I. Executive Summary

In compliance with FCC Order 10-19 released May 12, 2010 in the matter of Requests for Waiver of Various Petitioners to Allow the Establishment of 700 MHz Interoperable Public Safety Wireless Broadband Networks (Waiver Order), the State of Oregon is providing this document as an overview of the required plan for achieving interoperability with other public safety broadband networks (Interoperability Showing). This Interoperability Showing follows the outline and topics as required in the FCC Public Notice of May 21, 2010 (DA 10-923).

This document addresses the following areas, focusing on how the State of Oregon is planning to implement features, functions, and standards in the most prudent manner practical to ensure interoperability consistent with the terms of the Waiver Order. These topics are:

- System Architecture
    - Radio Access Network (RAN) Architecture
    - Core Network Architecture
    - Interfaces
    - Mobility and Handoff
    - Roaming
    - Priority Access and Quality of Service (QoS)
    - Security
    - Devices
- Applications
- Reliability and Availability
- Radio Frequency (RF) Engineering
    - Radio Access Network Planning
    - Interference Coordination
- Testing
- Deployment
- Operations, Administration And Maintenance (OA&M)

Since the State of Oregon is very early in their design and procurement process for the Oregon Public Safety Broadband Network (OPSBN), many of the specific details are yet to be determined. In each of the sections of this Interoperability Showing, we have strived to demonstrate how Oregon intends to use the 3GPP standards and other industry standards such as IP, to maximize the opportunity for interoperability. Across the entire span of Interoperable Components associated with **System Architecture**, Oregon has applied appropriate 3GPP standards making exceptions and additions as required to meet Public Safety needs.

Oregon has evaluated the minimum set of **Applications** as defined in the Waiver Order, as well as those defined by the NPSTC Broadband Task Force, Operations Working

Group, in their Required and Desired Applications document. The State evaluated the need for each application and the likelihood of suitable interoperable standards and equipment being available in the timeframe of the initial deployment. It is the intention of Oregon to deploy applications in a manner that maximizes interoperability and compatibility with other Public Safety Broadband networks.

Oregon will deploy a Public Safety grade LTE network meeting requisite **Reliability and Availability** standards. While it is not anticipated that reliability or availability directly impacts technical interoperability, we recognize that the network must meet the *functional* interoperability needs and expectations of public safety users. Oregon has defined several aspects that will be carefully addressed during the design and implementation to meet this goal.

Oregon has completed its initial **Radio Frequency (RF) Engineering** required for the OPSBN RAN planning and interference coordination. The OPSBN design adheres to industry guidelines for propagation modeling and uses state-of-the-art radio prediction software, calibrated to provide accurate estimates of LTE performance. To promote interoperability, Oregon has developed a plan to employ all reasonable efforts to minimize and/or mitigate interference, both within the State, and outside of the State.

Oregon has developed a **Deployment Plan** and a **Testing Plan** that meet the needs of the Broadband Technology Opportunity Program's (BTOP) timeline, and includes sufficient time and check-points to help ensure interoperability with other Public Safety Broadband networks. Specific attention was paid to governance establishment, sharing of internal Oregon resources (backhaul, infrastructure, etc.), and to the surrounding states' current Public Safety broadband plans.

The Deployment and Testing Plans for Oregon will be modified based on the results of the Public Safety Communications Research (PSCR) demonstration networks in Boulder and DC, and other network deployments which may precede OPSBN. The State of Oregon will participate in the PSCR demonstration network project and appropriate NIST National Broadband Network meetings.

Since no public safety LTE network field deployment exists today, testing new systems will most likely uncover unforeseen issues. We anticipate that the Testing Plan and processes developed for the OPSBN will be similar to those used for land mobile radio networks with the addition of appropriate LTE-specific testing.

The OPSBN will use widely-accepted industry models for **Operations, Administration and Maintenance (OA&M)**:

- Telecommunications Management Network (TMN)
- Fault, Configuration, Accounting, Performance, and Security (FCAPS)
- Information Technology Infrastructure Library (ITIL)

The integration of all three models will ensure superior operations, administration and maintenance of the LTE network.

Many of the proposed OPSBN sites are collocated with existing or planned Oregon Wireless Interoperable Network (OWIN) microwave backhaul sites. This will allow remote management of both the microwave and LTE sites from the OWIN Northern Command Center (NCC) and/or the Southern Command Center (SCC).

In order to control LTE operational expenses and efforts, the OPSBN will implement Self Organizing Networks (SON). SON is designed to be a multi-vendor solution allowing inter-operability between each vendor's subsystems. Implementing SON will minimize operating costs by reducing and eliminating manual configuration of the network over much of its lifecycle.

Oregon will also leverage the OPSBN's SON architecture and industry best practices to implement an effective maintenance strategy. Vendor service level agreements will also be leveraged as appropriate.

Due to the uncertainty associated with the early stages of the design, the State's Interoperability Showing document discusses the various interoperability factors at a high level. Oregon anticipates refining the Showing as the design of the OPSBN is developed further.

It is important to note that Oregon intends to adhere to the LTE standards as well as the recommendations and requirements of the Emergency Response Interoperability Center (ERIC) for the development, deployment and operation of the OPSBN. The impact of these standards and recommendations will be carefully considered during OPSBN design and deployment to ensure interoperability and compatibility with other Public Safety Broadband networks. Finally, Oregon anticipates that the OPSBN will be a willing and capable partner network in the Nationwide Interoperable Public Safety Wireless Broadband Communications Network.

Table of Contents

I. Executive Summary i

II. Interoperability Components 1

A. System Architecture 1

1. Radio Access Network (RAN) Architecture 1
2. Core Network Architecture 2
3. Interfaces 5
4. Mobility and Handoff 7
5. Roaming 9
6. Priority Access and Quality of Service (QoS) 10
7. Security 12
8. Devices 14

B. Applications 16

C. Reliability and Availability 18

D. Radio Frequency (RF) Engineering 20

1. Radio Access network Planning 20
2. Interference Coordination 21

E. Testing 23

F. Deployment 25

G. Operations, Administration and Maintenance (OA&M) 28

H. Appendix 31

1. Glossary 31

II. Interoperability Components

A. System Architecture

1. Radio Access Network (RAN) Architecture

The Oregon Public Safety Broadband Network (OPSBN) will use the Radio Access Network (RAN) architecture as defined by the 3rd Generation Partnership Project (3GPP) for Long Term Evolution (LTE), called the Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access Network (E-UTRAN). This architecture consists of a network of LTE base stations, termed Enhanced Node B (eNodeB), as illustrated in Figure 1. The E-UTRAN provides the wireless access for the Internet Protocol (IP) networks by the wireless LTE user equipment (UE).

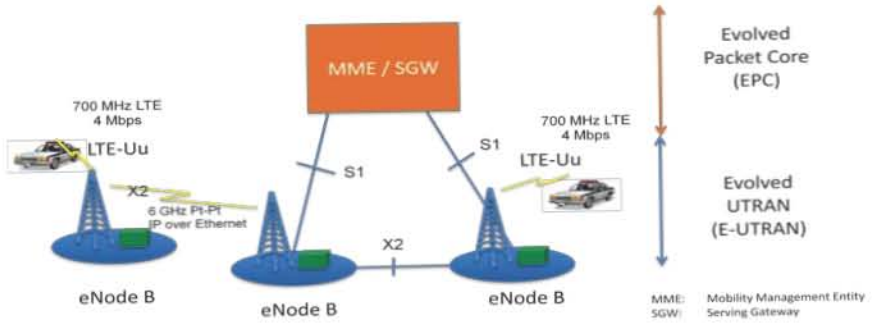


Figure 1 E-UTRAN

The E-UTRAN is responsible for all radio related functions such as:

- Radio Resource Management – including radio admission control, radio mobility control, scheduling, and dynamic allocation of resources to users
- Header Compression – compression of IP headers to conserve radio resources
- Security – encryption of the over the air data
- Interface to the Core network – interfaces with the Mobility Management Entity (MME) and Serving Gateway (SGW) of the Evolved Packet Core (EPC)

There is no central controller in this architecture for the eNodeBs, hence the E-UTRAN is considered a flat architecture. The eNodeBs are interconnected with each other via the standard 3GPP X2 interface, and connected to the core network via the standard 3GPP S1 interface. Each of the eNodeBs is capable of supporting the LTE air interface (LTE-Uu) over the 700 MHz channel. The use of standard 3GPP interfaces allows for ease of interoperability between other 3GPP compliant E-UTRAN and EPC.

The eNodeBs of the E-UTRAN are networked together via a combination of optical fiber and point-to-point microwave connections into a statewide fiber network allowing interconnection to other eNodeBs and the core network. The basic backhaul architecture is illustrated in Figure 2. This shows there is an Ethernet connection over fiber or microwave to each of the sites hosting the eNodeBs. In the Oregon network this amounts

to over 300 sites to provide sufficient wireless coverage to support 4 Mbps service to the UE in the service areas.

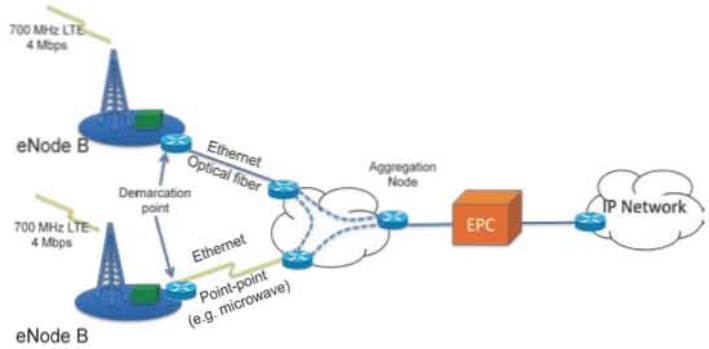


Figure 2 E-UTRAN Backhaul

A demarcation point is established at each of the sites to allow the isolation of the IP site equipment from the rest of the network for maintenance or servicing. Each of the backhaul links from the sites is capable of supporting a minimum of 30 Mbps of data throughput. The initial implementation of the Oregon public safety broadband network employs a single core network, but future enhancements for the network will incorporate multiple regional core networks. Each of the eNodeBs can be linked to more than one core network via the IP network in a meshed configuration as shown in Figure 3 affording ease of load sharing and redundant operation.

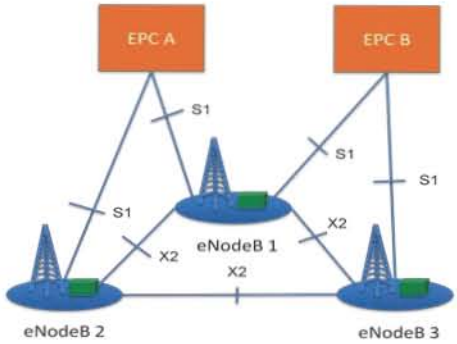


Figure 3 Meshed configuration

Oregon intends to adhere to the LTE standards as well as the recommendations and requirements of the Emergency Response Interoperability Center (ERIC) to assure interoperability and compatibility with other Public Safety Broadband networks.

2. Core Network Architecture

The OPSBN will use the network core architecture as defined by the 3GPP for Universal Mobile Telecommunication System (UMTS). The 3GPP core architecture is termed the System Architecture Evolution (SAE) that includes the EPC network. Together the LTE and SAE comprise the Evolved Packet System (EPS). The essential concept of the EPS is to route IP traffic between the Packet Data Network (PDN) and the UE via EPS bearers

each with a defined Quality of Service (QoS) between the gateway and the UE. Using the EPC's all-IP architectures will improve network performance and expand the range of services that can be provided. While the architecture is defined by the 3GPP, the State of Oregon cannot define the specific equipment until after a vendor is selected through an appropriate process, such as a competitive bid.

The EPC architecture has been optimized to deliver both real-time and non real-time packet based services.

In addition to providing reduced latency, higher data performance, and optimization for all services provided via IP; the EPC will also provide support for integration with other LTE networks and interworking with other radio access networks (e.g., 3GPP, 3GPP2) and data networks (e.g., WLAN). The interconnection of the EPC with the various LTE and non-LTE components is shown in Figure 4.

The EPC is comprised of the following logical functional elements. The actual integration of these functional elements into specific hardware is anticipated to vary somewhat depending on the selected vendor. The major logical nodes are:

- Mobility Management Entity (MME)
- Serving Gateway (SGW)
- Packet Data Network Gateway (PDN GW)
- Policy and Charging Rules Function (PCRF)
- Home Subscriber Server (HSS)

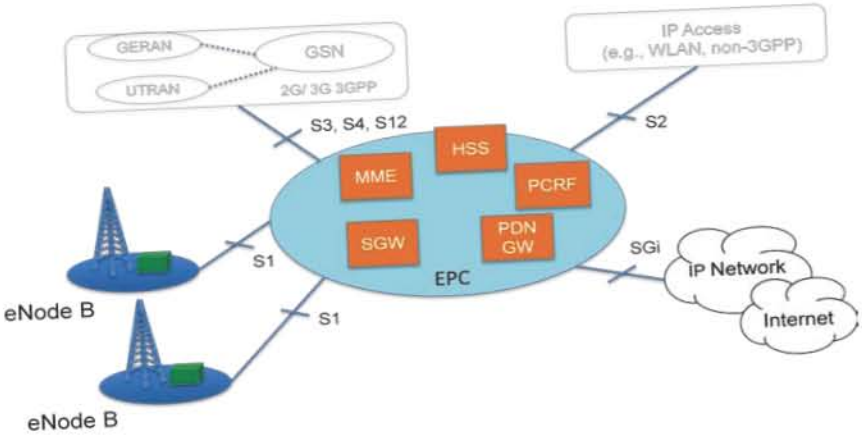


Figure 4 Core Network

Mobility Management Entity: The MME is the main control node for the LTE access network, handling a number of features:

- Idle mode UE tracking
- Bearer activation / de-activation
- Choice of SGW for a UE
- Intra-LTE handover involving core network node location

- Interacting with HSS to authenticate user on attachment and implements roaming restrictions
- It acts as a termination for the Non-Access Stratum (NAS)
- Provides temporary identities for UEs
- The MME acts the termination point for ciphering protection for NAS signaling. As part of this it also handles the security key management. Accordingly the MME is the point at which lawful interception of signaling may be made.
- Paging procedure
- The MME terminates the S6a interface for the home HSS for roaming UEs.
- The S3 interface terminates in the MME thereby providing the control plane function for mobility between LTE and 2G/3G access networks.

It can therefore be seen that the MME provides a considerable level of overall control functionality.

Serving Gateway: The SGW is a data plane element within the SAE. Its main purpose is to manage the user plane mobility and it also acts as the main border between the radio access network and the core network. The SGW also maintains the data paths between the eNodeBs and the PDN GWs. In this way the SGW forms an interface for the data packet network at the E-UTRAN. The SGW functions include:

- The Mobility Anchor point for inter-eNodeB handover
- Mobility anchoring for inter-3GPP mobility, including other LTE and UMTS networks.
- Transport level packet marking in the uplink and the downlink for various services and levels of QoS
- Accounting on user and QoS Class Identifier granularity for inter-operator charging
- Packet routing and forwarding
- Lawful (CALEA) Interception

Also when UEs move across areas served by different eNodeBs, the SGW serves as a mobility anchor ensuring that the data path is maintained.

Packet Data Network Gateway: The SAE PDN GW provides connectivity for the UE to external packet data networks, fulfilling the function of entry and exit point for UE data. The UE may have connectivity with more than one PDN GW for accessing multiple PDNs. PDN gateway functions include

- Policy enforcement
- Per-user based packet filtering
- Charging support
- Transport level packet marking for various services and levels of QoS
- User IP address allocation
- Dynamic Host Configuration Protocol (DHCP) functions
- Lawful (CALEA) Interception

Policy and Charging Rules Function: This is the generic name for the entity within the SAE EPC that detects the service flow, enforces charging policy. The features of the PCRF include:

- Policy and quota management functions based on 3GPP standards
- Network policy control by applying rules in response to conditions.
- Application policy control, controlling subscriber access by applying policies to applications and content

Home Subscriber Server: The Home Subscriber Server maintains information for the authentication, authorization, and establishment of user calls and sessions in LTE networks. In addition, the HSS stores significant user profile information and delivers user information to applications as required.

The primary function of the EPC is to provide bearer paths between the LTEs and the PDNs. The internal interfaces for the EPC are depicted in the section 3. Interfaces and will not be addressed here. The EPC interfaces to the LTE through the 3GPP standard interface S1, and completes the IP path via the standard 3GPP SGi interface to the external IP networks. This is the minimal support required to support broadband operation via the LTE network.

Additionally there is the support for interconnecting to non-LTE data networks. This is addressed as connecting to other networks of a 3GPP flavor (e.g., GMS, UMTS) via the 3GPP standard interfaces S3, S4, and S12; connections to non-3GPP networks (e.g., WLAN, CDMA) is handled via the standard 3GPP S2 interface. In this manner interoperability is afforded across neighboring LTE networks, and non-LTE networks alike.

These functions operate in a unified manner to provide the set of services required for the coordinated operation for the LTE network, and to manage its interconnection with other networks. This core will effectively and efficiently connect the Oregon Public Safety Broadband network to the commercial wireless networks providing services within the State, to the internal State of Oregon public safety and government operations networks, to the Internet, and to adjacent states broadband wireless networks as they are implemented.

3. Interfaces

The OPSBN utilizes interfaces from the set of standard 3GPP interfaces. The general interface diagram for the system is shown in Figure 5. This diagram shows the mandatory interfaces to afford operation within the Oregon public safety wireless broadband data network, and the secondary interfaces needed to extend the functionality of the network to adjacent networks of various types.

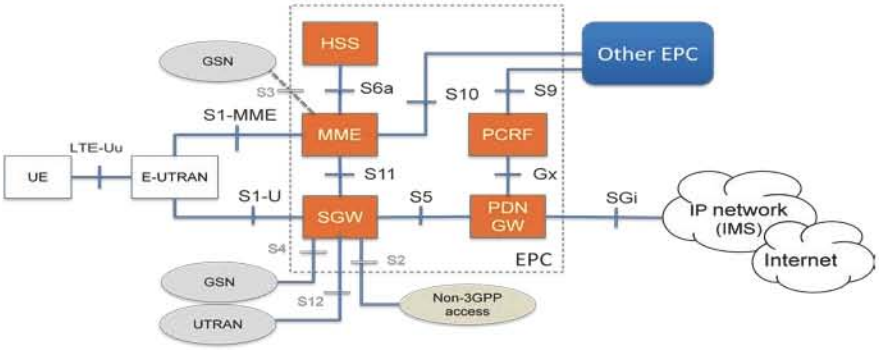


Figure 5 Network Interfaces

The mandatory interfaces define how the broadband network will allow an UE to interface to the network and subsequently to an IP endpoint. Interfaces that are considered mandatory are:

- S1-MME: - Reference point for the control plane protocol between E-UTRAN and MME.
- S1-U: - Reference point between E-UTRAN and SGW for the bearer user plane tunneling and inter-eNodeB path switching during handover.
- S5: - It provides user plane tunneling and tunnel management between SGW and PDN GW. It is used for SGW relocation due to UE mobility and if the SGW needs to connect to a non-collocated PDN GW for the required PDN connectivity.
- S6a: - It enables transfer of subscription and authentication data for authenticating/authorizing user access to the evolved system (AAA interface) between MME and HSS.
- Gx: - It provides transfer of QoS policy and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the PDN GW
- Gxc: - Allows PCRF to subscribe to appropriate event triggers in the Bearer Binding and Event Reporting Function (BBERF) located in the S-GW, as defined in 29.212.
- S8: - Inter-PLMN reference point providing user and control plane between the SGW in the VPLMN and the PDN GW in the HPLMN. S8 is the inter PLMN variant of S5.
- S10: - Reference point between MMEs for MME relocation and MME to MME information transfer.
- S11: - Reference point between MME and SGW.
- S9: - It provides transfer of (QoS) policy and charging control information between the Home PCRF and the Visited PCRF in order to support local breakout function.
- S13: - It enables UE identity check procedure between MME and EIR.
- SGi: - It is the reference point between the PDN GW and the packet data network. Packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. for provision of IMS services..
- Rf/Gz: - PCEF to Offline Charging System (OFCS) Interface as specified in 3GPP TS 32.240.
- Ro/Gy: - PCEF to Online Charging System (OCS) Interface as specified in 3GPP TS

32.240.

- LTE-Uu: – access network air interface
- X2: - intra-network eNodeB connection shall be required within a homogeneous public safety 700 MHz regional network; enables collaboration between eNodeBs for such as hand-overs.

The secondary interfaces are those that would be exercised to extend the scope of the broadband network. This would include the ability to interface to non-LTE based wireless networks, affording roaming support. With the potential of both 3GPP and 3GPP2 based commercial operators for roaming arrangements, it is necessary to provide some minimal interface capability to both types of access networks. The secondary interfaces are:

- S2: - It provides the user plane with related control and mobility support between evolved Packet Data Gateway (ePDG) and the PDN GW. It is based on Proxy Mobile IP
- S3: - It enables user and bearer information exchange for inter 3GPP access network mobility in idle and/or active state.
- S4: - It provides related control and mobility support between GPRS Core and the 3GPP Anchor function of SGW. In addition, if Direct Tunnel is not established, it provides the user plane tunneling.
- S12: - Reference point between UTRAN and SGW for user plane tunneling when Direct Tunnel is established. It is based on the Iu-u/Gn-u reference point using the GTP- U protocol as defined between SGSN and UTRAN or respectively between SGSN and GGSN. Usage of S12 is an operator configuration option.
- Gxa: - Allows PCRF to subscribe to appropriate event triggers in the Bearer Binding and Event Reporting Function (BBERF) located in a trusted non-3GPP access gateway, as defined in 29.212

At this time all other interfaces defined in the 3GPP suite for LTE are not considered necessary. In the future as the system evolves and expands this may change and additional interfaces may be desired.

4. Mobility and Handoff

Mobility is defined as the movement or handover of a properly authorized UE among sites within a Public Land Mobile Network (PLMN) defined area; that is the sites that broadcast the same PLMN. This may be within a Public Safety (PS) LTE network, a commercial LTE network, or a non-LTE network. The handover occurs due to physical movement of the UE or due to conditions at the current source site, such as failure at the site or the need to shed user load to other sites. Movement across PLMNs is considered Roaming and addressed separately.

The primary mobility and handoff considerations will be regarding the operations while registered to an LTE network. This network may be one of the PS LTE networks, or one of the commercial LTE networks. While in the jurisdiction of the LTE network there shall be standard LTE mobility applied as defined in TS 36.133. Handovers in LTE are ‘hard’

handovers, meaning that there is a short interruption in service when the handover is performed (the connection to the source eNodeB is dropped prior to establishing the connection to the target eNodeB), in contrast to soft handover in which the connection to the target is established while retaining the connection to the source.

The other mobility of interest to the PS LTE UE regards operation upon a non-LTE data network. These can take the form of networks such as 2G/3G cellular networks, wireless local area network (WLAN), etc. It is necessary for the PS LTE UE to be capable of normal operation upon the radio access technology associated with these non-LTE networks, and this includes the mobility management functionality. There are additional interfaces and functionality required in the LTE network to handle the handoff/handover scenarios between LTE networks and non-LTE networks. This is the standard 3GPP and 3GPP2 mobility management for 2G/3G. (The major interfaces have been identified in Figure 5 and discussed in the previous section.)

With the flat architecture of the E-UTRAN, most of the handover mechanics take place at the eNodeBs. The eNodeB that is handing over the UE must provide a full complement of the information regarding any active sessions for the UE to the target eNodeB that is to start handling this UE. There are currently two separate standard modes of handover defined for LTE, one makes direct use of the X2 interface between eNodeBs, and the other is an EPC assisted handover using the S1 interface between the eNodeB and the core network.

Typically eNodeBs that provide a regional coverage that can expect to experience numerous handover instances (e.g., nodes along a roadway, nodes in a dense population center) will have the X2 interface enabled among the eNodeBs to ease the handover experience.

There are two handover schemes defined currently in the Release 8 version of the 3GPP standard, backward handover, and radio link failure handover. These shall both be supported in the PS LTE implementation. Additionally as the 3GPP Release 9 standard is established, the new “forward handover” will be evaluated, potentially reducing the average download time by 50% during the handover.

The major issues for the PS LTE handover focuses upon the need for unique PLMN ID and IMSIs. The PLMN IDs are currently controlled addresses across the cellular networks. The PS network needs to have a standard PLMN assigned for its use allowing unique identification of that network and allowing roamers to potentially utilize the network. Additionally the IMSI that uniquely identifies the UE needs to be associated with a valid Home Network Identity (HNI) [derived from the PLMN]. The mobility can be controlled to a degree by the programming of the USIM of the UE.

Whether the PLMN for the PS LTE network is a common PLMN shared by the nationwide network of PS LTE networks or is unique to each PS LTE network, there is the need for this to be unique in the address space of the PLMNs that is shared across the cellular networks.

Oregon intends to adhere to the LTE standards as well as the recommendations and requirements of the ERIC with regard to the implementation of PLMN and other mobility and handover specifications to assure interoperability and compatibility with other Public Safety Broadband networks.

5. Roaming

Roaming is defined as movement of authorized UEs to a different PLMN ID networks. This may be due to the movement of the UE taking it out of operational range of the current source site, or a fault with the current source site. The unique IMSI for the UE will be used to track the unit back to its home PS network.

Roaming shall be addressed across the various types as shown in Figure 6:

- PS LTE networks – Intra PS Roaming
- Local commercial LTE networks – Homogeneous Roaming
- Local non-LTE networks – Heterogeneous Roaming

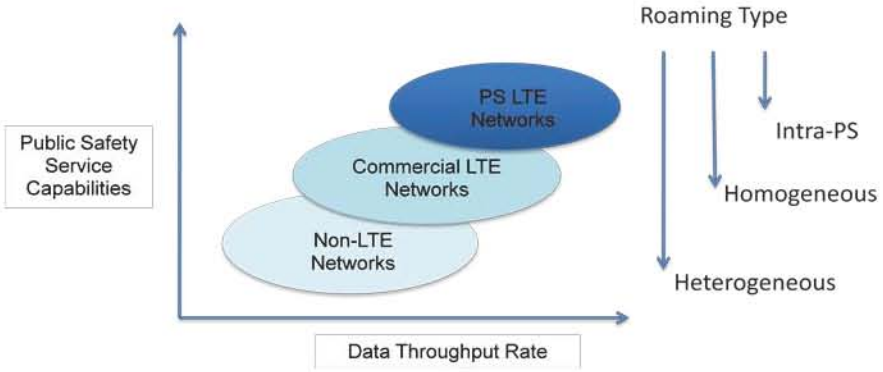


Figure 6 Roaming type

Roaming among the PS LTE networks will present a common set of public safety capabilities to the UE and shall maintain the UE data sessions between PS networks. This is being termed Intra-PS Roaming. This is the highest level of roaming conserving the expected PS capability and data service.

Roaming to and among commercial LTE networks, termed Homogeneous Roaming, shall support maintaining UE data sessions. The level of PS service capability will generally be less than that normally experienced by the UE in the PS LTE networks. Issues such as PS priority and special services will be dependent upon the service level agreements (SLA) within the roaming agreements established between the networks for the PS LTE UE. Some services normally supported in the PS LTE network, typically QoS controlled services, may not be available in the commercial LTE networks due to minimal QoS support. The data throughput rates negotiated for the roaming PS LTE UE may be less than that normally experienced in the native PS LTE networks.

Roaming to and among non-LTE networks (e.g., 2G/3G cellular networks, WLAN), termed Heterogeneous Roaming, will in general not support maintaining data sessions as the PS

LTE UE moves to these network sites. The level of PS service capability will generally be much less than that normally experienced by the UE in the PS LTE networks. Issues such as PS priority and special services will be dependent upon the SLA within the roaming agreements established between the networks for the PS LTE UE. Some services normally supported in the PS LTE network (typically QoS controlled services) will not be available in the non-LTE networks. The data throughput rates negotiated for the roaming PS LTE UE will generally be much less than that normally experienced in the native PS LTE networks.

Prior to any UE being allowed access to a network there is a need for authentication of the UE and subsequent authorization for the UE to function on this network. The authentication and authorization are the standard 3GPP operations using the HSS supplied information for the UE.

Some issues regarding roaming include:

- The PS LTE network needs a unique PLMN ID.
- The PS LTE UE needs a unique IMSI.
- There is the issue of retaining priority service as a UE moves from the PS LTE network to a non-PS network. There is also a need for a mechanism to negotiate QoS across networks.
- There may be an additional requirement to offer roaming reciprocity to allow non-PS users to roam to the PS network and receive a lower grade of service on the network than the resident PS users. The PS users shall always receive higher priority for resource access than a visiting non-PS user.
- Units roaming to other PS networks should retain their assigned security levels and should maintain any tunnels already established. Roaming to non-PS networks typically will not routinely support retaining any security levels from the PS network activity. The security levels would be negotiated with the current host network; if the appropriate level is not available then the network access would be disallowed or at a minimum there would be user feedback to indicate failure of security aspects of the session.

Oregon intends to adhere to the LTE standards as well as the recommendations and requirements of the ERIC with regard to the implementation of roaming specifications and requirements to assure interoperability and compatibility with other Public Safety Broadband networks.

6. Priority Access and Quality of Service (QoS)

For the successful implementation of Public Safety (PS) broadband networks there is the need to have a common definition of priority levels and how they are interpreted within the PS network (and globally across PS networks).

The priority levels should translate to specific QoS levels to associate to the associate bearer for the service. A UE may have multiple bearers active each with a unique priority level or QoS associated with it. This will be addressed across a service type and for specific user identities (individual and group). There is the potential need to have a means to increase the priority level of a particular session temporarily (e.g., during an event) and be restored to normal modes automatically later.

A potential priority scheme incorporates a multiple level priority assignment with a combination of global priority assignments and local network assignments. The Table 1 shows priority addressing proposed as follows:

Table 1 Priority Addressing Proposal

Priority	Level	Description
$0F-$0C	Global	High priority elements to be commonly supported across all PS LTE networks (e.g., emergency)
$08-$0B	Local	High priority elements to be supported local to a PS LTE network (tactical)
$04-$07	Global	Operational priority element shared across all PS LTE networks
$00-$03	Local	Operational priority element shared across a PS LTE network (e.g., dispatch levels)

The QoS definitions are defined in 3GPP TS 23.401. Generally the bearer QoS is concerned with defining the data throughput parameters such as maximum bit rates, guaranteed bit rates, etc. All activity for a bearer by default will subscribe to the bearer QoS assigned. There should be separate levels established minimally for such as:

- Real-time streaming video
- Voice
- Interactive
- Best effort

There are aspects of the QoS control at both the eNodeB and in the EPC. The eNodeB is concerned with the delivery of the IP messaging to the UE over the physical RF channel. This channel can actually be serving multiple different sessions for a UE and even multiple UEs each with their own separate sessions needs. The eNodeB needs to identify the class of service from the QoS Class Identifier. Each of the bearers handled by the eNodeB needs to be assigned a priority for retention, should local resource limitations arise at the eNodeB. The eNodeB must also view the grouping of bearers to control the aggregate bit rates, factoring in the need for any guaranteed bit rate bearers. The core network shall be tasked with maintaining and promoting the QoS Class Identifier to the PDN bearers. Additionally the core network shall be responsible for cataloging and recording the use of specific QoS classes by user and by service. This can be used to both determine the operational condition of the networks as well as a means for better determining user fees for IP services utilized based on QoS levels applied.

Some issues for supporting interoperable priority and QoS include:

- Priority access needs to be afforded the PS users when they roam to the commercial networks. This needs to be in the form of SLAs that define how the service is to be provided to the PS users.
- There is the issue of how to support QoS needs on networks that do not generally provide any QoS differentiation for their native non-PS users.
- There shall be a common definition of the supported priority levels assigned to users (individual and group) and services across a PS network
- There needs to be a global definition for maintaining priority level operation across different PS networks.
- The QoS span of control for the LTE network is essentially end-to-end from UE to the target IP network. There are questions as to how this is to be supported or approximated in non-LTE networks.

Oregon intends to adhere to the LTE standards as well as the recommendations and requirements of the ERIC with regard to the implementation of Priority Access and Quality of Service specifications to assure interoperability and compatibility with other Public Safety and possibly Commercial Broadband networks.

7. Security

As required by the Waive Order and recommended by Section 6.3.3 of the National Public Safety Telecommunications Council (NPSTC) Broadband Task Force (BBTF) report, the OPSBN will support 3GPP Release 8 LTE network and subscriber security features. These security features, as specified by TS 33.401, include Authentication and Key Agreement (AKA), complex key hierarchy and interworking security, and additional security for eNodeB. Figure 7 illustrates the proposed security architecture for the statewide network that complies with the 3GPP Release 8 specifications.

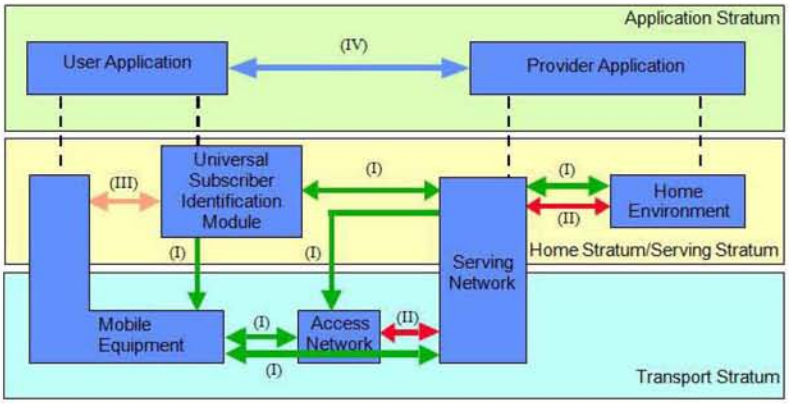


Figure 7 Security architecture

There are five feature groups in the architecture to meet certain threats and accomplish certain security objectives as follows:

(I) Network access security features – provide users with secure access to services, and which in particular protect against attacks on the (radio) access link.

(II) Network domain security features – enable nodes to securely exchange signaling data, user data, and protect against attacks on the wire line network.

(III) User domain security features – secure access to mobile stations.

(IV) Application domain security features – enable applications in the user and in the provider domain to securely exchange messages.

(V) Visibility and configurability of security features (not shown) – enable the user to determine whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

In addition to the above security features, the public safety LTE network will also employ the following protocol layers:

- The Radio Resource Control (RRC) protocol layer, as specified in TS 25.331, will support LTE signaling layer security features. Therefore, confidentiality and integrity protection terminates in the Mobility Management Entity (MME).
- The Non-Access Stratum (NAS) protocol layer, as specified in TS 24.301, will support EPC signaling layer security features. As a result, integrity and confidentiality protection terminates in eNodeB.
- The Packet Data Convergence Protocol (PDCP) layer, as specified in TS 36.323, will support user data plane security features. These features include integrity protection, verification, ciphering, and deciphering of data.

The LTE network will use 128-EEA1 and 128-EIA1 algorithms which are identical to the 3GPP Confidentiality and Integrity UEA2 and UIA2 algorithms. Advanced Encryption Standard (AES) and SNOW 3G will be used for encrypting and decrypting both control and message traffic and for message authentication of the traffic. All keys used for crypto-algorithms are currently 128 bits with a possibility to add 256-bit keys later if need be.

Key management is based on a common secret key K_{ASME} (Access Security Management Entity) which is available only in a secure part of the USIM and the HSS Authentication Center. Generated keys, checksums, and random numbers from the Authentication Center are transferred to the MME and passed to the UE. NAS protocols enable mutual authentication of UE and network computed checksums. Upon connection establishment, K_{ASME} is used to derive an eNodeB-specific base key K_{eNB} in the Access Stratum (AS). K_{eNB} is used to generate three AS derived-keys: one for integrity protection of RRC signaling, one for ciphering of RRC signaling, and one for ciphering of user data.

For performance reasons, handovers are possible directly between eNodeBs. However, backward or forward security mechanisms must be implemented so that one compromised

eNodeB does not compromise all eNodeBs in a handover chain. The LTE network will provide three options for mobility between 3GPP and non-3GPP networks as follows:

- Proxy Mobile IP – no user-specific security associations between the Proxy and Home Agent
- Client Mobile IPv4 (MIPv4) – tailor-made security mechanisms are used
- Dual Stack MIPv6 – Internet Protocol Security (IPSec) with Internet Key Exchange (IKEv2) is used between User Equipment and Home Agent

The use of network layer (Layer 3) Virtual Private Network (VPN) will be allowed on the deployed network. Although Layer 2 VPNs tend to be cost effective and simple to manage, Layer 3 VPNs can support an IPSec distributed architecture that provides service scalability and broadcast domain reduction. Multiprotocol Label Switching (MPLS) is used for IP service-aware transport in the network layer VPN approach. The IP/MPLS service routers will provide a mesh architecture that enables cell sites to communicate directly with one another. This architecture not only improves performance but provides significant operational savings as well. The network layer VPN approach meets LTE requirements for QoS, latency, synchronization, security and load balancing.

8. Devices

Although there are currently no production LTE devices available on the market, this is expected to change in late 2011 and early 2012. Therefore, this section addresses the anticipated requirements of OPSBN LTE UE devices.

OPSBN LTE mobiles will carry the benefits of incorporating multi-mode and multi-band radios, allowing LTE mobiles to roam freely while seamlessly crossing technology boundaries. LTE mobile device vendors are expected to provide a highly integrated chipset and complementary RF modules for multi-mode terminals. OPSBN expects mobiles to deliver improved performance in the Reverse Link, as the wider bandwidth of the LTE network supports improved speed and power. Initial mobile devices are likely to be data-cards (USB, PC-Card or embedded) for laptop PC and PDA (handheld) deployments.

The applications that are planned for the initial deployment of OPSBN (see Applications Subsection) will require the necessary devices (UEs) in support of those applications.

Mobile and portable devices to support OPSBN operation will be selected with special consideration to:

- Wireless Security

  OPSBN coverage and a new generation of faster, more capable mobile devices will provide users valuable tools to help do their work especially in the field, and beyond their LTE coverage. There is a potential downside to this: a user doing their job in the field increases the risk of compromising data security and/or allowing malicious users with access back to the EPC and beyond. OPSBN will take all

practical measures to secure their UEs and preventing unauthorized access to network resources. The wireless security strategy will include a means of securing the mobile device and its data, securing the communications to and from the mobile device to the corporate network, and optimizing the network to support user mobility. The most effective wireless security strategy is a proactive one. OPSBN will develop, educate, enforce and maintain such a wireless security policy.

- Mobile Device Management

  Mobile Device Management (MDM) of the rapidly growing ranks of UEs is another important consideration for OPSBN to deal with. MDM solutions allow administrators to manage mobile devices similar to the way that they manage desktop and laptop computers. The selected MDM solution shall include the capability to distribute firmware upgrades, applications and configuration settings over the air (OTA) to UEs connected to the LTE network. An MDM solution ensures that all UEs are up to date with the latest versions of applications, data and configurations, so, that their device is secure and efficient. An effective MDM solution shall include the following important features:

  - Over the Air (OTA) – OTA facilitates the configuration of mobile devices, application updates and device locks if the user device is lost or stolen.
  - Back-up and Restore – Back-up of a mobile device is an essential activity for dealing with hard-resets and lost or stolen devices. It will also be used for synchronizing files and folders between a desktop computer and a mobile device.
  - Asset and Configuration Management – Configuration management shall be designed to provide OPSBN administrators the ability to view and categorize devices by user role, device type or any other criteria. The administrator can then selectively use the categorization to configure application profiles, mobile device settings and registry entries.
  - Mobile Security Management – Security management shall be designed to allow the administrator to enforce power-on passwords and VPN settings or wipe clean all data stored on a lost or stolen device.

  As the number of mobile users within the OPSBN, and the number of UEs increase, an effective MDM solution will become a necessity. A MDM solution shall be designed to improve mobile security, reduce risk and make it easier for OWIN administrators to manage the growing number of mobile users.

- RF characteristics and general LTE characteristics

  Field UEs shall be chosen to operate OTA seamlessly with any other authorized LTE Networks., All devices shall be equipped with a GPS receiver and supporting mapping software.

- Physical Characteristics
  - Ruggedness: MIL specifications for environmental survivability shall be mandatory for handheld devices.
  - Special functions: UEs shall be selected with one-button operation for frequently used applications. Maps of current location shall be a one-button access to the user.
  - Standard Laptops: Laptops serving as UEs shall be equipped with appropriate software and PC-CARD, USB, or other standard interfaces. Modems shall be capable of supporting PS LTE operation.

B. Applications

The State of Oregon supports the work of the NPSTC Broadband Task Force, Operations Working Group in defining the appropriate required and desired applications for a public safety broadband network. It is the intention of the State of Oregon to provide the greatest level of interoperability and compatibility of its OPSBN with the applications which will be provided by the eventual nationwide public safety broadband network.

The State of Oregon anticipates implementing support for many general application types, including Internet access, fixed format data entry, real time video, interactive database access, etc. Specifically the following types of applications for use on the initial implementation of OPSBN:

- Computer Aided Dispatch / Records Management System (CAD/RMS) – The network shall provide access to various sophisticated CAD/RMS systems specific to each agency and/or branch of service. The following are some examples of CAD/RMS transactions to be supported:
  - Law enforcement records checks - police officers can runs wants and warrants checks on individuals and vehicles
  - Traffic citations – officers can transmit citations directly into their records sections as well as the appropriate court
  - EMS patient care forms – allows EMS units to transmit patient care forms from the field to hospitals and/or EMS headquarters
  - Agency, Team and/or Incident status information - allows public safety users to receive call details as well as monitor the status of their peers

  This application will be enabled through an IP connection between the 700 MHZ client subscribers and host processors interfaced to the LTE core IP network. While the standardization of the specific applications and applications data does not fall under this program, it is anticipated that the creation of an interoperable broadband data network will lead to the greater deployment of standardized CAD/RMS systems.

- Status/information homepage – The network shall provide separate homepages for local users and roamers to ascertain area specific information, significant incidents, etc.

  This application will be enabled through an IP connection between the 700 MHZ client subscribers and a webhost interfaced to the LTE core IP network.

- Internet access – the network shall provide controlled Internet access allowing users (both local and roaming) to access specific services available over the Internet (e.g. EOC management sites, traffic cameras, etc.) as allowed by the local authority.

  This application will be enabled through an IP connection between the 700 MHz client subscribers and gateway/firewall interfaced to the LTE core IP network. One or more common Internet browsers will be tested and approved to assure interoperability.

- VPN access to home networks – the network shall provide VPN support for roaming users to access their home networks while outside their home area.

  This application will be enabled through an IP connection between the 700 MHz client subscribers and a VPN gateway interfaced to the LTE core IP network. One or more common VPN applications/protocols will be be tested and approved to assure interoperability. Access by Responders Under ICS – the network shall provide all mutual aid responders managed under the ICS structure of a requesting agency access to carry out incident objectives and communicate with their home networks

  This application will be enabled through direct IP connections between the 700 MHz client subscribers and through an IP connection to a gateway interfaced to the LTE core IP network.

- Field-based server applications - the network shall support the field-deployment of application servers, accessible from 700 MHz network client subscribers and accessible from Internet connections outside of the OSPBN.

  This application will be enabled through direct IP connections between the 700 MHz client subscribers and a server connected to a 700 MHz client subscriber device.

- SMS/MMS messaging – The network shall support Short Message and Multimedia Message creation and delivery services and be interacted with commercial networks to allow seamless transfer of messages

  This application will be enabled through the implementation of an SMS/MMS gateway within the LTE IP Core providing standardized interfaces to other Public Safety and commercial networks.

- Location-based data information – The network shall provide the capability to collect and convey subscriber unit location data in real time. Data will be accessible to appropriate applications as authorized by management level policy.

  This application will be enabled through the implementation of a location application processor interfaced to the LTE core IP network.

- One-to-many communications – The network shall support one-to-many public safety communications when standards exist.

  This application will be enabled through the use of IP multicast technology within the RAN and Core IP networks. Some one-to-many applications may require an application or middleware server interfaced to the LTE core IP network.

The State of Oregon recognizes that the LTE technology is in the early stages of development, and that some applications defined may require the use of technologies and standards that are not fully developed.

It is the intention of the Oregon Public Safety Broadband Network to provide access and support of applications leveraging the use of standards wherever possible. Where standards do not yet exist, the State may decide to implement some services in a proprietary manner, or may decide to withhold implementation until an appropriate standard is available. The decision on the early implementation will be made using the best information available at the time, and will provide careful consideration of the long term interoperability and compatibility issues that may be inadvertently created due to the implementation of early non-standard methods.

The State of Oregon recognizes that the use of some applications may impact overall network traffic, stability, and/or security. It is the intention of the Oregon Public Safety Broadband Network to provide the highest level of access and application support wherever and whenever possible. It is noted that the State of Oregon anticipates implementing management level policies that define and potentially limit network and application access and traffic as required to provide for the security, stability and efficiency of the overall OPSBN.

C. Reliability and Availability

Reliability, Availability and Serviceability (RAS) is a set of related attributes that will be considered when selecting the vendor of the OPSBN LTE network. RAS is relevant to the LTE network and the entire supporting infrastructure as well as through to the UEs. RAS relates to end-to-end service to the Ues, including RF propagation and roaming issues.

Reliability usually refers to the ability of system hardware and software component to consistently perform according to its specifications. A 100% reliable component is totally free of technical errors, but experience shows that this is never the case. Because the OPSBN system vendor is unknown, it is not possible at this time to specify expected system hardware/software reliability. However, reliability shall be selected to be sufficient to support public safety standards. With respect to RF propagation reliability, OPSBN

engineering shall ensure that the best possible eNodeB site locations (albeit restricted for practical reasons) and tower/antenna designs are implemented. Since a vendor is not yet selected, it is not possible to quantify this system attribute.

Availability is the ratio of time the system is not functional, (as observed by Ues) to the total time it is required or expected to function. In the case of OPSBN the latter time is 24/7 year-round. Availability is expressed as a percentage so, for example, a 90% available system would be unavailable for an expected 36.5 days per year; this is totally unacceptable for network Safety users. Cellular operators are targeting an LTE availability of 99.999% end-to-end to the UE devices, which translates to roughly 5.25 minutes/year. This is a laudable goal for OPSBN and given the terrain and site availability, this may be very difficult to achieve without the possible future sharing of commercial and other jurisdictions' resources.

Serviceability is an expression of the ease (ergo time related to) the completion of maintenance, replacement or repair of any critical component, device or system, which may directly affect system availability. OPSBN considers that early detection of potential problems is critical in this respect. Systems to be considered by OPSBN shall have the ability to identify and correct most problems automatically before serious trouble occurs, and any detected faults shall be directed to the 24/7 maintenance division dispatcher consoles. Additionally, maintenance and repair operations shall cause minimum downtime and disruption, thus maximizing the system availability to end users.

The selection of a systems supplier by Oregon shall consider these major objectives to ensure acceptable RAS attributes:

- Over-engineering: Oregon will give priority to systems designed to specifications better than minimum requirements.
- Duplication: Oregon will give priority to the extensive use of redundant systems and fault-tolerant engineering methods and components. The issue of redundant backhaul facilities from the eNodeB sites to the EPC system will be addressed to the extent possible within budgetary constraints. There shall be NO single point of failure that will affect the entire system.
- System Updating: Oregon shall ensure that Oss and applications are current; Oregon is keenly aware of related security issues, so this shall be closely monitored by qualified security staff.
- Data Backup: Oregon will ensure backups to prevent catastrophic loss of critical information for restart/recovery needs.
- Power-on Replacement: Oregon will make it mandatory to enable hot swapping of components or peripherals.

- Lightning, Grounding and Power: Oregon will make it mandatory to implement rigorous industry standard lightning protection, tower and halo grounding for all eNodeB sites and communications rooms, as well as power conditioners to minimize the risk of component damage resulting from power-line anomalies.

- Uninterruptable Power Supply (UPS): Where appropriate, Oregon will make it mandatory to use UPS to keep systems operational seamlessly while switching from commercial power to backup or auxiliary power.

- Back-up Power: ALL Oregon eNodeB sites and communications rooms shall have backup power sources, which include batteries, generators and solar to keep systems operational during extended interruptions to commercial power.

D. RADIO FREQUENCY (RF) ENGINEERING

1. Radio Access network Planning

The RF design of the OPSBN adhered to industry guidelines for propagation modeling, using state-of-the-art radio prediction software that was calibrated to provide accurate estimates of LTE performance. The following elements were considered in the analysis:

- **Dynamic Throughput –** LTE equipment dynamically adjusts a given user's throughput based on the received signal strength at the radio, and the current task (e.g. video upload/download, static image transfer, text messaging). The coverage analysis for the State of Oregon system based its performance thresholds on an average throughput allowance.

- **User Loading –**LTE systems have the ability to assess the current user load on a given access point, and dynamically adjust the amount of bandwidth provided to a given user. The State of Oregon coverage analysis factored this element into the LTE performance thresholds, basing the usable coverage on an average loading scenario.

- **Radio Propagation at 700 MHz –** The software used for calculating the free space loss of 700 MHz frequencies was calibrated using real-world drive-tests performed in the State of Oregon. Using this measured data, the propagation model in the software was tuned to reflect accurate measurements of the 700 MHz channels that are dedicated for broadband public safety use.

Table 2 outlines specific technical parameters that were used in the OPSBN coverage analysis.

Table 2 OPSBN coverage parameters

Parameter	Value Used	Comment
Antenna Type	Omni-directional	Revised designs may incorporate multiple sectors, using directional antennas, to complete the 360-degree pattern
Antenna Gain	9 dBd	High-gain antennas are often employed at 700 MHz
Antenna Heights (Existing sites)	Variable	For existing locations, LTE RF antennas were often placed at heights 20-30' down from the top of the existing structure.
Antenna Heights (Greenfield sites)	80 ft.	Average AGL height at which the State feels comfortable being able to achieve with new construction.
Transmit Power (site)	50 Watts	Assumption, as equipment specifications are still being finalized.
Transmit Power (UE)	15 Watts	Assumption, as equipment specifications are still being finalized.
Channel Bandwidth	5 MHz	Consistent with the current broadband plan for PS LTE applications.

In addition to the coverage-specific technical parameters, considerations were also given to the possibility of implementing frequency reuse. By placing RF sites at optimal distances, and with consideration to terrain, frequency reuse can likely be employed throughout the State. This will likely decrease the amount of spectrum necessary to build the system.

2. Interference Coordination

The State of Oregon will make every effort to mitigate any potential interference issues both within the State jurisdictions, and outside of the State jurisdictions. The proposed plan for minimizing any interference shall consider the following:

- **Radiation control via antenna pattern selection and configuration** – Using the propagation tools at the State's disposal, various antenna patterns from many manufacturers shall be examined to determine the extent of the broadcast signals. In addition, tilting the antennas to limit any superfluous or potential destructive interference may be employed.

- **Power levels** – By reducing the power broadcast from access points, the State can limit potentially destructive signals from interfering with any 700 MHz incumbent users.

- **Geographic considerations** – By taking advantage of the rugged terrain in Oregon, many of the proposed LTE sites will have natural terrain features (i.e. mountains, ridges), which will likely block signals from propagating beyond the desired coverage area. These natural RF barriers can substantially limit interference potential, and allow for more efficient frequency planning.

The self-organizing network (SON) was recommended by the Next Generation Mobile Networks alliance as a key design principle for next-generation mobile networks. As a result, the 3GPP standardization body introduced SON in its LTE Release 8. SON offers many ways of improving operating efficiency such as automatic interference reduction, including coordination of sub-tones and power levels across eNodeBs.

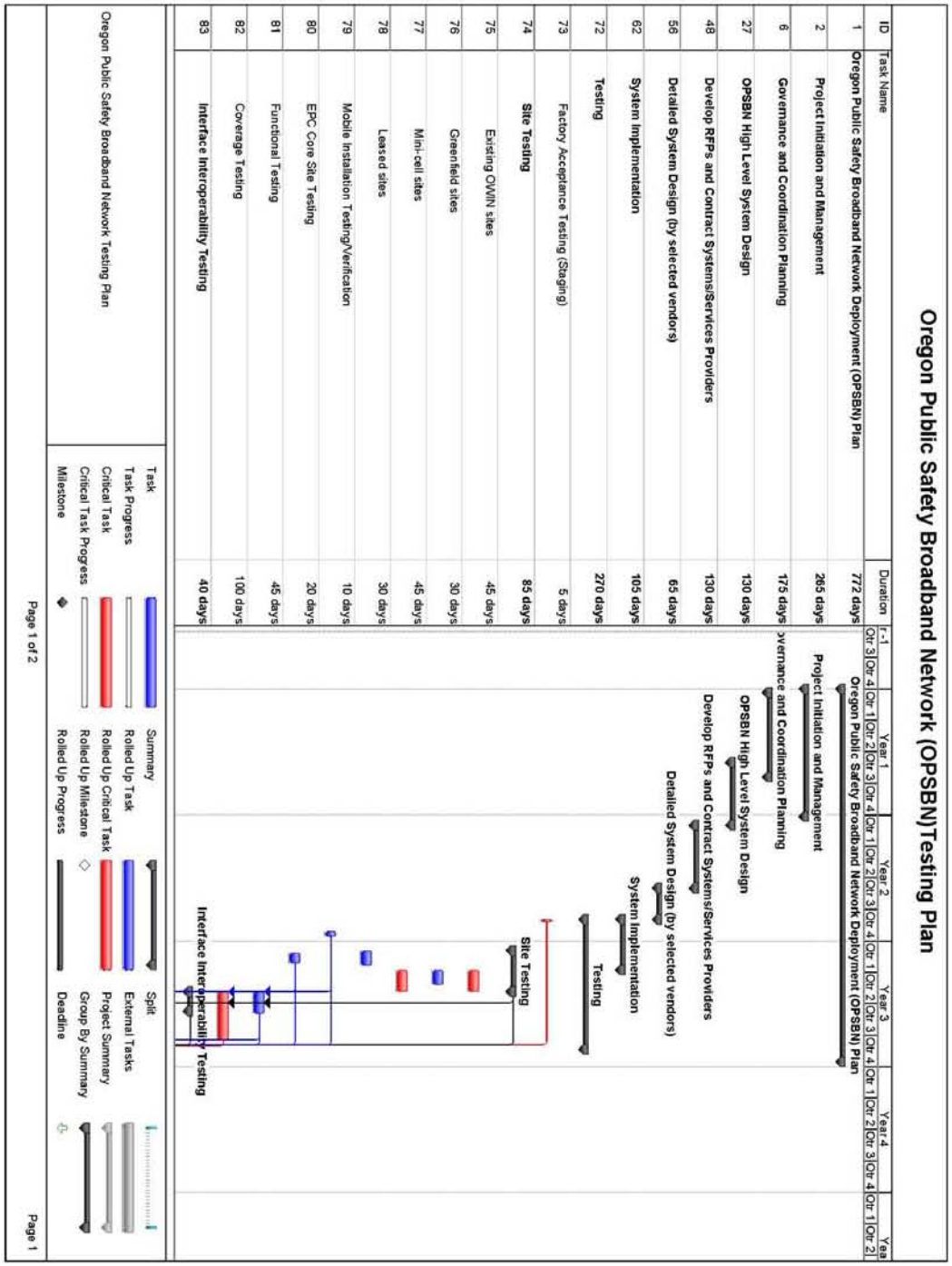
SON function may be used to properly tune configuration parameters in order to improve interference control, while reducing the effort of manual configuration and optimization. Use of SON in the OPSBN will have following expected results:

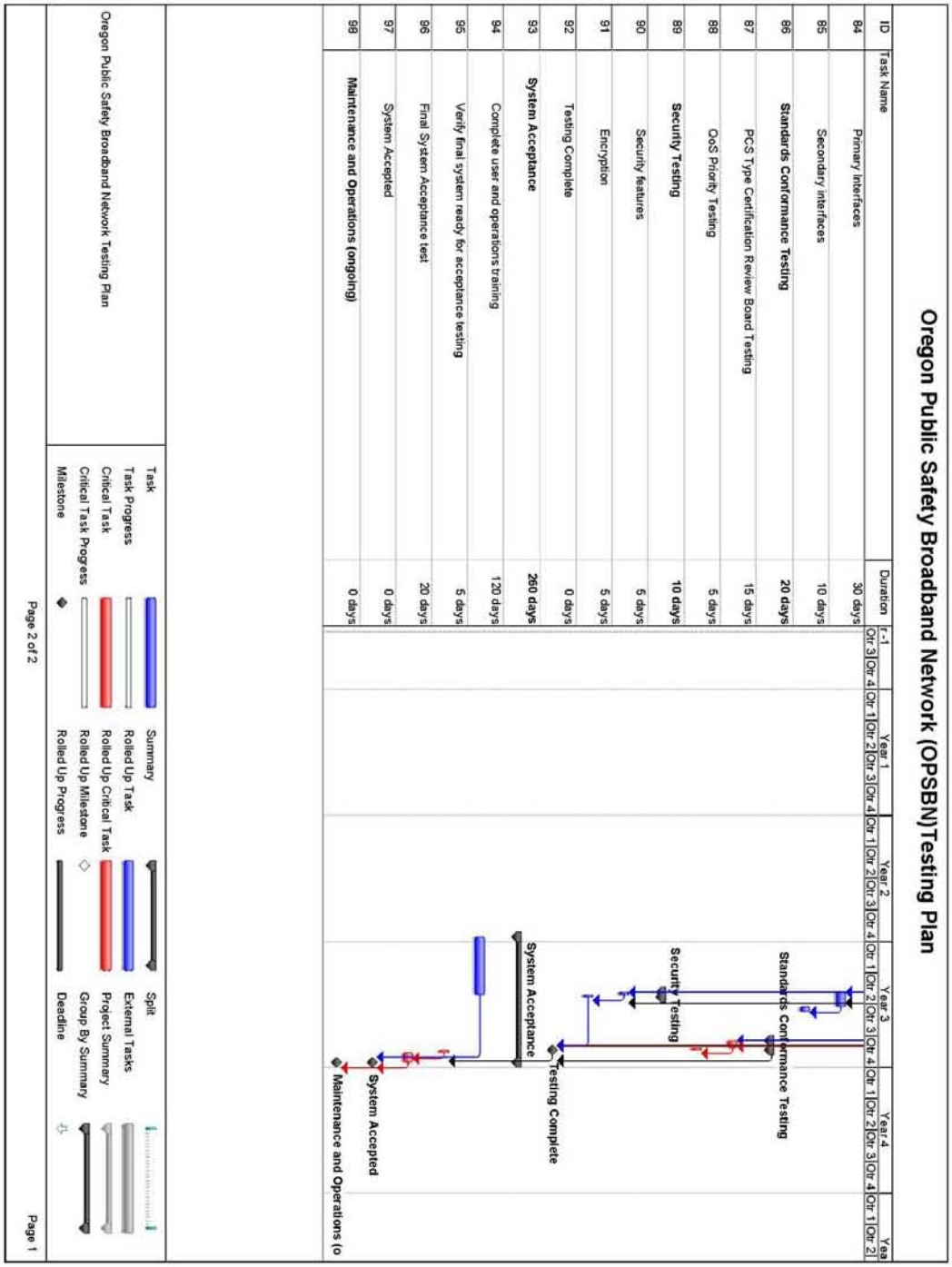
- Automatic configuration or adaptation, with respect to cell topology, of
  - Resource preferences in eNodeBs
  - Inter-cell Interference Coordination (ICIC) reporting thresholds/periods
  - Reference Signal Received Power (RSRP) threshold for ICIC

- Minimized human error in network management and optimization tasks

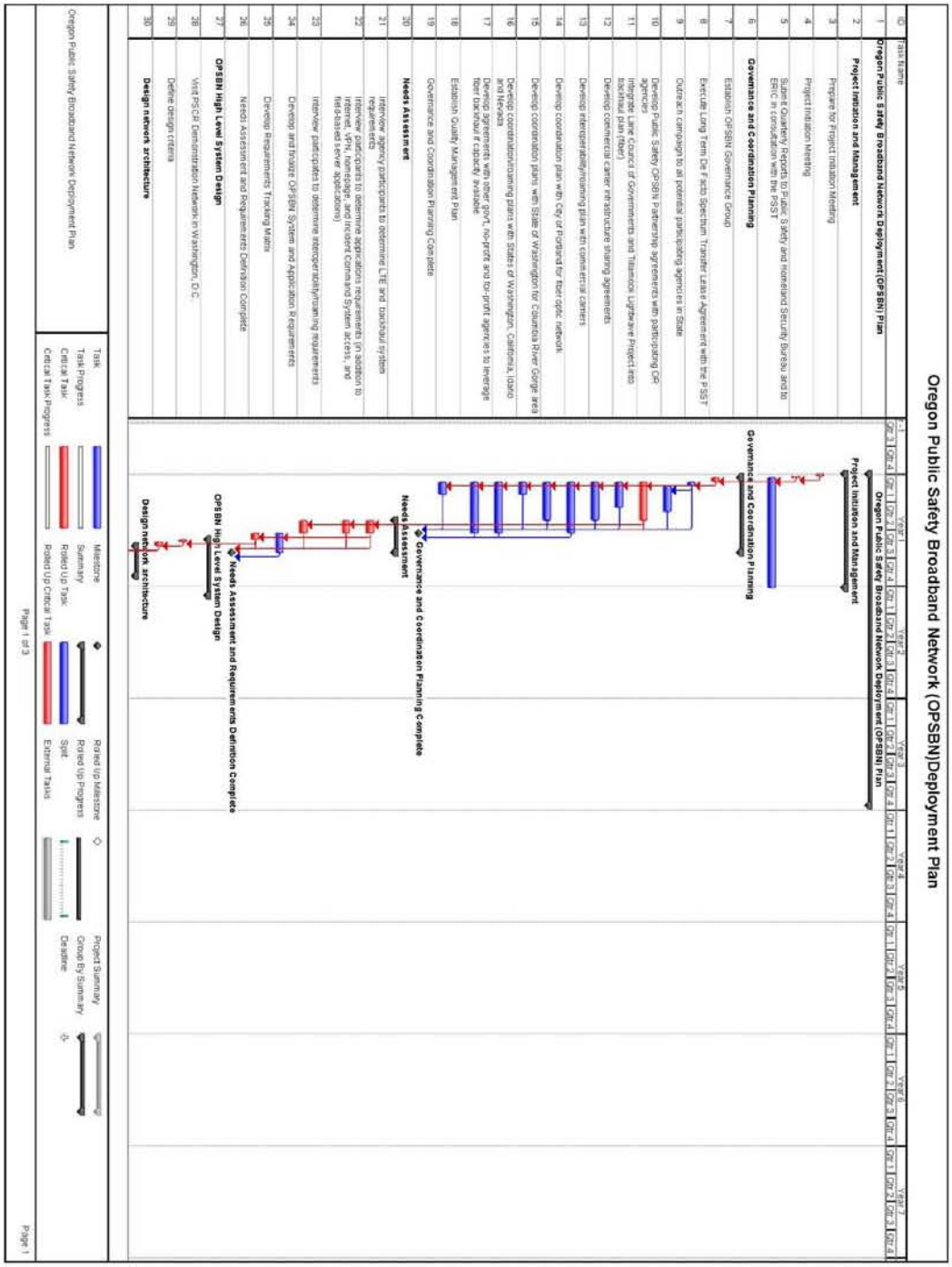
- Optimized capacity and radio network performance

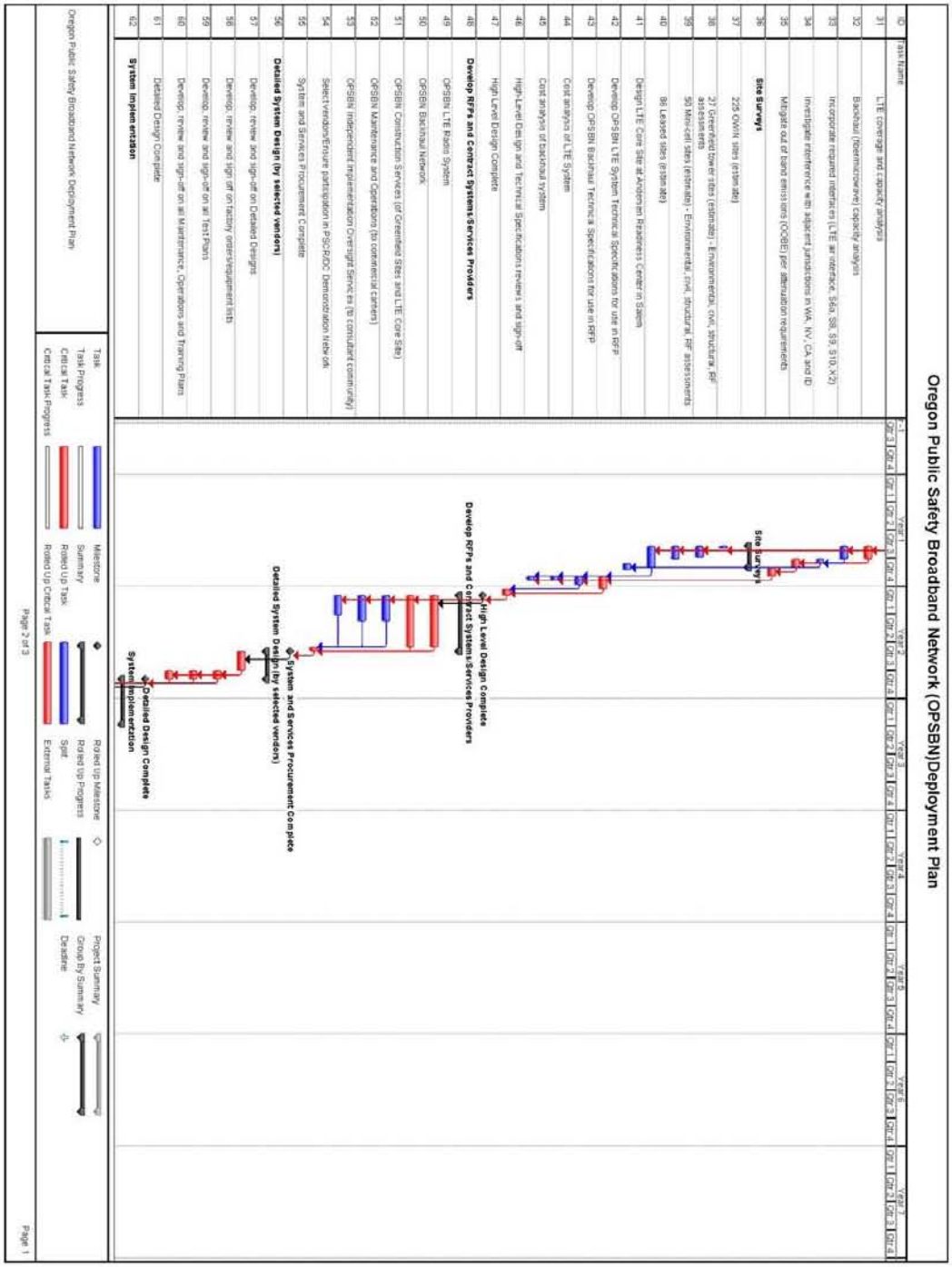
E. Testing

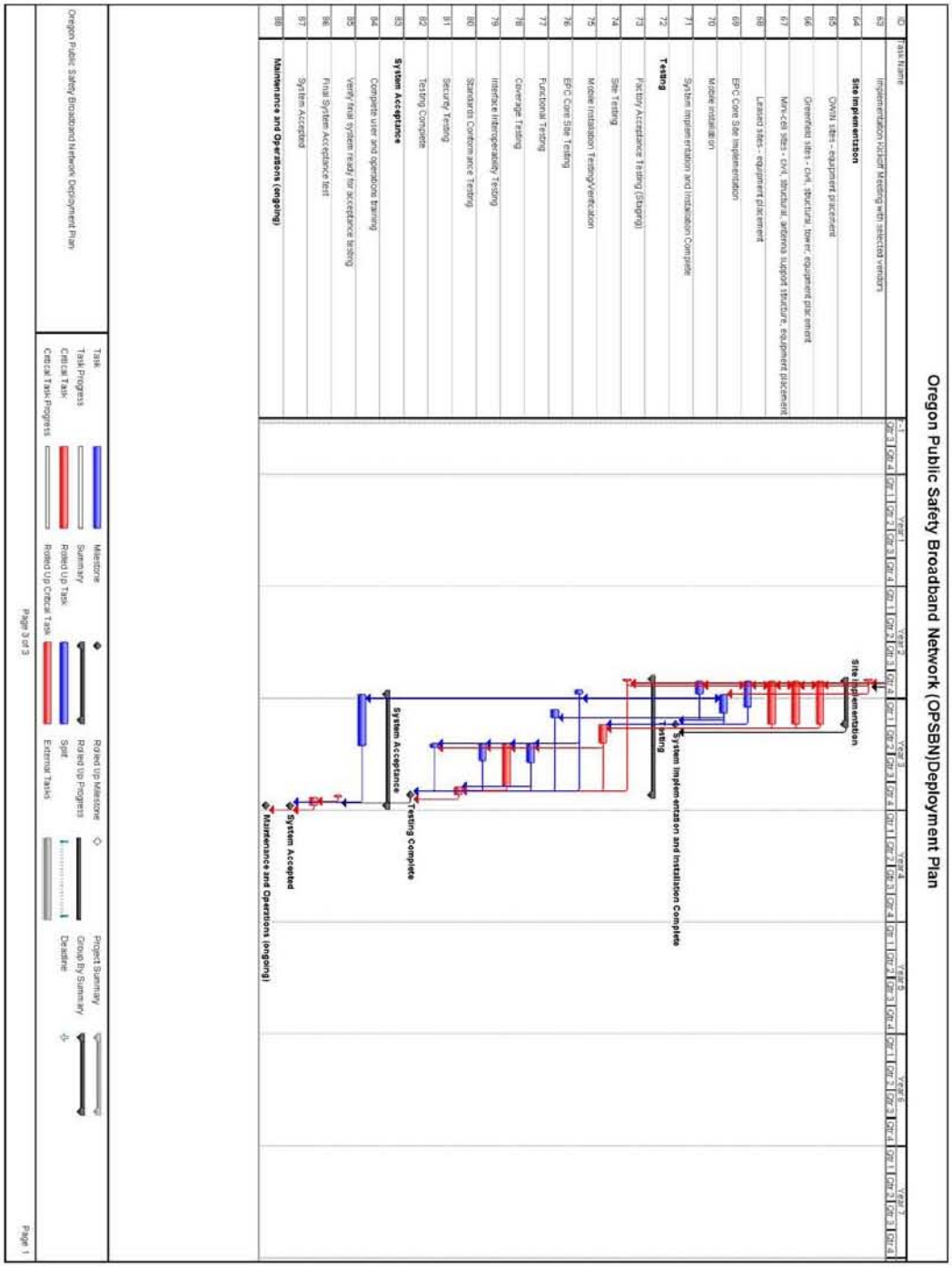

Oregon Public Safety Broadband Network (OPSBN)Testing Plan
ID
Task Name
Duration
Year 1
Year 2
Year 3
Year 4
1 Oregon Public Safety Broadband Network Deployment (OPSBN) Plan 772 days
2 Project Initiation and Management 265 days
6 Governance and Coordination Planning 175 days
27 OPSBN High Level System Design 130 days
48 Develop RFPs and Contract Systems/Services Providers 130 days
56 Detailed System Design (by selected vendors) 65 days
62 System Implementation 105 days
72 Testing 270 days
73 Factory Acceptance Testing (Staging) 5 days
74 Site Testing 85 days
75 Existing OWN sites 45 days
76 Greenfield sites 30 days
77 Mini-cell sites 45 days
78 Leased sites 30 days
79 Mobile Installation Testing/Verification 10 days
80 EPC Core Site Testing 20 days
81 Functional Testing 45 days
82 Coverage Testing 100 days
83 Interface Interoperability Testing 40 days
Oregon Public Safety Broadband Network Deployment (OPSBN) Plan
Project Initiation and Management
Governance and Coordination Planning
OPSBN High Level System Design
Develop RFPs and Contract Systems/Services Providers
Detailed System Design (by selected vendors)
System Implementation
Testing
Site Testing
Interface Interoperability Testing
Task
Task Progress
Critical Task
Critical Task Progress
Milestone
Summary
Rolled Up Task
Rolled Up Critical Task
Rolled Up Milestone
Rolled Up Progress
Split
External Tasks
Project Summary
Group By Summary
Deadline
Oregon Public Safety Broadband Network Testing Plan
Page 1 of 2
Page 1


Oregon Public Safety Broadband Network (OPSBN)Testing Plan
ID
Task Name
Duration
Year 1
Year 2
Year 3
Year 4
Qtr 3
Qtr 4
Qtr 1
Qtr 2
Qtr 3
Qtr 4
Qtr 1
Qtr 2
Qtr 3
Qtr 4
Qtr 1
Qtr 2
Qtr 3
Qtr 4
Qtr 1
Qtr 2
84 Primary Interfaces 30 days
85 Secondary interfaces 10 days
86 Standards Conformance Testing 20 days
87 PCS Type Certification Review Board Testing 15 days
88 QoS Priority Testing 5 days
89 Security Testing 10 days
90 Security features 5 days
91 Encryption 5 days
92 Testing Complete 0 days
93 System Acceptance 260 days
94 Complete user and operations training 120 days
95 Verify final system ready for acceptance testing 5 days
96 Final System Acceptance test 20 days
97 System Accepted 0 days
98 Maintenance and Operations (ongoing) 0 days
Standards Conformance Testing
Security Testing
Testing Complete
System Acceptance
System Accepted
Maintenance and Operations (o
Task
Task Progress
Critical Task
Critical Task Progress
Milestone
Summary
Rolled Up Task
Rolled Up Critical Task
Rolled Up Milestone
Rolled Up Progress
Split
External Tasks
Project Summary
Group By Summary
Deadline
Oregon Public Safety Broadband Network Testing Plan
Page 2 of 2
Page 1

F. Deployment




Oregon Public Safety Broadband Network (OPSBN)Deployment Plan
ID
Task Name
31 LTE coverage and capacity analysis
32 Backhaul (Microwave) capacity analysis
33 Incorporate required interfaces (LTE air interface, S6a, S8, S9, S10, X2)
34 Investigate interference with adjacent jurisdictions in WA, NV, CA and ID
35 Mitigate out of band emissions (OOBE) per attenuation requirements
36 Site Surveys
37 225 OWN sites (estimate)
38 21 Greenfield tower sites (estimate) - Environmental, civil, structural, RF assessments
39 50 Micro-cell sites (estimate) - Environmental, civil, structural, RF assessments
40 86 Leased sites (estimate)
41 Design LTE Core Site at Anderson Readiness Center in Salem
42 Develop OPSBN LTE System Technical Specifications for use in RFP
43 Develop OPSBN Backhaul Technical Specifications for use in RFP
44 Cost analysis of LTE System
45 Cost analysis of backhaul system
46 High-Level Design and Technical Specifications review and sign-off
47 High Level Design Complete
48 Develop RFPs and Contract Systems/Services Providers
49 OPSBN LTE Radio System
50 OPSBN Backhaul Network
51 OPSBN Construction Services (of Greenfield Sites and LTE Core Site)
52 OPSBN Maintenance and Operations (to commercial carriers)
53 OPSBN Independent Implementation Oversight Services (to consultant community)
54 Select vendors/Ensure participation in PSCR/DOC Demonstration Network
55 System and Services Procurement Complete
56 Detailed System Design (by selected vendors)
57 Develop, review and sign-off on Detailed Designs
58 Develop, review and sign-off on factory acceptance tests
59 Develop, review and sign-off on all Test Plans
60 Develop, review and sign-off on all Maintenance, Operations and Training Plans
61 Detailed Design Complete
62 System Implementation
Year 1
Year 2
Year 3
Year 4
Year 5
Year 6
Year 7
Site Surveys
High Level Design Complete
Develop RFPs and Contract Systems/Services Providers
System and Services Procurement Complete
Detailed System Design (by selected vendors)
Detailed Design Complete
System Implementation
Task
Task Progress
Critical Task
Critical Task Progress
Milestone
Summary
Rolled Up Task
Rolled Up Critical Task
Rolled Up Milestone
Rolled Up Progress
Split
External Tasks
Project Summary
Group By Summary
Deadline
Oregon Public Safety Broadband Network Deployment Plan
Page 2 of 3
Page 1


Oregon Public Safety Broadband Network (OPSBN)Deployment Plan
ID
Task Name
63 Implementation Kickoff Meeting with selected vendors
64 Site Implementation
65 OWN Sites - equipment placement
66 Greenfield sites - civil, structural, tower, equipment placement
67 Mini-cell sites - civil, structural, antenna support structure, equipment placement
68 Leased sites - equipment placement
69 EPC Core Site Implementation
70 Mobile installation
71 System implementation and installation Complete
72 Testing
73 Factory Acceptance Testing (Staging)
74 Site Testing
75 Mobile installation Testing/verification
76 EPC Core Site Testing
77 Functional Testing
78 Coverage Testing
79 Interface Interoperability Testing
80 Standards Conformance Testing
81 Security Testing
82 Testing Complete
83 System Acceptance
84 Complete user and operations training
85 Verify final system ready for acceptance testing
86 Final System Acceptance test
87 System Accepted
88 Maintenance and Operations (ongoing)
Site Implementation
System Implementation and Installation Complete
Testing
System Acceptance
Testing Complete
System Accepted
Maintenance and Operations (ongoing)
Task
Task Progress
Critical Task
Critical Task Progress
Milestone
Summary
Rolled Up Task
Rolled Up Critical Task
Rolled Up Milestone
Rolled Up Progress
Split
External Tasks
Project Summary
Group By Summary
Deadline
Oregon Public Safety Broadband Network Deployment Plan
Page 3 of 3
Page 1

G. Operations, Administration and Maintenance (OA&M)

Operations

The OPSBN will use widely-accepted industry models for OA&M best practices including:

- Telecommunications Management Network (TMN)
- Fault, Configuration, Accounting, Performance, and Security (FCAPS)
- Information Technology Infrastructure Library (ITIL)

While TMN is service management focused, its logical layered architecture presents technology at a level that the business can understand. FCAPS provides a framework for technology management and serves as the basis for most network management implementations. By focusing on process and workflow, ITIL provides organizations with a customizable framework of best practices to achieve quality service. The integration of all three models will ensure superior operations, administration and maintenance of the LTE network.

More than half of the proposed LTE sites for the OPSBN will be collocated with OWIN microwave backhaul sites. Therefore, remotely managing all microwave and LTE (including proposed Greenfield and cellular) sites from the OWIN Northern Command Center (NCC) and the Southern Command Center (SCC) may be a feasible option. Although not known at this time, additional regional network operations centers may be necessary for load sharing purposes.

The shared operations centers for OWIN and OPSBN will have the following capabilities:

- Ability of operations staff to monitor and manage all remote devices including physical and event alarms, LMR, LTE eNodeB and UE, microwave, power, routing, security, SONET, and switching systems
- Use of a statewide dashboard with individual equipment management systems that provide operational and provisioning capability
- Ability to support remote management standards such as Simple Network Management Protocol (SNMP), Windows Management Interface (WMI), or other industry standard protocols
- Capacity to store 365 days of network equipment system event logs
- Ability of the NCC to failover to the SCC backup site and vice versa
- Ability to support virtualization or remote clustering technology to enable the failover of the application servers to the associated backup site
- Use of a centralized storage array to assist in the replication of data and applications between sites
- Capability of applications to allow automated provisioning through SNMP interfaces or other point product based provisioning systems

Administration

Because of the widely-recognized need for reduced LTE operational expenses and efforts, the OPSBN will implement Self Organizing Networks (SON). Created by the Next Generation Mobile Networks (NGMN) and 3GPP, SON is designed to be a multi-vendor

solution, with standard interfaces utilized at key points to allow inter-operability between vendors. SON minimizes operating costs by reducing and eliminating manual configuration of network operational parameters during the entire network lifecycle including planning, deployment, operations, and optimization.

SON significantly decreases the traditional administration effort in deploying new elements on the network. For instance, the SON architecture specifies a newly-deployed eNodeB on the network to:

- Support complete plug and play capability – no provisioning of hardware resources is required and inventory information is automatically recorded and reported
- Algorithmically compute its physical cell ID through communication with neighboring eNodeBs
- Determine its neighbors with the help of user equipment, continuously optimizing and refining this list in real-time, discovering new neighbors and deleting stale neighbors
- Automatically determine and continually optimize its RF parameters, including antenna tilt, power output and interference control
- Automatically setup its transport capabilities, establishing contact with the EMS, MME, etc.
- Support a complete self-test of itself, allowing the technician to easily verify operation of the eNodeB after installation
- Automatically authenticate itself into the network and update to the correct version of software, if necessary

Maintenance

The OPSBN will leverage SON architecture and best practices for implementing an effective maintenance strategy. Although vendor service level agreements will vary, the following guidelines shall be considered:

- Preparation and planning – consisting of a documented plan that outlines network area responsibility, preventative maintenance criteria, performance metric types, problem escalation process, and network troubleshooting techniques
- Problem prevention plan – consisting of an accurately documented process for regularly updating and monitoring the network
- Early problem detection – consisting of robust network management system implementations for immediate identification and documentation of network performance and problems
- Quick problem isolation and resolution – consisting of sufficient and appropriate diagnostic tools that enable operations staff to locate problems faster and minimize downtime
- Quality improvement plan – consisting of continuous comparison of performance metrics against pre-defined networks goals

SON substantially reduces the level of monitoring and maintenance required from the operations staff by providing the following capabilities:

- Complete and standardized inventory reporting of all components from all network elements
- Robust cell outage detection capabilities for latent faults
- Integrated cell outage compensation capability that automatically reconfigures surrounding cells to offset the effect of a failed cell
- First and second order root cause analysis and recovery of faults
- Real-time performance management data to verify service capability after a repair or reconfiguration
- Multi-vendor subscriber and equipment trace, to aide system troubleshooting

Although the OPSBN will adopt open standards, it is important to note that SON solutions do allow for differentiation and competition between the infrastructure vendors. Because some SON algorithms are not standardized, potential issues may arise in the future development of a nationwide network.

H. Appendix

1. Glossary

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
AS	Access Stratum
BBERF	Bearer Binding and Event Reporting Function
BBTF	Broadband Task Force
BTOP	Broadband Technology Opportunities Program
CAD	Computer Aided Dispatch
CALEA	Communications Assistance for Law Enforcement Act
CDMA	Code Division Multiple Access
dBd	Decibels (related to dipole antenna)
DHCP	Dynamic Host Configuration Protocol
E-UTRAN	Evolved UTRAN
EIR	Equipment Identity Register
EMS	Emergency Medical Service
EOC	Emergency Operations Center
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
ERIC	Emergency Response Interoperability Center
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FCC	Federal Communications Commission
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobiles
HNI	Home Network Identity
HSS	Home Subscriber Server
ICIC	Inter-cell Interference Coordination
ICS	Incident Command System
ID	Identification
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	Internet Protocol Security
ITIL	Information Technology Infrastructure Library
LMR	Land Mobile Radio
LTE	Long Term Evolution
Mbps	Megabits Per Second
MDM	Mobile Device Management
MHz	Megahertz
MIP	Mobile IP
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MPLS	Multiprotocol Label Switching
NAS	Non-Access Stratum

NCC	OWIN Northern Command Center
NGMN	Next Generation Mobile Networks
NIST	National Institute of Standards and Technology
NPSTC	National Public Safety Telecommunications Council
OA&M	Operations, Administration, and Maintenance
OCS	Online Charging System
OFCS	Offline Charging System
OPSBN	Oregon Public Safety Broadband Network
OS	Operating System
OTA	Over the Air
OWIN	Oregon Wireless Interoperable Network
PC	Personal Computer
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PDA	Personal Digital Assistant
PDCP	Packet Data Convergence Protocol
PDN	Packet Data network
PDN GW	Packet Data network Gateway
PLMN	Public Land Mobile Network
PS	Public Safety
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RAS	Reliability, Availability, and Serviceability
RAT	Radio Access Technology
RF	Radio Frequency
RMS	Records Management System
RRC	Radio Resource Control
RSRP	Reference Signal Received Power
SAE	System Architecture Evolution
SAE	System Architecture Evolution
SCC	OWIN Southern Command Center
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SLA	Service Level Agreement
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SON	Self-Organizing Network
SONET	Synchronous Optical Network
TMN	Telecommunications Management Network
TS	Technical Specification
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
USIM	User Subscriber Information Module
UTRAN	UMTS Terrestrial Radio Access Network
VPN	Virtual Private Network
WLAN	Wireless Local Area network

WMI	Windows Management Interface