QoS	Quality of Service
RAN	Radio Access Netowrk
RF	Radio Frequency
RNC	Radio Network Controllers
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SQL	Structured Query Language
SoR	Statement of Requirements for Public Safety Communications & Interoperability
TDD	Time Division Duplex
TTY/TDD	Telecommunications Device for the Deaf
TIA	Telecommunications Industry Association
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over Internet Protocol
WiFi	Wireless Fidelity (IEEE 802.11b wireless networking)
WIPR	Wireless IP Router
WWW	World Wide Web

1 Introduction

Providing appropriate, effective and affordable mobile communications solutions to Public Safety has proven to be a goal that largely has eluded every constituency group that has pursued it. There is general agreement among all involved parties – government agencies, the Public Safety community and specialized equipment vendors – that the root of the difficulty lies in the fragmentation that can be found in every relevant ingredient: spectrum, funding, coordination, technology and interoperability. However gratifying the limited progress made through the well-motivated and diligent efforts of various bodies and projects (including APCO, SAFECOM, MESA and IWN) in attempts (some spanning decades) to address various discrete aspects of this problem area, a truly viable and generally applicable solution to the basic problems has yet to be achieved.

Addressing the problems areas, one at a time or in varying combinations, in piecemeal attempts to cobble together an overall approach that might work, has not been promising to date and shows no prospect of becoming so in the future. What is instead called for, and should be given fair and serious consideration, is an approach that would attack, in a simultaneous and comprehensive fashion, all aspects of the problem area. Public Safety requires a solution that goes beyond mere focused effort on the "problem du jour", against the certain backdrop that the next disaster or catastrophic event will present a new problem, or the same problem, but in a different way or in a different context. Rather, Public Safety requires a uniform nationwide solution, one that will permit it to accommodate the communications solutions it now has in place with those that it will want and need in the future, and that will permit it to leverage emerging broadband technologies effectively and economically, without surrendering the assurance of interoperability.

In short, although Public safety undoubtedly will continue to require (as it always has required) its own mobile communications network, it first needs a well-considered, recommended approach to architecting a Next Generation Public Safety (NGPS) network. Furthermore, Public Safety should leverage the support of the private sector to highlight issues surrounding the use of emerging technologies. Ideally, those most familiar with the evolving commercial technologies and the requirements of Public Safety should collaborate on mapping the plethora of Public Safety requirements to commercially available technologies.

A NGPS network must be based on commercial, state-of-the art, standards-based technology in order to insure an elegant and affordable path for on-going enhancements and upgrades, which has unfortunately been lacking in existing Public Safety networks. Finally, a NGPS network must be designed and built to meet the stringent requirements regarding high performance communications, interoperability, security, reliability and coverage; historically, Public Safety has not had the spectrum or the funding to deploy such technology.

This document attempts to aid Public Safety in understanding these issues in more detail and is structured as follows. It starts by describing Public Safety grade network design principles and requirements. It continues with an evaluation of the benefits of the design approach and technology choices as well as outlining some innovative network implementation ideas. Finally, it concludes with an overview and a detailed description of all the key design elements: spectrum, coverage, functions and advanced services – such as broadband on demand and command and control capabilities; and describing the commercial technologies considered to implement such a network and the enhancements and upgrades that will be required to bring the commercial technologies to a Public Safety grade.

2 NGPS Network Design Principles

When determining the NGPS network design principles, priority was given to those criteria that directly alleviated or addressed the Public Safety communications conundrum: the most demanding user group in terms of functionality and quality of service with the least amount of resources – spectrum, technology and capital. It is important that the network provides for, and prioritizes the functionalities that are most important to the Public Safety community while being built and deployed within financial and operational boundaries that secure on-going maintenance, enhancements and upgrades in accordance with the ever-growing communications demands of the Public Safety community.

In this context, the following design principles were chosen:

1. "Voice of Public Safety" will be the primary source of user requirements. Several entities –SAFECOM, APCO, IWN, ETSI, Project MESA, etc – have established working groups to collect and document the communications needs and priorities of the Public Safety community. This work must be the cornerstone of determining the functionalities and features of the network, associated services and applications and devices.
2. The network must be built on state-of-the art, commercially available, standard-based technology, which will be enhanced to meet the stringent requirements of the Public Safety community. This approach has several advantages. It will provide an elegant and affordable path for system upgrades by leveraging the commercial technology evolution paths; and by influencing those designs and implementations to meet the on-going needs of Public Safety.
3. The network design must include interoperability with legacy systems as well as with commercial networks. Public Safety must be able to establish voice and dispatch communications with other peers that use Association of Public Safety Communication (APCO) based or any other proprietary system as well as with individuals using either wireless or wireline networks – PSTN or cable VoIP.
4. Cost benefit analysis must be applied to determine the best combination of systems and solutions required to meet Public Safety requirements. For instance, the solutions deployed to meet coverage requirements must be vetted against economic,

operational and technology feasibility criteria. However, it is inevitable that satellite interoperability be a significant component of the network design. This is essential to providing coverage in isolated areas as well as an additional level of reliability in traditional coverage areas.

5. The network design must be flexible enough to leverage existing infrastructure in order to derive the maximum possible benefit of cost savings, speed and ease of deployment. The network design should not predispose or exclude existing or potential commercial entities from a role in the network deployment.

3 Public Safety Requirements

The network architecture proposed in this document draws from the requirements published by SAFECOM in its Statement of Requirements for Public Safety Communications & Interoperability[1] (SoR). The document describes the operational and functional capabilities and mechanisms for advanced communications for Public Safety. The document does not "explicitly identify specific technological approaches". However, recent advances in technologies, applications and solutions available in the commercial world (TIA, 3GPP, 3GPP2, ETSI, IEEE, IETF, etc.) have influenced the way Public Safety practitioners imagine the evolution of their jobs and their communications requirements. Based on the rapid and continual commercial technology evolution; and the possibility of reducing the cycle for Public Safety technology, the SoR includes current and future requirements envisioned to support Public Safety needs until 2019.

Given the influence of the SAFECOM requirements in the proposed network architecture and design, the following section summarizes the key architectural concepts and key requirements outlined in the SoR document. These requirements have been augmented from other sources – APCO, project MESA, project IWN and internal research. However, while every effort is being made to target technologies inherently capable of meeting Public Safety requirements, commercially viable and economically feasible; there is still much work to be done.

Public Safety requirements can be broadly classified in three categories: network requirements, applications and service requirements and device requirements. A description of each of these types of requirements follows:

1. **Network Requirements**: The SoR defines the network architecture as a System of Systems. It consists of a series of different logical networks seamlessly integrated.

[1] See SAFECOM Statement of Requirements for Public Safety Wireless Communication and Interoperability v1.1 published January 26, 2006

Ideally, devices must work in all of these networks. The System of Systems is a network hierarchy as defined in SAFECOM SoR Section 5.1 [2]:

a. Personal Area Network (PAN): The PAN for a first responder can take on many different forms. Primarily, it is intended to represent a set of devices on the person of a first responder that communicate with the first responder's Public Safety Communication Device (PSCD) as necessary. The devices on a PAN will include such items as heart rate monitors, location sensors, etc. This information could, and would in many cases, be transmitted to other areas of the network.

b. Incident Area Network (IAN): An IAN is a network created for a specific incident. This network is temporary in nature and is typically centered on a wireless access point attached to the first responder's vehicle. Multiple vehicles therefore dictate multiple wireless access points, all of which coordinate their coverage and transmissions seamlessly and automatically. This network scales to the size of the incident, from a local traffic stop, to a large-scale, multi-discipline, multi-jurisdiction event.

c. Jurisdiction Area Network (JAN): The JAN is the main communications network for first responders. It handles any IAN traffic that needs access to the general network and provides the connectivity to the EAN. Additionally, it is the instantiation of the network that will handle any and all communications from a first responder PSCD should a connection with the local IAN fail or be otherwise unavailable.

d. Extended Area Network (EAN): The local systems are, in turn, linked with county, regional, state, and national systems or EANs. It is expected that this network could be both wired and wireless, depending on the type of infrastructure deployed in the area, i.e., microwave point-to-point, fiber, etc. [3]

The association between these four types of networks has been established based on requirements and scenarios defined by the Public Safety community. It consists of standard links and interfaces that identify the methods and means that voice or data communications will follow. As an example, a link is defined between a policeman PAN and his communication device where the data collected by the heart rate sensor in the policeman vest is transmitted to the communications devices. The interface of this link has been determined as wireless.

---

[2] See SAFECOM Statement of Requirements for Public Safety Wireless Communication and Interoperability v1.1 published January 26, 2006

[3] See Statement of Requirements for Public Safety Wireless Communication and Interoperability v1.1 published January 26, 2006

SoR defines 9 different types of links and 6 types of interfaces to integrate the four different types of network seamlessly.[4]

Given the nature of the Public Safety operations these networks will have to meet specific performance criteria regarding: reliability, availability, scalability, survivability, restorability, spectrum/network efficiency, mobility, and end-to-end performance metrics[5]. For instance, as it relates to scalability, the network must accommodate all personnel present in an emergency. This implies the creation of temporary networks to accommodate additional resources and their integration with existing networks for seamless communication. In addition, they must allow automatic management and user led management in order to quickly identify and authorize the Public Safety personnel present in the emergency scenario. In addition the network should accommodate seamless mobility or roaming of Public Safety personnel across IAN or JAN during an emergency situation even if the JAN is not the one where Public Safety personnel are registered.

The Public Safety network will also need to interface with non Public Safety networks such as PSTN and Internet as well as public utility information with the appropriate level of security and data encryption. While not explicitly stated in the SoR, we believe that this System of Systems must also include legacy systems currently used by Public Safety personnel. This implies that the network should enable interoperability with all types of networks: legacy analog or digital, satellite and core terrestrial networks.

The network must also include mechanisms to dynamically allocate its capacity where it is most required. These mechanisms will be guided by processes and procedures determined by the Public Safety user community following a hierarchical "command-and-control" capability for the network that determines the "class of service" and the priorities that every resource in the network enjoys given its profile and given the situation.

2. **Applications and Services Requirements**: SoR defines functional requirements for applications and services along several dimensions: class of service, security, operations and design methodology

    a. Class of service: SAFECOM defines class of service as:

    "... a logical grouping of applications and services that share similar performance requirements. For instance, one class of service may be a grouping of jitter-sensitive, highly interactive traffic, while another class of service may consist of jitter-resistant, non-interactive traffic. Each

---

4 See a visual representation in Figure 23- SAFECOM Device Interfaces

5 See Section 8 of Statement of Requirements for Wireless Communication and Interoperability v1.1 published January 26, 2006

grouping of applications and services, or class of service, can then have network performance requirements applied to the class as opposed to the individual application or service." [6]

The SoR defines six classes of services to distinguish between different types of traffic and to assign different types of handling priorities. Applications and services have been categorized to determine class of service. For instance, full duplex voice and videoconferencing capabilities are assigned class of service 0 or 1, while peer-to-peer instant messaging and database transactions are considered class of service 3; data/video streaming and geolocation services are classified as class of service 4, e-mail and WWW applications are class of service 5. Finally, signaling and session control data is considered class of service 2.

b. Security is a key priority in Public Safety communications. The SoR defines several requirements concerning secure communications:

   i. Authentication – the process to grant network access – is required for all types of networks – PAN, IAN, JAN, EAN. Public Safety personnel should be able to authenticate themselves on the network regardless of their geographic location.

   ii. Authorization – the process to gain access to specific resources and priorities in the network- is required for all users in the network. Authorization must be granted conditionally on role definitions. Every user on the network will be tied to a specific role profile that will predetermine the level of service and resources available to him. Similar to authentication, authorization must be performed from every location on the network.

   iii. Privacy – inability to read the network by anyone other than authorized recipients – will apply to all traffic on the network and will conform to the Federal Information Processing Standards. In order to implement this requirement, encryption techniques and mechanism will be deployed at the device and network level.

   iv. Integrity – inability to modify data without detection – also applies to all data traffic crossing the network and will be implemented using advance encryption and detection techniques.

   v. Monitoring – ability of an administrator to maintain effective control over the network – includes having the ability to create an audit trail to allow for reconstructing events occurred in the network, log device and network failure events as well as detect

---

6 See Section 6 Statement of Requirements for Public Safety Wireless Communication and Interoperability v1.1 published January 26, 2006

and report failure after self-test and on-going monitoring procedure.

vi. Attack prevention and detection refers to the ability of the network to continue operations in the face of any denial of service attack as well as the ability of the network to prevent attackers from performing traffic flow analysis.

vii. Physical security of the network infrastructure must be guaranteed so that only authorized personnel can have access to the network equipment and devices.

c. Operations requirements define the roles and rules regarding the administration and maintenance of the network. Special attention is devoted to the administration of users rights and well as the creation of user groups in the network. In the network (described *infra*) these functionalities will be gathered in the "Command-and-Control" capability where authorized administrators will be able to control real-time access and priority levels of any user on the network.

d. SAFECOM design methodology describes best practices for the design and implementation of the network. It includes the use of "off-the-shelf technology" and standard systems whenever possible as well as enabling backwards compatibility with legacy systems.

The aforementioned functionalities will be used to guarantee the desired level of performance of the different services and applications that will be offered to the end users: High-performance PTT (sub 300ms), full-duplex voice (conventional or, ideally, VoIP,) data, streaming, surveillance and tri-dimensional location applications, instant messaging, videoconference, voice paging, file transfer, automated database search, real-time or near real-time video streaming, e-mail, www-based applications, etc.

3. **Devices**: SoR identifies three different classes of mobile devices, portable devices and sensors. Mobile devices are defined as in-vehicle devices while portable devices are those devices the user carries when not in the vehicle. Requirements that apply to these two types of devices include: biometric identification, device cloning, voice activation, hands-free, over the air reprogramming, geolocation information, voice language translation techniques, TTY,TDD interfaces, low probability detection techniques, etc.

   Sensors range from passive chemical sensors on the first responder – for instance to control the level of oxygen in the firefighter tank – to active sensors such biometrics sensors or surveillance cameras. Sensors must be able to transmit to mobile or portable devices based on their relative position in order to relay the information back to the network. This communication must be allowed regardless of the location, including RF hostile environments.

4 Technological Approach

Following the NGPS network design guiding principles, the network will be based on commercial, standard-based technology. While there are a myriad of these technologies available, the relevant set for consideration becomes relatively small when filtered through the key Public Safety requirements – class of service, command-and-control capabilities, interoperability, dynamic bandwidth allocation, etc.

Today's deployed technologies are not configured nor do they include the capabilities to implement the unique requirements of Public Safety services. Retrofitting these networks to meet the Public Safety requirements will be costly and inefficient, if not impossible. Only a handful of next generation technologies include the capabilities to implement the more advanced Public Safety requirements as well as enjoy the level of maturity to be commercially viable by early 2009 when the NGPS network could be viable for launch. Table 1 below shows a high level evaluation of the technology capabilities vis-à-vis several key Public Safety requirements:

Table 1 – Wireless technologies capabilities evaluation

Public Safety Requirements	CDMA EVDO Rev 0	CDMA EVDO Rev A	CDMA EVDO Rev B	UMTS Edge	UMTS HSPDA	F-OFDM	WiMax
Instant/RealTime Service	●	●	●	●	●	●	●
Mobility	◍	●	●	●	●	◍	●
Half Duplex PTT	●	●	●	◍	◍	◍	◍
Full Duplex Voice	●	●	●	●	●	◍	◍
Multicast/Broadcast Services	●	●	●	●	●	●	●
Multi-Media session	●	●	●	●	●	●	●
Streaming Media/Data	●	●	●	●	●	◍	●
Command/ Dispatch/ Operations Control	◍	◍	◍	◍	◍	◍	◍
Voice Interoperability to External Networks	◍	●	●	●	●	◍	●
Security/ AAA functions	◍	◍	◍	◍	◍	◍	◍
Distributed Group Access/ Control / Configuration	◍	◍	◍	◍	◍	◍	◍
Enhanced Coverage/ Availability/Reliability/ Scalability/Restorability	●	●	◍	●	●	●	●
QOS/ Priority Access	●	●	●	●	●	◍	●
Location/GPS	●	●	●	●	●	◍	◍
Intelligent Device/User Interface	●	◍	●	●	●	●	●
Monitoring and Status	◍	◍	◍	◍	◍	◍	◍
External Application Access/ Interoperability	◍	◍	◍	◍	◍	◍	◍
Hosted Applications: email, databases, FTP, etc.	◍	◍	◍	◍	◍	◍	◍

Legend		
	●	Minimal support of requirements
	◍	Moderate support of requirements
	●	Full support of requirement

While the leading technology candidates offer an appropriate set of underlying capabilities to meet the Public Safety requirements, their commercial implementations do not evolve these capabilities into actual, readily-available functionalities. For example, viable commercial technologies include QoS capabilities, which means that data packets can be tagged to include relevant priority information. However, there is no place in the standards that addresses how this priority tag information will be processed or used to reroute these data packets. The implementation of the mechanism and systems that deliver QoS based on the "priority tag" information needs to be specifically developed by the service provider that wants to offer this capability. Technology standards enable capabilities but do not deliver full implementation of these capabilities as ready-to-use functions.

This implies that several of the high performance applications and advanced services will still need to be developed as enhancements to the standard or commercial implementations. For instance, for Public Safety, greater than 500 ms delay in a half-duplex communication can represent missing an opportunity to save a life. Despite the specifications of Public Safety, many current dispatch systems incur call set-up delays above 500ms. The best push-to-talk commercial implementation is estimated to experience greater than 700ms call set-up delay. To bring commercial PTT deployment within the realms of Public Safety performance, several enhancements are required at the device, RAN and core network layers.

Given the nature of the Public Safety communications and its stringent requirements in terms of performance, security, flexibility, among others, a fair amount of customized development will be required. It is important to understand the capabilities of the technology alternatives considered as potential candidates for the NGPS network, to identify the gaps to meet Public Safety requirements and finally to describe the types of enhancements and system upgrades that will be required to enable and implement the most critical Public Safety requirements.

4.1 Commercial State of the Art Technology

4.1.1 IP Based Flat architecture

Traditional wireless architectures have been based on a hierarchical, dual-network – one for voice, one for data – model. The wireless network includes two independent subsystems – one to handle voice and the other to handle data. The network is also tiered in different layers. The radio layer is connected to the core network through a complex, legacy switching layer. Base Station Controllers (BTS) located at the towers send voice and data traffic to the Radio (Regional) Network Controllers (RNC) located at regional centers. At these points, the traffic is aggregated and sent to the switching centers for routing and final delivery. This legacy architecture of voice-centric, circuit switched networks, requires reconfiguration and re-dimensioning at every point of the hierarchy when, for instance, a new tower is connected to the network. This model results in high maintenance and operating costs as well as high exposure to failures in case of a network

node breakdown. In this model, network reliability is built through node redundancy directly impacting the total cost of the network.

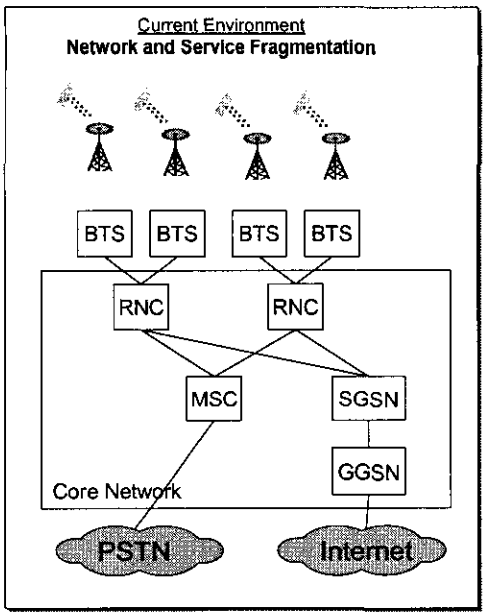

Figure 1– Current wireless network architecture

As voice and data communications become IP centric services, network architectures are also evolving towards an Internet model based on meshed network model rather than a hierarchical model.

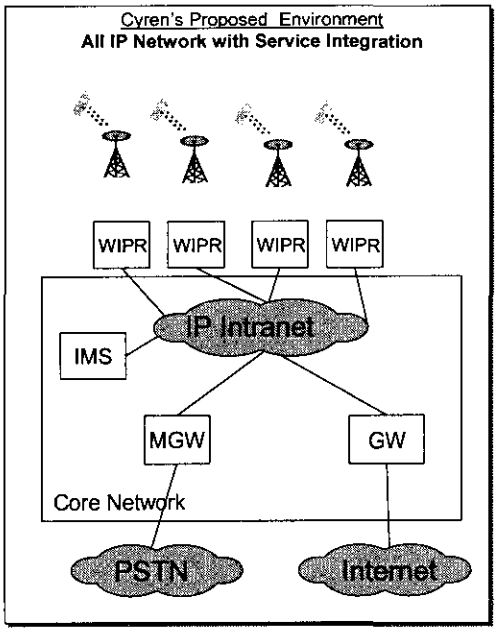

Figure 2– Next generation wireless network architecture

In the wireless world, this implies the collapse of several functions, which in the legacy architecture, resided in several discrete layers in the network – BTS-RNC, and certain MSC functions- into just one network node – the Wireless IP Router (WIPR).

Several benefits derive from this collapsed architecture:

- Elimination of failure points, congestion points and signal processing delays positively impacting latency sensitive voice applications such push-to-talk and VoIP.
- Increased flexibility and scalability, which facilitates the expansion and reconfiguration of the network. When the network needs to expand coverage a new tower will be built and a new WIPR connected to the core network with limited impact to the existing nodes in the network. The network expansion will follow the same model as the Internet where network hierarchies are eliminated and the addition of a new node only implies a small modification (often dynamic) in the routing tables of the adjacent nodes.
- Improved capital and operational cost savings as well as reduced maintenance and backhaul costs[7]. WIPRs reduce the number of elements in the network; furthermore, they reduce the need to reconfigure or upgrade other network elements when expanding the network capacity.

In the context of the NGPS network, this "flat" architecture will enable the implementation of several critical requirements:

1. Class of Service and Command and Control capabilities: See a description of these functionalities in section 6.10 Command-and-Control. The NGPS network implementation for class of service will enable Public Safety to assign service categories to different functions and user profiles with different priorities for each service. For example:

Table 2 – Public Safety Class of Service categorization by user profile

Role	Class of Service 0	Class of Service 1	Class of Service 3
Field agent	PTT	Voice	Video
Dispatcher	PTT	Video	Voice
Incident Coordinator	Voice	PTT	Video

7 Lucent Technologies Unveils New Base Station Route – Feb 25, 2006

Public Safety must control and manage these designations (including real time capabilities) in order to reassign and reprioritize roles and applications based on the situation. This capability was envisioned in the early commercial technology specifications but has not been implemented in a way that it could be retrofitted to meet the needs of Public Safety.

A new approach to an old concept is required and the flat, all IP architecture is particularly well suited for this implementation. This dynamic capability requires a high degree of signal processing capability at the base station, which is not realistic from legacy infrastructure. Furthermore, significant enhancements are also required in Core network technology, which again, is better addressed in the flat IP architecture.

2. Capacity-on-Demand–See description of this capability in section 6.4 Capacity on Demand. The NGPS network must enable the allocation of additional spectrum in the event of an incident. Furthermore, this should not be a simple allotment of additional spectrum, rather, an intelligent mechanism for sharing the allotment of spectrum more efficiently and across all users and all services. This capability can be far better achieved in a flat IP architecture than in the current hierarchical approach. This architecture is also essential to the support of a shared network between commercial and public safety users. Finally, this WIPR architecture is essential to supporting the variety of logical networks specified by SAFECOM.
3. An additional argument for the flat IP architecture is the delivery of end-to-end encryption capabilities. This architecture makes much more feasible to tailor the network capabilities to specifically support unique encryption requirements, particularly multiple forms of encryption.

4.1.2 Core Network

A critical element to fully leverage the capabilities of "all-IP" networks is the IP Multimedia Subsystem (IMS).

> *"The IP Multi-Media Subsystem (IMS) is an IP multimedia and telephony core network. It is defined by 3GPP and 3GPP2 standards and organizations based on IETF Internet protocols. IMS is access independent as it supports IP to IP session over wireline IP, 802.11, 802.15, CDMA, packet data along with GSM/EDGE/UMTS and other packet data applications. IMS is standardized reference architecture. IMS consists of session control, connection control and an applications services framework along with subscriber and services data. It*

enables new converged voice and data services, while allowing for the interoperability of these converged services between subscribers."[8]

The NGPS network must leverage this standard technology and perform additional forward looking enhancements geared toward Public Safety requirements first and foremost[9]. Furthermore, Public Safety must have a strong voice in the on-going development of the IMS standards.

Building on IMS capabilities, Public Safety will have the opportunity to develop and deploy application servers to deliver high performance voice and data services. For instance, for PTT, the combination of application servers and IMS can more gracefully enable implementation of dynamic incident group call, or broadcasting emergency messages to all first responders on an incident network. Additional value added services include better integration and interoperability functions for Public Safety Data Applications (DMV, AFIS, Proprietary Access to Agency Data, etc,), Video Surveillance, Audio Surveillance, Streaming, etc.

4.1.3 Air Interface

Several air interface technologies can be considered. Priority must be given to those capable of meeting Public Safety requirements in addition to being commercially ready by early 2009 when the NGPS networks should ideally be on air.

Regarding technology capabilities, priority must be given to those that enable:

1. Dynamic allocation of bandwidth including capacity on demand during emergency situations
2. High performance services and applications: encryption, high performance PTT (broadcast and multicast, low latency call set-up (<400ms), incident dynamic group call, emergency broadcast integration, etc, as well as commercial grade VoIP, streaming, surveillance, etc
3. Integration and interoperability with other networks: satellite integration at the devices, roaming capabilities to commercial networks, wifi integration, etc
4. Integration/deployment capabilities for Satellite, micro cells, pico cells, vehicular cells, etc.
5. Direct device to device communication (mobiles, portables, etc.)

---

8 http://www.lucent.com/products/solution/0,,CTID+2019-STID+10488-SOID+1284-LOCL+1,00.html

9 See TELECOMNEXT: CTOs want IMS, home networking by Carol Wilson, March 20, 2006 (http://telephonyonline.com/telecomnext/news/telecomnext_cto_ims_032006/)

6. Independent site operations in the event of loss of backhaul capability, dynamic mesh capabilities amongst devices, device (mobile) relaying capabilities, etc.

As Figure 3 shows below, the challenge resides in selecting an air interface that is technologically stable to effectively accommodate required enhancements. Given that the technology development cycle traditionally ranges from 18 months to 24 months for commercial networks, development for NGPS network needs to start in the next six months if Public Safety is to have an operational network by early 2009. This combined with our guiding principle that the technology should be in a commercial state to derive the benefits associated with economies of scale, imposes some limitations on the technology choices in the short term.

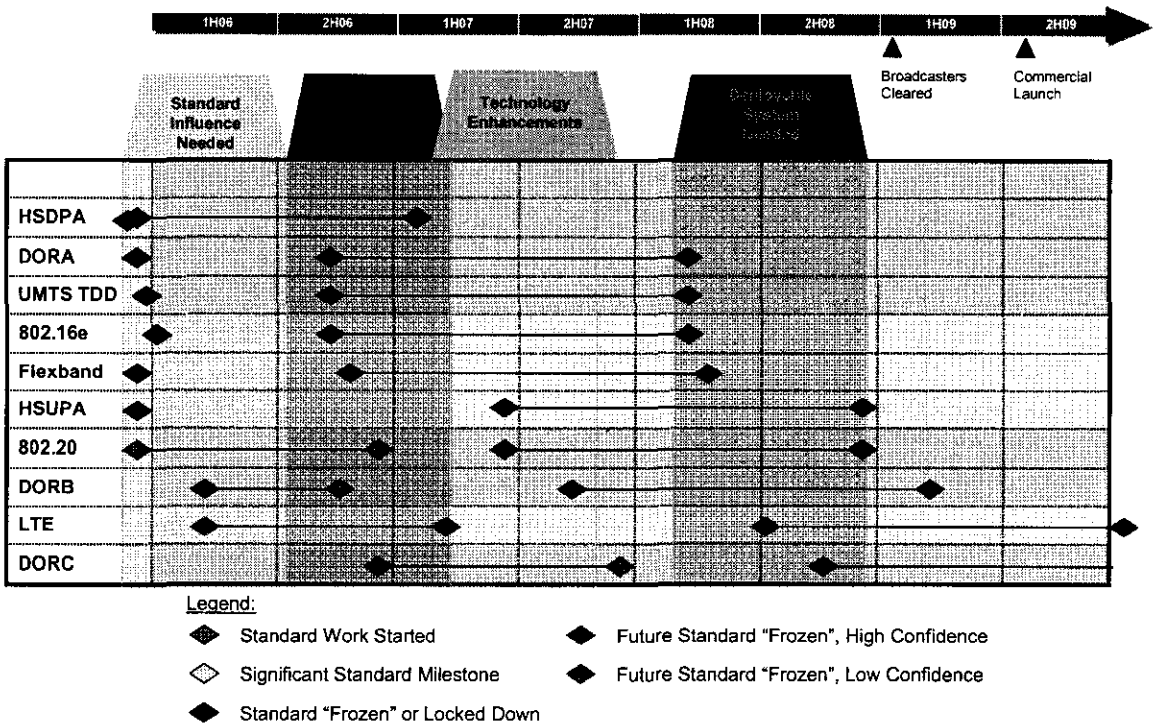

Figure 3– Next generation of wireless technology standards timelines

However, an interesting opportunity exists for Public Safety to influence subsequent generations of air interfaces. Furthermore, advancements in commercial base station technology make it entirely conceivable that Public Safety could utilize the best available air interface for its initial network deployment, while still having the flexibility to add additional air interfaces, with differing capabilities after launch. While the standardization process remains open for technologies such as: CDMA DO Rev. B, 3GPP LTE, IEEE 802.20, etc, Public Safety has the opportunity to influence and shape development in order to include their more stringent requirements. This approach could bring both operational and financial benefits. Securing the concept that Public Safety requirements should be part of the standards will result in fewer customizations and

enhancements; therefore, impacting positively the time and the cost to develop and deploy these new generation networks.

An additional hurdle in the selection of the most appropriate air interface technology is the companion issue: state of the underlying technology (microprocessors, software environment, etc.) to support the unique device needs of the Public Safety. None of the aforementioned technologies readily contemplate the need for biometric data processing, sensor data processing, identity cloning capabilities, secure software development environments capable of supporting the end-to-end encryption capabilities required for all types of services (some can support voice or data encryption today but not at the levels that the requirements dictate,) etc. The unique requirements of Public Safety dictate that there is much work to be done by the core technology vendors of the underlying hardware and software to support the vast family of devices and their interoperability as spelled out by SAFECOM. Development of enhancements in the core technology must be as carefully assessed, if not more so than the capabilities of the infrastructure. Typically the core technology development for devices lags the infrastructure development by six to twelve months depending on the technology standard.

4.2 Technology Enhancements to meet Public Safety Requirements

When mapping public safety requirements to existing deployed technology capabilities – currently operated by CMRS – or next generation of commercial, standard-based technologies, a tremendous gap can be observed. Appendix A[10] summarizes the results of a detailed analysis that 4DK Technologies, Inc. conducted recently. The exercise consisted of mapping how adequately the next generation technologies met the SAFECOM requirements. We evaluated each of the 306 SAFECOM requirements along two dimensions:

1. The first dimension focused on understanding the level of involvement of each layer of the wireless ecosystem – RAN, core, devices, services and external interfaces – in the delivery or enablement of the service, function or feature that will meet the requirement.
2. The second dimension focused on understanding the level of development that will be needed to enable the requirement.

The table in the appendix shows a summary of that assessment based on 4DK Technologies, Inc. experience in wireless technology and a thorough evaluation of the capabilities of each next generation of technologies. The methodology used consisted in

[10] See Appendix A Evaluation of required technology enhancements to meet SAFECOM requirements

grading each requirement qualitatively along the two dimensions. When more than one technology could be considered as a potential solution, an average estimate was performed. The result is a visual representation that provides revealing insight on the amount and depth of enhancements that will need to be conducted to meet the public safety requirements.

The most significant gaps revealed by the requirement map are summarized in Figure 4 below. The list does not try to be exhaustive but to depict the type of enhancements that the NGPS network will need to address.

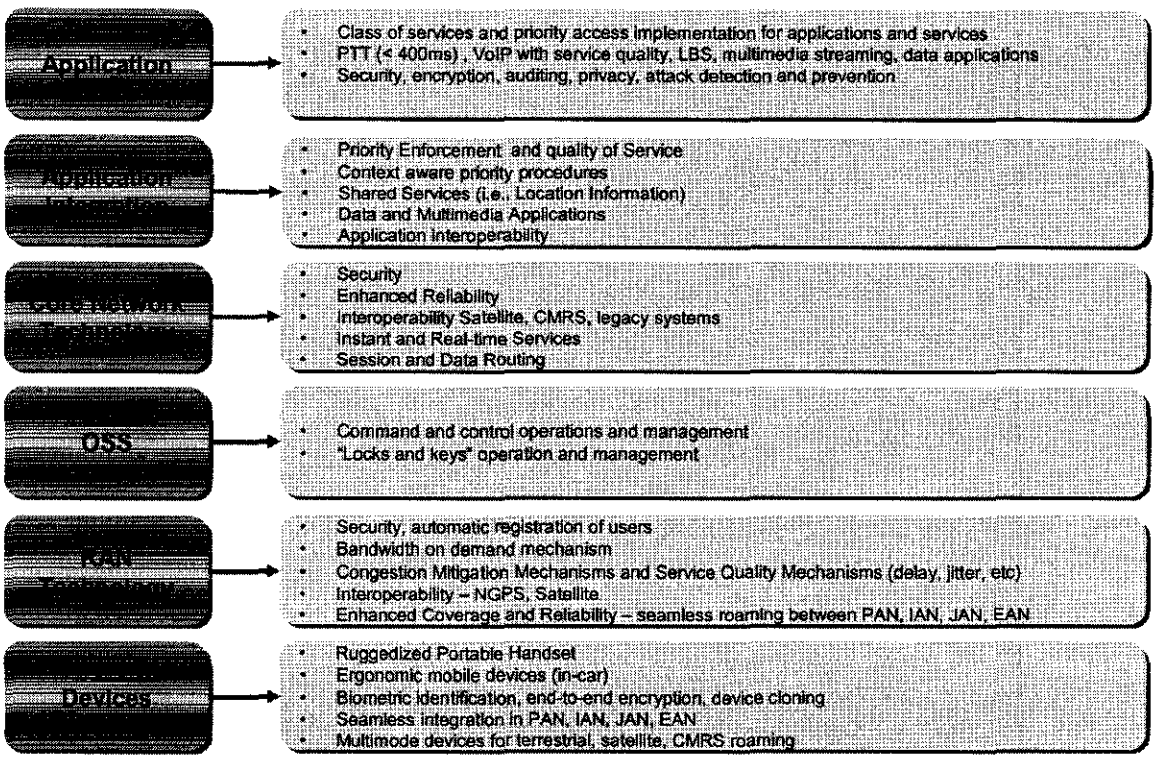

Figure 4– Technology enhancements to meet Public Safety requirements

Beyond these pure technology enhancements, additional enhancements and innovations will need to be considered at the infrastructure level. For instance, consideration must be given to splitting the core network in order to address public safety security and traffic control issues. At the RAN level, some splitting may need to be considered to include and integrate different types of base stations for different type of RAN cells: Macro, Micro, Pico, Satellite, PAN, IAN. In addition, special attention will be given to address any unique requirement that these types of BTS may have.

Two approaches can be considered to implement these enhancements. Retrofitting the existing CRMS networks, the other is following a green-field approach. The CMRS evolution approach does not seem an adequate solution. It may become more costly and certainly will yield poorer performance than a green-field. Table 3 below demonstrates the underlying reasons. Until today, the strategic, business, operational

performance and financial motives behind the commercial networks and public network almost sit in opposite poles.

Table 3 – Comparison of Public Safety vs Commercial Operators network design criteria

	Public Safety	Commercial Operator
Device Philosophy	Rugged, Fully Featured	Inexpensive, Fully Featured
Design Metric	Worst Case Imaginable	Worst Hour of a Typical Day
Technology Requirements	Safecom, APCO, ETSI, etc. Government oriented	3GPP, 3GPP2, Consumer and Enterprise oriented
Blocking	<1%	~2%
Coverage	Maximum Geography	Maximum Population Density
Availability	24x7	Available When User Needs It (Night time maintenance)
Reliability	Must work; lives are at stake	Must work; dollars are at stake
Key Stakeholders	First responders, Public interest	Consumers, Shareholders
Scale	Millions	100s of Millions (Billions world wide)
System Evolution	Driven by needs and reliability	Driven by Competition

Trying to unite these divergent approaches based on legacy deployments and infrastructure will certainly be taxing, particularly for performance sensitive services. For instance, re-dimensioning these networks to meet <1% blocking would have a huge impact on existing network capacity given that today's networks do not have QoS and are not able to discriminate users and associate class of service per type of user. Including these functionalities in the old technology is plainly not realistic. Unquestionably it requires new core and RAN technologies.

When such dramatic technological upgrades are required, the optimal approach is to start with a network design that directly addresses, by design, key functional and operational requirements. History has shown that when a new generation of technology appeared in the market, CMRS operators were not able to follow a green-field approach, as they needed to secure backwards compatibility with existing technologies, limiting the full potential of the new technology.

The NGPS network does not have to face this type of constraint. The public safety community recognizes that many of their existing systems are already obsolete and that the level of backwards compatibility required with their legacy systems is interoperability – ability that one legacy device can talk to a new device. This will be better achieved by

keeping the networks apart and building an interoperability bridge between the two. In this manner, the NGPS network will be able to leverage the best of what the new technologies have to offer and put it to work with an innovative network design that brings to fruition advanced solutions and applications to meet the most stringent public safety requirements.

The green-field approach at the design level does not exclude the possibility of leveraging existing physical infrastructure to host the new network. There is much wireless infrastructure deployed, which can be leveraged to reduce the cost and speed of implementation of new, green-field technology. For instance, there are many types of base stations used by CMRS, which could host a new channel element, based on the flat IP architecture, while still allowing those channel elements to operate on discrete spectrum, connect to discrete core networks, etc.

5 Public Safety Network Overview

The proposed NGPS network must leverage the best of Public Safety, Commercial Wireless, and Satellite technology to offer mission critical and advanced services, which are reliable and robust. It is multiple systems that are architected seamlessly to meet the stringent requirements of Public Safety[11] while offering unused capacity that can be leveraged by commercial interests. The SAFECOM requirements specify a network design incorporating a "System of Systems" consisting of multiple logical networks with varying spans of control[12]. This network provides that, plus an additional logical network that provides communication to commercial entities

The diagram - Figure 5- below provides a high level view of the network:

11 As outlined in SAFECOM Statement of Requirements, APCO proceedings, ETSI requirements and others

12 See Section 5 from "Statement of Requirements for Public Safety Wireless Communications and Interoperability", SAFECOM Program, Department of Homeland Security, Version 1.1, January 26, 2006

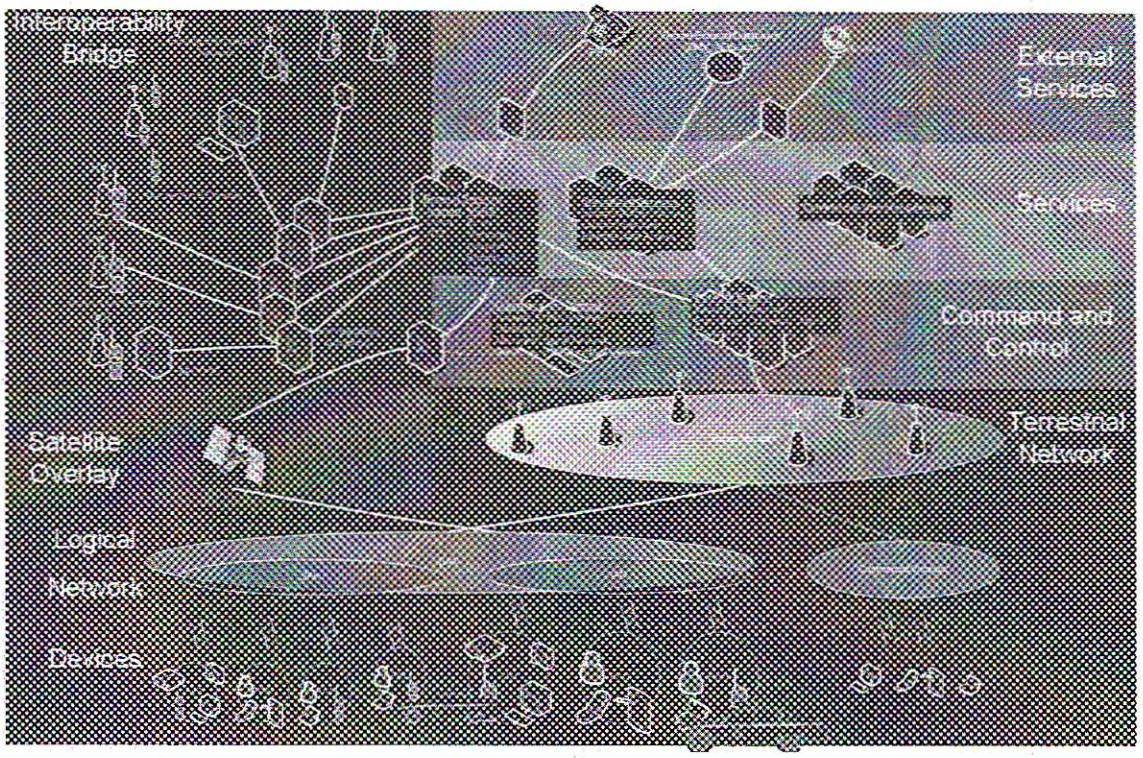

Figure 5– Next Generation Public Safety Network Overview

6 Architecting The Public Safety Network

As depicted above, the NGPS network is a complex system of systems composed of many elements. The way that each of these elements is designed and architected will have a definite impact on the overall performance of the system. This section presents 4DK Technologies, Inc. perspectives on some of the most critical elements of the network. It is by no means the intention of this section to propose specific solutions the public safety demands. Such endeavor requires a more diligent approach. The only objective is to share perspectives on how certain problems can be addressed by leveraging state-of-the-art technology.

This section will cover the following aspects of the NGPS network:

1. Spectrum
2. Coverage
3. Reliability
4. Capacity on demand
5. Satellite overlay
6. Services

7. Evolutionary interoperability
8. Devices
9. Logical networks
10. Command-and-Control
11. Network Control
12. External services

6.1 Spectrum

With the reallocation order in 1997, the Commission attempted to pave the way for a new era in Public Safety communications[13]. In 1996, APCO finished its initial Project 25 specifications[14] and sought a new spectral home for its technology. The Commission satisfied this need with the reallocation of 24 MHz of "Upper 700" spectrum. This spectrum was an ideal allocation for many reasons: the propagation characteristics, the neighboring 800 MHz Public Safety licenses and the relatively few, although powerful incumbent licensees, the broadcasters. As matters currently stand, the broadcasters do not have to vacate the spectrum until 2009, although Public Safety, the wireless industry and the Congress are attempting to move up this date. The fact that the reallocation of this 24 MHz to Public Safety has been a work in progress for nearly a decade suggests that no initiative should be allowed to disturb this progress.

The Commission has recently issued its 8th NPRM relative to the Public Safety 24 MHz Allocation at 700 MHz[15]. This proceeding is being driven from the Public Safety community to support its needs for broadband data and emerging services and applications. The Public Safety community has put forth a number of compelling proposals to rechannelize the allocation to support better use of broadband technologies, 4DK Technologies, Inc. fully supports the concepts put forth in the NPRM and strongly encourages the Commission to act swiftly in adopting rules, which will permit the Public Safety community to better utilize the spectrum it has been given for new and advanced technologies and services.

---

13 See 47 U.S.C. § 337(a)(1); Reallocation of Television Channels 60-69, the 746-806 MHz Band, ET Docket No. 97-157, Report and Order, 12 FCC Rcd 22953 (1997) (Reallocation Report and Order).

14 See SPECTRUM NEEDS OF EMERGENCY RESPONSE PROVIDERS comments in response to the Commission's *Public Notice*, FCC 05-80, released March 29, 2005, WT Docket No. 05-157 and Final Report of the Public Safety Advisory Board to FCC, September 11. 1996, www.ntia.doc.gov/osmhome/pubsafe/PSWAC_AL.pdf

15 See *Eigth Notice of Proposed Rulemaking, (WT Docket No. 96-86), FCC 06-34*

Both the Upper 700MHz and Lower 700 MHz proceedings are filled with analysis and commentary on the tremendous benefits of these bands. Particularly beneficial are the propagation characteristics of the band for full mobility, wireless communications systems[16]. The Figure 6 below shows an analysis from Aloha on the propagation characteristics of the different bands as well as the financial implications of those. Although the cost shown may not apply to Public Safety, they are nonetheless a good reference.

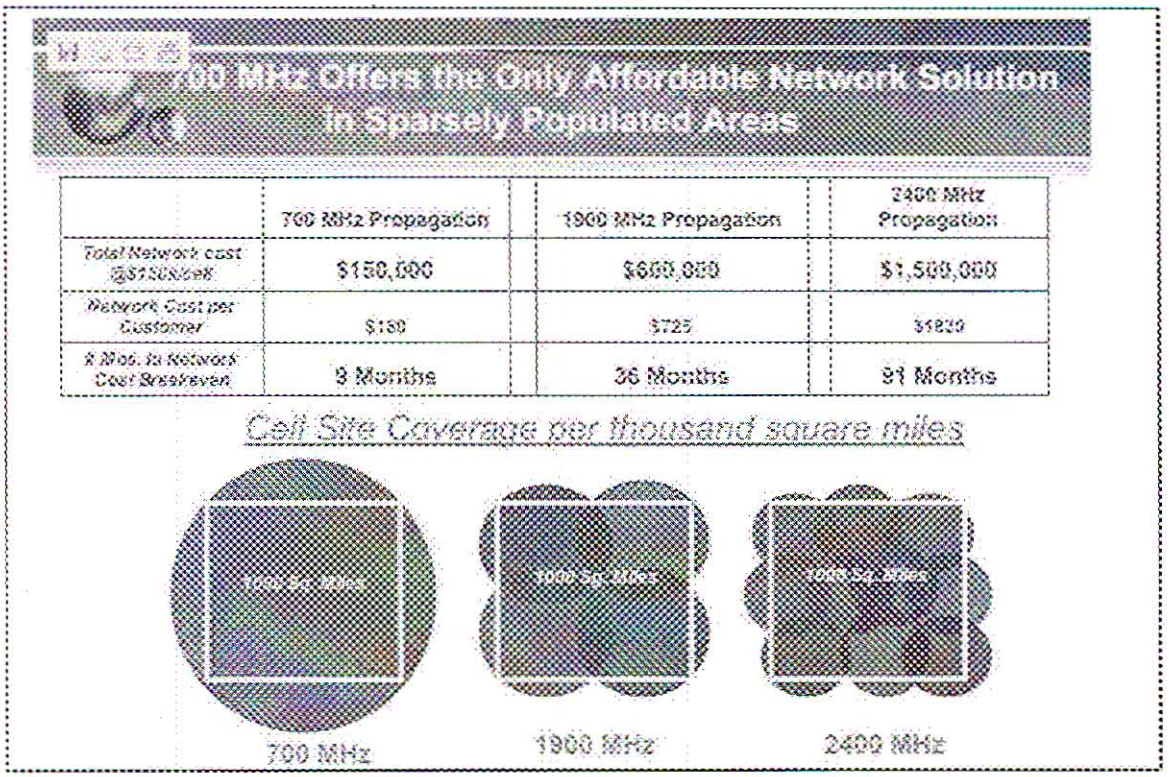

Figure 6 – 700 MHz, 1900 MHz, 2400 MHz spectrum comparison[17]

These benefits make the wisdom of the Commission's initial allocation to Public Safety in this band obvious to all - the best spectrum yields the best economics, particularly for new deployments. However, all on-going Public Safety proceedings and emerging analysis continue to argue that the current 24 MHz allocation is not enough[18].

---

16 See Aloha presentation, by Charlie Townsend, CEO

17 Source Aloha presentation, by Charlie Townsend, CEO

18 See Project Mesa report: User needs and scenarios drive spectrum requirements by Steffen Ring (www.projectmesa.com)

particularly to support emerging technologies and the ever critical and still unaddressed issue of interoperability.

> *"While the 24 MHz previously allocated will address many public safety communications requirements, by itself, it will not respond to public safety's growing need for wide-area, broadband mobile communications. PSWAC anticipated this requirement, and identified a need for over 90 MHz of spectrum for "wideband data and video."* [19]

For this reason and many others, the logical place to look for an additional allocation for Public Safety is in the vacant, adjacent 700 MHz. This adjacent spectrum, commonly referred to as the "C & D" blocks is optimal due to its very nature of being adjacent to the current Public Safety 700 MHz allocation, the clearing rules (like the current 24 MHz allocation) are in place and the cost for Public Safety to deploy emerging technology in this spectrum will be many orders of magnitude less than the 4.9 GHz (or other higher frequency bands.)

If an 8th NPRM rechannelization recommendation is adopted; the ultimate opportunity exists for a radical new approach in spectrum sharing, consolidation and management. It is utterly conceivable to imagine a scenario where Public Safety spectrum can ultimately be combined with the PSBT spectrum to promote even more efficient use of the entire "Upper 700 MHz" band. A visualization of this scenario can be seen in table below:

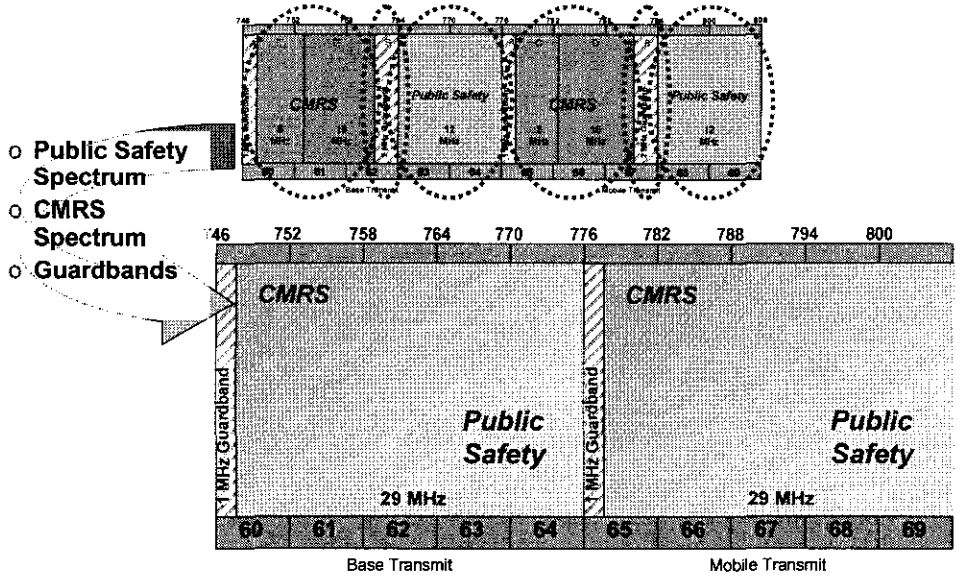

Figure 7 – Increasing spectral efficiency by sharing spectrum

---

[19] SPECTRUM NEEDS OF EMERGENCY RESPONSE PROVIDERS comments in response to the Commission's *Public Notice*, FCC 05-80, released March 29, 2005, WT Docket No. 05-157

In fact, should this come to fruition, it would likely be the first time that a "secondary market" driven by Public Safety could yield one of the most efficient utilizations of spectrum seen yet.

> *"Although spectrum is conceptualized as property, it is treated in an odd way – particularly Public Safety spectrum. The FCC allocates it in a command-and-control fashion to licensees who are deemed fit by the government, for uses approved by the government in the form of a hidden subsidy. Public Safety licensees receive only limited property rights. The FCC is left to decide exactly how much spectrum they can receive, what technologies they may use in their spectrum, and it prohibits secondary markets. No other resource is granted to agencies in this manner; this hidden subsidy provides a disincentive to agencies to make efficient use of their resource."*[20]

However, there is a compelling solution to the dilemma to which Mr. Marsh refers. The following is a brief synopsis of an additional spectrum reallocation scenario for the entire "Upper 700 MHz" band, which will be submitted concurrently and in detail as part of the on-going 8th NPRM.

In the present allocation of the "Upper 700 MHz" band, there is a disproportionate use of guard bands[21], which is the most inefficient use of spectrum of all. Modern technologies, particularly green field deployments can be designed from the inception to need little or no guard band[22]. Unfortunately, the narrow band nature of current Public Safety technologies still requires the use of guard bands. Due to this limitation, careful consideration must be given to the new proposals in the 8th NPRM for rechannelization, however, we would recommend the Commission to consider future opportunities such as the following.

Phase 1 – Create Public/Private Partnership and allow the spectrum to be used by both Commercial and Public Safety Interests with ultimate control under Public Safety.

---

[20] See *Analysis of Secondary Markets in Non-Federal Public SafetyPublic Safety Spectrum by Joshua Marsh*

[21] See Figure 7 – Increasing spectral efficiency by sharing spectrum

[22] See, Memorandum of Opinion & Order in the Matter of Access Spectrum, LCC Request for Waiver of Section 27.60, August 12, 2004