PCT3 Clay Rd 16635
Transtar
Houston
Pasadena
Baytown N Main Tower
T Mobile McElroy Park
T Mobile TX99
HC PID N5S
Tomball
Spring
Cypress
Humble
Atascocita
Aldine
Bellaire
Sugar Land
Missouri City
Seabrook
League City
Galveston Bay
Trinity Bay
Harris County
Fort Bend County
Brazoria County


MOTOROLA
Harris County LTE Coverage - 16 Sites
The Woodlands
New Caney
Liberty County
Prairie View
Tomball
Porter
Spring
Dayton
Cypress Creek EMS
Huffman
Liberty
Humble
Atascocita
Harris County
Cypress
Waller County
DPS West
Aldine
HC Gessner
PCT3 Clay Rd 16635
Baytown N Main Tower
T Mobile Pinehurst
Traustar
WARFN H
Brookshire
T Mobile McElroy Park
Houston
T Mobile TX99
Pasadena JP Annex
T Mobile Evergreen
WARFN I
Bellaire
Mission Bend
Pasadena
Trinity Bay
Fort Bend County
WARFN K
HC PID 14SS
Pecan Grove
Sugar Land
Galveston Bay
Richmond
Brazoria County
Greatwood
Missouri City
League City
Bacliff
Fort Bend
0 1.5 3 6 Miles
Uplink @ 256 Kbps - On Street Portable
Projection: World_Mercator
Michael Hanson
Aug 17, 2011


MOTOROLA
Harris County LTE Coverage - 16 Sites
The Woodlands
New Caney
Liberty County
Prairie View
Tomball
Porter
Spring
Dayton
Cypress Creek EMS
Huffman
Liberty
Humble
Atascocita
Harris County
Cypress
Waller County
DPS West
Jersey Village
Aldine
HC Gessner
PCT3 Clay Rd 16635
Baytown N Main Tower
T Mobile Pinehurst
Traustar
WARFN H
Cloverleaf
Channelview
Brookshire
T Mobile McElroy Park
Houston
Galena Park
T Mobile TX99
Baytown
Pasadena JP Annex
T Mobile Evergreen
WARFN I
George Bush Park
Bellaire
Mission Bend
Deer Park
Pasadena
La Porte
Trinity Bay
Fort Bend County
WARFN K
HC PID 14SS
Pecan Grove
Sugar Land
Galveston Bay
Seabrook
Richmond
Brazoria County
Greatwood
Missouri City
League City
Bacliff
Fort Bend
0 1.5 3 6 Miles
Downlink @ 768 Kbps - On Street Portable
Projection: World_Mercator
Michael Hanson
Aug 17, 2011





For both of the USB Dongle maps above, no no external antenna was used.

Appendix F. Commitment to Compliance Summary

The following table summarizes the of State of Texas' commitment to comply with the Bureau's requirements regarding Public Safety LTE. This is not an all inclusive list but rather key elements are presented here for easy reference.

In summary, the State of Texas agrees and commits to remain subject to existing technical rules, the requirements of the *Texas Waiver Order* (11-863), the *Interoperability Order* (10-2342), the January 2011 *Third Report and Order* (11-6), the May 2011 *Fourth Report and Order* (10-79) and any future rules which may be adopted in future proceedings.[37]

Item No.	Statement of Commitment to FCC Requirement	FCC References
Public Safety Roaming on Petitioners' Networks		
1	The State of Texas agrees and commits to honoring roaming and access requests from any qualified entity.[38] Additionally, the State agrees to refer the matter to the Bureau if an agreement with the outside entity cannot be reached within ninety days.	**10-2342 Appendix A, ¶A;** 10-2342 ¶10
2	The State of Texas commits to supporting home-routed traffic, such that a "visiting" user's traffic is routed back to the home network to enable the use of visitors' home resources.	**10-2342 Appendix A, ¶A;** 10-79 ¶45; 10-2342 ¶9
3	The State of Texas commits to supporting local breakout traffic, such that a "visiting" user is able to utilize the resources of the State of Texas PS LTE network.	**10-2342 Appendix A, ¶A;** 10-79 ¶45; 10-2342 ¶9
Technology Platform and System Interfaces		
4	The State commits to a uniform deployment of at least 3GPP standard E-UTRA Release 8 and associated EPC, prior to the date of service availability.	11-6 ¶10, ¶12; 10-79 ¶38
5	Public Safety LTE devices deployed in the State of Texas shall support Band Class 14 using a 5 MHz broadband channel in FDD mode per 3GPP TS 36.101.	10-79 ¶47
6	The State commits to deploying LTE such that backward compatibility between all subsequent releases from Release 8 and onwards is ensured.	11-6 ¶11

[37] *See Third Report and Order*, 11-6, PS Docket 06-229, January 26, 2011, ¶14. See also Waiver Order, Recommended Requirements, ¶ A.

[38] *See Waiver Order*, DA 10-2342, PS Docket 06-229, Recommended Requirements, Public Safety Roaming on Petitioners' Networks, Appendix A,¶ A.

7	Prior to the Date of Service Availability, the State of Texas agrees to support the following interfaces as defined by the 3GPP Standard: Uu – LTE over the air interface S1-MME – eNb and the MME S1-u – eNb and the SGW S5 – SGW and PGW S6a – Visited MME and the Home HSS S8 – Visited SGW and Home PGW S9 – Visited PCRF and Home PCRF S10 – MME to MME for Category 1 Handover S11 – MME and SGW SGi – PGW and external PDN X2 – eNodeB to eNodeB Gx – PGW and PCRF Rx – PCRF and AF located in PDN Gy/Gz – online/offline charging interfaces	**10-2342 Appendix A, ¶B;** 10-79 ¶47, 10-2342 ¶11, ¶19; 11-6 ¶12
8	The State of Texas commits to supporting both IPv4 and IPv6.[39]	**10-2342 Appendix A, ¶B;** 10-2342 ¶13
System Identifiers		
9	The State commits to submitting, at least ninety days prior to its date of service availability, notice to the Bureau of its need for a PLMN ID for its network.	**10-2342 Appendix A, ¶C;** 10-2342 ¶16
Interoperability Testing (IOT)		
10	Within six months of either the availability of PTCRB testing or the Date of Service Availability, whichever is later, the State of Texas commits to completing the PRCRB process and to submitting these certification as part of the quarterly reports.	**10-2342 Appendix A, ¶D;** 10-2342 ¶18
11	The State of Texas commits to performing interoperability testing (IOT) on a minimum of Uu, S6a, S8 and S9 interfaces, recognizing a more comprehensive scope may be needed. The state also commits to testing on a regular basis as the network changes and evolves.	**10-2342 Appendix A, ¶E.**
Operation of Fixed Stations		
12	The State of Texas agrees and commits to limiting network access of fixed stations on a secondary, non-interference basis only.	**10-2342 Appendix A, ¶F;**
Performance		
13	The State of Texas commits to implementing the network such that the network provides outdoor	**10-2342 Appendix A, ¶G;** 10-2342 ¶22

[39] A breakout of IPv4 vs IPv6 by core functional element is provided in Section E.2 of this document.

	coverage at minimum data rates of 256 Kbps uplink (UL) and 768 Kbps downlink (DL), for all types of devices, for a single user at the cell edge, based on a sector loading of seventy percent, throughout the entire PS LTE network coverage area.	
Coverage and Coverage Reliability		
14	The State of Texas commits to submitting a plan to achieve significant population coverage within Texas within ten years of the initial Date of Service Availability.	**10-2342 Appendix A, ¶H;** 10-2342 ¶23
15	The State of Texas commits to implementing the PS LTE coverage such that the probability of coverage is 95 percent for all services and applications throughout the network.	**10-2342 Appendix A, ¶I;** 10-2342 ¶24
Security and Encryption		
16	The State of Texas commits to supporting the optional security features specified in 3GPP TS 33.401, which include integrity protection, verification of data and ciphering and deciphering of data. The State also commits to supporting network layer VPNs.	**10-2342 Appendix A, ¶J** 10-2342 §25; 10-79 §47
Interference Mitigation		
17	Before deploying, the State commits to coordinating and addressing interference with bordering and adjacent jurisdictions.	**10-2342 Appendix A, ¶K** 10-79 §42
18	Prior to the Date of Service Availability, the State of Texas commits to implementing Static Inter-Cell Interference Coordination on and among the eNodeBs to ensure the network operates without interference.	**10-2342 Appendix A, ¶K** 10-2342 ¶26
19	The State of Texas commits to implementing the PS LTE network in Band Class 14, in a mutually agreeable manner which eliminates out of band emissions (OOBE) by attenuating transmission power outside the band by at least 43+10 log (P) dB below the transmitter power.	10-79 ¶43-4
Applications		
20	Consistent with the NPSTC Broadband Task Force report, and to support a common set of applications for the nationwide network, the State of Texas commits to deploying, at a minimum, the following applications and services on the PS LTE network: authorized VPN access, Status Information Homepage, access to users under ICS and field-based server applications.	10-79 ¶46

Reporting		
21	The State of Texas commits to submit Interoperability Showings which details how the State of Texas, as a waiver recipient, will ensure operability and interoperability for its PS LTE network. Additionally, under the Order, as Texas deploys the network in phases, each phase will carry an independent obligation to submit an updated Interoperability Showing.[40]	11-863 ¶3
22	The State of Texas commits to only deploying equipment from vendors who are certified participants in the PSCR Demonstration Network.	10-79 ¶61
23	The State of Texas commits to submitting Quarterly Reports in consultation with the PSST. These reports will provide updates and progress in three areas: (1) planning, (2) funding and (3) deployment.	10-79 ¶63-64
24	In the Quarterly Report following the Date of Service Availability, the State of Texas commits to submitting a plan for conducting interoperability testing (IOT) for the Uu, S6a, S8 and S9 interfaces.	**10-2342 Appendix A, ¶E;** 10-2342 ¶20

[40] *See Texas Waiver*, DA 11-863, ¶13, footnote 33.

Appendix G. BIG-Net Deployment Schedule in Gantt Format

See following pages.

Appendix H. Device Frequency Information

[redacted]

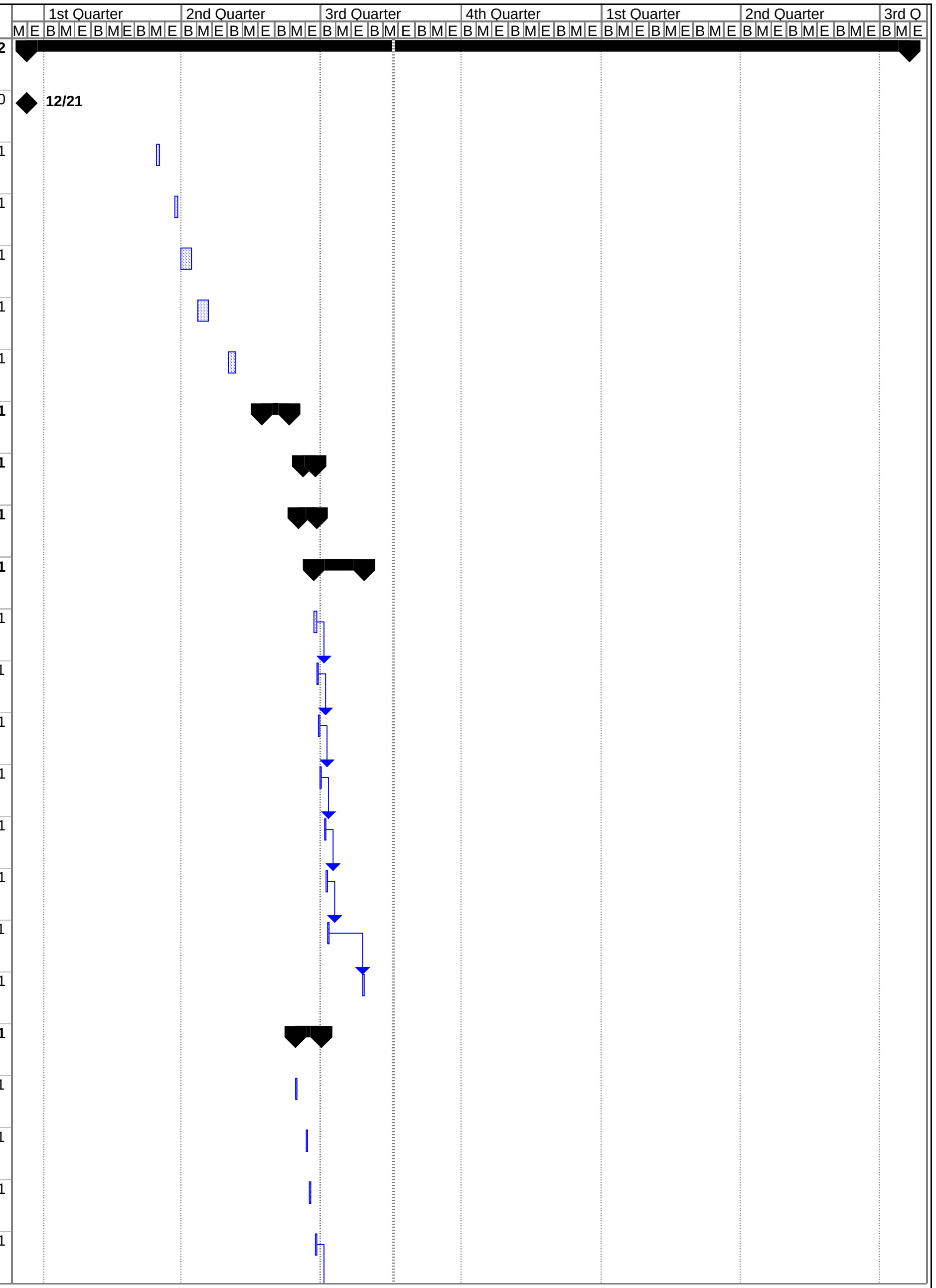
Appendix I. MTBF Information

[redacted]

Appendix J. Sector Utilization Information

[redacted]

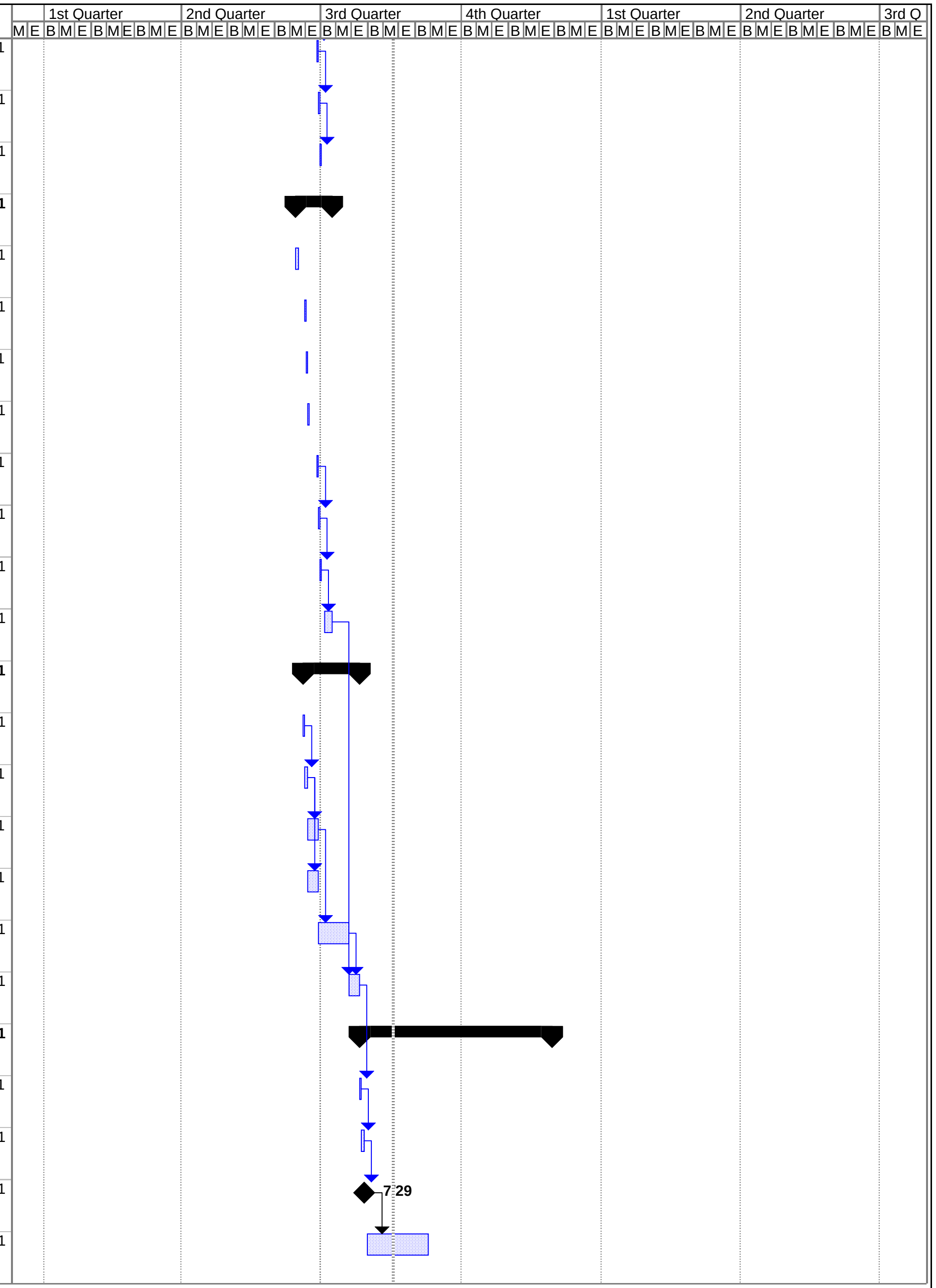
ID		Task Name	Duration	Start	Finish
1		**BIGNET LTE Project Integration**	**414 days?**	**Tue 12/21/10**	**Fri 7/20/12**
2		Contract Signed	0 days	Tue 12/21/10	Tue 12/21/10
3		Post Sale Transition Meeting	2 days	Wed 3/16/11	Thu 3/17/11
4		System Design Review	2 days	Mon 3/28/11	Tue 3/29/11
5		Equipment order booked	5 days	Fri 4/1/11	Thu 4/7/11
6		Microwave Path survey #1 (original 6 Baytown sites)	5 days	Tue 4/12/11	Mon 4/18/11
7		Microwave Path survey #2 (5 new sites)	5 days	Mon 5/2/11	Fri 5/6/11
8		**Tower Structural Analysis**	**14 days**	**Tue 5/24/11**	**Fri 6/10/11**
15		**Tower Structural Refurb**	**6 days**	**Mon 6/20/11**	**Mon 6/27/11**
19		**Site Equipment Platform Fabrication & Installation**	**8 days**	**Fri 6/17/11**	**Tue 6/28/11**
27		**Microwave equipment Installation**	**25 days**	**Mon 6/27/11**	**Fri 7/29/11**
28		Microwave equipment inventoried and staged	2 days	Mon 6/27/11	Tue 6/28/11
29		Wallisville Site Microwave Installation	1 day	Wed 6/29/11	Wed 6/29/11
30		Gessner Site Microwave Installation	1 day	Thu 6/30/11	Thu 6/30/11
31		DPS Site Microwave Installation	1 day	Fri 7/1/11	Fri 7/1/11
32		WARFN_H Site Microwave Installation	1 day	Mon 7/4/11	Mon 7/4/11
33		WARFN_I Site Microwave Installation	1 day	Tue 7/5/11	Tue 7/5/11
34		WARFN_K Site Microwave Installation	1 day	Wed 7/6/11	Wed 7/6/11
35		Microwave end to end path testing	1 day	Fri 7/29/11	Fri 7/29/11
36		**LTE Antenna & Transmission Line Installation**	**13 days**	**Wed 6/15/11**	**Fri 7/1/11**
37		Site antenna/line hardware inventory	1 day	Wed 6/15/11	Wed 6/15/11
38		Wallisville Site Antenna Installation	1 day	Wed 6/22/11	Wed 6/22/11
39		Gessner Site Antenna Installation	1 day	Fri 6/24/11	Fri 6/24/11
40		DPS Site Antenna Installation	1 day	Tue 6/28/11	Tue 6/28/11



Project: Bignet 8-17-2011 18 Sites
Date: Wed 8/17/11

Task | Progress | Summary | External Tasks | Deadline
Split | Milestone | Project Summary | External Milestone

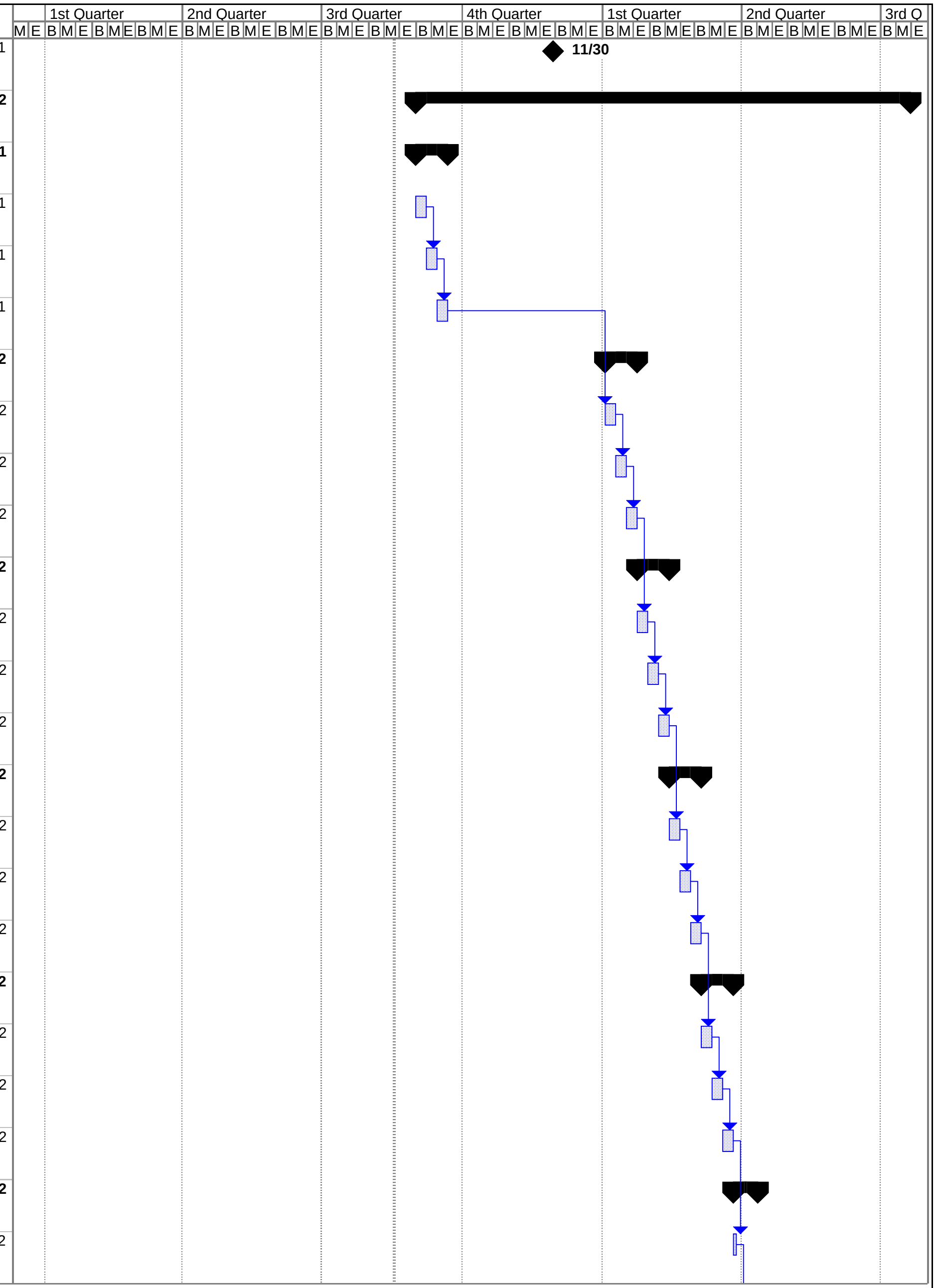
ID		Task Name	Duration	Start	Finish
41		WARFN_H Site Antenna Installation	1 day	Wed 6/29/11	Wed 6/29/11
42		WARFN_I Site Antenna Installation	1 day	Thu 6/30/11	Thu 6/30/11
43		WARFN_K Site Antenna Installation	1 day	Fri 7/1/11	Fri 7/1/11
44		**LTE Site Radio equipment (eNodeB) Installation**	**18 days**	**Wed 6/15/11**	**Fri 7/8/11**
45		Site radio equipment inventory	2 days	Wed 6/15/11	Thu 6/16/11
46		Wallisville Site eNodeB Installation	1 day	Tue 6/21/11	Tue 6/21/11
47		Gessner Site eNodeB Installation	1 day	Wed 6/22/11	Wed 6/22/11
48		DPS Site eNodeB Installation	1 day	Thu 6/23/11	Thu 6/23/11
49		WARFN_H Site eNodeB Installation	1 day	Wed 6/29/11	Wed 6/29/11
50		WARFN_I Site eNodeB Installation	1 day	Thu 6/30/11	Thu 6/30/11
51		WARFN_K Site eNodeB Installation	1 day	Fri 7/1/11	Fri 7/1/11
52		Site link fiber & microwave link end-to-end testing	5 days	Mon 7/4/11	Fri 7/8/11
53		**Core Equipment Installation & Commissioning**	**27 days**	**Mon 6/20/11**	**Tue 7/26/11**
54		DPS Site Prep	1 day	Mon 6/20/11	Mon 6/20/11
55		DPS Core Site hardware installation	2 days	Tue 6/21/11	Wed 6/22/11
56		DPS Core site commissioning and integration	5 days	Thu 6/23/11	Wed 6/29/11
57		Hensel (A&M) Core Site hardware installation	5 days	Thu 6/23/11	Wed 6/29/11
58		Hensel (A&M) Core site commissioning and integration	14 days	Thu 6/30/11	Tue 7/19/11
59		Site load configuration testing	5 days	Wed 7/20/11	Tue 7/26/11
60		**Acceptance Testing**	**90 days?**	**Wed 7/27/11**	**Wed 11/30/11**
61		On the air end-to-end testing (preliminary)	1 day?	Wed 7/27/11	Wed 7/27/11
62		Acceptance Testing	2 days	Thu 7/28/11	Fri 7/29/11
63		Conditional Acceptance	0 days	Fri 7/29/11	Fri 7/29/11
64		Punch list resolution	30 days	Mon 8/1/11	Fri 9/9/11



Project: Bignet 8-17-2011 18 Sites
Date: Wed 8/17/11

Task | Split | Progress | Milestone | Summary | Project Summary | External Tasks | External Milestone | Deadline

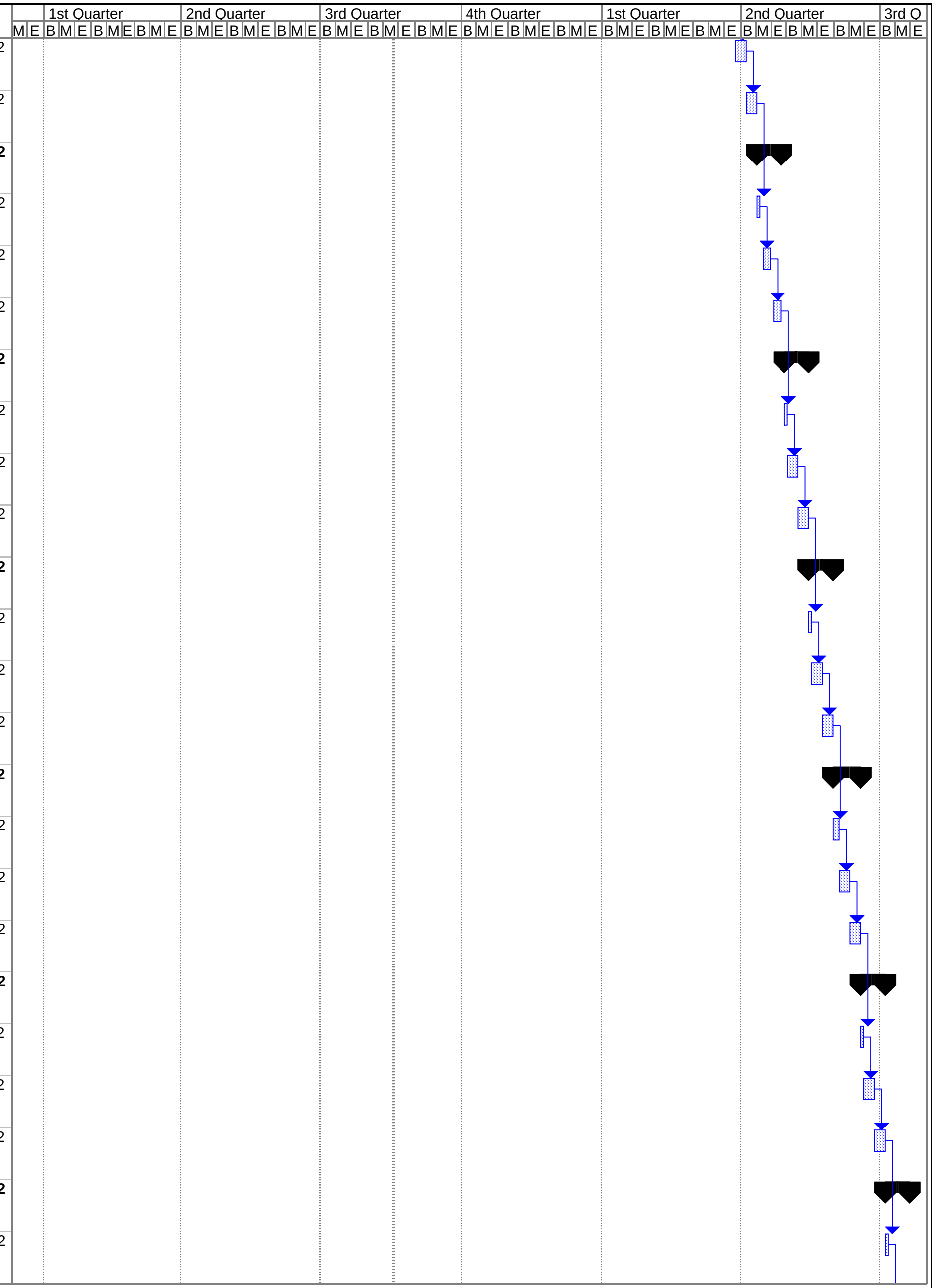
ID		Task Name	Duration	Start	Finish
65		Final Acceptance (SR 1.0)	0 days	Wed 11/30/11	Wed 11/30/11
66		**Site Expansion**	**232 days**	**Thu 9/1/11**	**Fri 7/20/12**
67		**Texas A&M Site 7**	**15 days**	**Thu 9/1/11**	**Wed 9/21/11**
68		Antenna & Line Installation	5 days	Thu 9/1/11	Wed 9/7/11
69		eNode B Installation	5 days	Thu 9/8/11	Wed 9/14/11
70		Integration & Testing	5 days	Thu 9/15/11	Wed 9/21/11
71		**Tmobile Pinehurst Site 8**	**15 days**	**Tue 1/3/12**	**Mon 1/23/12**
72		Antenna & Line Installation	5 days	Tue 1/3/12	Mon 1/9/12
73		eNode B Installation	5 days	Tue 1/10/12	Mon 1/16/12
74		Integration & Testing	5 days	Tue 1/17/12	Mon 1/23/12
75		**Tmobile McElroy Park Site 9**	**15 days**	**Tue 1/24/12**	**Mon 2/13/12**
76		Antenna & Line Installation	5 days	Tue 1/24/12	Mon 1/30/12
77		eNode B Installation	5 days	Tue 1/31/12	Mon 2/6/12
78		Integration & Testing	5 days	Tue 2/7/12	Mon 2/13/12
79		**Tmoibile TX99 Site 10**	**15 days**	**Tue 2/14/12**	**Mon 3/5/12**
80		Antenna & Line Installation	5 days	Tue 2/14/12	Mon 2/20/12
81		eNode B Installation	5 days	Tue 2/21/12	Mon 2/27/12
82		Integration & Testing	5 days	Tue 2/28/12	Mon 3/5/12
83		**Baytown North Main Tower Site 11**	**15 days**	**Tue 3/6/12**	**Mon 3/26/12**
84		Antenna & Line Installation	5 days	Tue 3/6/12	Mon 3/12/12
85		eNode B Installation	5 days	Tue 3/13/12	Mon 3/19/12
86		Integration & Testing	5 days	Tue 3/20/12	Mon 3/26/12
87		**Tmobile Evergreen Site 12**	**12 days**	**Tue 3/27/12**	**Wed 4/11/12**
88		Antenna & Line Installation	2 days	Tue 3/27/12	Wed 3/28/12



Project: Bignet 8-17-2011 18 Sites
Date: Wed 8/17/11

Task		Progress		Summary		External Tasks		Deadline	
Split		Milestone		Project Summary		External Milestone			

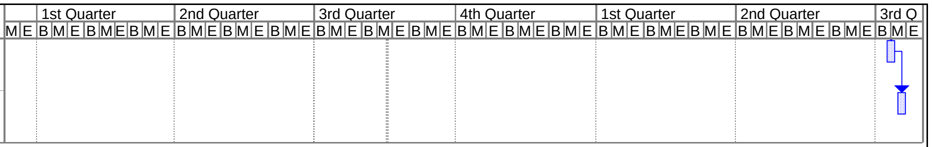
ID		Task Name	Duration	Start	Finish
89		eNode B Installation	5 days	Thu 3/29/12	Wed 4/4/12
90		Integration & Testing	5 days	Thu 4/5/12	Wed 4/11/12
91		**Tmobile Lyondell Site 13**	**12 days**	**Thu 4/12/12**	**Fri 4/27/12**
92		Antenna & Line Installation	2 days	Thu 4/12/12	Fri 4/13/12
93		eNode B Installation	5 days	Mon 4/16/12	Fri 4/20/12
94		Integration & Testing	5 days	Mon 4/23/12	Fri 4/27/12
95		**HC PID I45S Site 14**	**12 days**	**Mon 4/30/12**	**Tue 5/15/12**
96		Antenna & Line Installation	2 days	Mon 4/30/12	Tue 5/1/12
97		eNode B Installation	5 days	Wed 5/2/12	Tue 5/8/12
98		Integration & Testing	5 days	Wed 5/9/12	Tue 5/15/12
99		**Cypress Creek EMS Site 15**	**12 days**	**Wed 5/16/12**	**Thu 5/31/12**
100		Antenna & Line Installation	2 days	Wed 5/16/12	Thu 5/17/12
101		eNode B Installation	5 days	Fri 5/18/12	Thu 5/24/12
102		Integration & Testing	5 days	Fri 5/25/12	Thu 5/31/12
103		**Pasadena Annex Site 16**	**12 days**	**Fri 6/1/12**	**Mon 6/18/12**
104		Antenna & Line Installation	2 days	Fri 6/1/12	Mon 6/4/12
105		eNode B Installation	5 days	Tue 6/5/12	Mon 6/11/12
106		Integration & Testing	5 days	Tue 6/12/12	Mon 6/18/12
107		**Harris County Clay Road Site 17**	**12 days**	**Tue 6/19/12**	**Wed 7/4/12**
108		Antenna & Line Installation	2 days	Tue 6/19/12	Wed 6/20/12
109		eNode B Installation	5 days	Thu 6/21/12	Wed 6/27/12
110		Integration & Testing	5 days	Thu 6/28/12	Wed 7/4/12
111		**Mobile Unit (COW) Site 18**	**12 days**	**Thu 7/5/12**	**Fri 7/20/12**
112		Antenna & Line Installation	2 days	Thu 7/5/12	Fri 7/6/12



Project: Bignet 8-17-2011 18 Sites
Date: Wed 8/17/11

Task | Split | Progress | Milestone | Summary | Project Summary | External Tasks | External Milestone | Deadline

ID	Indicators	Task Name	Duration	Start	Finish
113		eNode B Installation	5 days	Mon 7/9/12	Fri 7/13/12
114		Integration & Testing	5 days	Mon 7/16/12	Fri 7/20/12



Project: Bignet 8-17-2011 18 Sites
Date: Wed 8/17/11

Task | Split | Progress | Milestone | Summary | Project Summary | External Tasks | External Milestone | Deadline