NPSTC

# Broadband Deployable Systems in the Nationwide Public Safety Broadband Network

*A Report from the National Public Safety Telecommunications Council and the Defence Research and Development Canada's Centre for Security Science*

Canadian Safety and Security Program
Programme canadien pour la sûreté et la sécurité

Defence Research and Development Canada
Recherche et développement pour la défense Canada

# Table of Contents


Executive Summary ..... 4

Public Safety Technical Requirements List ..... 18

Chapter 1: Introduction ..... 26

1.1 Continuity of Service Experience ..... 28

1.2 Public Safety LMR Deployable Systems ..... 28

1.3 Scope of Report ..... 29

Chapter 2: Public Safety Operational Uses of Deployable Systems ..... 32

2.1 Seamless Handover ..... 32

2.2 Priority, Pre-Emption, and Quality of Service ..... 33

2.3 Public Safety Use Cases ..... 33

2.4 BBDS Organized Response Plan ..... 36

Chapter 3: BBDS Form Factor and Architecture ..... 37

3.1 Deployable System Components ..... 37

3.2 Core-Enabled and Core-Ready Systems ..... 38

3.3 BBDS Form Factors ..... 42

Chapter 4: BBDS Network States ..... 49

4.1 Connected Mode ..... 49

4.2 Limited Connectivity Mode ..... 49

4.3 Stand Alone Mode ..... 50

4.4 Cluster Mode ..... 51

4.5 Device-to-Device Communications ..... 53

Chapter 5: Deployment Considerations ..... 55

5.1 First Responder Training ..... 55

5.2 Spectrum and Regulatory Issues ..... 56

5.3 BBDS Equipment Decision Matrix ..... 56

Chapter 6: International/Cross Border Considerations ..... 59

6.1 Cross Border Operational Considerations: U.S. / Canada ..... 59

6.2 Cross Border Operational Considerations: U.S. / Mexico ..... 67

Chapter 7: Role of Backhaul Communications ..... 70

7.1 Backhaul Connectivity ..... 71

7.2 Backhaul and BBDS Form Factors ..... 74
Chapter 8: Role of Applications ..... 76
8.1 Application Availability ..... 76
8.2 Internet of Things ..... 77
8.3 Home Status Page ..... 77
8.4 Network and Application Recovery ..... 78
8.5 Application Types in a Public Safety Broadband Network ..... 79
8.6 BBDS Specific Application Requirements ..... 80
8.7 Discovery ..... 81
8.8 Application Packages ..... 81
8.9 Content Transfer and Access Requirements ..... 82
Chapter 9: Voice Considerations for Deployable Systems ..... 85
9.1 Types of Voice Communications ..... 85
9.2 Mission Critical PTT ..... 87
9.3 MC-PTT Implementation ..... 87
Chapter 10: Operations and Maintenance ..... 90
10.1 General O&M Considerations ..... 90
10.2 Data Storage and Synchronization ..... 90
10.3 Software and Firmware ..... 91
10.4 Local Control Access Levels ..... 92
10.5 Configuration and Default Status ..... 92
Chapter 11: Deployable Systems Security / Assurance ..... 95
11.1 BBDS Security Elements ..... 95
11.2 BBDS Security – Stand Alone Operations ..... 97
Chapter 12: Technical Challenges ..... 98
12.1 Interference Management ..... 98
12.2 International Operations ..... 98
12.3 ICAM/HSS Database Management ..... 98
12.4 Inter-PLMNID Handover, Service Continuity and Session Persistence ..... 99
12.5 BBDS Inter-working with the NPSBN ..... 99
12.6 Voice inter-working between NPSBN macro and BBDS, among BBDS, and between 3GPP and non-3GPP networks ..... 99
12.7 ProSe Direct Mode Communications ..... 100
12.8 Device and applications management ..... 100
Chapter 13: Operational Policy & Governance Considerations ..... 102

13.1 Interoperability Elements ..... 102
13.2 Comparison to LMR Governance and Procedure ..... 103
Chapter 14: Conclusions and Recommendations ..... 106
LIST OF APPENDICES ..... 112
APPENDIX A: Operational Capabilities List ..... 113
APPENDIX B: Technical Challenges Chart ..... 118
APPENDIX C: Use Cases ..... 124
APPENDIX D: Deployable Systems Incident Commander Decision Matrix ..... 185
APPENDIX E: Working Group and Contributor List ..... 193
APPENDIX F: Bibliography ..... 204
APPENDIX G: Terminology, Definitions, and Acronyms ..... 210
APPENDIX H: Detailed Diagrams ..... 230

# Document Notices

Following is publication information for this document.

## Abstract

This document contains public safety technical requirements for the use of LTE Broadband Deployable Systems to support first responder communications. The National Public Safety Telecommunications Council (NPSTC) is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

## Acknowledgements

This report is a binational work product of the National Public Safety Telecommunications Council (NPSTC) and the Defence Research and Development Canada – Centre for Security Science (DRDC-CSS). This document was drafted by NPSTC's Broadband Deployable Systems Working Group and reviewed by the NPSTC Technology and Broadband Committee. NPSTC extends its thanks to Claudio Lucente from DRDC-CSS for his leadership as Chair of the Working Group. This report was approved in final form by the NPSTC Governing Board on March 31,2017.

**National Public Safety Telecommunications Council**

The National Public Safety Telecommunications Council is a federation of public safety organizations whose mission is to improve public safety communications and interoperability through collaborative leadership. NPSTC pursues the role of resource and advocate for public safety organizations in the United States on matters relating to public safety telecommunications. NPSTC explores technologies and policy involving public safety telecommunications, analyzes the ramifications of particular issues and submits comments to governmental bodies with the objective of furthering public safety telecommunications worldwide. NPSTC serves as a standing forum for the exchange of ideas and information for effective public safety telecommunications.

The following 16 organizations comprise the NPSTC Governing Board:

American Association of State Highway and Transportation Officials
American Radio Relay League
Association of Fish and Wildlife Agencies
Association of Public-Safety Communications Officials-International
Forestry Conservation Communications Association

International Association of Chiefs of Police
International Association of Emergency Managers
International Association of Fire Chiefs
International Municipal Signal Association
National Association of State Chief Information Officers
National Association of State Emergency Medical Services Officials
National Association of State Foresters
National Association of State Technology Directors
National Council of Statewide Interoperability Coordinators
National Emergency Number Association
National Sheriffs' Association

Several federal agencies are liaison members of NPSTC. These include the Department of Homeland Security (the Federal Emergency Management Agency, the Office of Emergency Communications, the Office for Interoperability and Compatibility, and the SAFECOM Program); Department of Commerce (National Telecommunications and Information Administration); the Federal Partnership for Interoperable Communications (FPIC); Department of the Interior; and the Department of Justice (National Institute of Justice, CommTech Program). In addition, Public Safety Europe (PSCE) and the University of Melbourne Centre for Disaster Management and Public Safety (CDMPS) are liaison members. NPSTC has relationships with associate members, the Canadian Interoperability Technology Interest Group (CITIG) and the Utilities Telecom Council (UTC), and affiliate members: The Alliance for Telecommunications Industry Solutions (ATIS), Open Mobile Alliance (OMA), Project 25 Technology Interest Group (PTIG), Telecommunications Industry Association (TIA), and TETRA Critical Communications Association (TCCA).

**Canadian Safety and Security Program (CSSP)**

The Canadian Safety and Security Program (CSSP) is a federally funded program. The program's mandate is to strengthen Canada's ability to anticipate, prevent, mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime, and terrorism through the convergence of science and technology (S&T) with policy, operations, and intelligence.

The CSSP is led by Defence Research and Development Canada's Centre for Security Science (DRDC CSS), in partnership with Public Safety Canada (PSC), which provides security and public safety policy guidance to the program. The CSSP supports federal, provincial, territorial and municipal government-led projects in collaboration with response and emergency management organizations, non-governmental agencies, industry, and academia.

**Broadband Deployable Systems Working Group**

The NPSTC-CSS Broadband Deployable Systems Working Group is composed of 166 members of public safety, academia, and industry who have conducted an extensive review of issues and requirements impacting deployable system operations.

The Working Group's report has been through a series of internal and external reviews to ensure that the content, recommendations, and requirements reflect the needs of public safety personnel. Draft documents are reviewed by a designated Public Safety Review Team and are forwarded to the NPSTC Governing Board for further review prior to approval. This report will then be transmitted to the FirstNet Public Safety Advisory Committee (PSAC) for their review and consideration.

Contact Information
Support Office
8191 Southpark Lane, Suite 205
Littleton, CO 80120-4641
Fax: (303) 649-1844
Toll Free: (866) 807-4755
NPSTC: support@npstc.org
NIIX: support@niix.org

NPSTC Administration
Marilyn Ward, Executive Director
mward@npstc.org
http://www.npstc.org

# Executive Summary

The passage of the Middle Class Tax Relief and Job Creation Act of 2012 enabled the creation of the First Responder Network Authority. This legislation establishes the governance and provides the funding necessary to build a Nationwide Public Safety Broadband Network (NPSBN) which will transform the way first responders communicate and manage daily operations and emergency incidents. A key component of this project will involve the use of LTE broadband deployable systems to augment the coverage and capacity provided by the NPSBN's network of towers and other infrastructure.

The First Responder Network Authority's (FirstNet) development of the NPSBN depends on the articulation of public safety's technical and operational requirements in the immediate, medium, and long-terms. The National Public Safety Telecommunications Council (NPSTC) prepared this document to articulate both short-and long-term requirements and recommendations for the operation and use of broadband deployable systems.

Likewise, the Government of Canada is in the process of authorizing a Public Safety Broadband Network (PSBN). Canada's radio frequency regulatory body, the Innovation, Science and Economic Development (ISED-Canada) has set aside 20 MHz of spectrum to support this initiative. This spectrum is aligned with the 700 MHz spectrum allocated for use by FirstNet.

While this report focuses on the U.S. and Canadian public safety broadband programs, it should be noted that there is no harmonization of 700 MHz spectrum between the U.S. and Mexico. This will create unique problems for both the implementation of the NPSBN and interoperability between first responders from the U.S. and Mexico.

**Purpose of This Report**

The principal purpose of this document is to define, from the perspective of NPSTC, public safety requirements for the operation and use of LTE Broadband Deployable Systems (BBDS). A secondary purpose of this report is to establish the baseline for an iterative process to develop successively more detailed public safety requirements for BBDS as the NPSBN evolves based on FirstNet's decisions in deploying, administering, operating, and maintaining the NPSBN.

This report also provides background information and informative text on many technical challenges, operational issues, and governance considerations which impact the use of these systems by first responders.

This report considers extensive inputs and comments by a wide variety of stakeholders in public safety communications, including representatives of U.S. and Canadian first responder

communities at the local, state/provincial/territorial, tribal, and federal level,[1] as well as domestic and international communications service providers, manufacturers, other industry segments, and consultants.

The requirements identified in this report are critical to ensure the necessary flexibility required by public safety agencies to successfully utilize the NPSBN to protect their constituent populations.

There are four main components of this report:

- **Operational, technical, and background information.** This information is contained throughout the report in the various chapters relating to specific BBDS components and issues.
- **Public Safety Technical Requirements**. Fifty-four technical requirements have been identified which articulate necessary capabilities of BBDS technology.
- **Technical Challenges**. A series of technical challenges have been identified that may negatively impact the maximum utilization of BBDS by public safety agencies.
- **Conclusions and Recommendations**. Eighteen conclusions have been identified which illustrate public safety's expectations of BBDS technology and 16 action items articulate a "path forward" for the implementation and use of BBDS.

This report does not address those issues which are common to both the NPSBN macro network and BBDS. These include issues relating to network standards, security, and authentication, among others. Public safety technical requirements for these areas have already been published in prior NPSTC reports.

**Nationwide Public Safety Broadband Network**

This report will use the acronym "NPSBN" to refer to both the U.S. FirstNet initiative as well as the Canadian Public Safety Broadband Network. If necessary, a country-specific reference will be made to identify issues unique to either the U.S. or Canada.

Throughout the document the term "macro network" refers to the fixed (terrestrial) NPSBN LTE infrastructure and "BBDS" (Broadband Deployable System) to account for all types of deployable units and solutions.[2]

[1] For brevity, this report will use the phrase "Local, State/Provincial and Federal" when referring to the larger set of government entities in both the U.S. and Canada.

FirstNet has stated that mission critical voice services will not initially be offered as a service on the NPSBN. Many public safety agencies have indicated that they will continue to utilize their land mobile radio (LMR) networks for mission critical voice operations into the foreseeable future. It is expected that the NPSBN will initially provide "administrative push to talk" (PTT) which will transition to Mission Critical Push-To-Talk (MC-PTT) services. This report anticipates the eventual usage of MC-PTT by first responders who are connected to a BBDS and further highlights the need for first responders using BBDS MC-PTT to interoperate with other public safety agencies who continue to use LMR.

First responders in the U.S. and Canada need reliable coverage and sufficient network capacity to conduct mission critical public safety activities. While much of the NPSBN coverage and capacity will be provided by a network of fixed tower sites, certain geographical areas will require the deployment of supplemental infrastructure including mobile and portable systems. There are areas in both countries where it is not economically feasible to build tower sites (e.g., rural areas with very low population density), where it is not permissible to erect tower sites (e.g., national parks and forests), as well as locations the fixed infrastructure cannot reach (e.g., lower levels of concrete parking garages). Public safety agencies also respond to a variety of large-scale emergency incidents and preplanned events in which existing network capacity is insufficient to meet the operational need.

BBDS represents one solution[3] to help address the need for coverage and capacity. BBDS systems come in a variety of sizes and configurations and this report examines how BBDS technology may be used in backpacks, vehicles, aerial and waterborne units, and towed trailer solutions. BBDS may be provided as a standalone technology or may come integrated with other complementary systems, including onboard power (batteries, generators, shore power connections), backhaul capabilities (microwave, satellite, and wired connection), LMR interconnection capabilities, and wireless connection points (Wi-Fi).

Regardless of the form factor or integration, all BBDS may be categorized in one of two ways:

1. "**Core-Enabled BBDS"** include the LTE Radio Access Network (RAN) and the Evolved Packet Core (EPC) and may also include local application servers and databases. This allows for completely autonomous operation of the BBDS when not connected to the NPSBN

[2] Public safety agencies and industry use a variety of different terminologies when referring to a broadband deployable system. These include, among others, "Broadband Deployable System," "Broadband Deployable Solution," and "Broadband Deployable Platform."

[3] There are a variety of other fixed infrastructure solutions to provide in-building coverage, including small cell technology, use of WiFi, and other systems as well as technologies to boost the NPSBN RF signal into buildings and to provide greater rural coverage through the use of higher powered transmitter sites.

macro network. It may also provide certain mission critical capabilities4 including MC-PTT, video sharing and access to incident command applications. A Core-Enabled BBDS may also provide local application support to first responders even when connected to the NPSBN macro network. This is a more complex solution than the Core-Ready BBDS described below. However, these Core-Enabled BBDS are preferred in a variety of settings because they more fully support first responders at an incident scene. In essence, this type of BBDS has its own LTE Core that can provide a minimum level of functionality.

**2. "Core-Ready BBDS"** only include basic RAN components and are designed to provide simple network extension functions. These solutions do not include an EPC and therefore require a connection to the NPSBN macro network[5] to access services. They do not include onboard application servers. The phrase "Core Ready" indicates that these BBDS do not include a "core" but may be designed to support the later addition of core components (transforming them into a "Core-Enabled" BBDS). However, Core-Ready BBDS are likely to be installed in first responder vehicles to extend NPSBN coverage to the immediate area around an incident or into a building. This basic network extension capability will play an important role in the overall deployment of the NPSBN.

**Key Attributes**

It is important to recognize the differences between BBDS solutions and the NPSBN macro network. The following key attributes define a BBDS:

- It is **transportable** and brought to the scene of an incident on an as-needed basis.
- It is a **self-contained** system in accordance with the functions that it is equipped to provide. This typically includes the provision of onboard power, antenna systems, and backhaul capabilities.
- It is capable of operating with either full backhaul connectivity, limited backhaul connectivity, or **no backhaul connectivity** to the macro network.[6]
- It can be **activated quickly** at the scene of an incident.
- It can be made operational by first responders with **minimal technical training**.

[4] When a BBDS is operated in a disconnected state (Stand Alone mode), first responders will not be able to access remote databases such as statewide driver's license records, DMV records, and other data stored on agency servers.

[5] NPSBN Core Network refers to the main infrastructure and components of the LTE Network.

[6] The level of service provided by the BBDS is variable based on BBDS type and availability of a backhaul connection to the NPSBN macro network.

**NPSBN Assumptions**

There are many unknowns regarding how FirstNet and its selected contractor will organize the NPSBN and implement the use of BBDS technology. The NPSBN contractor will determine to what extent various standards and capabilities will be implemented on the network. This report is based on a number of assumptions, which include:

- LMR systems continue to provide mission critical voice service to public safety agencies.
- In the longer term, the NPSBN will also provide MC-PTT services.[7]
- BBDS technology will continue to evolve with improved capabilities and features.
- 3GPP International standards work will continue to evolve and address issues unique to BBDS.
- FirstNet will permit local public safety agencies to acquire (or lease), operate, and maintain certain types of BBDS (subject to appropriate oversight). It is acknowledged that this approach may complicate network operations and require extensive coordination between the NPSBN and local agencies.[8] However, the rapid and efficient deployment of BBDS by local public safety agencies is considered essential in order to provide necessary coverage and capacity that impacts first responder safety.
    - It is envisioned that public safety agencies may operate certain types of BBDS including backpacks, vehicle based systems, and small lightweight airborne units.
    - It is envisioned that the NPSBN contractor will likely own and operate more complex types of BBDS including towed trailer solutions.
- FirstNet's contractor will provide BBDS to support restoration of service following a network failure in addition to providing BBDS to enhance NPSBN capacity at large-scale events and incidents.

**Public Safety Operational Issues**

This report addresses key issues which are critical to the successful implementation of BBDS. These include the concept of seamless transition, the need for applications and services to be hosted locally on the BBDS, management of security and credentialing information on the

[7] It is recognized that standards and technology continue to evolve in this area.

[8] Local agencies should be able to deploy stand-alone BBDS with little coordination; however, adding BBDS to enhance capacity (e.g., during a planned event) should not be attempted without significant NPSBN cooperation. Cooperation is necessary for proper tuning and interference mitigation, and to ensure that other agencies sharing the network are not adversely impacted.

BBDS, and the need for rapid deployment of BBDS services by personnel who are likely to be on the scene of the incident.

**1. Seamless Transition**

Seamless transition is based on two technical approaches, Service Continuity and Session Persistence. **Service Continuity** involves the handover of a public safety device as it moves between nodes of the same or different networks. **Session Persistence** means that the first responder's voice and data applications will not be interrupted as they move from one node of the same or different network to another. Both of these components must be addressed during system design and implementation in order to assure that first responders can safely use the NPSBN and BBDS solutions. Police officers must have continuous voice and data communication as they move between different tower sites on the NPSBN macro system and as they transition from the NPSBN to a BBDS solution providing extended coverage.

**2. BBDS Hosted and Remote Hosted Applications**

Core-Enabled BBDS will need to host and support mission critical applications (and corresponding databases[9]) used by first responders. These include the need for mission critical voice communications and access to certain incident command and incident management applications. In some instances, public safety personnel will access databases and applications that reside on the NPSBN macro network, using the BBDS backhaul connection. In other cases, first responders will need guaranteed access to certain applications that must continue to operate even if backhaul connectivity to the NPSBN core is lost. Mission critical voice communications are one example of an application (or service) that provides support for first responders operating on the BBDS. In other cases, first responders who are operating on the NPSBN macro network will need access to applications and data that reside on the BBDS.

There are a variety of reasons why a Core-Enabled BBDS may need to house application servers and databases:

- A BBDS may be implemented as a stand-alone communications site in a rural area to support a specific mission where backhaul is either not available, not possible, or not needed.
- A BBDS may be implemented as a component of a disaster recovery response where NPSBN service has been disrupted due to damaged infrastructure.
- A BBDS may suffer an interruption or loss of its backhaul link to the NPSBN macro network due to a technology failure or other cause.

[9] For example, an MC-PTT subscriber credential database.

This report discusses different approaches to the management of applications and services. For example, application data must be resynced between users and systems operating on the NPSBN macro network and the BBDS following recovery from a backhaul failure. An incident commander and a dispatcher may be viewing a list of engine companies at the scene of a wildland fire. If the backhaul link is temporarily lost the incident commander will not see changes to engine company assignments made by the dispatcher. The dispatcher will not be aware of changes to crew assignments made by the incident commander. This data must be rapidly reconciled immediately upon restoration of the backhaul connectivity. This issue of data synchronization and recovery is discussed in greater detail in Chapter 8.

Another example focuses on how MC-PTT services should be configured. A team of first responders may be communicating among themselves through a BBDS at the scene of an incident while also communicating with other first responders who are connected to the NPSBN macro network. If the backhaul connection linking the BBDS and the NPSBN core is lost, one or both groups may lose communications:

- If the MC-PTT service is running on a local BBDS server, first responders at the scene should continue with uninterrupted communications, while those first responders connected to the NPSBN macro network will be dropped (including the incident dispatcher).
- If the MC-PPT service is running on the NPSBN macro network, first responders at the scene would lose communications while those operating on the NPSBN macro would still have service.

In order to provide the highest level of reliability for these services, first responders should access MC-PTT and other mission critical applications locally using BBDS components. Work is currently underway in the 3GPP International standards body to examine the use of dual MC-PTT servers.

### 3. Security and Credentials

Public safety personnel cannot access a BBDS without appropriate credentials. First responder subscriber devices must be registered to the BBDS and public safety personnel must be authenticated using their personal log on credentials. All of this information is stored or referenced in a Home Subscriber Service (HSS) and MC-PTT database. This issue becomes critical when a BBDS is operating in Stand-Alone mode with no backhaul connectivity to the NPSBN macro network, or if BBDS backhaul connectivity is lost. Core-Enabled BBDS will need to synchronize a subset of the NPSBN HSS database to capture information needed to support local first responders who will be using this particular BBDS. Physical and cyber security issues

must be addressed to ensure that this data remains secure and up-to-date on the BBDS local database and the NPSBN macro database.

A solution will also be needed to support the arrival of other first responders and devices from outside the local area. For example, a major earthquake in the Seattle, Washington, region would likely disrupt the macro infrastructure of the NPSBN. This would require the use of BBDS to provide localized broadband coverage to support emergency operations including search and rescue activities. Firefighters from Portland, Oregon, arriving to assist the Seattle Fire Department might not be listed in the HSS security database of BBDS operated by Seattle area public safety agencies. In another instance, mutual aid units responding from the Province of British Columbia, Canada, to assist the City of Seattle would probably not be listed in the HSS security database. Devices carried by both groups of these mutual aid responders would need to be authorized to access the BBDS.

Finally, discussion is needed on how non-public safety agency subscribers will access the BBDS. Will the NPSBN operator allow commercial subscribers to access the excess capacity of the BBDS when it is deployed for large public gatherings like sporting events. Should the public have access to a public safety BBDS at a disaster scene in order to dial 911?

**4. Speed and Ease of Deployment**

The overarching requirement for public safety is to activate BBDS services quickly and with minimal effort by first responders. There are a variety of BBDS form factors and a wide range of technology capabilities that can be implemented. While certain types of BBDS will require the presence of trained technicians, other classes of BBDS should be configured for easy and quick activation. While trained technicians will be needed for more complex activations, it is important to note that some BBDS services may be needed in forward operating areas which involve hazardous conditions which will preclude technician assistance. Also, large-scale operations will require 24x7 technician assistance. These issues are important when considering the extent of first responder and contractor maintained systems. Chapter 5 of this report reviews BBDS deployment considerations.

**BBDS Deployment Challenges**

There are a number of challenges and considerations when assessing the deployment of BBDS service. These include technical, operational, and administrative components that are necessary to successfully implement the use of BBDS. These challenges are detailed in Chapter 2 and include:

- BBDS operations with limited or absent backhaul connectivity to the NPSBN macro network.

- Rapid ad hoc deployments of BBDS to emergency incidents at locations with no preplanned integration with the NPSBN macro network.
- Complex life-cycle configuration management of a widely diversified pool of BBDS assets.
- Complex inter-working environments between BBDS and the NPSBN macro network.
- The need to secure sensitive user profile and device authentication information in unsecured BBDS operating environments.
- Enabling interoperability during mutual aid operations in which first responders arrive from outside the normal service area of the BBDS and who are not provisioned in the local BBDS databases or who are using non LTE subscriber devices.

**Public Safety Technical Requirements**

This report includes a series of public safety technical requirements which articulate the operational vision for BBDS usage by first responders. It should be noted that the applicability of some requirements is based on form factor and whether the BBDS is Core-Enabled or Core-Ready. Notations have been added to the requirements table to indicate if a given item is applicable to all BBDS (ALL) or only to Core-Enabled (CE) or Core-Ready (CR) systems. The list of requirements immediately follows the Executive Summary. Requirements unique to each section in the report are also listed at the end of the applicable chapter.

**Technical Challenges**

Chapter 12 identifies a number of inferred technical challenges that need to be addressed in order to realize the full potential of BBDS technology. These include challenges in several key areas of BBDS deployment and operation.

- Interference management between BBDS and the macro network, as well as between multiple BBDS operating in Cluster Mode.
- International operations in which first responders may need to access BBDS infrastructure hosted by an adjacent border country.
- ICAM/HSS database management and the need for local copies of these security and authentication databases to be resident (and updated) on the BBDS.
- Aerial operations requiring interference management and high speed, low latency backhaul to the NPSBN macro network.

- Inter-PLMNID handover, service continuity, and session persistence for first responders as they transition between various network nodes.

- Voice inter-working between NPSBN macro and BBDS, among BBDS, and between 3GPP and non-3GPP networks.

- BBDS device and applications management challenges associated with use of multiple vendor-supplied equipment platforms.

**Conclusions and Recommendations**

Chapter 14 provides a series of high-level conclusions and a set of "next steps" regarding the provision of BBDS technology by the NPSBN operator and the use of BBDS technology by public safety agencies.

A series of **high-level conclusions** were developed following a review of the operational, technical, and policy information contained in this report. These high level conclusions identify important considerations for successful use of BBDS by public safety agencies:

*1.* Public safety agencies will require the NPSBN to include certain capabilities to extend the range, capacity, and delivery of mission critical services. This includes the provision of public safety broadband connectivity on an itinerant basis in a variety of settings (e.g., supplementing existing service, activating service in an area with no coverage, and access to disaster recovery services to restore the NPSBN network). *Chapter 2: Public Safety Use of Deployable Systems.*

2. A broad range of BBDS solutions are required to meet the operational requirements of public safety agencies, including various form factors (e.g., backpack, vehicular, aerial, towed) and different levels of onboard technology (e.g., local area range extension, provision of mission critical applications, LMR/LTE interconnection, etc.). *Chapter 3: BBDS Form Factor and Architecture*

3. First responders will require a seamless transition of voice and data services, with no interruption in service, as they move between the NPSBN macro network and a connected BBDS[10]as well as between a cluster of connected BBDS. *Chapter 4: BBDS Network States*

[10] It is recognized that seamless transition is not possible in all instances, including transition from the NPSBN macro network to a BBDS operating in Stand Alone mode (which is disconnected from the NPSBN).

4. Public safety agencies also need access to mission critical voice, data, and video in a stand-alone environment in which the BBDS has no connection to the NPSBN core or remote services. *Chapter 4: BBDS Network States*

5. For BBDS to be effective it must provide mission critical services in the early stages of the incident. BBDS must therefore arrive quickly and support "ease of activation" to allow operation by first responders with minimal training. 11 *Chapter 5: Deployment Considerations*

6. Systems, policies, and technology must be in place to facilitate the coordination of key parameters that impact the inter-working between the BBDS and the NPSBN macro network thereby, enabling a rapid activation of BBDS. 12 *Chapter 5: Deployment Considerations*

7. First responders will require public safety broadband services at, and across, the international borders to support their mission. This may require access to another country's NPSBN infrastructure, including BBDS. (*Chapter 6: International/Cross Border Considerations)*

8. First responders also require NPSBN voice, data and video interoperability in order to communicate with public safety agencies in an adjoining country. (*Chapter 6: International/Cross Border Considerations)*

9. Secure and reliable backhaul connections linking the BBDS to the NPSBN macro network are critical13 in order to support access to mission critical services and databases. (*Chapter 7: Role of Backhaul and Link Communications)*

10. Public safety agencies will require access to a minimum set of applications and services which are installed on the BBDS to support mission critical activities. This includes periods when the BBDS is disconnected from the NPSBN macro network. *Chapter 8: Role of Applications*

11. First responders require reliable access to Mission Critical Push-To-Talk when connected to a BBDS and loss of the backhaul connection to the NPSBN macro network must not compromise push to talk service with personnel at the incident scene. *Chapter 9: Voice Considerations for Deployable Systems*

[11] BBDS deployment should include a formal ordering process that details response and set up time. BBDS deployment should also accommodate the skill set of the user likely to be responsible for its operation.

[12] Examples include algorithms for Self-Organizing Network (SON) functions and interference control.

[13] Backhaul connectivity is not always possible and a BBDS may need to operate in Stand-Alone mode. See Conclusion #4.

12. Authorized first responder LTE devices must automatically connect to the BBDS, even when they are isolated from the rest of the NPSBN, requiring synchronization of the BBDS HSS (Home Subscriber Service) database with the NPSBN macro network database. *Chapter 10: Operations and Maintenance*

13. When connected BBDS are deployed, the NPSBN network management team should be able to monitor and control them, regardless of their provenance. *Chapter 10: Operations and Maintenance*

14. Given its itinerant deployment role, the BBDS must support a high level of security including physical security of the BBDS equipment (including server and database components), network security (including RAN and backhaul connections), and cyber security systems. *Chapter 11: Deployable Systems Security and Assurance*

15. Coordination of the configuration of Security Gateways on the BBDS and in the NPSBN is a key consideration. *Chapter 11: Deployable Systems Security and Assurance*

16. Full implementation of BBDS technology will require significant focus to resolve a number of technical challenges. *Chapter 12: Technical Considerations and Challenges*

17. Successful adoption and implementation of BBDS must include attention to issues beyond the technology and should address all lanes of the SAFECOM Interoperability Continuum including governance, SOP, training, and usage. *Chapter 13: Operational Policy and Governance Considerations*

The following **recommendations** establish "next steps" in the process to fully realize the operational potential of BBDS for public safety agencies.

1. Following consultation with public safety agencies, NPSBN management and its operator must determine and articulate the role of BBDS technology, including rules regarding the licensing, procurement, and operation of these systems by local public safety agencies.

2. NPSBN management and its operator should prepare interoperability guidelines for BBDS due to the use of multi-vendor equipment and multi-agency governance of these systems. Interoperability guidance should cover a number of technical issues, including IPsec configurations; OAM interfaces and protocols; configuration management; assignment of unique network identifiers; and IP address schemes among others.

3. NPSBN management should ensure that network design and planning includes necessary components and strategies to allow for future successful usage of BBDS at, and across, the international border, ensuring that authorized first responders may

access BBDS infrastructure from either country during an emergency. This recommendation acknowledges the need for spectrum management and policy coordination with the involved countries.

4. In order to ensure consistency and standardization of technology, NPSBN management should identify minimum mandatory requirements for BBDS in order to set the required level of interoperability between agencies and BBDS from different vendors.

5. Technical challenges with BBDS identified in this report should be evaluated by the Public Safety Communications Research (PSCR) Lab and other government organized or sponsored entities for validation.

6. Management of interference between the NPSBN Mode of Operation and BBDS Mode of Operation (either Connected, Standalone, Clustered) will be critical to ensure minimum interference in Band 14 usage. This applies within the FirstNet NPSBN, Canadian PSBN, and any locally operated BBDS.

7. During BBDS operation, a significant consideration involves the security of Data-at-Rest, meaning data resident onboard the BBDS that must be maintained in a highly safe and secure manner. This has physical security as well as data encryption components.

8. Additional research and public safety collaboration is needed to establish best practices for the provision of mission critical services via a BBDS. This includes an assessment of the impact of macro hosted mission critical services vs. BBDS local hosting of these services. Mission critical services includes both mission critical PTT and other mission critical data applications deemed essential for incident response.

9. NPSBN management should support the evolution of 3GPP standards to enhance the capabilities of BBDS, including issues addressed in this report.

10. Work is needed to develop a nationwide standard for identification of LTE talkgroups and to address best practices for on-network usage (both macro network and BBDS) and off-network usage (direct mode).

11. Consideration should be given to update the National Incident Management System (NIMS) sections on Resource Typing to standardize the various form factors and capabilities of BBDS, providing uniformity during requests for service.

12. Further research and advocacy are needed regarding utilization of non-700 MHz spectrum to support backhaul from BBDS to the macro network and between BBDS operating in a cluster.

13. Further research is needed regarding how to best manage the access and credentialing solution for BBDS, including how HSS database records are stored and secured on a local BBDS.

14. NPSBN management should place a high priority on development of strategies and solutions on effective management of the BBDS HSS database. In order for HSS databases to exchange information it is necessary that the interface protocols and data models be implemented the same way by all the parties that own the BBDS systems. This would likely require national guidance [1].

15. NPSBN management should continue to leverage knowledge gained from the Early Builder communities who are using BBDS technology.

16. A set of Best Practices for the deployment of BBDS technology should be created to help ensure that the BBDS solution matching the needs of the incident is dispatched at the right time.

It is acknowledged that some of the recommendations made in this report may eventually be deemed inconsistent with NPSBN policy due to technical complexity, operational complexity, or cost.

Finally, NPSTC would like to acknowledge the hard work and contributions of the Broadband Deployment Systems Working Group members who participated on weekly conference calls over a 2 ½ -year period to research, discuss, and articulate the vast amount of information contained in this report. NPSTC also wishes to extend its sincere thanks to the Defence Research and Development Canada's - Centre for Security Science (DRDC CSS) and the Public Safety Communications Research (PSCR) program for their ongoing collaboration and technical contributions to this report.

# Public Safety Technical Requirements List

This chart lists the public safety technical requirements for BBDS and notes if the requirement is applicable for all types of BBDS (ALL BBDS) or only to certain types of BBDS (Core-Enabled BBDS are displayed as CE-BBDS).

| **National Public Safety Telecommunications Council<br>Broadband Deployable Systems Public Safety Technical Requirements** | | |
|---|---|---|
| **Technical Requirement Statement** | **Chapter** | **Requirement Applicability to BBDS Type** |
| Connected BBDS SHALL support service continuity and session persistence for users during transition to and from the NPSBN macro network. | Chapter 2 Public Safety Use | ALL BBDS |
| Connected BBDS SHALL support service continuity and session persistence for users transitioning between different BBDS operating in Cluster Operations Mode. | Chapter 2 Public Safety Use | CE BBDS |
| BBDS SHALL support the same priority, pre-emption, and QoS features as the NPSBN macro network. | Chapter 2 Public Safety Use | ALL BBDS |
| During handover, the BBDS SHALL maintain the PQOS settings of first responders as they transition to and from the NPSBN macro network**.** | Chapter 2 Public Safety Use | ALL BBDS |
| BBDS SHALL be fully operable self-contained systems in accordance with the applicable category of the deployable equipment. | Chapter 3 Form Factor | ALL BBDS |
| Certain BBDSs, such as backpacks and those installed in emergency vehicles, SHALL be designed for ease of use and activated with minimal human intervention by trained first responders. | Chapter 3 Form Factor | ALL BBDS |

| | | |
|---|---|---|
| The BBDS SHALL support continuous operations for the period of time specified by the owner/operator (based on form factor and other considerations). | Chapter 3 Form Factor | ALL BBDS |
| To prevent interference, a BBDS SHALL disable the radio access network when the vehicle carrying the deployable system is in motion. | Chapter 3 Form Factor | ALL BBDS |
| BBDS SHALL be available for use by first responders in both Core-Ready BBDS and Core-Enabled BBDS configurations. | Chapter 3 Form Factor | ALL BBDS |
| BBDS SHALL be available in form factors that can be used on aerial platforms. | Chapter 3 Form Factor | ALL BBDS |
| BBDS that are deployed in transportable cases SHALL support both AC and DC power sources. | Chapter 3 Form Factor | ALL BBDS |
| An aerial BBDS SHALL be capable of coordinating with the NPSBN macro network to minimize mutual interference. | Chapter 4 Network | ALL BBDS |
| A BBDS operating in Stand-Alone mode SHALL support registration of authorized subscriber devices. | Chapter 4 Network | CE BBDS |
| The BBDS SHALL alert user devices when the deployable system is operating in or has transitioned to Stand-Alone mode. | Chapter 4 Network | CE BBDS |
| BBDS SHALL be able to serve those users who are accessing a UE to Network Relay to reach the BBDS network. | Chapter 4 Network | ALL BBDS |
| BBDSs SHALL be capable of interworking with other properly provisioned BBDSs. | Chapter 4 Network | ALL BBDS |
| BBDS sourced from approved but different vendors and maintained by different public safety entities SHALL inter-operate when they are used at a common incident. | Chapter 4 Network | ALL BBDS |

| | | |
|---|---|---|
| The BBDS SHALL meet minimum environmental and hardening requirements applicable to the service area. | Chapter 5 Deployment | ALL BBDS |
| BBDSs SHALL integrate with existing BBDSs in proximity to each other without causing harmful degradation to other BBDS system performance and user experience. | Chapter 5 Deployment | ALL BBDS |
| BBDSs SHALL integrate into existing macro NPSBN infrastructure without causing harmful degradation to the NPSBN system performance and user experience. | Chapter 5 Deployment | ALL BBDS |
| BBDSs SHALL support session persistence and service continuity for first responders that belong to other partner Mobile Network Operators (MNOs), (e.g., other public safety broadband mobile network operators, international and domestic commercial carriers). | Chapter 6 Cross Border | CE BBDS |
| To provide first responders with access their local agency data, BBDS SHALL allow first responders from either country access to their home jurisdiction's information networks, regardless of whether they are served by the NPSBN or the C-PSBN, (subject to authorization by the home information networks' administrators). | Chapter 6 Cross Border | ALL BBDS |
| To provide first responders with data interoperability, BBDS SHOULD allow first responders from either country access to the local information networks of the other country, regardless of whether they are served by the NPSBN or the C-PSBN, (subject to authorization by the local information networks' administrators). | Chapter 6 Cross Border | ALL BBDS |

| | | |
|---|---|---|
| BBDS SHALL support priority, pre-emption, and QoS in accordance with the local NPSBN and C-PSBN policies. | Chapter 6 Cross Border | ALL BBDS |
| When A Core-Enabled BBDS from one country connects to the macro network of the other country, that BBDS SHALL apply the PQOS settings of the host (macro network). [e.g., If a U.S. based BBDS connects to the macro network of the Canadian PSBN, the BBDS would adopt the PQOS settings of the Canadian macro network]. | Chapter 6 Cross Border | CE BBDS |
| BBDS SHALL support service continuity and session persistence as first responders transition between the NPSBN and the C-PSBN, and vice-versa, (i.e., there is no perceptible interruption in service during the handover). | Chapter 6 Cross Border | ALL BBDS |
| BBDS from one country that overlaps in coverage with the macro network or BBDS from the other country SHALL be activated and made fully operational with minimal human intervention. | Chapter 6 Cross Border | ALL BBDS |
| BBDS operated by Canadian or U.S agencies SHALL support authentication of first responders from either country when the BBDS is isolated, (i.e., the BBDS is not connected to either the NPSBN or the PSBN macro networks). | Chapter 6 Cross Border | CE BBDS |
| Designated BBDS SHALL be able to interface with designated alternative backhaul technologies (e.g., satellite, microwave radio, and other backhaul technologies to provide alternative backhaul in the event the macro infrastructure is unavailable). | Chapter 7 Backhaul | ALL BBDS |
| The BBDS SHALL include backhaul connectivity to the NPSBN macro network with sufficient capacity to support available applications and services. | Chapter 7 Backhaul | ALL BBDS |

| | | |
|---|---|---|
| If a BBDS uses a satellite system to support backhaul connectivity, it SHOULD support automatic alignment of satellite antennas. | Chapter 7 Backhaul | ALL BBDS |
| The BBDS SHOULD provide a locally hosted authentication service for applications and users. | Chapter 7 Backhaul | CE BBDS |
| A BBDS-hosted authentication service SHALL be interoperable with the NPSBN authentication service to support operations during periods of compromised or absent connectivity. | Chapter 7 Backhaul | CE BBDS |
| A vehicular BBDS SHOULD be capable of being served by any donor eNodeB (DeNB). | Chapter 7 Backhaul | ALL BBDS |
| The BBDS SHALL allow subscriber devices to access the general Internet based on security and local control profile configuration settings. | Chapter 8 Applications | ALL BBDS |
| The BBDS SHALL support a minimum defined set of local databases and applications in order to meet essential operational needs, including when the BBDS is operating in Stand-Alone Mode. | Chapter 8 Applications | CE BBDS |
| BBDSs SHALL support the provision of a “home status page” web application that provides location specific incident content. | Chapter 8 Applications | CE BBDS |
| BBDSs SHALL provide a method whereby the “home status page” application is available via an alternate access network, other than the NPSBN (e.g., Wi-Fi and other RF technologies used by the BBDS). | Chapter 8 Applications | ALL BBDS |
| The Deployable System SHALL automatically reconnect applications and services that were lost or transitioned when backhaul connectivity was disrupted (e.g., when the BBDS recovers from Limited Connectivity or Stand-Alone modes) | Chapter 8 Applications | CE BBDS |

| | | |
|---|---|---|
| The BBDS SHALL be capable of data synchronization during recovery of a lost connection to the NPSBN macro network, providing reconciliation of updates to applications and databases made by BBDS and macro network users. | Chapter 8 Applications | CE BBDS |
| A BBDS SHOULD be able to interface with internal and external device and environmental sensors in order to monitor the status of the BBDS, of first responders and their equipment, and the incident area. | Chapter 8 Applications | ALL BBDS |
| The BBDS SHALL support the same IP voice services (including push to talk voice) and IP telephony communications as the NPSBN macro network. | Chapter 9 Voice | CE BBDS |
| A BBDS operating in Stand-Alone mode SHALL support the same PTT/MC-PTT services and features that are present on the NPSBN macro network. | Chapter 9 Voice | CE BBDS |
| A BBDS operating in Stand Alone mode SHALL support registration of authorized MC-PTT users and affiliations to LTE talkgroups. | Chapter 9 Voice | CE BBDS |
| The BBDS SHALL support service continuity and session persistence for users transitioning between a BBDS and Pro Se Scheduled Direct Mode (Pro Se Mode 1) | Chapter 9 Voice | ALL BBDS |
| The BBDS SHOULD comply with macro network auditing based on limitation of the BBDS type. | Chapter 10 O&M | ALL BBDS |
| The BBDS SHOULD collect sufficient information to support the accounting and billing system. | Chapter 10 O&M | ALL BBDS |

| | | |
|---|---|---|
| BBDSs SHALL be maintained by the operating entity to the level of service required by the NPSBN operator including specific actions to sustain interoperability, manage revision levels, and required configuration settings. | Chapter 10 O&M | ALL BBDS |
| The BBDS SHALL support a local management interface for viewing and modifying configuration parameters of the unit. | Chapter 10 O&M | ALL BBDS |
| The BBDS SHALL allow an authorized user to restrict system access to only support a designated group of UEs. | Chapter 10 O&M | ALL BBDS |
| The BBDS SHALL support wired and/or wireless standards-based Ethernet connections (e.g.,connect a laptop to the BBDS) to provide access to local services, NPSBN services, and internet. | Chapter 10 O&M | ALL BBDS |
| The BBDS SHALL provide at least one Ethernet port on the LAN side to interface with IP-based services such as LMR gateways, remote terminal units, Wi-Fi access point routers, etc. | Chapter 10 O&M | ALL BBDS |
| The BBDS SHALL support local and remote monitoring and reporting of unit status to include the health of the BBDS system components (LTE routers, servers, RAN that impact capacity, connections, performance, etc.) and associated support components (e.g.,fuel status, temperature, security, etc.) | Chapter 10 O&M | ALL BBDS |
| The BBDS SHOULD report its configuration status through an "Operations Administration and Maintenance" application while off-line (i.e., not deployed) in order for an authorized entity to validate the compatibility of the configuration with the existing network. | Chapter 10 O&M | ALL BBDS |

| | | |
|---|---|---|
| BBDSs SHALL interface with network management systems using standardized interfaces and protocols. | Chapter 10 O&M | ALL BBDS |
| The BBDS SHALL enable authorized personnel to modify designated technical parameters at the scene of the incident. | Chapter 10 O&M | ALL BBDS |
| BBDS SHALL be capable of resetting to a default configuration at the completion of a mission (so each deployment starts from a known and standardized configuration state). | Chapter 10 O&M | ALL BBDS |
| A BBDS SHALL be capable of displaying a list of connected subscriber devices to authorized technical personnel for security, administrative, and configuration purposes. | Chapter 10 O&M | ALL BBDS |
| The BBDS SHALL allow an authorized user to disable the unit in a secure manner in accordance with NPSBN policy (e.g., during an emergency situation or compromise of the BBDS security). | Chapter 11 Security | ALL BBDS |
| The BBDS SHALL provide security mechanisms through encryption or other means to protect information passing through the network in accordance with NPSBN Security Policy. | Chapter 11 Security | ALL BBDS |
| A BBDS SHALL comply with the same NPSBN security requirements that are present on the macro network, including relevant components of physical, information, network, and communications security policies. This applies to all modes of operation, including when operating in, or transitioning to, Stand-Alone mode. | Chapter 11 Security | CE BBDS |

# Chapter 1: Introduction

While many law enforcement, fire, and EMS organizations use commercial broadband services today, those systems lack the mission critical reliability and priority access required for emergency response. There are many documented instances in which commercial networks have failed during largescale public gatherings and following major emergencies. Public safety agencies must have reliable access to high-speed voice, data, and video communications services at the scene of an emergency incident and while performing their day-to-day mission. The Nationwide Public Safety Broadband Network or NPSBN[14] is envisioned to address these deficiencies through the use of spectrum prioritized for public safety use and by leveraging priority and quality of service policies in the system architecture.

While the NPSBN is expected to provide nationwide coverage, there are a variety of instances in which access to the NPSBN broadband services may be compromised and would require supplemental network coverage. These include:

- The need to enhance the existing terrestrial footprint (e.g., to provide coverage in under-served areas, inside buildings and along geographical impediments such as urban canyons, mountainous terrain, large bodies of water, etc.).
- The need for added coverage and capacity at the scene of large-scale public gatherings, including parades, and sporting events.
- The need for added coverage and capacity at the scene of major public safety incidents, including operations at disaster scenes.
- The need for coverage in areas with no terrestrial footprint (e.g., wilderness areas) and into areas where it is not economically feasible to install infrastructure.
- The need for replacement coverage following damage to NPSBN infrastructure (e.g., after a tornado, hurricane, earthquake, or manmade catastrophic event).

Per FirstNet's RFP requirements, the NPSBN will be constructed in a phased deployment which will result in non-contiguous coverage areas. This may result in a situation in which a city is covered by FirstNet while the surrounding county is not. This would require network augmentation to provide sufficient service to public safety agencies throughout their entire jurisdictional area.

[14] The information and requirements in this report are applicable to both the U.S. and Canadian efforts to deploy a public safety broadband network. NPSBN (U.S.) and PSBN (Canada) references have been consolidated to NPSBN.

Broadband Deployable Systems (BBDS) are a logical solution to fill many of these gaps. BBDS technology has been maturing rapidly and now is available in several form factors, including:

- Backpack BBDS systems that are carried by a first responder.
- Portable BBDS systems that are delivered to the scene in self-contained units.
- Vehicle-based BBDS systems that are installed in first responder vehicles.
- Aerial BBDS systems carried by Manned and Unmanned Aerial Systems (UAS) or Vehicles (UAV) which may involve drones, balloons, and other types of aircraft.
- Towed/Trailer BBDS solutions which include larger capacity and higher levels of system capability.

There are a wide range of features and capabilities that may be provided by a BBDS. For example, a BBDS may include different components to support expanded operation:

- A simple BBDS may consist of an eNodeB connected to the NPSBN core which extends broadband service into areas not covered by the macro network.
- A BBDS may also include an Evolved Packet Core (EPC), gateways, and application servers to support interoperability and the provision of local mission critical services
- A BBDS may include a more complex set of network services and capabilities and could include all the components necessary for "turnkey" operations, including antenna arrays, portable power systems, and backhaul connectivity.

Chapter 3 of this report describes the various form factors and capabilities of the BBDS described above. This report will use the acronym "NPSBN" to refer to both the U.S. FirstNet initiative as well as the Canadian Public Safety Broadband Network. If necessary, a country-specific reference will be made to identify issues unique to either the U.S. or Canada. Throughout the document the term "macro network" refers to the fixed (terrestrial) NPSBN LTE infrastructure and "BBDS" (Broad Band Deployable System) to account for all types of deployable units and solutions.[15]

[15] Public safety agencies and industry use a variety of different terminologies when referring to a broadband deployable system. These include, among others, "Broadband Deployable System," "Broadband Deployable Solution," and "Broadband Deployable Platform."

## 1.1 CONTINUITY OF SERVICE EXPERIENCE

An important requirement for the successful use of BBDS is the concept of uninterrupted service. It is important that first responders maintain seamless voice and data communications as they transition between different components of the NPSBN. For example, police officers must remain in contact with other first responders as they enter a building to investigate an emergency. They should not experience a loss of communications while their device reconnects or re-affiliates to a network extension device or a BBDS. Thus, Service Continuity and Session Persistence are two key factors in the implementation of BBDS and other network components.

Some BBDS may function solely as a network extension while other BBDS must support a full range of broadband services when there is no connection to the NPSBN macro network. The latter is also referred to as operation in "Stand-Alone mode." Broadband services necessary for public safety operations include Mission Critical Push-to-Talk (MC-PTT) as well as access to a set of mission critical applications to support situational awareness and incident command. These services are necessary because a BBDS may be activated in an area where is not possible to establish a backhaul connection to the NPSBN macro network. In other circumstances, the loss of backhaul connectivity cannot result in the failure of mission critical services. The sudden loss of MC-PTT would compromise first responder safety, negatively impact incident operations, and make public safety agencies reluctant to use the service. Therefore, in order to provide the highest level of reliability, consideration should be given to using local components on the BBDS to provide these services. This would include the local provision of designated mission critical services even if backhaul connectivity to the NPSBN is available. If ten law enforcement officers are engaged in a tactical emergency that requires immediate voice communications, the routing of their PTT traffic through backhaul to NPSBN application servers injects unnecessary risk. The loss of backhaul connectivity, even momentarily, could have catastrophic results.

There is also a desire to ensure that public safety broadband services are coordinated effectively to support cross border operations. The U.S. and Canada are in different stages of development for their NPSBN systems. First responders from both countries frequently have an urgent operational need to share voice, data and video information with their public safety counterparts across the border. First responders also need the ability to transition seamlessly between their home NPSBN and the other country's NPSBN as they move about an incident scene. This is especially true in wild land firefighting operations where first responders need to communicate over a wide area and where personnel may relocate to a new position that is outside the area of their local NPSBN coverage.

## 1.2 PUBLIC SAFETY LMR DEPLOYABLE SYSTEMS

It is important to note that public safety agencies currently use Deployable LMR systems to supplement radio coverage and provide additional capacity. These units may include LMR vehicle repeaters which extend the range of a first responder's portable radio inside a building or a towed trailer solution which carries a turn-key portable trunked radio network. Some units are operated by first responders with basic training while other systems are deployed with trained technicians. In all cases, the speed of deployment and total time for system activation are critical considerations for incident commanders today. BBDS solutions will likely function in ways which are similar to these LMR deployable systems.

## 1.3 SCOPE OF REPORT

This report covers a wide range of topics and is based on a number of assumptions. These include:

- LMR systems continue to provide mission voice service to public safety agencies.
- In the longer term, the NPSBN will also provide mission critical Push-to-Talk services.[16]
- BBDS technology will continue to evolve with improved capabilities and features.
- 3GPP International standards work continues to evolve and address issues applicable to BBDS.
- FirstNet will permit local public safety agencies to acquire (or lease), operate, and maintain certain types of BBDS (subject to appropriate oversight). It is acknowledged that this approach may complicate network operations and require extensive coordination between the NPSBN and local agencies. However, the rapid and efficient deployment of BBDS by local public safety agencies is considered essential in order to provide necessary coverage and capacity that impacts first responder safety.
    - It is envisioned that first responder agencies may operate certain types of BBDS including backpacks, vehicle-based systems, and small lightweight airborne units.
    - It is envisioned that the NPSBN contractor will likely own and operate more complex types of BBDS including towed and trailer solutions.
- FirstNet's contractor will provide BBDS to support restoration of service following a network failure in addition to providing BBDS to enhance NPSBN capacity at large-scale events and incidents.

[16] It is recognized that standards and technology continue to evolve in the area of LTE Mission Critical Voice.

The scope of this report will focus on issues unique to BBDS and will exclude the following topics:

- BBDS issues which are the same as those to be addressed with the NPSBN macro network.
    - For example, public safety access to the Internet and PSTN dial tone would involve similar requirements whether the first responder was on the NPSBN macro network or accessing a BBDS.
- The issue involving access to public safety BBDS systems by non-public safety personnel. It is unknown to what extent the NPSBN operator will want citizen/commercial access the excess BBDS capacity at a large parade or sporting event.
- Off-network voice communications and their relationship to the BBDS. This work is complex and is being examined in a larger context with the NPSTC LMR to LTE Interoperability and Integration Working Group.

BBDS should not be envisioned as the only solution for coverage and capacity in areas lacking macro network service, including in-building coverage. While these systems are a logical solution for certain situations it is important to recognize the availability of other technology options, including indoor small cell technology and leveraging other RF networking systems. Those additional technologies are not a component of this report.

Finally, it should be noted that the content of this report may be superseded by the rapidly evolving nature of the technology. Some recommendations made in this report are subject to change as technology and implementation policy and strategy evolve with the NPSBN. FirstNet is working with a number of communities across the U.S. which are participating in Early Builder[17] demonstration projects to provide 700 MHz broadband service to local public safety agencies. Several of these initiatives involve the use of BBDS equipment in a variety of operational and implementation configurations. It is expected that FirstNet will receive important feedback on technical issues and deployment considerations from these projects. Standards and best practices will also play an important role in the evolution and integration of BBDS. The Third Generation Partnership Project (3GPP) is a global standards body that is actively engaged in the development of technical standards to support public safety mission critical services. The NPSBN's selected contractor will also determine to what extent various standards and capabilities are implemented on the network.

[17] See the FirstNet website for additional information on early builder projects: http://www.firstnet.gov/search/node/FirstNet%20Early%20Builder%20Projects

It is acknowledged that some of the recommendations made in this report may eventually be deemed inconsistent with NPSBN policy due to technical complexity, operational complexity, or cost.

# Chapter 2: Public Safety Operational Uses of Deployable Systems

This chapter will review operational uses of BBDS by public safety agencies. In order to identify as many scenarios as possible, the Working Group defined nine unique use cases which cover a broad range of public safety operations. Some of the use cases have variants to the baseline incident to acknowledge different operational and technical components. These variants identify additional challenges for public safety when using BBDS. These include operations involving lack of backhaul connectivity to the NPSBN macro network, utilization of BBDS from different vendors, and the use of multiple deployable systems at the scene of a single incident. The introduction of these variants resulted in a total of 14 separate use case scenarios.

## 2.1 SEAMLESS HANDOVER

One issue of particular importance to public safety is the need for continuous service as the first responder transitions between different networks. A police officer arriving at the scene of a domestic disturbance would be conducting voice and data communications through the NPSBN macro network. As the officer enters the apartment building their coverage may switch from the NPSBN macro network to BBDS network coverage provided by equipment in their patrol car.[18] The officer will need to have uninterrupted communication with the dispatcher and with other officers who are responding to the incident. Key issues relating to officer safety during network transition include:

- The officer should maintain connectivity with voice and data applications that are already in use.
- The officer should not have to log on to take any action in order to complete the transition onto or off of each network.
- In-progress voice and data transmissions should not be interrupted during the handover between these networks. An active MC-PTT voice exchange should not be interrupted or dropped. A data request for a license plate look up should not be aborted or delayed.

These public safety issues are grounded in technical work relating to Service Continuity and Session Persistence and are predicated on the availability of radio coverage from the NPSBN macro network, the BBDS, or other non 3-GPP access network that is integrated with the NPSBN.

[18] BBDS coverage provided by the officer's patrol car is designed for use when the vehicle is stationary. This statement is not intended to indicate that a BBDS solution would radiate coverage while the vehicle is in motion.

"***Service continuity***" refers to the handover of the public safety user device as it moves between different components and nodes of the same or different network(s). This can include the transfer of user device control from one NPSBN tower to another or from the NPSBN macro network to a BBDS. "***Session persistence***" means that a public safety user device will continue its active data sessions as it changes its active network attachment from the NPSBN core to the BBDS (and vice versa) with no impact from a user experience perspective. Session persistence and service continuity are commonly used interchangeably although the latter is typically an attribute that is perceived by the user.

3GPP has been identifying standards for service continuity as a component of their work on Specification 24.237 and continues to revise and enhance the material. Stage 3[19] work is currently ongoing.

## 2.2 PRIORITY, PRE-EMPTION, AND QUALITY OF SERVICE

Priority, pre-emption, and Quality of Service (QoS) [collectively referred to as "PQOS"] are also essential components of the NPSBN. They allow a first responder to gain immediate access to the network during periods of congestion and help organize public safety user and application traffic. First responders arriving at an incident scene may transition from the NPSBN macro network to coverage provided by a BBDS. It is important that these PQOS capabilities are supported by the BBDS and that they transition with the first responder as they move to and from BBDS coverage.

## 2.3 PUBLIC SAFETY USE CASES

The public safety incidents featured in the use cases are centered around a variety of diverse operational environments including wildland fires, visiting dignitaries, mass casualty incidents, search and rescue operations, and disaster responses. The information below provides a summary of each use case. A complete listing of the use cases documents is included in **Appendix C.**

**USE CASE 1 Wildfire in an Isolated Area.** This use case examined public safety operational needs during a wildland fire in an isolated area without NPSBN macro network coverage. The incident required more than one BBDS system to support the geography involved in the fire. The use case highlights issues involving the presence (or absence) of backhaul and the presence (or absence) of connectivity between various BBDS systems. The use case also examined the

[19] 3GPP performs standards work in stages. Stage 1 is an overall service description from the user's standpoint. Stage 2 is an overall organizational description of the network functions to map service requirements into network capabilities. Stage 3 is the definition of switching and signaling capabilities needed to support services defined in stage 1.

impact on interoperability that may occur when deployable systems are sourced from the same or different manufacturers.

**USE CASE 2: Large Sporting Event.** This use case examined public safety operational needs to manage personnel and respond to incidents occurring at a large sporting event inside a stadium. This incident posed a number of issues involving control of subscriber access to the BBDS and the need for applications and services.

**USE CASE 3: Dignitary Visit.** This use case involved coordination among multiple local, state/provincial, and federal authorities to manage a visit from a senior governmental official. This use case focused on the need for BBDS systems to support encryption and a variety of other security features. Additionally, this use case examined the requirement to monitor a moving convoy of vehicles and support transfer of video between sites.

**USE CASE 4: Mass Casualty Incident (MCI).** This use case focused on the need for EMS personnel to monitor a large number of patients at the scene of a mass casualty incident which has also disrupted macro NPSBN services. The use case examined the role of BBDS to support additional coverage and capacity at the incident scene while also managing sensor and video data.

**USE CASE 5: Search and Rescue**. This use case involved coordination of search and rescue activities to locate a lost child in a heavily forested area. An aerial BBDS was needed to provide broadband coverage including support for MC-PTT communications across the search area. Variants to this use case included the need for first responders to communicate through the macro NPSBN network as well as the aerial BBDS. The availability (and absence) of backhaul for the aerial BBDS was also reviewed.

**USE CASE 6: Disaster Incident.** This use case examines a large-scale public safety response following a major earthquake along the U.S. Canadian border near the Cascadia Fault. Widespread damage included loss of the NPSBN macro coverage, necessitating the use of multiple BBDS systems.

**USE CASE 7: Service Continuity**. This use case focused on the need for seamless handoff as first responders transitioned from an outdoor to an indoor environment with an associated transition from the NPSBN macro network to the BBDS network. Specifically, this involved public safety personnel who were exiting their vehicles and moving inside a large building to handle a call for service.

**USE-CASE 8 Bring Your Own Coverage (BYOC)**.This use case is a collection of six emergency events which involve law enforcement, fire, and EMS personnel. It was constructed to address

other operational components of BBDS use by first responders, including an examination of FirstNet's proposed Vehicular Network System [2] (VNS).
The use case envisions that first responders will access a variety of services and applications through the BBDS networks. These include:

- **Mission critical voice services**, including push to talk and full duplex voice communications. These solutions will need to interface with existing LMR networks to support interoperability between different agencies.

- **Mission critical data services**, including access to remote public safety databases (e.g., criminal history, driver's license, vehicle registration), agency computer-aided dispatch systems, agency records management systems, and agency intranet services.

- **Mission critical video**, including access to remote cameras and streaming video data from a first responder to a supervisor or PSAP.

- **Applications** that support incident command and situational awareness, including the ability to share tactical information about the incident, note the location of first responders, and distribute notes and updates.

- **Sensor data** from a variety of devices will be used to establish and maintain situational awareness at the incident scene.

- **GIS data** which is essential for first responders including rapid access to maps and building plans.

- **Location based services** which provide a greater level of accuracy in locating both first responders and citizens in distress.

The uses cases revealed 54 operational capabilities deemed necessary for public safety operations when connected to a BBDS. These capabilities became the basis for the public safety requirements statements included in this report. The capability statements and resulting requirements also revealed a number of technical challenges[20] that will impact full adoption of BBDS technology.

These use cases also illustrate that first responders will need to share broadband data with other public safety personnel who are on scene as well as with supervisors, managers, and telecommunicators who are off site. First responders, therefore, need to communicate with other public safety personnel who may be connected to the NPSBN macro network or the

[20] Technical challenges are discussed in greater detail in Chapter 12 and a complete list of technical challenges is contained in Appendix B.

BBDS. Public safety personnel may also be transitioning from BBDS network coverage to Pro Se Direct Mode operations.[21]

## 2.4 BBDS Organized Response Plan

A BBDS solution becomes viable when it is a part of an organized response plan[22] allowing it to reach the scene quickly and be activated within a specified period of time. Vehicular-based BBDS are likely the most practical because they would arrive simultaneously with first responders as an embedded asset. Airborne BBDS may be launched using a small drone that could be stored in a suitcase carried by a first responder or public safety field supervisor. The use of larger and more complex BBDS, including those on towed trailers, should be codified in a Service Level Agreement (SLA) between the operator and users of the equipment. The SLA should document expected response times, staffing plans, and capabilities for these systems. It is further recommended that the National Incident Management System (NIMS) sections on Resource Typing be updated to standardize the various form factors and capabilities of BBDS, providing uniformity during requests for service.

It should also be acknowledged that first responders will increasingly use sensors and analytics to support their mission. The Internet of Things is poised to bring a new set of capabilities to public safety agencies. These include sensors and devices that monitor the health of first responders, their environment, and their equipment. Public safety personnel may also connect to external devices and sensors to gain real time information. These issues are discussed in greater detail in **Chapter 8.**

| # | Requirements |
|---|---|
| 2.1 | Connected BBDS SHALL support service continuity and session persistence for users during transition to, and from, the NPSBN macro network. |
| 2.2 | Connected BBDS SHALL support service continuity and session persistence for users transitioning between different BBDS operating in Cluster Operations Mode. |
| 2.3 | BBDS SHALL support the same priority, pre-emption, and QoS features as the NPSBN macro network. |
| 2.4 | During handover, the BBDS SHALL maintain the PQOS settings of first responders as they transition to and from the NPSBN macro network**.** |

[21] ProSe Direct Mode is fully described in Chapter 9.

[22] The National Incident Management System (NIMS) provides a standardized approach for the management of emergency events.

# Chapter 3: BBDS Form Factor and Architecture

BBDS come in a wide range of form factors with a variety of configurations. They include many individual components designed to meet the unique needs of public safety. This diversity of BBDS design supports varying capability and complexity and allow agencies to select the "right system" at the "right time." For example, a small vehicle-based BBDS may be sufficient to support two officers investigating a burglary while a more sophisticated Core-Enabled BBDS may be needed to support a large building fire at a warehouse involving multiple public safety agencies.

## 3.1 Deployable System Components

Beyond basic network extension functions, a BBDS may also a number of complementary technologies:

- **Communication System** – An LTE communication system, which may include RAN components (eNodeB, EPC) and security gateway components.
- **Backhaul** – Used to connect the BBDS to the macro network. This may be accomplished in a variety of ways including LTE, satellite, and use of supplemental radio networks (microwave, 4.9 GHz, etc.). Chapter 7 provides an overview of backhaul technology and options.
- **Secondary backhaul** communications for both user plane data flow and control plane (such as communication with external EPC components).
- **Power Supply** providing external power connections/conversion or stand-alone power source (generator, battery, fuel cell, etc.).
- **Local Applications and Services** using servers and databases housed on the BBDS to support mission critical applications directly to first responder subscriber devices. These might include MC-PTT, video and incident command applications, as well as ProSe application servers.[23]
- **Secondary client communications** such as Wi-Fi, Bluetooth, ZigBee, or LMR integration, allowing different subscriber devices, sensors, and other equipment to interface with the BBDS.

Each of these components is discussed in greater detail throughout this chapter.

[23] Further detail regarding MC-PTT and Pro Se communications are included in Chapter 9.

## 3.2 CORE-ENABLED AND CORE-READY SYSTEMS

Regardless of their form factor or component capabilities all BBDS can be allocated into two basic categories:

**Core-Enabled BBDSs** include the LTE Radio Access Network (RAN) and the Evolved Packet Core (EPC) and may also include local application servers and databases. This allows for completely autonomous operation of the BBDS when not connected to the NPSBN macro network. It may also provide certain mission critical capabilities including MC-PTT, video sharing, and access to incident command applications. A Core-Enabled BBDS may also provide local application support to first responders even when connected to the NPSBN macro network. This is a more complex solution than the Core-Ready BBDS described below. However, these Core-Enabled BBDS are preferred in a variety of settings because they more fully support first responders at an incident scene. In essence, this type of BBDS has its own LTE Core that can provide a minimum level of functionality.

**Core-Ready BBDSs** only include basic RAN components and are designed to provide simple network extension functions. These solutions do not include an EPC and therefore require a connection to the NPSBN macro network to access services. They do not include onboard application servers. The phrase "Core Ready" indicates that these BBDS do not include a "core" but may be designed to support the later addition of core components (transforming them into a "Core Enabled" BBDS). However, Core-Ready BBDS are likely to be installed in first responder vehicles to extend NPSBN coverage to the immediate area around an incident or into a building. This basic network extension capability will play an important role in the overall deployment of the NPSBN.

The following diagrams illustrate various configurations of both the Core-Ready and Core-Enabled systems. These are only intended to serve as examples to support the recommendations made in this report. Other technologies, options, and configurations may also be used with these systems. Security considerations for various implementations are discussed in Chapter 11 and are not shown in these diagrams.

**Core-Ready BBDS.** Figure 3.1 shows a basic Core-Ready BBDS configuration. Core-Ready systems do not include any of the EPC components. These are the most basic form of BBDS and typically involve simple range extension of the NPSBN core network.

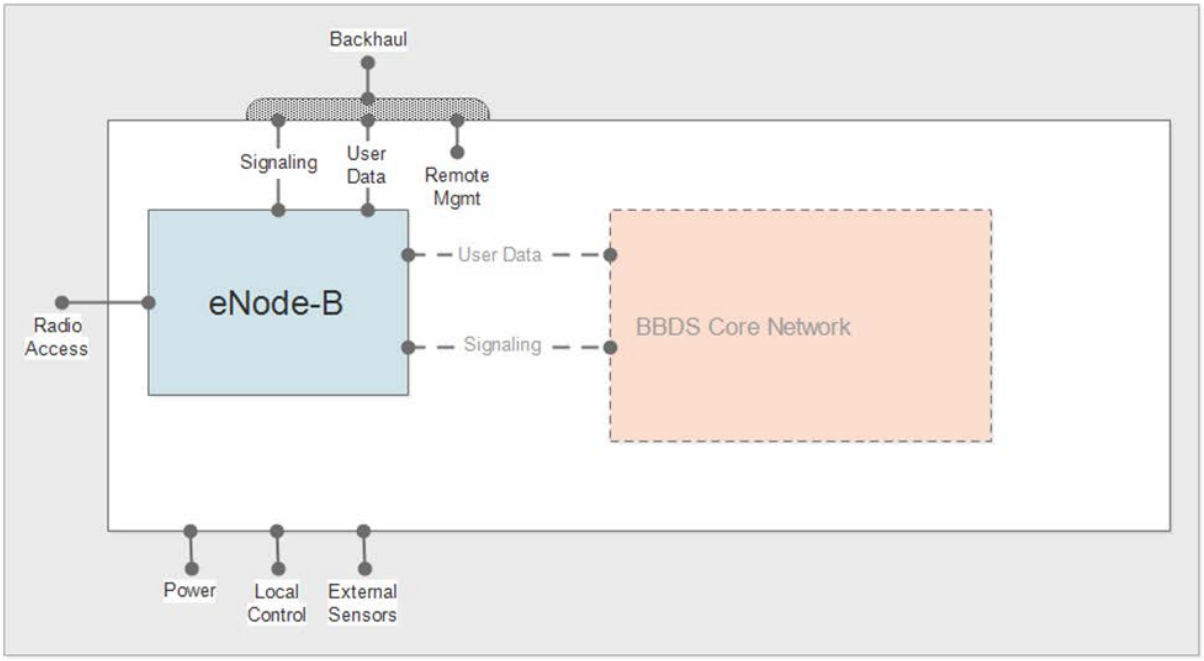



*Figure 3.1 Core-Ready BBDS*

If a backhaul connection is not available for the BBDS, the Core-Ready BBDS can operate as a Relay Node (RN). The RN requires an additional component known as a "UE Relay" which is shown in Figure 3.2. The backhaul connection for this configuration is between the RN and a Donor eNodeB (DeNB). The Relay Node is intended to be used to increase capacity or coverage of a macro eNodeB at its cell edge.

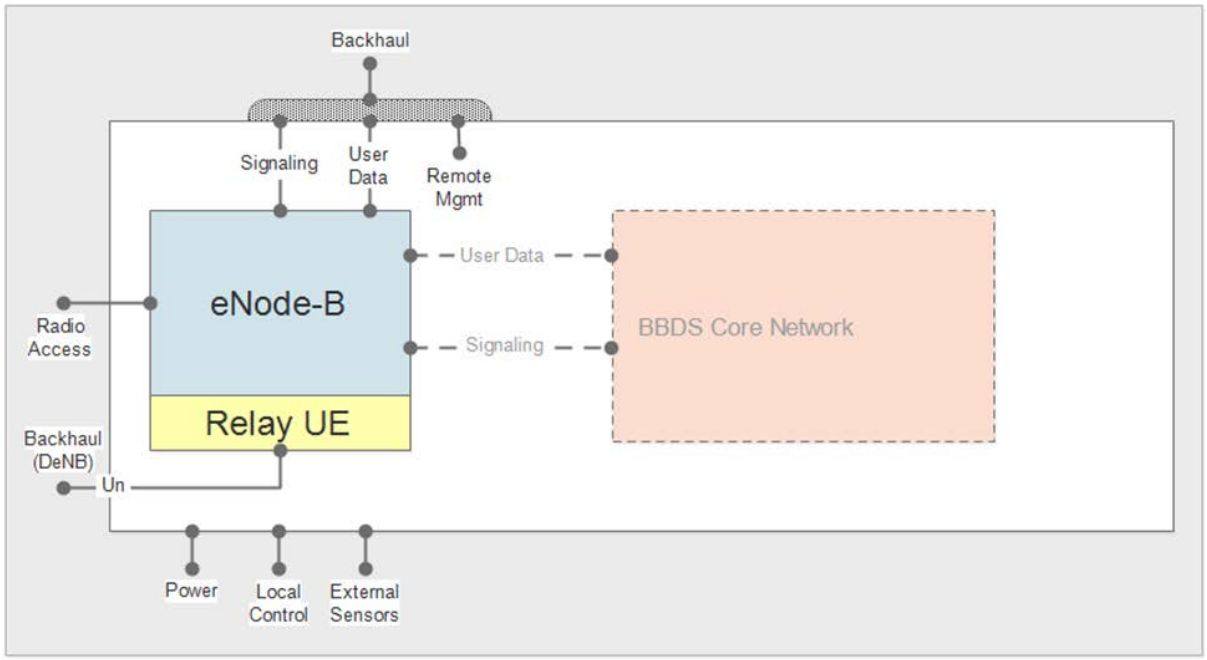



*Figure 3.2: Core-Ready BBDS as a Relay Node.*

A Core-Ready BBDS may also contain a non-LTE radio access network to provide an alternative access mechanism. The Wide Area Network (WAN) connections of the non-LTE radio access network may be pre-provisioned to interface with the BBDS' LTE core network. Non-LTE radio networks may include 4.9 GHz, WiFi, and other RF spectrum systems. A Core-Ready BBDS may also host an LMR radio base station or repeater as shown in Figure 3.4. The LMR network-to-network interface to the BBDS is an Ethernet connection.[24] These elements are displayed in Figure 3.3

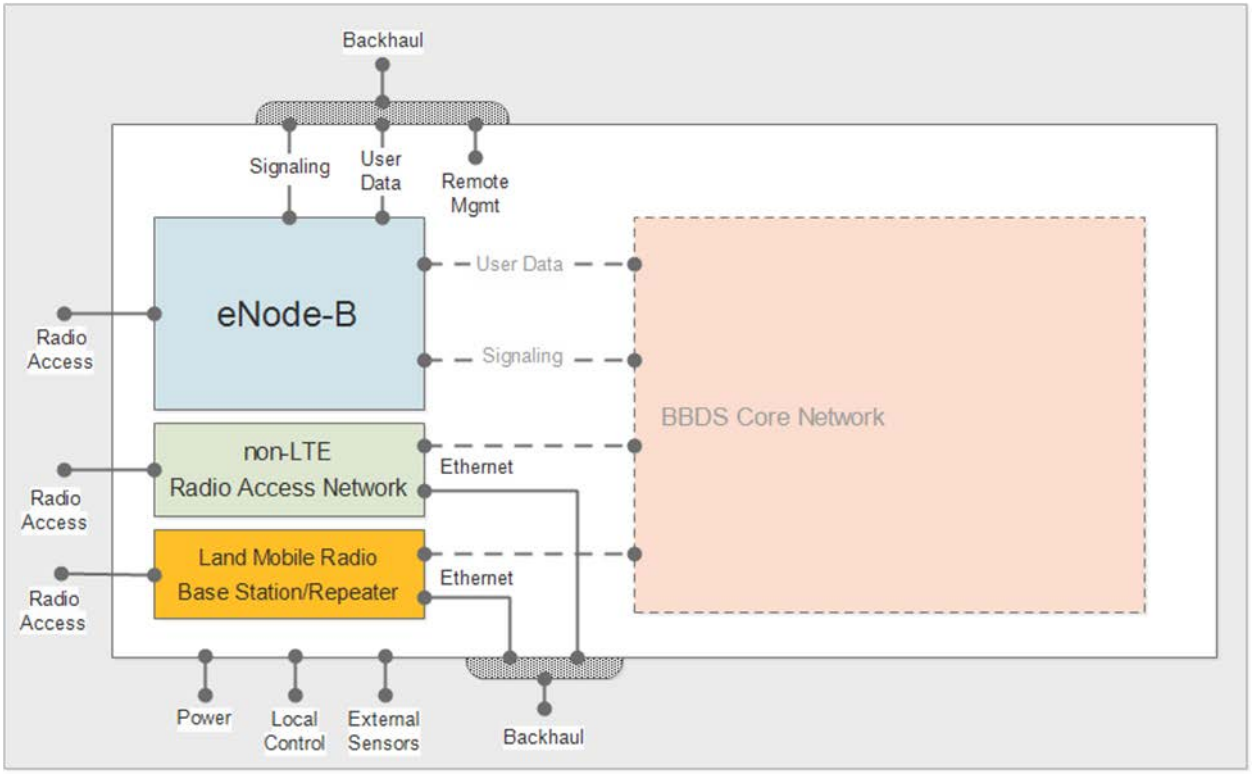



*Figure 3.3: Core-Ready BBDS equipped with non-LTE and LMR radio access networks.*

**Core-Enabled BBDS**

As stated previously, the Core-Enabled BBDS contains all network components of a Core-Ready BBDS with additional network elements and applications functions required to deliver services locally. This includes the ability for the Core-Enabled BBDS to authenticate first responder devices using an HSS database. Network-to-Network interfaces for the BBDS core are also provided [3].

[24] There is no requirement in this report pertaining to the protocols since it will depend on what LMR technology is used.

The roaming interfaces can be exposed to allow a Core-Enabled BBDS to be used in conjunction with a foreign network or with a co-located commercial network. The signals that comprise the set of roaming interfaces may be augmented in order to support service continuity during hand-over between networks.

MC-PTT and Group Communication synchronization interfaces are used to interconnect the local servers and the NPSBN macro servers for these applications. ProSe Sync refers to an interface to synchronize ProSe Applications Servers. No standard is specified.

Core-Enabled BBDS can also inter-work with an un-trusted non-LTE network. An example of an un-trusted non-LTE network could be an external Wi-Fi network that is present in a large venue such as a hotel or stadium. In this case, an additional set of interfaces are needed. A Core-Enabled BBDS could be equipped to interface with such an external network.

All of these elements described in this section are displayed in Figure 3.4.

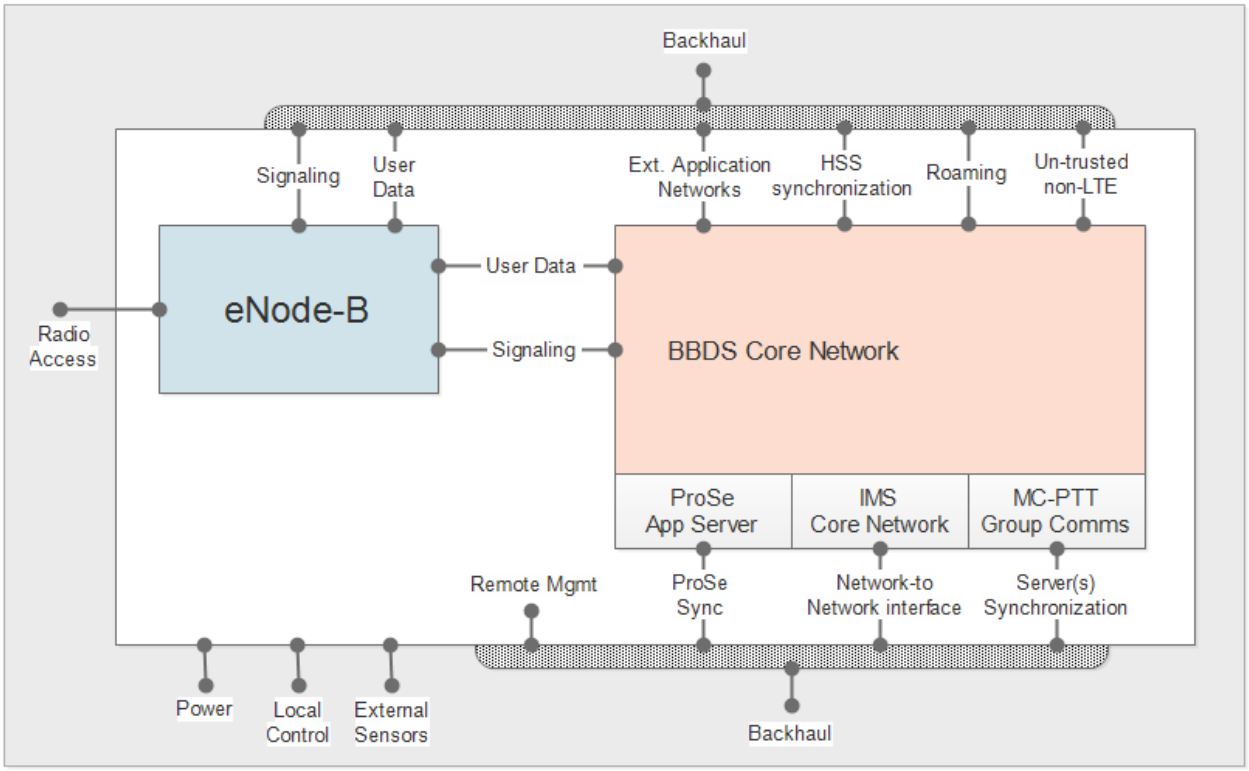



*Figure 3.4: Core-Enabled BBDS with additional interfaces including those for interworking with un-trusted non-LTE networks.*

A detailed review of network architecture concepts for a BBDS implementation is available in Appendix H and includes the corresponding Long Term Evolution (LTE) interfaces (protocols and methods) operating over each connection.

## 3.3 BBDS Form Factors

BBDS form factors are varied and range from small units that can be placed in a firefighter's backpack to large systems that are towed on special trailers. Typically, larger BBDS provide more coverage, capacity, and services while smaller BBDS units are less complex and are easier to operate. These systems are designed to be nomadic and provide temporary service during both planned events and unplanned incidents. They are not designed to be used while in motion. The exceptions are aerial BBDS which would be used under special circumstances and would have limitations on their altitude and location to avoid interference with the NPSBN macro network.

The following sections describe the range of BBDS form factors available and their associated technical components.

**Backpack BBDS.** This is a BBDS that may be carried by an individual first responder and which is typically used in geography not accessible by other BBDS form factors. These systems may have the following attributes:

- Sufficiently light weight to be carried by a single person.
- Should contain a portable power supply and can also accept various types of external power input.
- May or may not have backhaul connectivity.
- Must provide for external antenna systems via RF connections.
- May be Core-Ready or Core-Enabled.

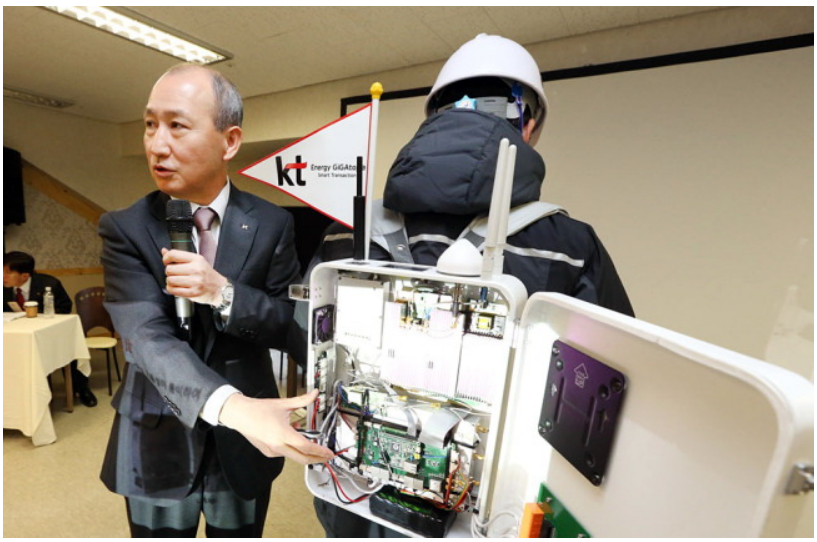


*Figure 3-8: LTE Backpack Solution [4]*

**Transportable BBDS.** This is a type of BBDS that is self-contained and can be relocated to an area via vehicle, helicopter, or watercraft. These systems are designed for delivery to the operational area and then activated as a self-contained unit. They typically have the following attributes:

- Each device container should be sufficiently light weight allowing it to be carried by two first responders.
- May contain a portable power supply and/or can accept various types of external power input.
- May or may not have backhaul connectivity.
- Must provide for external antenna systems via RF connections.
- May be Core-Ready or Core-Enabled.
- May or may not contain local application servers.
- Compatible with small aircraft and other small transport vehicles.
- May also be connected to a ground-based robot to manage placement of the BBDS.

*Figure 3-9: Transportable BBDS Solution [5]*

**Vehicular BBDS**. This is a type of BBDS that is mounted in a public safety or support vehicle. This may include a patrol car, fire truck, EMS unit, or field supervisor's SUV. These systems typically have the following attributes:

- Typically includes backhaul connectivity to the NPSBN macro network.
- May be Core-Ready or Core-Enabled.
- May contain local application servers.
- May contain vehicle-based user provisions such as workstations and internal services.
- May contain LMR interoperability systems.
- May support varying degrees of functionality based on the size of the vehicle in which it is installed.


*Figure 3-10: Fire truck equipped with in-vehicle BBDS solution to extend range into subbasement levels of large brick apartment complex [6].*

**Trailer/Towed BBDS.** A Trailer/Towed BBDS is typically a larger vehicle or is mounted on a trailer that requires a support vehicle. These systems typically have the following attributes:

- May be towed by a range of vehicles, from an SUV to a large truck, depending on capabilities and services.
- May contain a generator or other power supply system.
- May have an external power input capability for primary operations or shoreline input for maintaining readiness.
- May have a battery system for initial operations.
- Typically includes one or more backhaul connectivity options.
- May be Core-Ready or Core-Enabled.
- May contain application servers and databases.
- May contain a large antenna mast or provide for an externally connected mast-based antenna system via RF connectors.
- May contain LMR interoperability systems.

*Figure 3-11: Trailer/Towed BBDS Unit [7]*

**Aerial BBDS**. This type of BBDS solution is mounted as an aerial platform on a drone, aircraft, or balloon. These systems would typically operate from a fixed location[25] and would support the following attributes:

- May be heavier than air (aerodyne) or lighter than air (aerostat).

[25] Mobile operation of an aerial BBDS (vs. stationary placement) may create significant interference problems between the BBDS and the macro network. In some cases, including wildland fires in remote areas, a mobile aerial BBDS may be needed to provide coverage to firefighters as they move to new positions.

    - An aerodyne BBDS may be in the form of a helicopter or fixed-wing aircraft, or even a tethered helicopter (usually a drone).
    - An aerostat BBDS may be in the form of a tethered or untethered balloon, and may or may not be capable of full control of flight path.
- May be remotely controlled or onboard a staffed aircraft.
- May be delivered to site by a range of vehicles, from a small car (for a small drone-type BBDS) to an 18-wheeler type vehicles (for a large aerodyne or aerostat), depending on capabilities and services.
- May contain batteries and other options for power support including solar charging.
- For tethered aerostats or aerodynes, power may be delivered from ground.
- Typically requires backhaul connectivity for air-to-ground control signaling.
- May or may not include separate backhaul connectivity linking the unit to the NPSBN macro network.
- Backhaul may be ground-based, via tether or relay from ground-to-air, or on-board, for large aerodynes or aerostats.
- May be Core-Ready or Core-Enabled.
- May contain local application servers and databases.
- May contain LMR interoperability equipment and interfaces.

*Figure 3-12: Aerial BBDS [8]*

**Water-Based BBDS**. These BBDS are designed to operate in open waters at lakes, rivers, and ocean areas, providing local area communications with units operating in the water as well as linking first responders to the NPSBN macro network. They may support the following attributes:

- May be remotely controlled or used on a vessel that is staffed.
- May contain batteries or other power support systems including solar charging (for small buoy-type BBDS).
- May contain or interface with fuel-based generators.
- May or may not include backhaul connectivity.
- Will require an antenna mast (main ship mast for ships and boats for required clearance, especially in salt-water conditions).
- May be Core-Ready or Core-Enabled.
- May include local application servers and databases.
- May contain LMR interoperability equipment and interfaces.

*Figure 3-13: A Canadian Coast Guard mid-shore patrol vessel is an example of a marine vehicle which may use a BBDS [9]*

The following public safety requirements were identified for BBDS based on the information in this chapter of the report:

| # | Requirements |
|---|---|
| 3.1 | BBDS SHALL be fully-operable self-contained systems in accordance with the applicable category of the deployable equipment. |
| 3.2 | Certain BBDSs, such as backpacks and those installed in emergency vehicles, SHALL be designed for ease of use and activated with minimal human intervention by trained first responders. |
| 3.3 | The BBDS SHALL support continuous operations for the period of time specified by the owner/operator (based on form factor and other considerations). |
| 3.4 | To prevent interference, a BBDS SHALL disable the radio access network when the vehicle carrying the deployable system is in motion. |
| 3.5 | BBDS SHALL be available for use by first responders in both Core-Ready BBDS and Core-Enabled BBDS configurations. |
| 3.6 | BBDS SHALL be available in form factors that can be used on aerial platforms. |
| 3.7 | BBDS that are deployed in transportable cases SHALL support both AC and DC power sources. |

# Chapter 4: BBDS Network States

BBDS solutions support a variety of network configurations based on their design and the availability of backhaul connectivity to the NPSBN macro network. This chapter describes the four common networking states for BBDS:

**Connected Mode**. In many cases, BBDS will be operating in "**Connected Mode**" which uses a backhaul link to maintain connectivity with the NPSBN macro network.

**Limited Connectivity Mode**. Limited Connectivity Mode represents a situation in which the backhaul connection between the BBDS and the NPSBN macro network is insufficient to support all operations.

**Stand-Alone Mode.** Stand Alone Mode occurs when the BBDS solution is not connected to the NPSBN macro network and all services must be provided locally.

**Cluster Operations Mode**. Clustered Operations Mode occurs when more than one BBDS is used to provide service to an incident or geographic area.

Operational and technical considerations typically dictate how a BBDS network will be configured and whether the BBDS will be connected to the NPSBN macro network. Many BBDS are capable of operating in all four of these modes. The following sections describe each mode of operation.

## 4.1 CONNECTED MODE

BBDS that are operating in connected mode have a backhaul connection with the NPSBN macro network. The BBDS unit may also have local resources to support authentication and provision of services and applications that may supplement the NPSBN core network services. Therefore, connected mode operations allow a full extension of NPSBN services to first responders. This is an important concept, since many public safety applications require access to remote databases and services. A police officer needing to access a driver's license photograph could only do if the BBDS unit had backhaul connectivity. Some BBDS may support more than one type of backhaul connection in order to provide additional capacity and for redundancy

## 4.2 LIMITED CONNECTIVITY MODE

A BBDS may be connected to the NPSBN macro network with a backhaul link that is insufficient to provide full access to services and applications. In these cases, the limited data throughput may only support control and management plane data such as security and credentialing. Access to applications, databases and services would have to be provided using servers housed on the BBDS, which would function in a similar fashion to Stand-Alone Mode (see below).

## 4.3 STAND ALONE MODE

BBDS that are operating in Stand Alone mode do not have a backhaul connection to the NPSBN macro network or have experienced a failure of the backhaul link. BBDS may be activated in Stand Alone mode to support a localized public safety mission that does not require services from the NPSBN core. For example, a BBDS may be used to support a team of wildland firefighters who only need basic voice, data, and video group services within their own team. Those services would be provided by local application servers on the BBDS. In this example, the first responders do not need access to any remote services available from the NPSBN macro network. Other examples include large-scale public events occurring in national parks and remote areas without easy access to the NPSBN macro network.

The failure of the backhaul link between the BBDS and the NPSBN macro network may result in the complete loss voice, data, video, and applications (for Core-Ready BBDS) or may result in the automatic transition to Stand-Alone mode where only essential features and functionality are available (Core-Enabled BBDS). First responders need to be alerted when they have lost connectivity to the NPSBN macro network. This change in network state will have a significant impact on operations based on the loss of some functionality. There are tactical and operational decisions that are based on the level of communications capability. In LMR trunked systems, first responders receive an alert when the network changes and functionality is impacted. For example, a "site trunking" alert informs a first responder that certain features and capabilities are no longer available on their device.

The 3GPP International standards organization has developed requirements for Isolated E-UTRAN Operations for Public Safety or "IOPS." Those requirements seek to address how macro network base stations may continue to operate following loss of backhaul connectivity to the reset of the LTE network. This would allow an NPSBN tower site to continue providing some level of functionality to first responders following the accidental disruption of the fiber optic connection to the main NPSBN macro network. Some of these technical standards may support enhanced capabilities for BBDS.

First responders using a BBDS in Stand Alone mode will need access to a small number of essential public safety applications, databases and services. These will likely include MC-PTT and incident command applications to manage situational awareness including tracking and exchanging information on incidents and personnel; and video sharing. Availability of these local services is also essential if the backhaul link is disrupted causing a connected BBDS to transition to Stand Alone mode. In other cases, the mission environment prevents the creation of a backhaul connection and the BBDS is initially activated in Stand-Alone mode.

There are several technical considerations that impact stand-alone operations. First, the BBDS must be Core-Enabled to support local services and applications. If the BBDS has no connection

to the NPSBN macro network (either regular or limited) processes must be in place to manage device provisioning and user authentication. This requires that an HSS security database function be resident on the BBDS. Local application servers and some databases will be needed to provide basic services. These details are discussed in Chapter 8 (Applications) and Chapter 11 (Security).

## 4.4 CLUSTER MODE

Certain emergency incidents span large geographic areas in which a single BBDS may not provide sufficient coverage for the incident area. This may require the activation of two or more BBDS. In other situations, more than one BBDS equipped emergency vehicle may arrive at an incident and activate their service. This simultaneous use of more than one BBDS is called Cluster Operations. BBDS Clusters may operate with or without a backhaul connection to the NPSBN macro network.

The need for multiple BBDS may occur in the following situations:

- A wildland fire involving a wide geographic area. The National Interagency Fire Center (NIFC) tracks data on large U.S. wildland fires [10] including their size. The November 2016 update shows five active fires that are each larger than 10,000 acres in fire spread. For example, the Rock Mountain fire in the Chattahoochee Oconee National Forest covered 24,725 acres which is the equivalent of more than 38 square miles. This incident required more than 4,100 firefighters [11], logistical and support personnel. The provision of broadband data services to an incident of this size would likely require multiple BBDS systems.

- Emergency response following a tornado, hurricane, or earthquake would be hampered due to likely damage to the NPSBN infrastructure. Public safety broadband service would be needed in targeted geographic areas to support search and rescue operations. On May 25, 2016, a large EF4 tornado with 180 mph winds struck central Kansas causing widespread damage to the communities of Solomon and Abilene. The tornado was approximately a half-mile wide in some areas. Hundreds of law enforcement, fire/rescue, and EMS responders arrived to assess damage and treat the injured. This incident response area was approximately 20 square miles and was in a rural area that would likely have minimal NPSBN macro network coverage. Multiple BBDS systems would be needed to support this response.

- Supplemental broadband coverage may be needed to support public safety operations at a large stadium complex. Sporting events, including football, soccer and baseball, draw significant numbers of attendees and require a large public safety response to manage their health and safety [12].

NFL STADIUM COMPARISONS

| Name | Team(s) | Capacity |
|---|---|---|
| AT&T Stadium | Dallas Cowboys | 80,000 |
| Bank of America Stadium | Carolina Panthers | 73,778 |
| CenturyLink Field | Seattle Seahawks | 67,000 |
| Edward Jones Dome | St. Louis Rams | 66,000 |

These venues are typically large concrete structures that do not propagate LTE signals efficiently. Two or more BBDS systems may be required to provide sufficient coverage across the stadium footprint.

- NPSBN coverage for outdoor festivals and concerts. Many local communities support outdoor events which draw large crowds. Some of these events include concerts and festivals held in rural areas which will have less broadband capacity than urban areas. The Sasquatch Music Festival is held annually at the Gorge Amphitheater in a rural portion of the State of Washington. In 2015, more than 25,000 people attended this 3-day event [13]. The nearest hospital, The Quincy Valley Medical Center, is a small 25 bed facility and is located 17 miles from the concert venue. Their Emergency Department sees a large surge in patients during the weekend [14]. The Grant County Sheriff's Office and the local fire district must also assign large numbers of personnel to the festival. It is likely that more than one BBDS system would be needed to provide sufficient coverage across the entire concert footprint which includes the amphitheater, nearby camping areas, and remote parking facilities.

There are unique deployment considerations and technical challenges that must be addressed when activating multiple BBDS systems in a single geographic area:

- At least one of the BBDS must be Core-Enabled and contain EPC components.
- A system will be needed to manage radio interference from overlapping coverage between BBDS units or between BBDS units and the macro network.
- One of the BBDS will need to be designated as the "prime" to coordinate service delivery with the other BBDS. This will require backhaul connectivity between each BBDS and the Prime BBDS to manage necessary subscriber and device authorizations.
- Specialized configuration of each BBDS will be necessary to provide service continuity and session persistence within the cluster and also while transitioning to or from the NPSBN macro network.

- Interworking of BBDS may be complicated if BBDS equipment is sourced from different vendors.
- An additional complexity may involve interworking of BBDS arriving from an adjacent country (in the case of emergency incidents occurring near the international border).

The impact on these four modes of operation on voice, data and video services are discussed in the following chapters.

## 4.5 Device-to-Device Communications

In addition to providing local application servers and MC-PTT service, first responder devices will also communicate directly from device-to-device. A BBDS must be able to support this method of direct mode communications. First responder devices may automatically switch to Direct Mode communications when their device senses a loss of network connectivity. For example, this could occur when a Core-Ready BBDS loses its connection to the NPSBN macro network. Public safety personnel may also manually switch their devices to Direct Mode for different operational reasons. A BBDS[26] can facilitate and enhance Direct Mode communications through the use of ProSe application servers. Chapter 9 provides further insight into the role of voice services.

The following public safety requirements were identified based on the information in this chapter. It is important to note that the requirements also apply when a BBDS is in transition between the different network modes described in this section:

| # | Requirements |
|---|---|
| 4.1 | An aerial BBDS SHALL be capable of coordinating with the NPSBN macro network to minimize mutual interference. |
| 4.2 | A BBDS operating in Stand-Alone mode SHALL support registration of authorized subscriber devices. |
| 4.3 | The BBDS SHALL alert user devices when the deployable system is operating in, or has transitioned to, Stand-Alone mode. |
| 4.4 | BBDS SHALL be able to serve those users who are accessing a UE to Network Relay to reach the BBDS network. |

[26] This Direct Mode assistance also occurs when a first responder is within the coverage footprint of the NPSBN macro network.

| | |
|---|---|
| 4.5 | BBDSs SHALL be capable of interworking with other properly provisioned BBDSs. |
| 4.6 | BBDS sourced from approved but different vendors and maintained by different public safety entities SHALL inter-operate when they are used at a common incident. |

# Chapter 5: Deployment Considerations

As stated throughout this report, public safety agencies need rapid and reliable access to BBDS services to manage day-to-day operations and to respond to emergency events. While the specific details on BBDS operation have not been finalized by FirstNet, this report envisions that first responder agencies will operate some BBDS and that the NPSBN contractor will manage deployment and operation of larger and more complex BBDS. Regardless of the eventual design of the BBDS program, the overarching goal is to provide BBDS services quickly and with minimal effort by first responders.

Today, many public safety agencies own, operate, and maintain deployable LMR systems which are used to support first responders in the same way this report envisions the use of BBDS. Deployable LMR systems may be vehicle repeaters units which provide range extension or towed trailer solutions that provide conventional and trunked radio network access. Public safety agencies have come to rely on these units to support mission critical voice operations during large-scale public gatherings and following major emergencies.

It is expected that BBDS equipment may be procured by local public safety agencies from a FirstNet approved vendor list. BBDS would be provisioned and maintained per FirstNet approved configurations. This would include requirements for software revisions and updates, file and database updates, and other maintenance activities.

## 5.1 First Responder Training

Like LMR deployable systems, BBDS solutions will have different levels of complexity based on the form factor and type of BBDS device. A backpack or vehicular BBDS might be activated with a simple on/off switch while a towed BBDS solution may require significant technical skill (e.g., provisioning backhaul, interference mitigation, startup of local application servers, etc.). In some cases, a BBDS should not be activated until the NPSBN operator has been contacted to coordinate the operation.

While trained technicians will be needed to manage complex BBDS solutions, most BBDS equipment will likely be installed in public safety vehicles and must be activated by first responders with minimal effort. BBDS services may also be needed in forward operating areas which involve hazardous conditions that preclude technician assistance. Large-scale emergencies may require continuous operations over a multi-day period and will require 24 x 7 technician assistance. These issues are important when considering the extent of public safety agency and contractor maintained systems.

BBDS systems which are maintained and operated by public safety agencies will require those agencies to provide appropriate technical staffing. Personnel responsible for these systems must have initial and recurring training on the proper operation of the systems. There are maintenance considerations that must be addressed when the units are awaiting deployment as well as when they are mobilized for service. There are ongoing conversations regarding the role of the Communications Unit Leader (COML) to support this function. Today, COML personnel support the deployment of LMR-based deployable systems, but not every agency has access to these personnel and they are not typically able to reach the scene fast enough to impact the first few hours of an incident. However, utilization of these personnel represents a logical approach to bring trained and credentialed support staff to the scene.

As noted in the prior chapter, BBDS can be activated in a number of different network modes and with varying degrees of functionality and capability. There are also additional technical considerations for the use of BBDS services near the international border. These variations in deployment add to the complexity of the operation and highlight the need for adequate technician training.

One example of this technical complexity can be found in the need to configure the BBDS to support the targeted geographical area of the incident. The maximum distance from an eNodeB that UEs can be served is configurable within the BBDS to one of 16 values, ranging from approximately 0.7km to 118km (for low-speed UEs). Care should be taken to set the maximum range according to the needs of the incident to minimize the possibility of not being able to synchronize a UE to an eNodeB.

## 5.2 Spectrum and Regulatory Issues

There are also spectrum issues to be managed in order to reduce or mitigate potential interference between various BBDS units that are in simultaneous use at an incident scene or between the BBDS solution and the macro network.

Finally, there are a number of regulatory issues that impact BBDS. The use of RF equipment and the deployment of antenna masts are restricted near airports and other critical facilities. The use of radio frequencies near the international border is also restricted by the Federal Communications Commission based on agreements with Canada and Mexico.

## 5.3 BBDS Equipment Decision Matrix

To address the multitude of deployment factors the Working Group examined numerous scenarios and use cases. A draft decision matrix was created to provide guidance to an incident commander on the selection of the most appropriate BBDS to meet their operational needs. Public safety organizations operate in demanding environments and have unique voice and data requirements based on the incident they are managing. A decision matrix would typically

be used when requesting a BBDS to support a large-scale incident and would not be used for Vehicle Network Services (VNS) and other standardized BBDS units.

The matrix correlates the type of BBDS needed to specific information about the incident scene and needed BBDS capabilities. The following elements are addressed in the matrix:

- Site Access
- Site Location
- Power Availability
- Backhaul Connectivity
- BBDS Network Considerations
- Applications and Services
- Speed of Deployment
- Technical Assistance
- Site Terrain and Access

The checklist attempts to capture the information necessary to determine the most appropriate BBDS equipment while identifying supplemental equipment and personnel capabilities that may also be needed. The full matrix is available in **Appendix D.**

The deployment of a BBDS may be required at a moment's notice and with little time to address integration of the newly introduced system, especially by the users who must focus on the incident itself. How the system is deployed and integrated – that is, made available and useful to first responders – must be considered and planned well in advance of the incidents it would support. The speed of deployment and total time to system activation are important considerations for public safety agencies.

Introduction of the BBDS equipment should be as transparent as possible to the first responders. Technical issues must be kept to a minimum to ensure successful implementation of the system. It remains critical that deployment of a BBDS be planned in the most generic of fashions. While there will be various issues and requirements that are specific to a particular incident (or class of incidents), the more unique integration requirements there are for each incident type, the less likely deployment will be easy and with minimal interaction with the users.

It is important that first responders have sufficient training on the operational capabilities of BBDS equipment so they understand its features and limitations. This is especially critical when a BBDS may be operating without any backhaul to the macro network or when the BBDS loses its connection during an emergency incident. These systems should be used with sufficient

frequency to ensure that public safety agency technical teams are versed in its operation and first responders are familiar with the system. This usage may occur in actual day-to-day use of the systems at an incident or through simulated training sessions.

Mitigation of interference is also a critical consideration during the deployment of a BBDS. If BBDS equipment is going to be operated within the footprint of the existing macro network, steps must be taken to ensure that neither system comprises the operation of the other.

Environmental variables must be considered when purchasing equipment and planning the deployment of a BBDS solution. BBDS equipment should be able to operate in wide variety of weather conditions (temperature, precipitation, wind) as well as in the aftermath of various natural or man-made disaster scenarios. A BBDS should adapt to expected changing environmental conditions, whether due to physical relocation of the BBDS equipment or changes in weather conditions at a single location. With that said, it is not expected that every BBDS will have the same degree of environmental hardening.

Environmental variables will sometimes preclude the use of a particular type of BBDS and the possibility of such circumstances must be considered. For example, severe flooding or post-hurricane debris may prevent a towed/trailer BBDS from being introduced into the area requiring coverage. In general, any BBDS must be sufficiently protected from the elements and resilient to changing conditions.

The following public safety requirements were identified for BBDS based on the information in this chapter of the report:

| # | Requirements |
|---|---|
| 5.1 | The BBDS SHALL meet minimum environmental and hardening requirements applicable to the service area. |
| 5.2 | BBDSs SHALL integrate with existing BBDSs in proximity to each other without causing harmful degradation to other BBDS system performance and user experience. |
| 5.3 | BBDSs SHALL integrate into existing macro NPSBN infrastructure without causing harmful degradation to the NPSBN system performance and user experience. |

# Chapter 6: International/Cross Border Considerations

Public safety agencies at the local, state/provincial, and federal level have worked for many years to improve communications interoperability between first responders in the U.S., Mexico, and Canada. In 2015, NPSTC and CITIG published a comprehensive review of public safety interoperability issues at the U.S. Canadian border, "Cross Border Communications Report, Barrier, Opportunities and Solutions for Border Area Emergency Responders [15]." That report documents the daily response of fire and EMS units across international borders to provide emergency assistance to neighboring communities.

The report details a number of regulatory, governance and procedural challenges to public safety communications interoperability between Canadian and U.S. public safety agencies. These include mismatches in radio spectrum use and allocation and differing regulatory standards that prohibit first responders from using their radios as they travel into another country. The report also includes many success stories in which local public safety agencies and federal regulatory authorities have worked to overcome many of these obstacles to improve cross border communications capabilities.

The implementation of NPSBN networks in the U.S., Canada, and Mexico represents a unique opportunity to improve voice and data interoperability. Careful attention to network design and collaboration among all countries may allow for a comprehensive set of interoperability capabilities. BBDS technology is an important factor in this planning process. It is likely that BBDS will be used extensively along the international border based on the rural nature of much of the border geography.

## 6.1 Cross Border Operational Considerations: U.S. / Canada

U.S. and Canadian public safety agencies respond across the international border to assist each other on a daily basis. Large-scale incidents occurring near and across the international border require coordination and mission critical voice and data communications between all involved parties. For example, wildland fires involve large geographic areas impacting both nations. It is important that the technical design and policy components of the NPSBN systems anticipate the need for seamless communications between first responders. A Canadian firefighter may move to a new position on the side of a mountain and lose the connection to their "home" NPSBN network. That firefighter should be able to roam onto the U.S. NPSBN and continue accessing local applications and databases while communicating with first responders on both sides of the border.

**Cross Border Key Assumptions.** Seamless communications between U.S. and Canadian public safety entities is based on several key assumptions:

- The FirstNet NPSBN and the Canadian operator equivalent (C-PSBN) would both operate on Band-14 spectrum.
- The NPSBN and C-PSBN systems would have unique (different) PLMN ID numbers.
- The NPSBN and C-PSBN operators have entered into an agreement that allows for service continuity and handover between the two network's PLMN IDs.
- BBDS equipment could be dispatched and activated as needed at the discretion of local public safety agencies within the scope of agreements with the operators of the NPSBN and the C-PSBN.
- BBDS equipment may be procured (either purchased or leased) by local public safety agencies based on agreements with the operators of the NPSBN and C-PSBN.
- BBDS equipment could be sourced from multiple vendors to meet varying operational needs of public safety agencies and based on the use of an approved equipment list managed by the NPSBN and C-PSBN network operators.
- The authorized BBDS equipment and vendor lists issued by the NPSBN and C-PSBN operators may not be identical, resulting in the need for each operator to support additional BBDS equipment.

**Cross Border Infrastructure Scenarios.** The use cases developed for this report involve operation of NPSBN macro and deployable assets along the border, including operation of BBDS equipment within the home agency's country or across the border. First responders from one country may be operating in the other country using their handheld or vehicle mounted communications devices (UEs). It is assumed that fixed eNodeBs (e.g., NPSBN LTE tower sites) will be operating along the U.S-Canada border with overlapping coverage. The following infrastructure assumptions were used:

- U.S BBDS equipment will be operating within the macro coverage area of the C-PSBN and vice-versa.
- U.S and Canadian BBDS equipment may be operating in proximity to each other with overlapping coverage while also within the macro NPSBN or C-PSBN coverage footprint.

- U.S and Canadian BBDS equipment may be operating in proximity to each other with overlapping coverage, but not operating within the footprint of either country's macro network. (Each BBDS may have backhaul to the macro network of either the NPSBN or C-PSBN or may be operating in Stand-Alone mode with no backhaul connectivity).

- BBDS equipment using an aerial eNodeB platform may be radiating from one country into the other country.

**Cross Border Key Operational Capabilities**. Several key operational capabilities are needed to support emergency response along the international border, including issues unique to border area operations:

- First responders from either country can access their home jurisdiction's information networks, regardless of whether they are served by the NPSBN or the C-PSBN (subject to authorization by the home information networks' administrators).

- To provide data interoperability, first responders from either country can access the local information networks of the other country, regardless of whether they are served by the NPSBN or the C-PSBN (subject to authorization by the local information networks' administrators).

- First responders from either country are assigned priority, pre-emption, and QoS in accordance with applicable NPSBN or C-PSBN policies of the network they are connected to.

- Handover from the NPSBN to the C-PSBN, and vice-versa, is seamless (i.e., there is no perceptible interruption in service during the handover).

- BBDS solutions from one country may overlap with the BBDS coverage of another country or with the macro network of either country. The BBDS can be activated and made fully operational with minimal human intervention. In particular, there should be no specialized technical knowledge required to render certain classes27 of BBDS fully operational.

- First responders operating along or near the border can share the bandwidth of the eNodeBs that are located on either side of the border.

[27] This report envisions the use of a variety of BBDS form factors that support a range of features and capabilities which will impact the technical complexity of their operations. Certain basic level BBDS should only require minimal training of first responders, while larger and more sophisticated BBDS would require the presence of trained technicians.

- Canadian and U.S first responders can be authenticated on BBDS from either country when the BBDS solutions are isolated, (i.e., the BBDS is not connected to either the NPSBN or the C-PSBN macro networks).

**Cross Border Key Technical Challenges**. A number of challenges were identified which will impact the technical and policy based decision making for BBDS implementation:

- If multiple BBDSs are deployed from Canada and the U.S to the same incident there is an issue of getting the SON algorithms to interoperate.

- To enable inter-PLMN seamless handover, NPSBN and C-PSBN operators will need to share atypical roaming interfaces, (e.g., S10).

- The operators of the NPSBN and the C-PSBN may need to use the Local Breakout (LBO) roaming architecture to enable inter-PLMN service continuity and session persistence for VoLTE [16].

- First responders who are "visitors" on the NPSBN or C-PSBN and who are trying to access local information networks could be blocked if the servers require a VPN session between the client and the firewall protecting the information network.

- The NPSBN and C-PSBN eNodeBs have separate PLMNIDs but need to communicate to optimize the allocation of radio resources between them, (i.e., management of interference).

**Cross Border Key Operational Challenges.** A number of important operational challenges were identified which must also be addressed:

- If multiple Core-Enabled BBDSs from Canada and U.S are deployed to the same incident, it will be necessary to determine which one will function as the "anchor" or "prime" BBDS that will synchronize the other BBDS units. Presumably only one EPC/HSS will be used in the cluster of BBDS.

- In the case of a Stand-Alone BBDS (operating with no backhaul to the NPSBN or C-PSBN macro network) there is an issue regarding how first responder UEs will authenticate if they are not registered in the HSS security database internal to the BBDS. The challenge is how to ensure that authorized first responders who are "visiting" users from outside the local area become registered on the BBDS's HSS.

- There is a need to harmonize the priority, pre-emption, and QoS assignments between NPSBN and C-PSBN. This does not necessarily mean that the individual PQOS settings

are the same, but that the NPSBN and C-PSBN will support PQOS for first responders from the other country.

- Interoperability test plans should be coordinated between the NPSBN and C-PSBN operators to include BBDS-to-BBDS and BBDS-to-macro network functionality using all approved equipment configurations. This is a significant cost consideration and agreement will be needed regarding which party pays for the testing if one operator introduces new or upgraded equipment into its approved list. This should be addressed in a bi-lateral interoperability sustainment program that would also include configuration management. The sustainment plan would require some degree of flexibility to allow for unilateral changes by the NPSBN or C-PSBN operators without the necessity of having to submit a formal change request to a bi-lateral committee for approval.

- The NPSBN and C-PSBN operators will need to harmonize the default assignment of Physical Cell IDs (PCI) for the eNodeBs along the border. They would also need to agree on an assignment strategy for several technical issues:

    - PCIs for BBDS to prevent handover problems
    - Zadoff-Chu root sequences for Random Access Channel preambles
    - UpLink Reference Signals

- The NPSBN and C-PSBN operators will need to standardize on the ProSe Function and its associated Key Management Function in the core networks of their BBDS. This is necessary to allow direct mode communications between first responders from each country during a joint operation.

- The NPSBN and C-PSBN operators will need to coordinate the IP addressing schemes for all BBDSs to ensure that that IP address spaces do not overlap when the BBDSs are used in the same sub-net.

- The NPSBN and C-PSBN operators will need to standardize on an HSS architecture in order for Core-Enabled BBDS solutions (with local HSS) to interoperate with both core networks. For example, if a network uses Unified Data Convergence then the BBDS HSS would need a Front-End function and implement the Ud interface. Although 3PP defines the Ud interface, it does not specify the data model of this interface. The NPSBN and C-PSBN operators will need to standardize on a common data model for the Ud interface.

- The NPSBN and C-PSBN operators will need to standardize the network management APIs of the BBDS so they can be monitored and controlled by authorized representatives of the NPSBN and the C-PSBN.
- In case RAN sharing in a Multi-Operator Core Network (MOCN [17]), the NPSBN and C-PSBN operators will need to (at a minimum) standardize on the Security Gateway configuration parameters (IPsec) and key management scheme of the BBDS for the S1 interface.
- The NPSBN and C-PSBN operators will need to standardize on the X2 interface connection between BBDSs from both countries.

**Cross Border Handover Scenarios.** The Working Group identified a number of different handover scenarios that may occur during an emergency incident. There are a number of technical complexities based on how the BBDS network connections are implemented. This implementation will impact the capabilities to support first responder transition between networks.

***Roaming with no Coverage Overlap***: In this scenario, first responder user equipment must re-attach when crossing the border and leaving one network before connecting to the other network. This is illustrated in Figure 6-1 below and shows the macro networks of both countries.

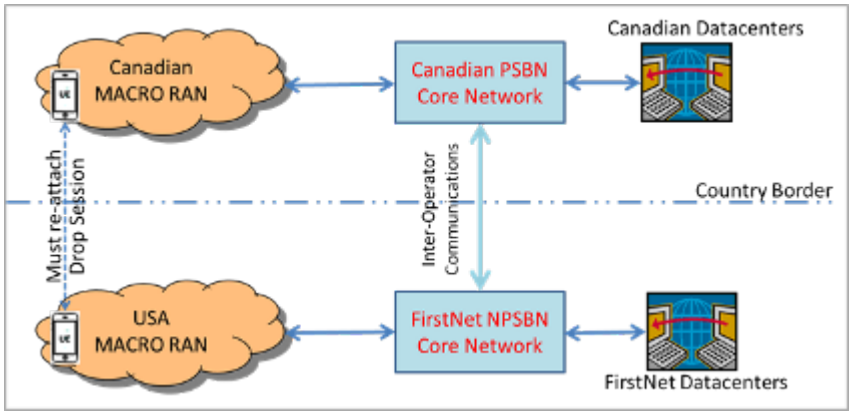



*Figure 6-1: Roaming with no coverage overlap of the U.S. and Canadian macro networks*

A similar situation occurs when either country deploys BBDS near the border. First responder devices must disconnect from the macro network (or the BBDS network) of their home country and reconnect to the macro network (or BBDS network) of the other country. This is illustrated in Figure 6-2 below.

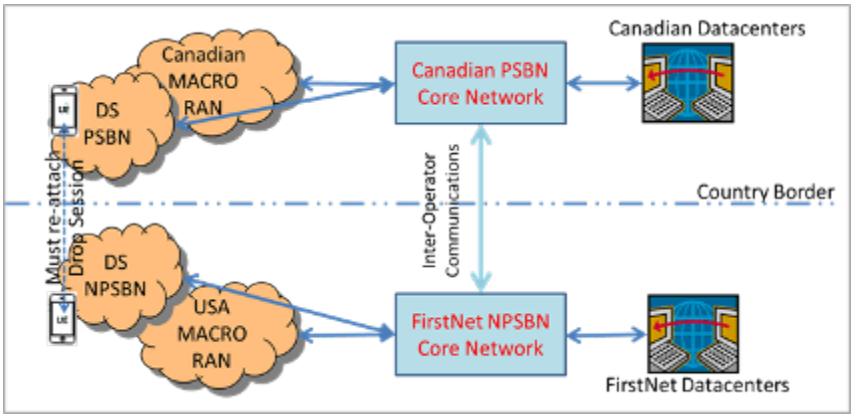



*Figure 6-2: Roaming with no coverage overlap of the U.S. and Canadian macro-connected BBDS systems.*

A third scenario involves the use of BBDS by both countries operating in Stand-Alone mode. First responder devices must still disconnect from their home BBDS network in order to reconnect to the Stand-Alone BBDS network of the other country. This is illustrated in Figure 6.3 below. It should be noted that this same scenario may involve "mixed modes" of operation, where one country is operating a BBDS in Stand-Alone mode while the other country has their BBDS connected to their macro infrastructure. In all cases, the first responder will lose connectivity supporting voice services, mission critical applications, and remote database access as they transition off of one countries network and onto the network of the other country.

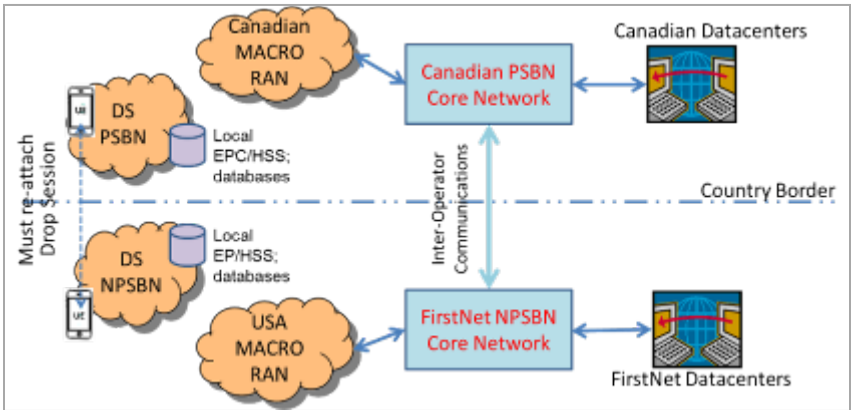



*Figure 6-3: Roaming with no coverage overlap of the U.S. and Canadian stand-alone BBDS systems.*

***Roaming with Coverage Overlap***. In this second scenario, first responder user equipment can maintain connectivity during the transition from the network of one country to the network of the other country, through implementation of a network design that keeps bearer sessions

alive as users cross the border and enter the coverage area of the other country. This involves an Inter-PLMN handover at the Canada-U.S. border and is illustrated in Figure 6-4 below.

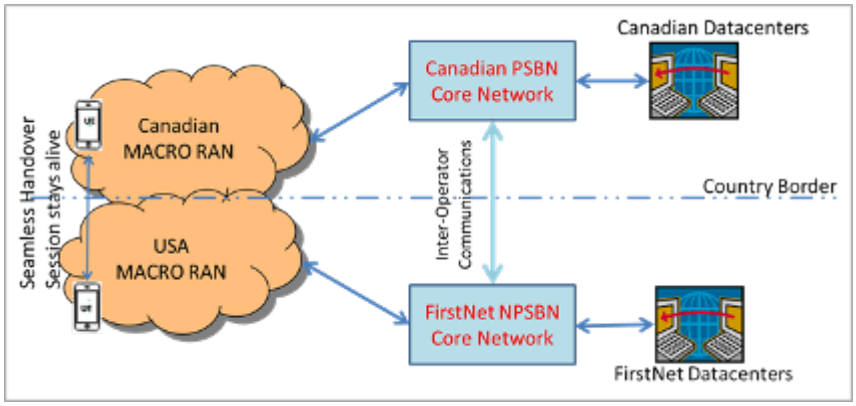



*Figure 6-4: Inter-PLMN handover at the Canada-U.S border with coverage overlap of the U.S. and Canadian macro networks.*

A similar situation occurs when either country deploys BBDS near the border. The use of an Inter-PLMN handover would allow first responders to maintain communications during transition between the macro and BBDS networks of either country. This is illustrated in Figure 6-5 below and involves macro-connected BBDS.

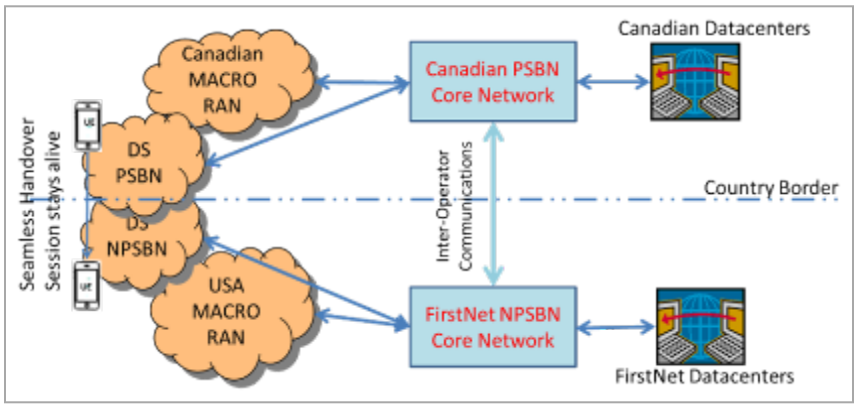



*Figure 6-5: Inter-PLMN handover at the Canada-U.S border with coverage overlap of the U.S. and Canadian macro-connected BBDS systems.*

The same network design strategy can be implemented to address situations involving deployment of BBDS in Stand-Alone mode. An Inter-PLMN handover can occur between the BBDS of one country and the BBDS of the other country if the two BBDS share a common network connection and other services have been coordinated, (e.g., HSS database). This is illustrated in Figure 6-6 below.

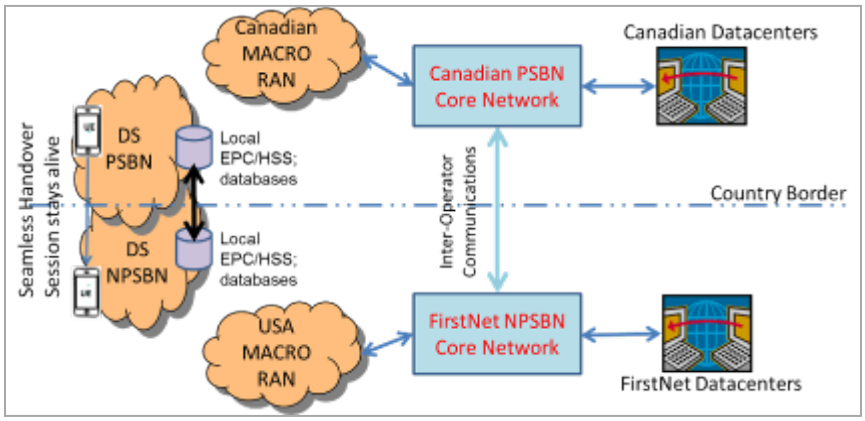



*Figure 6-6: Inter-PLMN handover at the Canada-U.S border with coverage overlap of the U.S. and Canadian stand-alone BBDS systems.*

The final scenario involves a different implementation strategy in which the BBDS of one country is provisioned to connect to the macro network of the other country. This is illustrated in Figure 6-7 below and shows a Canadian BBDS with a connection to the FirstNet NPSBN.

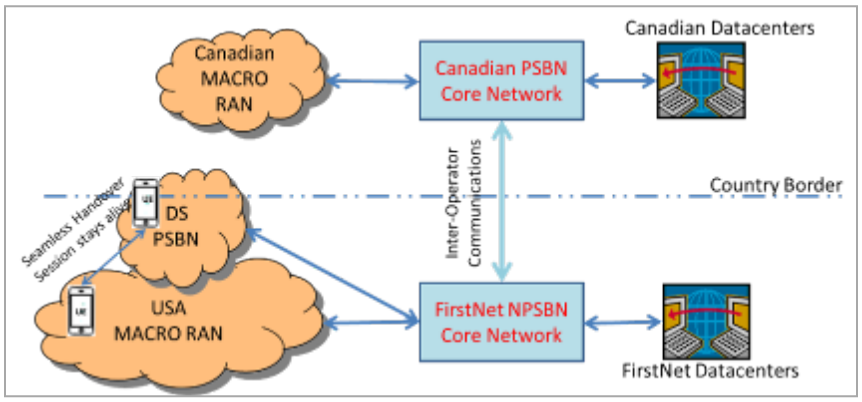



*Figure 6-7: Handover using a Canadian BBDS connected to the U.S core network and a U.S. macro eNB.*

## 6.2 Cross Border Operational Considerations: U.S. / Mexico

The U.S. Department of Homeland Security has sponsored a number of LMR interoperability solutions along the U.S. / Mexico border to enhance communications at the local, state, and federal level. Mexico is also currently selecting a nationwide provider of commercial broadband services which will also include a public safety component [18]. The Mexico network will use Band 14 spectrum which is reserved for public safety use in the U.S. and Canada. In November of 2016, a large provider [19] of public safety communications equipment provided a demonstration to Mexico officials on how a public safety broadband network could support mission critical services.

The U.S. and Canada have already harmonized their 700 MHz narrowband voice spectrum and are actively working to harmonize their 700 MHz broadband spectrum. Unfortunately, there is a lack of alignment in the band plan assignments between the U.S. and Mexico. Mexico recently adopted the Asia Pacific Telecommunity (APT) band plan, using Frequency-Division duplexing (FDD). Figure 6.8 shows the 700 MHz channel assignments for uplink and downlink traffic in the U.S. which has been assigned to exclusively manage downlink traffic in Mexico.[28]

The lack of spectrum alignment will create barriers to interoperability between U.S. and Mexico public safety operations affecting both LMR narrowband operations in 700 MHz and NPSBN broadband operations in 700 MHz. The APT band plan will also impact 700 MHz commercial cellular operations. Site-to-site interference can occur due a rise in the noise floor from adjacent Mexico base stations. This can prevent a first responder's LMR or LTE device from communicating to the network and can also interfere with the first responder receiving voice and data traffic from the network. It is likely that a protection zone will be established which will require that certain frequencies be restricted near the international border, thus reducing the overall capacity of the network.

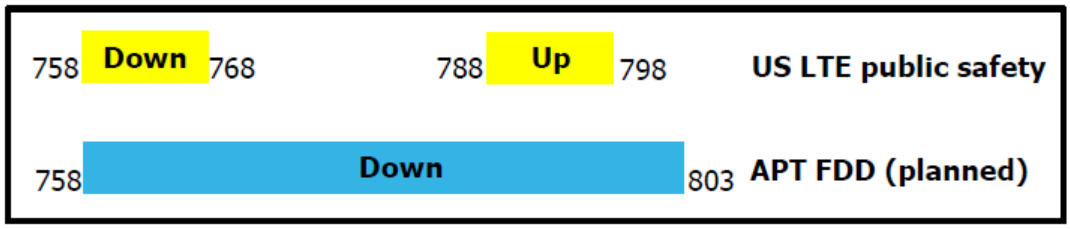



*Figure 6.8: The 700 MHz channel assignments for uplink and downlink traffic in the U.S. which has been assigned to exclusively manage downlink traffic in Mexico.*[29]

Officials at the Federal Communications Commission are in active discussions with Mexico authorities to address a wide range of radio spectrum issues, including 700 MHz band coexistence strategies along the international border.

The following public safety requirements were identified for BBDS based on the information in this chapter of the report:

[28] The Mexico APT uplink spectrum is not illustrated in this diagram because, while it overlaps with U.S. commercial carriers, it does not overlap the U.S. LTE Band 14 used by FirstNet.

[29] Graphic courtesy of Alcatel-Lucent, 2013 Presentation on Cross Border Operations

| # | Requirements |
|---|---|
| 6.1 | BBDSs SHALL support session persistence and service continuity for first responders that belong to other partner Mobile Network Operators (MNOs), (e.g., other public safety broadband mobile network operators, international, and domestic commercial carriers). |
| 6.2 | To provide first responders with access their local agency data, BBDS SHALL allow first responders from either country access to their home jurisdiction's information networks, regardless of whether they are served by the NPSBN or the C-PSBN, (subject to authorization by the home information networks' administrators). |
| 6.3 | To provide first responders with data interoperability, BBDS SHOULD allow first responders from either country access to the local information networks of the other country, regardless of whether they are served by the NPSBN or the C-PSBN, (subject to authorization by the local information networks' administrators). |
| 6.4 | BBDS SHALL support priority, pre-emption, and QoS in accordance with the local NPSBN and C-PSBN policies. |
| 6.5 | When A Core-Enabled BBDS from one country connects to the macro network of the other country, that BBDS SHALL apply the PQOS settings of the host (macro network). [e.g., If a U.S. based BBDS connects to the macro network of the Canadian PSBN, the BBDS would adopt the PQOS settings of the Canadian macro network]. |
| 6.6 | BBDS SHALL support service continuity and session persistence as first responders transition between the NPSBN and the C-PSBN, and vice-versa, (i.e., there is no perceptible interruption in service during the handover). |
| 6.7 | BBDS from one country that overlaps in coverage with the macro network or BBDS from the other country SHALL be activated and made fully operational with minimal human intervention. |
| 6.8 | BBDS operated by Canadian or U.S agencies SHALL support authentication of first responders from either country when the BBDS is isolated, (i.e., the BBDS is not connected to either the NPSBN or the PSBN macro networks). |

# Chapter 7: Role of Backhaul Communications

This chapter focuses on key considerations for transport links as an integrated component supporting BBDS. In a typical Wireless Wide-Area Network (WWAN) communication between an ensemble of distributed local radio access nodes and one or more remote or centralized core networks is facilitated through a network of wireline and wireless transport links between the two domains. User devices and content become the end points of such a network.

Transport links, including backhaul and other RF links, are necessary for many types of BBDS (e.g., Core-Ready BBDS) in order for first responders to access applications, services, and databases that reside elsewhere on the network.

For this report, the term "***backhaul***" refers to those RF or wired connections which attach the BBDS to the macro network as illustrated in Figure 7-1. This is similar LMR tower sites which are connected to the main components of a trunked radio system, typically using microwave (wireless) or fiber-optic (wired) connections.

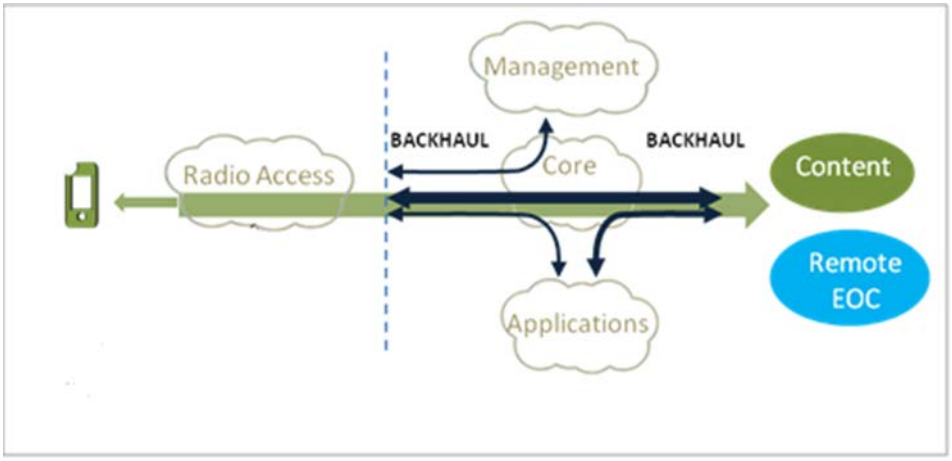



*Figure 7-1 Backhaul links*

The black lines represent communications links provisioned to carry management, signaling, and user traffic data while the green line is indicative of the communications service flows between endpoints--the thicker the line the larger the required pipe. Application and user data is more bandwidth intensive than the data traffic flow for signaling and management. Figure 7.1 depicts various domains whose functions can be centralized or distributed across multiple locations but, ultimately, the need for backhaul is determined by where content resides and whether remote access or operation is required.

For example, if a New York City police officer needs to check for warrants on a visitor from Montana, they would have to access the National Information Crime Information Center (NCIC)

database. This would require a backhaul link to provide connectivity from the BBDS to the NPSBN macro network infrastructure which will access the remote database. On the other hand, access to a database that is embedded in the BBDS (e.g., building fire plans) does not require a backhaul link. Backhaul may be needed to access a variety of public safety databases and applications involving wide variation in network design. Databases and application servers may reside on the BBDS solution, or they may reside on an adjacent BBDS device, or in other network locations remote from the incident scene.

In traditional wireless IP networks architectures, a variety of secure transport networks are implemented along with varying degree of redundancy, throughput, and latency targets. Further, in LTE the flat IP architecture helps to distinguish between control (signaling) type of packets and the more bandwidth-intensive content (user) data leading to more flexibility in selecting transport options. For example, a low-bandwidth satellite link may be used to connect the BBDS with a remote *national* subscriber database for user registration/authentication while leveraging application servers and databases installed in the BBDS to provide tactical information for the first responders (e.g., MC-PTT application, access to building blue prints, etc.). This approach keeps all bandwidth intensive traffic localized to the BBDS.

## 7.1 BACKHAUL CONNECTIVITY

Certain types of BBDS are designed to be lightweight and easily carried by a first responder (e.g., a BBDS backpack solution). These BBDS may not contain a backhaul solution. However, most BBDS should either have an installed backhaul capability or should be "backhaul ready" meaning they have the necessary connections to interface with other equipment that can provide the service. There are a wide variety of backhaul options including in-band Relay Node backhaul, microwave (and other RF links), fiber and satellite. Each backhaul option has pros and cons in terms of performance and provisioning and there are a host of technology issues that need to be addressed (see Chapter 12). Various types of backhaul technologies are described in the following paragraphs. Note that certain large-scale and/or complex operating environments may require the use of multiple backhaul solutions. For example, a wildland fire may require the activation of three BBDSs because of the size of the incident area. One of the BBDS must be Core-Enabled to serve as a "master" site to coordinate resources with the other BBDS supporting the incident. The "master" BBDS may connect to the NPSBN macro network using a fiber connection available at a government building while using microwave hops to connect with other BBDS.[30]

**Relay Node:** While not considered optimal, it is possible to leverage LTE spectrum to provide a backhaul solution from the BBDS to the macro network. This type of solution requires that a

[30] There are a variety of configuration options available and a number of factors influence the selection of the most appropriate solution.

portion of available LTE spectrum be diverted from supporting on-scene users in order to provide an RF backhaul link. This kind of backhaul is best used when other types of backhaul are not possible and when the donor eNodeB's radio resources are not highly allocated. Because the Relay Node will share the donor eNodeB's radio resources with first responders who are accessing data, congestion may occur resulting in poor service quality. In addition, Relay Node backhaul can be established using out-of-band spectrum.

Diagram 7.2 [20] illustrates this concept and displays how a Donor eNodeB and a Relay Node could support the usage of in-band spectrum or out-of-band spectrum [31] for the purposes of backhauling S1 (S1-MME and S1-u) traffic between a Core-Ready BBDS and a Core-Enabled BBDS.

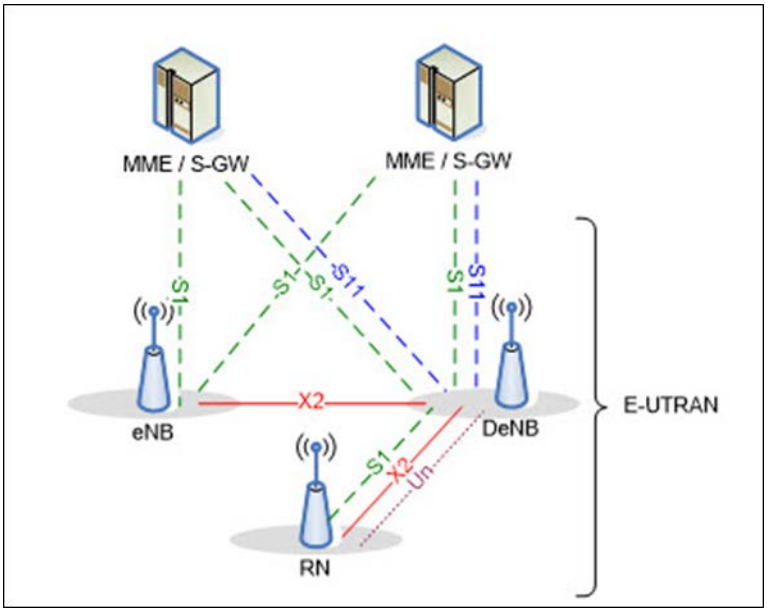



*Figure 7-2 showing an example of a donor and relay node.*

**Fiber Optics:** When available, fiber represents the best type of backhaul transport when considering bandwidth and latency. Use of fiber can be maximized when public safety and government agencies collaborate on emergency response scenarios and establish predetermined fiber points of presence. Because of its high bandwidth, low latency, and high reliability, fiber is one of the preferred means for both fronthaul and backhaul links.

**Microwave:** When line-of-sight communications are possible between two endpoints (e.g., between a Core-Ready BBDS and a mobile command center) a microwave link may be the preferred option for backhaul. Automated dish positioning technology is available and would

[31] Out of Band spectrum refers to a segment of Band 14 reserved for connection between the donor and the relay nodes.

minimize the complexity of activating the backhaul by first responders. This technology can assist both Line-Of-Sight (LOS) and Non-Line-Of-Sight (NLOS) systems (e.g., those involving satellite connectivity). Each type of backhaul technology requires appropriate equipment on both ends of the backhaul connection. A microwave radio on a BBDS is only useful if there is another radio site to communicate with. Further, microwave systems can be characterized as line-of-sight, non-line-of-sight, point-to-point, and point-to-multipoint. Some of their capabilities are based on the licensing regime and regulatory framework of the frequency bands utilized. Unlicensed operation is often the choice for quick deployments but can be subject to harmful RF interference.

**Satellite**: When microwave and fiber are not feasible options, (e.g., in the case of a BBDS deployment in a forested area), satellite becomes an alternative as long as a view of the sky is unobstructed. There are a number of satellite services and each has different technical capabilities and cost points. Geostationary (GEO) satellites have the highest latency, Medium Earth Orbit (MEO) satellites have lower latency, and Low Earth Orbit (LEO) satellites have the lowest latency. Commercial satellite service operators have different tiers of service and there are new service providers entering this field. Consideration shall be given to the achievable throughput capacity, hop/multi-hop latency, and quality of service. Because of the potential service expense, the spectrum band, bandwidth, access method (e.g., DAMA), terminal type, and satellite provider must be decided well in advance of any deployment and typically involves a contract for service. Bulk purchase of bandwidth may be appropriate in some cases, especially when a state is managing a satellite contract on behalf of multiple local entities. A satellite connection must generally have an extra security encryption and access control layer due to the open nature of satellite downlink transmissions. Additionally, the effect of latency on interfaces and protocols must be examined. In particular, while link layer accelerators are typically used to mitigate bandwidth delay involving protocol performance problems, they may not be fully functional over a satellite unless *outer link acceleration* architecture is used.

**WiFi:** WiFi access points (located in the vicinity of a BBDS lacking proper backhaul connectivity) may be routed back through the open Internet to provide backhaul connectivity. WiFi is more typically used in the access segment with wireless cellular as backhaul (e.g., hotspots). Backhaul over WiFi will involve an examination of security protocols, achievable quality of service, end-to-end performance (because of potential over-the-air contention), the mitigation of potential RF interference, and the multiple management/ownership layers. Use of WiFi should be preplanned to ensure that appropriate technical and security issues are resolved.

**Emerging Technologies:** There are a variety of new backhaul solutions in the research and development phase. One such experiment involves the use of modified UEs to create a packet relay channel between two eNodeBs [21]. This work and other projects like it are seeking to

address the challenges that are present with standard backhaul solutions. For example, the use of microwave backhaul can be hampered in that the siting of the BBDS equipment is ad hoc and LOS access may not be possible. NLOS Orthogonal Frequency Division Multiplex (OFDM) based radios leverage reflections to reconstruct the signal, making them more efficient in urban environments. However, in rural or forested areas where there are no reflections, NLOS systems perform like LOS systems. Furthermore, depending on how BBDS equipment is sourced there may be incompatibility with microwave systems between the BBDS and remote sites and between two BBDS systems. Mesh systems are typically inefficient in proportion to the number of nodes.

## 7.2 BACKHAUL AND BBDS FORM FACTORS

From an implementation perspective, certain BBDS form-factors may not be able to support the full range of backhaul communications technologies:

- **Backpack/Transportable BBDS:** These types of BBDS offer extremely limited options for backhaul technology due the size and weight of the extra required equipment. Backhaul for these units may consist of a UE Relay or Wi-Fi solutions that could support a small number of users and applications. Some backpack solutions may be "backhaul ready" with necessary connections to interface to external backhaul solutions, including satellite.

- **Vehicular BBDS:** The provision of backhaul for vehicular-based BBDS will be contingent on the type of vehicle including its size, the availability of space in the vehicle, availability of power sources, and vehicle's structural loading capabilities. For example, while microwave and satellite dishes are unlikely to be installed on a standard police cruiser they would be possible on a mobile command vehicle. Wi-Fi, UE Relay, and other RF technologies may be appropriate for smaller sized vehicles.

- **Aerial BBDS:** While airborne BBDS solutions are likely to be provide service from a stationary position in order to mitigate interference, they may be able to cover a very large geographic area (up to a 100 km radius) and can provide service to many users. If the aerial BBDS is configured as a Relay Node, then UE Relay can be used for backhaul as long as the aerial platform remains within the coverage zone of the donor eNodeB.[32]

[32] The donor eNodeB providing backhaul connectivity for the aerial BBDS could be an NPSBN macro tower site or another BBDS.

- **Aerial systems:** Aerial BBDS may consist of a device as small as a hobby drone or a large aerostat balloon. The type of backhaul will be based on the size and payload capacity of the aerial device.
- **Stationary/Tethered Aerial Vehicles:** These aerial BBDS systems are able to accommodate more backhaul solutions due to their size and operating environment. In addition to traditional RF backhaul technologies, a tethered BBDS may utilize a wired backhaul connection.

The following public safety requirements were identified for BBDS based on the information in this chapter of the report:

| # | Requirements |
|---|---|
| 7.1 | Designated BBDS SHALL be able to interface with designated alternative backhaul technologies (e.g., satellite, microwave radio, and other backhaul technologies to provide alternative back haul in the event the macro infrastructure is unavailable). |
| 7.2 | The BBDS SHALL include backhaul connectivity to the NPSBN macro network with sufficient capacity to support available applications and services. |
| 7.3 | If a BBDS uses a satellite system to support backhaul connectivity, it SHOULD support automatic alignment of satellite antennas. |
| 7.4 | The BBDS SHOULD provide a locally hosted authentication service for applications and users. |
| 7.5 | A BBDS-hosted authentication service SHALL be interoperable with the NPSBN authentication service to support operations during periods of compromised or absent connectivity. |
| 7.6 | A vehicular BBDS SHOULD be capable of being served by any donor eNodeB (DeNB). |

# Chapter 8: Role of Applications

One of the key capabilities the NPSBN will give public safety agencies are reliable, high-speed access to a variety of applications and services. These include the ability for first responders to communicate with voice, text and video; to access and share a wide range of data; and to interface with sensors and other technologies.

First responders use some of these applications today which typically run over commercial LTE networks. Commercial network access may be hampered by network congestion and lack of sufficient throughput during peak periods and in the immediate aftermath of a major incident. The lack of guaranteed throughput prevents most public safety agencies from using commercial broadband services for mission critical operations. Reliable access to a high-capacity broadband network will be transformational for the public safety community. NPSBN services will improve first responder safety, dramatically increase the efficiency of public safety response, and allow for data interoperability on a scale not yet seen.

For the purpose of this report, the phrase "applications" means both applications and services including Over-The-Top (which are typically accessed over the Internet) and those that are hosted on the NPSBN macro network (e.g., Mission Critical PTT).

Public safety personnel need continuous access to mission critical applications and services as their devices seamlessly transition from the NPSBN macro network to a BBDS network. Applications may also be running exclusively on a BBDS in areas without access to the NPSBN macro network. Finally, first responders may use applications and services that operate locally on their devices and which are not supported by any network. Public safety user devices will be transitioning between all three of these network environments.

## 8.1 Application Availability

It is not reasonable to expect that every public safety application, service, and feature will be available on every BBDS solution. Smaller BBDS units, including those installed in vehicles, may be designed primarily to extend the macro network into a building or other area that lacks macro network coverage. These BBDS would rely on the macro network to service their application needs. Other types of BBDS would provide more robust features including onboard servers and databases that direct support applications and services. This is important in two critical situations:

- **First responders need access to applications and services when using a BBDS solution operating in Stand Alone mode**. Certain BBDS activations may occur in areas where a backhaul connection to the NPSBN macro network is not possible. This may include

operations supporting a large wildland fire in an isolated area or BBDS implementation following a disaster where NPSBN macro network infrastructure has been damaged and is inaccessible.

- **First responders need continuous access to certain mission critical applications even if the backhaul link to the NPSBN macro network is diminished or lost**. A group of firefighters would be placed in a life-threatening situation if they suddenly lost mission critical voice communications [33] due to the failure of the microwave backhaul link connecting the BBDS to the NPSBN macro network.

It is important to note that applications may reside on different networks and may be managed by individual public safety agencies. For example, most public safety agencies have a mobile data application that extends their agency's Computer Aided Dispatch (CAD) system into the field. Other public safety agencies share regional applications that aggregate information from multiple sources. These may include applications that manage criminal justice information for all law enforcement agencies in a given county or applications that manage the status and alerting of all hospitals and healthcare facilities in the area. Applications may also be managed on a statewide and nationwide basis, including vehicle registration and wanted person's databases. Some of these applications may run on internal public safety agency networks at the local, regional, and state level or they may reside on a national NPSBN application platform. Other applications may be accessed through the general internet. The availability of backhaul connectivity from the BBDS to the NPSBN macro network is required in order to access any applications or databases that are remote from the BBDS. Therefore, public safety agencies should not expect that all applications and services will be available in all BBDS deployments.

## 8.2 INTERNET OF THINGS

The Internet of Things (IoT) will enable the use of a variety of sensors and devices which will enhance situational awareness and provide an additional layer of safety for first responders. These sensors and devices may be equipped to operate on NPSBN spectrum or may leverage other spectrum and technology options to communicate data. First responders will use applications to "find" nearby sensors and systems that they may access to gain information. For example, a police officer may use an application to identify a security camera near the incident and access video footage directly from that device. A firefighter may use an application to connect to a building's fire alarm control panel to obtain detailed information on the status of various systems during an emergency.

## 8.3 HOME STATUS PAGE

[33] In addition to mission critical voice, the use of incident command and situational awareness applications are essential in many complex public safety operations.

The NPSBN will also provide a mechanism through which public safety agencies can share real time data on events and incidents. The availability of a "home status page" will allow first responders to visualize critical information and may serve as a portal to access certain applications and services [22]. Firefighters responding to a major fire could access the Status Page from any device to view incident information, including the staging area for incoming units, the radio channels assigned to the incident, and the current tactical conditions. A sheriff's deputy's user device might sound an audible and visual alarm as the deputy approaches a convenience store which has reported a robbery in progress to the local police agency. This Home Status Page functionality should also be available to public safety personnel who are connected to a BBDS and may need to include specific information unique to the BBDS or the incident receiving coverage from the BBDS.

Finally, some applications may be designed to operate without network assistance. Firefighters and other public safety personnel may be operating in Direct Mode/Pro Se and still need to access and share local information. In addition to communicating via voice with other public safety personnel, certain applications may allow for the exchange of video, messages, and files directly between first responders.

## 8.4 Network and Application Recovery

There are a number of operational considerations that must be addressed when multiple network modes are in use. As stated previously throughout this report, first responders need reliable access to NPSBN voice, data, and video services. Disruption of these services can negatively impact the safety of the first responder and endanger the public.

There are two types of network transition that will occur as public safety personnel traverse different environments. First responders may experience a planned transition as they shift from the NPSBN macro network to a vehicular-based BBDS service and again as they may transition to Direct Mode (off network) communications. These transitions are expected to occur and the network and subscriber devices should be appropriately provisioned to accommodate a seamless shift between networks. The second type of transition occurs when there is an unexpected loss of connectivity, either between the subscriber device and the NPSBN macro network or between the BBDS solution and the NPSBN macro network (e.g., loss of backhaul).

From a public safety user perspective, problems with a planned or unexpected transition may severely impact their ability to communicate and share data. If the backhaul connection is lost, designated mission critical applications, including Mission Critical PTT, must continue to operate. If a fire department incident commander is using an Incident Command System (ICS) application to track equipment and personnel, access to that data must be maintained. If the application is running on the macro network, then the application must seamlessly fail over to an application server on the BBDS that has a mirror image of the data. When the backhaul

connection is restored, the ICS application should automatically reconnect to the NPSBN macro network. Updates to the status of personnel and equipment must be rapidly synchronized between the two versions of the application. If an NPSBN macro user made updates to the application, those must also be reconciled with the version on the BBDS solution. For example, a dispatcher may have added additional fire engines to support the incident while the backhaul connection was down and an incident commander may have changed personnel assignments for multiple firefighters. This data must be reconciled so the dispatcher and the incident command share the same "view." Applications used by first responders should be designed to operate efficiently because backhaul connections may be intermittent. The unreliability of backhaul connections should be a fundamental assumption in the design of mission critical applications.

## 8.5 Application Types in a Public Safety Broadband Network

First responders will have a variety of ways in which they can access public safety applications. The NPSBN will likely allow a number of network and device configurations which support public safety operations in different environmental and tactical scenarios. Applications may be accessed in the following ways:

**Type 1: NPSBN Core-Hosted Applications**. These are applications that are hosted by the NPSBN operator on the LTE core network. In many cases, they require that client application software be installed on the UEs. One example would be a mobile application that allows first responders to access their agency's CAD system from their LTE device.

**Type 2: BBDS-Hosted Applications.** A Core-Enabled BBDS may include application servers and databases. These application servers can deliver similar services as with the NPSBN Core-Hosted mode. Applications running on BBDS servers should be optimized to operate with intermittent or non-existent backhaul to the NPSBN macro network. Locally-hosted OTT applications can also be served from Core-Enabled BBDS that has a working Internet connection.

**Type 3: Remote-Hosted Applications.** Remote-Hosted applications are usually managed by a 3rd party and are typically accessed over the Internet using Secure Hyper-Text Tunneling Protocol (https). While some require specialized software on the UE, others do not and can be accessed via a web browser. Examples of browser enabled applications include two situational awareness mapping programs, MASAS™ and Virtual USA.® Over-The-Top applications typically require client software on the UE. An example would be Skype™ video conferencing.

**Type 4: UE-Hosted Applications.** These applications are hosted on the first responder's UE and are intended to serve a local area network of devices such as an array of sensors. Each sensor can be authenticated by the UE before its data is allowed to be accessed or shared. This includes sharing of data between sensors or the extraction of data to be analyzed, filtered, and

processed by the UE before uploading to a remote host. This is a part of an emerging field associated with the push towards edge computing.

There are also Peer-to-Peer applications that are resident on UEs, which don't require any infrastructure to operate other than the UE devices themselves. An example is Proximity Services (ProSe) for public safety [23]. ProSe services allow users to communicate using push-to-talk voice directly between two or more UE devices. Another example is Wi-Fi Direct™ whereby two devices can exchange data directly between them without the need for an access point and router.

## 8.6 BBDS Specific Application Requirements

BBDS have unique requirements for the management of applications. These include the need for certain applications to continue functioning following the loss of backhaul or to gracefully disconnect and reconnect to the macro network.

With respect to the modes described in Section 8.1, Type 1 (NPSBN Core-Hosted) and Type 3 (Remote-Hosted) require a backhaul connection to the macro network. Type 2 (BBDS-Hosted) requires a Core-Enabled BBDS. However, all types generally require applications to be able to discover that they are operating on a BBDS and to access necessary connections and services.

Transition between the various application connection types should be automatic and transparent for all mission critical applications. Degradation or loss of service during operations could result in catastrophic loss of voice and data communications and jeopardize first responder safety.

In some settings, LTE connectivity may be temporary and occasional, and thus applications may run in Type 4 (UE-Hosted) when LTE connectivity is lost, and transition to other modes when LTE connectivity becomes available, uplinking and downlinking data to other user devices and networked applications.

Mission critical services, including MC-PTT and certain incident command applications, must have the potential to run either as direct UE-to-UE applications (Type 4) or BBDS-hosted services (Type 2). In fully ProSe-enabled networks, such functionality should be implemented as Type 4. Mission-critical voice may be implemented via applications and also support LMR interoperability. LMR interoperability may also be supported by specialized dedicated UE devices providing the interoperability service, which will increasingly be possible in a ProSe-enabled network.

First responders from one agency may connect to a Stand-Alone BBDS of another agency or may connect to one BBDS in a cluster of several BBDS supporting a major incident. It is necessary for the UE to point to the correct BBDS within the cluster that is hosting the selected

application. The NPSBN operator will need to standardize on the manner by which applications will select the correct local host.

Agencies may provide their own application servers to be housed or interconnected to a BBDS solution. They may be connected via trusted network connections to the BBDS or via untrusted network connections.

## 8.7 DISCOVERY

In order to maximize the efficiency of applications, it will be necessary for first responders and devices to discover each other on both the NPSBN macro network and on the BBDS network. This is especially important since a BBDS solution from one agency will support users, devices, and services from other agencies, including while operating in Stand Alone Mode. The following discovery services should be expected on a BBDS:

- **UE IP number discovery**: ABBDS OTT service to allow one UE to discover the IP number of another, up to security limitations, when in Direct Mode.
- **UE service discovery**: Aversion of UE IP number discovery (OTT service) focused on discovering application-based services on UEs in the network (note: a function built into ProSe-enabled networks).
- **BBDS service discovery:** Allows discovery of OTT services on a BBDS, such as IP numbers of LMR interoperability services, location-based services, messaging services, direct voice services, blue force tracking services, incident command services, etc.

The 3GPP SA6 [24] working group is currently working on standards regarding discovery services.

## 8.8 APPLICATION PACKAGES

A BBDS should provide interoperable application services to all public safety agencies involved in a response, even when the BBDS solution is operating in Stand-Alone mode. Therefore, a minimum set of application packages must be made available on designated Core-Enabled BBDS, using an application delivery platform installed in the BBDS solution. The minimum set of application packages should be consistent across the entire NPSBN network and will likely include mission critical voice, incident command tracking and management, and basic sensor and analytic programs. Local agencies may consult with regional partners and jointly agree on other services and applications that they need. Industry will likely provide a variety of application packages and local public safety agencies should be able to select from a list approved by the NPSBN operator. These could be unique to that region and do not need to be standardized nationwide.

It is important to note the following: move up and emphasize3GPP TS 22.346 contains standards regarding continued public safety services when an LTE tower site loses connectivity to the LTE macro network. "*The UEs in the coverage of the Isolated E-UTRAN are able to continue communicating and provide a restricted set of services supporting voice, data and group communications, to their Public Safety users.* These requirements should also logically extend to a BBDS that is operating in Stand-Alone mode.

## 8.9 CONTENT TRANSFER AND ACCESS REQUIREMENTS

Whatever the mode of operation and transport of data across the network, the demands of the applications may constrain the usefulness of the network transportation capabilities, and the capabilities of the network may constrain the applications that can be used. This is also true for BBDS network connections. For instance, real-time control of a bomb disposal robot using data and video may place significantly more requirements on network latency and jitter than streamed general observation data, such as that from security cameras. Similar constraints apply to other forms of telemetry and tele-command, and to general audio vs. mission-critical voice communications. The requirements arise from the following constraints on the use of the BBDS solution (see Figure 8.2):

- The **mission.** Public safety defines what is needed [i.e., the requisite application should be capable of meeting the operational requirements of the first responder]. There are several important technical factors that must match the operational needs. For example, is lower resolution video needed to determine if a roadway is congested or is higher resolution video needed to read vehicle license plates?

- The **content** owner. Whoever owns the data to be transferred or shared must authorize their content to be discovered and accessed. The data, especially video, must provide the quality necessary to meet the mission need.

- The **transport** network must accommodate the bandwidth necessary to deliver the content to the user. This is especially critical when sharing video as compression and bandwidth limitations can downgrade the image to the point it is not usable for tactical operations.

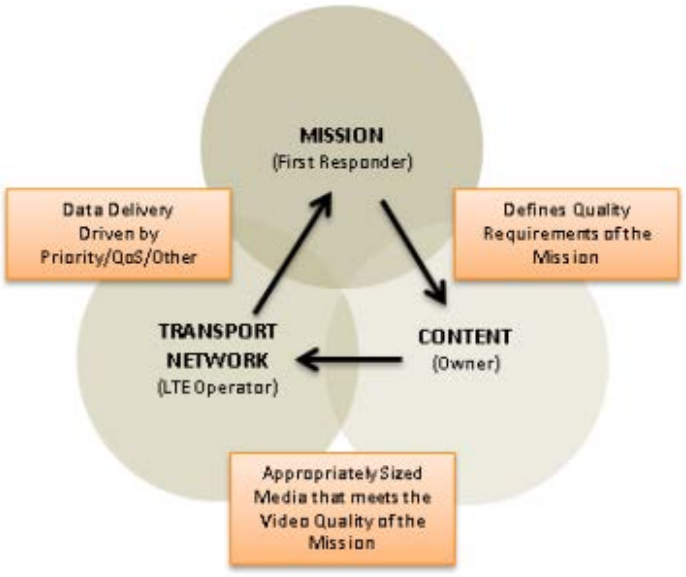



*FIGURE 8.2: The interplay of content, mission, and transport **[25]**.*

The following public safety requirements were identified for BBDS based on the information in this chapter of the report:

| # | Requirements |
|---|---|
| 8.1 | The BBDS SHALL allow subscriber devices to access the general Internet based on security and local control profile configuration settings. |
| 8.2 | The BBDS SHALL support a minimum defined set of local databases and applications in order to meet essential operational needs, including when the BBDS is operating in Stand-Alone Mode. |
| 8.3 | BBDSs SHALL support the provision of a “home status page” web application that provides location specific incident content. |
| 8.4 | BBDSs SHALL provide a method whereby the “home status page” application is available via an alternate access network, other than the NPSBN (e.g., Wi-Fi and other RF technologies used by the BBDS). |
| 8.5 | The Deployable System SHALL automatically reconnect applications and services that were lost or transitioned when backhaul connectivity was disrupted (e.g., when the BBDS recovers from Limited Connectivity or Stand-Alone modes) |
| 8.6 | The BBDS SHALL be capable of data synchronization during recovery of a lost connection to the NPSBN macro network; providing reconciliation of updates to |

| | |
|---|---|
| | applications and databases made by BBDS and macro network users. |
| 8.7 | A BBDS SHOULD be able to interface with internal and external devices and environmental sensors in order to monitor the status of the BBDS, of first responders and their equipment, and the incident area. |

# Chapter 9: Voice Considerations for Deployable Systems

Today, first responders use several different types of voice communications. They include Push-to-Talk Voice, Conversational Voice (e.g., two way, full duplex communications such as Voice over IP, Voice over LTE, PSTN Voice) and Device-to-Device (off network/direct mode) communications. These types can be further grouped into single user-to-user "one to one" calls, one user to multiple users "one to many," and broadcast communications ("one to all"). This chapter will group the operational requirements for voice that were identified in the nine use cases described in Chapter 2. Moreover, this chapter will describe how each of these voice communication types would be used whether a BBDS is **connected or disconnected** from the NPSBN macro network.[34]

It should be noted that 3GPP [26] has done considerable work on standards to support mission critical voice. Much of that work was derived from early requirements work facilitated by NPSTC [27] [28], including delivery of several reports which captured key public safety expectations for LTE voice services.

## 9.1 Types of Voice Communications

The following types of voice communications will be available to first responders. Access to some applications is based on the presence (or absence) of network coverage.

- **Push-to-Talk (PTT)** communications are provided to First Responders today via existing LMR systems, using various technologies including P25 digital communications and legacy conventional analog systems. There are a number of non-mission critical communications options for LTE. These include PTT over cellular networks[35] and PTT over third party applications (e.g., Over The Top or OTT services). MC-PTT is designed to provide mission critical voice communications. The SA6 working group of the 3GPP International standards organization has done extensive work in this area and expects to finalize the MC-PTT standard in March 2017.

- **Device-to-Device** (e.g., Peer-to-Peer) Voice communications are possible in the absence of any network infrastructure as long as the two devices are within range of each other and have been properly provisioned to support the service. This type of device-to-device communication is referred on public safety LMR systems as "direct mode" or "talk-

[34] This chapter assumes that the necessary Interworking equipment and operator interconnect agreements are in place.

[35] The Open Mobile Alliance has specified a Push-To-Talk over Cellular (PoC) standard.

around" mode. In LTE, this is referred to as ProSe D2D service which currently supports Push-to-Talk and Group Call Communications.[36] 3GPP standards identify two unique modes of operation for public safety. **Pro Se Mode 1,** also known as "Scheduled," is network assisted using an application server allowing the eNodeB to dynamically allocate resource pools and to assign and schedule resources within those pools. First responder user devices are thus managed by the network, even though they are communicating directly from device-to-device. This type of Pro Se service (Mode 1) would be required to support the seamless transition of first responders between NPSBN and Direct Mode service, or between a BBDS and Direct Mode service. **Pro Se Mode 2**, also known as "Autonomous," does not require a connection to the macro network and is designed specifically for public safety use when first responders are beyond network coverage (or at the edge of network coverage). In Mode 2, the first responder's UE will select from a set of predefined resource pools. In some configurations, the network may also provide data on available resource pools.

- **Conversational Voice** supports full duplex conversation and allows either party to speak at the same time, (e.g., a cellular telephone call). Public safety agencies use the Public Switched Telephone Network (PSTN) for voice communications, along with other types of conversational voice technologies.[37] Conversational voice would allow a hands-free communication between a paramedic and a medical control physician.

- **Video Chat** is another example of voice service which is coupled with a one-way or two-way visual feed between the parties. Video chat may be extremely helpful in certain public safety environments, including EMS incidents when paramedics need to engage in a video consultation with a physician or when a firefighter needs to brief an incident commander. Therefore, certain video chat applications should provide the same level of priority and assured connection as MC-PTT. The 3GPP organization had identified standardized QCI's[38] to help manage priority and quality of service issues.[39]

BBDS have the unique capability to operate in both a connected mode (as a node of the NPSBN macro network) and in a Stand Alone mode (as a completely isolated network). When the BBDS is operating in a connected state, it is possible to support all of the network-assisted voice communications types. Interoperability between the BBDS and other networks may be

[36] 3GPP standards also support data and video exchange using ProSe communications.

[37] These include Voice over Private IP, WebRTC Voice (http://www.webrtc.org/) as well as Voice over LTE/IMS (i.e. 3GPP VoLTE/IMS).

[38] QCI is the Priority/Quality of Service Class Identifier.

[39] 3GPP SA6 R14 specifications support Mission Critical Video over LTE as a complementary service to MC-PTT. Dynamic QOS and Priority management are also supported.

provided by the NPSBN macro network. This allows connectivity and interworking to MC-PTT services, PSTN telephone communications, and public safety LMR networks.

When the BBDS solution is operating in a Stand Alone mode, voice communication options are limited to those services which can be provided locally by the BBDS and supporting components. For example, a BBDS may be able to support MC-PTT but not support dial tone for PSTN telephone traffic.

## 9.2 MISSION CRITICAL PTT

Voice communication options on the NPSBN will evolve over time as standards are refined, technology is tested, and infrastructure is built. It is likely that the NPSBN will initially offer an administrative grade40 PTT solution as well as access to the PSTN for telephone calls. Implementation of mission critical PTT on the NPSBN will eventually occur. This report describes both the near-and long-term vision for use of BBDS and includes MC-PTT requirements.

Public safety agencies may initially shift certain users to the NPSBN administrative PTT service. A number of public safety agencies today are using both commercial carrier network PTT services as well as OTT PTT applications running on commercial carrier networks. Personnel using these services are typically not public safety personnel who are responding to emergency calls and thus need a MC-PTT solution. They are more likely personnel assigned to functions which carry a low safety risk. However, in some areas of the country, local agencies are using these alternate PTT technologies to provide voice communications in areas with insufficient LMR radio coverage. In this context, they become mission critical. For example, deputies with the Grant County, Washington Sheriff's Office use an OTT Push-to-Talk solution to communicate with their dispatcher while on traffic stops in areas with poor LMR coverage.

However, true MC-PTT services are those which support a high priority on the network, which are designed to operate in a tactical environment and which nearly guarantee the ability of one first responder to communicate with another. These requirements are the same whether the first responder is communicating through the NPSBN macro network or through a BBDS solution.

## 9.3 MC-PTT IMPLEMENTATION

Finally, discussion is needed on how to best manage mission critical voice services for first responders who are communicating through a BBDS solution. Since a BBDS may be required to operate in Stand-Alone Mode, it should be equipped with local application servers that can support mission critical voice services. However, when the BBDS is connected to the NPSBN

[40] This has also been referred to as "secondary push to talk."

macro network, there are several considerations that must be examined to determine the most reliable solution for public safety.

The Working Group identified two implementation scenarios:

- **Mission critical voice services could be provided by the BBDS local application servers, even if the BBDS is connected to the NPSBN macro network**. Users external to the BBDS would either connect to the BBDS MC-PTT server, or they would communicate through a separate MC-PTT server on the macro network that was interconnected to the BBDS application server.[41] This arrangement would ensure that first responder MC-PTT communications were not interrupted by a failure of or temporary interruption to the backhaul link. If the backhaul link to the NPSBN failed, then only those users external to the BBDS coverage would be dropped from the group. Public safety personnel at the scene of the emergency would continue with their PTT sessions. If dual MC-PTT servers were in use, both groups of first responders would remain connected to only those members sharing their connection type (e.g., first responders at the scene would continue communicating with other first responders connected through the BBDS while other first responders – and the dispatcher – would be regrouped to a new talkgroup and could continue talking with personnel connected via the NPSBN macro network.

- **Mission critical voice services could be provided by the NPSBN macro network application servers** and MC-PTT voice services would flow from the macro network to first responders connected to the BBDS. If the backhaul link failed or was temporarily interrupted, communications among public safety personnel at the incident scene would be disrupted. It is unclear how much time might elapse for MC-PTT services to "fail over" to a local application server on the BBDS solution. This potential blackout period could have serious safety and operational consequences for first responders. Depending on how subscriber devices were provisioned, some public safety personnel devices would switch automatically to ProSe direct mode communications and redistribute first responders onto different LTE direct mode talkgroups.

There are a number of important technical and operational factors to consider beyond those identified in this report. The NPSTC LMR LTE Integration and Interoperability Working Group will further examine this specific issue.

The following public safety requirements were identified for BBDS based on the information in this chapter of the report:

[41] 3GPP is currently working on a standard to support the use of two Mission Critical PTT servers (GPP 23.281)

| # | Requirements |
|---|---|
| 9.1 | The BBDS SHALL support the same IP voice services (including Push-to-Talk voice) and IP telephony communications as the NPSBN macro network. |
| 9.2 | A BBDS operating in Stand-Alone mode SHALL support the same PTT/MC-PTT services and features that are present on the NPSBN macro network. |
| 9.3 | A BBDS operating in Stand Alone mode SHALL support registration of authorized MC-PTT users and affiliations to LTE talkgroups. |
| 9.4 | The BBDS SHALL support service continuity and session persistence for users transitioning between a BBDS and Pro Se Scheduled Direct Mode (ProSe Mode 1) |

# Chapter 10: Operations and Maintenance

This chapter covers Operations and Maintenance (O & M) considerations relating to BBDS and will cover issues that are common across all BBDS form factors and technologies. It is not the intent of this chapter to detail specific vehicle or aerial based O & M components that address the unique operating requirements of the transportation unit itself.

## 10.1 General O&M Considerations

At a high level, BBDS should be monitored and maintained using a formal set of process and procedure which has been standardized by the NPSBN operator. BBDS should be monitored to assess Key Performance Indicators (KPIs) and configuration status:

- The monitoring should be done at regular intervals to verify that the BBDS is compliant with the upgrade schedule, the BBDS is fully functional, and that interoperability readiness is assured. This should include the capability for remote monitoring while a unit is in service or in storage awaiting activation.
- The specific KPIs and allowable configuration parameters should be provided by the NPSBN operator and will likely include monitoring of the BBDS in-service status, verification of software and firmware release levels, verification of HSS and ICAM database updates, and other elements of the unit's physical readiness (e.g., battery status).
- Regular inspection should be performed on all BBDS components, including power, backhaul, and other RF, technology and mechanical systems.

## 10.2 Data Storage and Synchronization

An area of extreme importance involves the management of data synchronization between BBDS and the NPSBN macro network.

**HSS synchronization** between the BBDS and the NPSBN core should occur on a regular basis to insure that registration and database information is up to date. This is necessary if the BBDS will be operated in Stand Alone Mode and is also necessary in the event the backhaul connection to the NPSBN macro network is lost.

The HSS database is the interface to subscriber information and manages connections to other databases which are necessary for device verification. There is no standard for transfer of data from one database to another (e.g., from the macro network to the BBDS). The HSS points to the information but does not hold the actual subscriber data. There are no standardized

specifications on how this data is stored or transferred. Today, this functionality is proprietary and is secured by vendors which may make it challenging to transfer the data.

However, 3GPP standards do define the structure of an HSS through the provision of a data schema in the profile. The HSS can be implemented with a relational database to enable better management and movement of the information. Updates and synchronization of HSS data with the BBDS solution may not occur in real time based on the connection status of the deployable unit.

The NPSBN operator will have to provide guidance on how HSS data is managed and stored. The BBDS would likely contain a local or regional subset of the HSS data which resides on the macro network. Guidance will be needed on what records may be stored in the HSS database of BBDS operated by local public safety agencies.

Those decisions may impact the registration of public safety subscriber device that come from outside the "home" area of the locally operated BBDS. A system must be provided to register those first responder devices that arrive with mutual aid personnel from adjoining regions or from out of state (and how are likely not in the BBDS HSS database). Device registration may be a manual process (e.g., device registration and user authorization keyed in at a command post) or one that is technology assisted.

## 10.3 Software and Firmware

Software and firmware updates must be managed uniformly across the NPSBN service area to insure that all BBDS are in a consistent and ready state. Software and firmware updates present unique challenges that are compounded when BBDS equipment from multiple vendors are in use. Recommendations in this area include:

- A comprehensive testing and certification plan will be required to ensure that an update from one vendor does not "break" compatibility and interoperability with another vendor's system. This testing should occur before user agencies are notified to update their BBDS software.
- An update schedule should be a required component of the Service Level Agreement between the NPSBN operator and the public safety agency operating the BBDS. This update schedule should identify the window of time allowed between notification of a new software release and the actual implementation of the update.
- An update plan should include requirements for implementing the software release including full testing of BBDS functionality at the completion of the upgrade.

- Update procedures and requirements should also cover other software and firmware including security patches, 3GPP release upgrades, and other vendor specific equipment (e.g., routers, satellite terminals, microwave systems, etc.).

## 10.4 Local Control Access Levels

From an O&M perspective, the BBDS should support at least four levels of authorization for local control. The first (lowest) level shall allow an authorized user to only view the configuration parameters of the BBDS and other remote BBDS whose configuration parameters are accessible locally. The second level shall have the same privileges as the level below it and can modify the configuration parameters of the local BBDS only. The third level shall have the same privileges as the level below it and can modify the configuration parameters of remote BBDS. The fourth (highest) level shall have the same privileges as the level below it and can also set permissions for the authorized users below it.

It is expected that all public safety agencies will have equal access to BBDS. For example, a BBDS operated by a county sheriff's office should be accessible to Fire, EMS, and other first responders. However, there may be certain high-risk tactical situations where access to the BBDS should be restricted to a particular class or subset of users. For example, during a complicated hostage situation with poor network coverage it may be necessary to restrict BBDS access to only support SWAT teams. This would be necessary if there was a risk of saturating the capacity of the system and blocking an urgent transmission. While not considered a normal course of business, authorized technical personnel should be able to make these adjustments as necessary. COML and COMT personnel may be trained and certified to perform some of these functions.

Authorized personnel may need to modify other BBDS technical parameters to account for necessary changes in the configuration to support the operational mission. The NPSBN operator will need to determine which parameters are eligible for modification. Control and monitoring of BBDS technical parameters will require standardized interfaces and protocols to allow them to be supported within the same network management domain.

## 10.5 Configuration and Default Status

In order to manage the BBDS, authorized technical personnel will need to be able to view a list of all subscriber devices that are connected to the BBDS network. There are security and risk implications in exposing subscriber device information to non-authorized individuals. It should be noted that 3GPP standards mask the identity of the individual user following authentication. However, application and server data can provide information on who is logged in.

When a BBDS has completed its mission it will be necessary for the configuration of the system to be returned to a "default" status, which will reset any changes to the BBDS internal settings that were necessary for the prior incident. Each BBDS should arrive at an incident scene with a known set of technical parameters. It is important that the ability to reset the BBDS be implemented in such a way as to prevent an accidental reset during an active incident.

The following public safety requirements were identified for BBDS based on the information in this chapter of the report:

| # | Requirements |
|---|---|
| 10.1 | The BBDS SHOULD comply with macro network auditing based on limitation of the BBDS type. |
| 10.2 | The BBDS SHOULD collect sufficient information to support the accounting and billing system. |
| 10.3 | BBDSs SHALL be maintained by the operating entity to the level of service required by the NPSBN operator including specific actions to sustain interoperability, manage revision levels, and required configuration settings. |
| 10.4 | The BBDS SHALL support a local management interface for viewing and modifying configuration parameters of the unit. |
| 10.5 | The BBDS SHALL allow an authorized user to restrict system access to only support a designated group of UEs. |
| 10.6 | The BBDS SHALL support wired and/or wireless standards-based Ethernet connections (e.g., connect a laptop to the BBDS) to provide access to local services, NPSBN services, and Internet. |
| 10.7 | The BBDS SHALL provide at least one Ethernet port on the LAN side to interface with IP-based services such as LMR gateways, remote terminal units, Wi-Fi access point routers, etc. |
| 10.8 | The BBDS SHALL support local and remote monitoring and reporting of unit status to include the health of the BBDS system components (LTE routers, servers, RAN that impact capacity, connections, performance, etc.) and associated support components (e.g., fuel status, temperature, security, etc.) |
| 10.9 | The BBDS SHOULD report its configuration status through an "Operations Administration and Maintenance" application while off-line (i.e., not deployed) in order for an authorized entity to validate the compatibility of the |

| | |
|---|---|
| | configuration with the existing network. |
| 10.10 | BBDSs SHALL interface with network management systems using standardized interfaces and protocols. |
| 10.11 | The BBDS SHALL enable authorized personnel to modify designated technical parameters at the scene of the incident. |
| 10.12 | BBDS SHALL be capable of resetting to a default configuration at the completion of a mission (so each deployment starts from a known and standardized configuration state). |
| 10.13 | A BBDS SHALL be capable of displaying a list of connected subscriber devices to authorized technical personnel for security, administrative, and configuration purposes. |

# Chapter 11: Deployable Systems Security / Assurance

This chapter will focus on both the physical and cyber security considerations for BBDS. BBDS are more vulnerable to these attacks due to the physical space of their footprint and their use in areas that are more difficult to secure than a terrestrial LTE tower.

Cybersecurity is a prominent component of the First Responder Network Authority (FirstNet) Request for Proposal (RFP) Statement of Objectives [29] (SOO). Several federal organizations are also actively working on security related issues. The National Institute for Science and Technology (NIST) released an LTE Architecture Overview and Security Analysis [30] in November of 2016 which describes a number of important considerations when securing LTE networks.

In general, the security policies and procedures defined and implemented for the NPSBN macro network must also apply to BBDS, regardless of the form factor of the unit (backpack, vehicle, towed, aerial, etc.).

## 11.1 BBDS Security Elements

Certain security issues were identified as being unique to the BBDS ecosystem. These items help ensure that the BBDS are deployed in a secure manner and include the following:

- The same security policies and controls that apply to the macro portion of the NPSBN are also necessary for BBDS to include all associated security requirements of FirstNet's E-UTRAN consisting of the UE (Devices), eNodeBs, and requirements affecting the X2 and S1 interfaces.
- When operating as part of a vehicular system, the BBDS must include security mechanisms to ensure that deployable network interfaces and functionality are isolated and protected from vehicle operations and functionality. This would prevent a first responder from accessing BBDS control settings from their vehicle's mobile data terminal.
- Upon power up, and prior to accessing any network services, applications or data, a BBDS will:
    - Attest health and status information to the network in a trustworthy manner.
    - Ensure that the network is authenticated in a trustworthy manner.

- A BBDS may need to be remotely disabled in a secure manner, in accordance with applicable law and NPSBN policy. This remote capability will require some level of a backhaul connection to the relevant NPSBN Security or Network Operations Center. For the purposes of this report "disable" can mean:
    - Clear all user data.
    - Clear all keying material.
    - Inhibit establishing any communications with UEs.
    - Allow local administration to access the system.
    - Prevent the unit from radiating an RF signal.
- BBDS should be secured against intrusion and theft.
- The BBDS shall provide security through encryption or other means to protect information passing through the network.
- Data stored on the BBDS shall be physically and digitally protected.
- The policies and operating procedures for BBDS should include:
    - Guidelines for maintaining a list of authorized technicians.
    - Associated authentication methodologies for those technicians.
    - Policies and procedures to enable systems that have been remotely disabled.
- Hardware platforms used on the BBDS should not have any external manual reset buttons or external unprotected management control interfaces (e.g., telnet sessions).
- BBDS installed in vehicles should have physical security implemented both when being operated and stored.
- The backhaul connection for any BBDS should mirror backhaul security as specified for the overall NPSBN.
- As stated in the FirstNet RFP "Special Notice on Cyber Security [31]" Appendix C-10, Cyber Security Architecture Objective for support for IP Infrastructure Network Elements, FirstNet may consider requiring network elements on BBDS to be compliant and certified with NIST FIPS-140-2 standard.
- Careful consideration should be given for managing security patches on BBDS that are in storage. It is recommended the NPSBN operator develop a configuration management and maintenance strategy to ensure that BBDS solutions in storage

remain functionally viable and current with respect to operational software and security patches.

## 11.2 BBDS Security – Stand Alone Operations

BBDS may operate as a node on the NPSBN or in Stand-Alone Mode. Those operating in a Stand-Alone mode require additional security considerations. This includes BBDS activated in Stand-Alone mode or when transitioning to Stand-Alone mode following a failure of the backhaul connection. BBDS operating in this state:

- Will comply with NPSBN operator security requirements.
- Will provide secure communications:
    - Authentication of the UE and User.
    - Encrypt the UE/RAN control/Data.
    - Authenticate any administrative user.
- Will use firewalls to provide protection between the BBDS and any non NPSBN external network.
- Will maintain the same security mechanisms as were present before the BBDS became isolated.

The following public safety requirements were identified for BBDS based on the information in this chapter of the report:

| # | Security Requirements |
|---|---|
| 11.1 | The BBDS SHALL allow an authorized user to disable the unit in a secure manner in accordance with NPSBN policy (e.g., during a failure of the BBDS or compromise of the BBDS security). |
| 11.2 | The BBDS SHALL provide security mechanisms through encryption or other means to protect information passing through the network in accordance with NPSBN Security Policy. |
| 11.3 | A BBDS SHALL comply with the same NPSBN security requirements that are present on the macro network, including relevant components of physical, information, network, and communications security policies. This applies to all modes of operation, including when operating in, or transitioning to, Stand-Alone mode. |

# Chapter 12: Technical Challenges

This chapter identifies technical considerations and challenges that need to be addressed in order to realize the full potential of BBDS technology. This involved a full review of the use case documents and the 45 operational capabilities described in the documents on BBDS deployment. This information formed the basis for the public safety technical requirements and helped define a number of technical challenges and considerations. An assessment was then completed regarding the current state of technology, policy, and standards which yielded a number of gaps.

Technical challenges were identified in several key areas:

## 12.1 Interference Management

Interference can easily occur between the BBDS and the NPSBN if not properly managed. Interference is also possible between different BBDSs operating in proximity to each other. Effective management of this interference requires a high-speed, low latency connection between the various nodes. This connection may be difficult to establish based on technical factors (e.g., sustained high speed connection between an aerial BBDS and the NPSBN macro network) as well as operational reasons (e.g., the need for technician grade personnel at the scene to manage the connection).

## 12.2 International Operations

Introducing a BBDS from one PLMN into an area that is served by a BBDS or the macro network of the other country may create interference issues. It can be mitigated by connecting the inserted BBDS into the network that receives it and enabling interference control mechanisms. The tech challenge for interference mitigation is to provide local interconnection of the BBDS to the adjoining eNodeBs of the other network since interference control requires low latency and high bandwidth connection. The capability would not be achievable in disconnected mode.

## 12.3 ICAM/HSS Database Management

When a BBDS is operating in Stand-Alone mode, the provisioning of services (device keys, subscriber data, etc.) must occur through a local HSS database resident on the BBDS. Technical challenges involve the need for the BBDS to maintain an up-to-date copy of a portion of the macro HSS database (for a subset of records needed to support first responders in the given service area of the BBDS). Mutual aid responders arriving from outside the service area will also need to be added to the local HSS database.

## 12.4 INTER-PLMNID HANDOVER, SERVICE CONTINUITY AND SESSION PERSISTENCE

First responders voice and data sessions must remain active during the hand-over of service between a BBDS and the NPSBN macro network with no noticeable degradation of service.[42] This transition may involve movement between network nodes that have different PLMNID's.

## 12.5 BBDS INTER-WORKING WITH THE NPSBN

There are a number of technical challenges related to the interconnection between the BBDS and the NPSBN macro network. These include:

- **Security gateway configurations** must be the same for BBDS and points where they attach to the NPSBN. Key management would be a difficult challenge due to the potentially large number of BBDS and public safety agencies that could own and operate BBDS.

- **IP address management for the BBDS**. The BBDS addresses must not overlap amongst each other nor with the NPSBN. There is a technical challenge to design a nationwide IP addressing scheme that involves all the BBDS, and to maintain it over the life cycle of the NPSBN. Coordination between Canada and U.S. is required. Different IP address schemes are required for user plane and control plane.

- **BBDS OAM interfaces and protocols** must be standardized across the entire NPSBN and coordinated between U.S. and Canada in order to monitor and control any BBDS that connects to the NPSBN.

- **Life cycle management of the changes** to BBDS and the macro network requires stringent controls on what is allowed to be connected to the macro network. The technical challenge is to monitor and control the inventory, including configuration states of the BBDS. There is a technical challenge in the test coverage when new BBDS or updates are presented for validation. Large number of permutations increase the risk of missing test cases during the test and verification process. A large number of permutations increases the risk that feature interactions analysis misses some connections.

## 12.6 VOICE INTER-WORKING BETWEEN NPSBN MACRO AND BBDS, AMONG BBDS, AND BETWEEN 3GPP AND NON-3GPP NETWORKS

First responders in the vicinity of two emergency vehicles that both contain active BBDS can communicate wirelessly using either BBDS. If one of the BBDS is operating in a Limited

[42] Seamless handover is also important as first responders transition from a commercial mobile network to the NPSBN (and back).

Connectivity Mode, a first responder's UE may attach to the strongest source BBDS, but it would not be possible to dynamically optimize the interference environment at the areas of coverage overlap. A user attached to one BBDS may not be able to communicate with a user attached to the other BBDS. If both users are attached to the same BBDS they can communicate with each other.

First responders must also be able to communicate with other users in their assigned talk groups when all or some of the users, in any combination, are connected to the macro network, the deployable system, or in device-to-device mode. Significant technical challenges include how to manage isolated UEs in the same talkgroups as those UEs connected to the macro network or the BBDS.

First responders' encrypted communications sessions will maintain session persistence during the handover of service from the macro network to the deployable system, deployable system to device-to-device, and vice-versa. Technical challenges are noted when the BBDS is operating with either a limited connection or no backhaul connection (e.g., the capability is not supported). When working in a connected environment, if the ProSe Key Management server in the macro network is not synchronized with the ProSe Key Management server in the core-enabled BBDS, there is a high risk of incompatible encryption between UEs. If MVPN is used as an additional encryption layer, technical challenges involve ensuring that all the VPN clients at the incident are associated with the same VPN server.

## 12.7 PRO SE DIRECT MODE COMMUNICATIONS

Technical challenges were noted regarding how a BBDS may support ProSe direct mode communications. ProSe servers in the BBDS and the macro network would have to be synchronized before the UE disconnected in order for the UEs from different jurisdictions to establish D2D communications. If ProSe application clients are configured from different ProSe function servers, the ProSe function servers must be synchronized.

## 12.8 DEVICE AND APPLICATIONS MANAGEMENT

First responders should experience similar priority and QoS treatment when they are connected to a WiFi network as when they are connected to the BBDS' LTE radio access network. This would require the WiFi network to be "HotSpot2" or "NextGen HotSpot." Technical challenges when using eligible HotSpot technology include the mapping of QoS parameters (QCI) onto the relevant Differentiated Services Code Point (DSCP) value to be used in the transport layer; mapping LTE QoS parameters to the WiFi QoS parameters (WiFi Multimedia Extensions). This mapping must be done a priori and all implicated systems must be configured to support the QoS mapping.

A complete listing of all technical challenges is included in Appendix B.

The following recommendations were identified for BBDS based on the information in this chapter of the report:

| # | Recommendations |
|---|---|
| 12.A | Technical challenges with BBDS identified in this report SHOULD be evaluated by the Public Safety Communications Research (PSCR) Lab and other government organized or sponsored entities for validation. |
| 12.B | NPSBN management SHOULD place a high priority on mitigation of interference between the NPSBN Mode of Operation and BBDS Mode of Operation (either Connected, Stand-Alone, or Clustered). |
| 12.C | NPSBN management SHOULD place a high priority on development of strategies and solutions for effective management of the BBDS HSS database. In order for HSS databases to exchange information it is necessary that the interface protocols and data models be implemented the same way by all the parties that own the BBDS systems. This would likely require national guidance. |

# Chapter 13: Operational Policy & Governance Considerations

This chapter will discuss a variety of non-technical considerations regarding the use of BBDS. Successful implementation of these systems will require action at the local, state/provincial, and federal level. The policy and governance issues with BBDS are very similar to the issues faced with LMR interoperability. The SAFECOM Interoperability Continuum [32] identifies five unique "lanes," each with their own progression steps to help provide excellence in public safety communications. The lanes include Governance, Standard Operating Procedures, Technology, Training and Exercises, and Usage (see Figure 13.1). Public safety agencies have embraced this approach and many successful LMR deployable systems are based on agreements involving all five areas of the continuum.

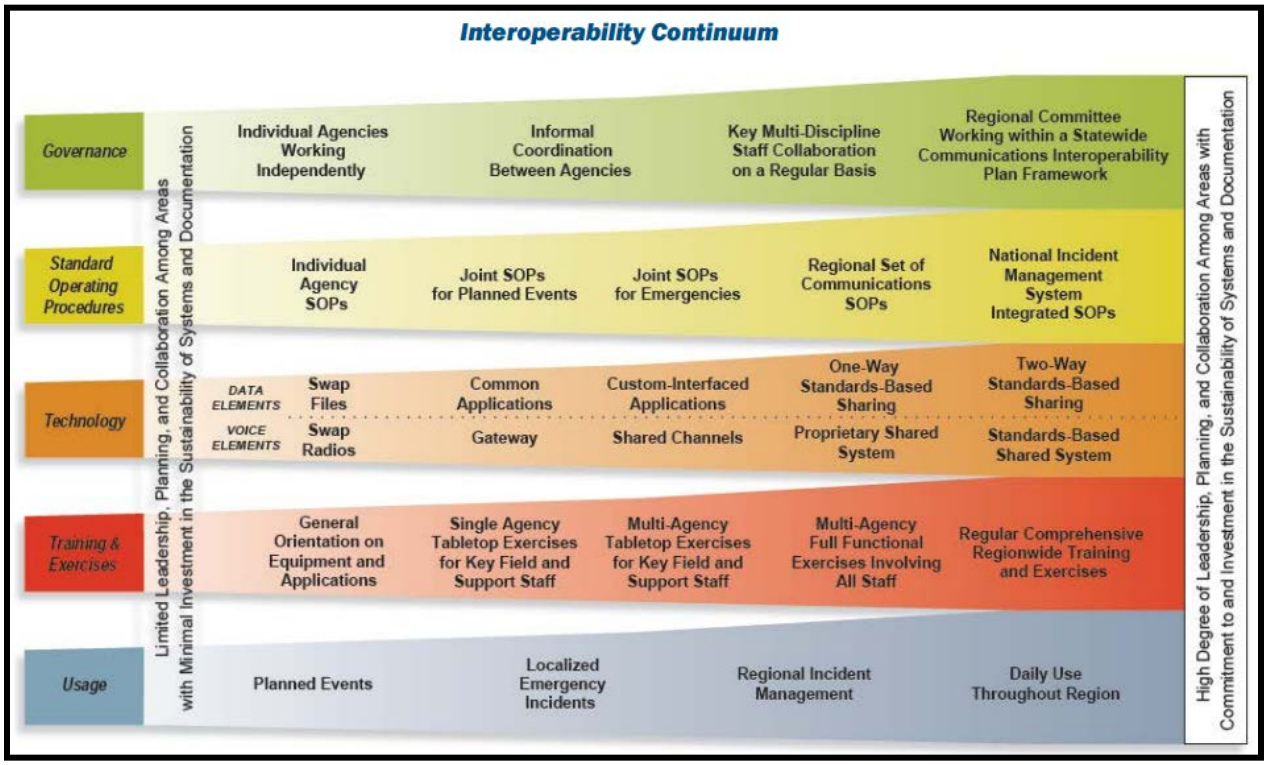



*Figure 13.1 SAFECOM Interoperability Continuum*

## 13.1 Interoperability Elements

The following elements of BBDS operation directly relate to these specific areas of the Continuum:

- **Governance**. Public safety agencies must agree on the specific way in which BBDS will be shared in the region. Those agreements form the basis of policy which must be codified by a governing body. There is also the potential for regional coordination over the procurement and ownership of BBDS units. Statewide and national level coordination is also necessary to ensure that all stakeholders are involved in the initial decision making for BBDS usage as well as ongoing collaboration regarding procurement, configuration, and operations.

- **Standard Operating Procedures**. BBDS activation procedures should be documented in agency approved SOPs. Public safety agencies in a region should agree on a standardized procedure to request BBDS resources, including identification of who is authorized to request BBDS activation, and specific procedures on how the BBDS will be staffed and operated.

- **Technology**. It is important that the BBDS technology be designed to support the operational needs of the public safety agencies. Local and regional collaboration will be needed to determine which services and capabilities should be provided by BBDS. This is especially important for applications and services which are to be installed on the BBDS unit itself.

- **Training and Exercises**. Public safety agency personnel must receive training on the use of the BBDS solutions in their area, including necessary technical training on the activation of the BBDS equipment. Regular exercises, including drills and simulated emergencies, should be scheduled to ensure that the BBDS is functional and that first responders have experience in using the system.

- **Usage**. The successful integration of BBDS technology into an agency or region is based in large part on the degree to which the systems are embraced and used by public safety agencies on a routine "day-to-day" basis. Problems occur when specialized systems are only used on an occasional basis (e.g., during a disaster). First responders need to interact with BBDS on a regular basis.

## 13.2 COMPARISON TO LMR GOVERNANCE AND PROCEDURE

The success of LMR communications interoperability is related to a formal process of public safety collaboration occurring at the national, state, and local level. This is based on existing organizational structures within each level that advocate for each lane of the Interoperability Continuum for LMR operations. The U.S. federal government manages the National Emergency Communications Plan (NECP) which identifies priorities and recommended approaches. They then coordinate with the Statewide Interoperability Coordinators (SWICs), who manage a Statewide Communications Interoperability Plan (SCIP) that provides specific guidance on

interoperable resources within each state. This information is then shared at the regional level where Tactical Interoperable Communications Plans [43] (TICPs) are produced by local public safety officials. This process ensures a standardized nationwide approach to public safety communications interoperability which allows specific tactical and operational plans at the local agency level. These relationships should be leveraged to achieve appropriate coordination of BBDS services, including the adoption of BBDS specific plans at the national, state, and local level.

Another example of synergy between LMR and LTE is found in an October 2015, NPSTC report on deployable LMR systems, *"700 MHz Nationwide Deployable Trunked Solutions: A Report by NPSTC and NRPC"* [33]. This document provided guidance to ensure successful interoperability between LMR deployable trunked systems which are owned and operated by various public safety agencies across the U.S. It includes technical information which provides a nationwide standard for the programming of LMR deployable trunked systems. The use of standardized ID structures allows those deployable systems to be relocated anywhere in the U.S. while also enabling communications for first responders traveling from anywhere in the U.S. This approach to nationwide itinerant coverage could be replicated by the NPSBN which will require standardized process and procedure on the use of BBDS technology**.**

The Department of Homeland Security, Office of Emergency Communications (DHS-OEC), is currently working on a revision of its LMR LTE convergence document which addresses the co-existence and potential merger of LMR and LTE functionality. DHS also provides a robust Technical Assistance Program to support local public safety agencies with communications planning[44] including programs on LMR and NPSBN governance and policy.

FirstNet is working with a number of communities across the U.S. which are participating in "early builder"[45] demonstration projects to provide 700 MHz broadband service to local public safety agencies. Several of these initiatives involve the use of BBDS equipment in a variety of operational and implementation modes. It is expected that FirstNet will receive significant feedback on technical issues and deployment considerations from these projects.

Standards and best practices will also play an important role in the evolution and integration of BBDS. The Third Generation Partnership Project (3GPP) is a global standards body that is actively engaged in the development of technical standards to support public safety mission critical services. The NPSBN's selected contractor will also determine to what extent various standards and capabilities are implemented on the network.

[43] Example: North Carolina TIC FOG https://www2.ncdhhs.gov/dhsr/EMS/pdf/ncticfog.pdf

[44] DHS OEC website for Technical Assistance Program: https://www.dhs.gov/oec-technical-assistance-program

[45] See the FirstNet website for additional information on early builder projects: http://www.firstnet.gov/search/node/FirstNet%20Early%20Builder%20Projects

Finally, there are a number of complex issues that must be addressed when BBDS cross border operations are contemplated. The U.S., Mexico and Canada each have specific laws and policies governing spectrum use and sharing and data privacy, and there are differences in which types of agencies are classified as public safety entities.

**The following public safety recommendations** were identified for BBDS based on the information in this chapter of the report:

| # | Recommendations |
|---|---|
| 13.A | BBDS deployment strategies SHALL include planning and consideration of all lanes of the SAFECOM interoperability continuum. |
| 13.B | BBDS design and configuration SHOULD be planned with neighboring countries to achieve the maximum possible level of interoperability. |
| 13.C | BBDS implementation SHOULD leverage best practices and lessons learned from FirstNet Early Builder programs and other users of this technology. |
| 13.D | BBDS capabilities and recommended procedures SHOULD be included in future versions of public safety communications planning documents at the national, state and local level. |
| 13.E | Gaps in standards impacting BBDS SHOULD be monitored and solutions advocated for by authorized representatives to 3GPP and other standards organizations. |

# Chapter 14: Conclusions and Recommendations

This chapter is designed to provide high-level conclusions and a set of basic recommendations regarding the provision of BBDS technology by the NPSBN operator and the use of BBDS technology by public safety agencies.

**Conclusions.** Following the review of multiple use cases and after discussion with public safety agency representatives, a number of conclusions have been identified regarding BBDS implementation:

1. Public safety agencies will require the NPSBN to include certain capabilities to extend the range, capacity, and delivery of mission critical services. This includes the provision of public safety broadband connectivity on an itinerant basis in a variety of settings (e.g., supplementing existing service, activating service in an area with no coverage, and access to disaster recovery services to restore the NPSBN network). [*Chapter 2: Public Safety Use of Deployable Systems)*

2. A broad range of BBDS solutions are required to meet the operational requirements of public safety agencies, including various form factors (e.g., backpack, vehicular, aerial, towed) and different levels of onboard technology (e.g., local area range extension, provision of mission critical applications, LMR/LTE interconnection, etc.). (*Chapter 3: BBDS Form Factor and Architecture)*

3. First responders will require a seamless transition of voice and data services, with no interruption in service, as they move between the NPSBN macro network and a connected BBDS,[46]as well as between a cluster of connected BBDS. (*Chapter 4: BBDS Network States)*

4. Public safety agencies also need access to mission critical voice, data, and video in a stand-alone environment in which the BBDS has no connection to the NPSBN macro network or remote services. (*Chapter 4: BBDS Network States*)

5. For BBDS to be effective it must provide mission critical services in the early stages of the incident. BBDS must therefore arrive quickly and support “ease of activation” to allow

[46] It is recognized that seamless transition is not possible in all instances, including transition from the NPSBN macro network to a BBDS operating in Stand Alone mode.

operation by first responders with minimal training.[47] (*Chapter 5: Deployment Considerations)*

6. Rapid activation of BBDS can only be accomplished if there are systems, policies, and technology in place to facilitate the coordination of key parameters that impact the inter-working between the BBDS and the NPSBN macro network.[48] (*Chapter 5: Deployment Considerations)*

7. First responders will require public safety broadband services at and across the international borders, which may require access to another country's NPSBN infrastructure, including BBDS. (*Chapter 6: International/Cross Border Considerations*)

8. First responders also require NPSBN voice, data, and video interoperability with public safety agencies in an adjoining country. (*Chapter 6: International/Cross Border Considerations)*

9. Secure and reliable backhaul connections linking the BBDS to the NPSBN macro network are critical [49] in order to support access to mission critical services and databases. (*Chapter 7: Role of Backhaul and Link Communications*)

10. Public safety agencies will require access to a minimum set of applications and services which are installed on the BBDS to support mission critical activities. This includes periods when the BBDS is disconnected from the NPSBN macro network. (*Chapter 8: Role of Applications)*

11. First responders require reliable access to Mission Critical Push-To-Talk when connected to a BBDS and loss of the backhaul connection to the NPSBN macro network must not compromise Push-to -Talk service with personnel at the incident scene. (*Chapter 9: Voice Considerations for Deployable Systems*)

12. Authorized first responder LTE devices must automatically connect to the Core-Enabled BBDS, even when they are isolated from the rest of the NPSBN, requiring exchange of the HSS (Home Subscriber Service) database records with the NPSBN macro network database. (*Chapter 10: Operations and Maintenance*)

[47] BBDS deployment should include a formal ordering process that details response and set up time. BBDS deployment should also accommodate the skill set of the user likely to be responsible for its operation.

[48] Examples include algorithms for Self-Organizing Network (SON) functions and interference control.

[49] Backhaul connectivity is not always possible and a BBDS may need to operate in Stand-Alone mode. See Conclusion #4.

13. When any connected or limited connection BBDS are deployed in the NPSBN network, the NPSBN network management team should be able to monitor and control them according to network policies, regardless of their provenance. (*Chapter 10: Operations and Maintenance*)

14. Given its itinerant deployment role, the BBDS must support a high level of security including physical security of the BBDS equipment (including server and database components), network security (including RAN and backhaul connections), and cyber security systems. (*Chapter 11: Deployable Systems Security and Assurance*)

15. Coordination of the configuration of Security Gateways on the BBDS and in the NPSBN is a key consideration. (*Chapter 11: Deployable Systems Security and Assurance*)

1. Full implementation of BBDS technology will require significant focus to resolve a number of technical challenges including interference management, inter-PLMNID handover, service continuity and session persistence, and management of ICAM/HSS databases. (*Chapter 12: Technical Considerations and Challenges*)

17. Successful adoption and implementation of BBDS must include attention to issues beyond the technology and should address all lanes of the SAFECOM Interoperability Continuum including governance, SOP, training and usage. (*Chapter 13: Operational Policy and Governance Considerations*)

18. BBDS capabilities and recommended procedures should be included in future versions of public safety communications planning documents at the national, state, and local level. (*Chapter 13: Operational Policy and Governance Considerations*)

**Recommended Next Steps.** The elements examined point to a number of basic recommendations involving the next steps in BBDS implementation. The high-level recommendations listed below establish a "path forward" for the implementation and use of BBDS. These steps are not listed in any priority order:

1. Following consultation with public safety agencies, NPSBN management and its operator must determine and articulate the role of BBDS technology, including rules regarding the licensing, procurement, and operation of these systems by local public safety agencies. Public safety agencies need to communicate their operational needs to the NPSBN operator through established channels and collaborate on the role that BBDS technology can fill. The NPSBN operator must provide nationally standardized guidance on the use of BBDS.

2. NPSBN management and its operator should prepare interoperability guidelines for BBDS due to the use of multi-vendor equipment and multi-agency governance of these systems.

Interoperability guidance should cover a number of technical issues, including IPsec configurations, OAM interfaces and protocols, configuration management, assignment of unique network identifiers, and IP address schemes among others. Public safety agencies need fully interoperable BBDS services during large-scale incidents which may necessitate the use of more than one BBDS. Technical and operational factors may be complicated with the introduction of multi-vendor equipment.

3. NPSBN management should ensure that network design and planning includes necessary components and strategies to allow for future successful usage of BBDS at and across the international border, ensuring that authorized first responders may access BBDS infrastructure from either country during an emergency. This recommendation acknowledges the need for spectrum management and policy coordination with the involved countries. The United States, Canada, and Mexico are all in the early stages of NPSBN deployment. Consideration of future interoperability should be a factor in the design of these networks, so as to not implement a technology solution that prevents this cooperation at a later date.

4. In order to ensure consistency and standardization of technology, NPSBN management should identify minimum mandatory requirements for BBDS in order to set the required level of interoperability between agencies and BBDS from different vendors. Public safety agencies need reliable broadband service from a BBDS to support mission critical activities. Interoperability between multiple first responder entities is also essential. These two capabilities may only be assured if BBDS procurement is standardized to ensure that necessary features and requirements are included in all BBDS systems.

5. Technical challenges with BBDS identified in this report should be evaluated by the Public Safety Communications Research (PSCR) Lab and other government organized or sponsored entities for validation. BBDS technology and product offerings are changing rapidly. Existing technical challenges may be overcome by the time this report is published, while new technical challenges will be introduced.

6. NPSBN management should place a high priority on mitigation of interference between the NPSBN Mode of Operation and BBDS Mode of Operation (either Connected, Stand-Alone, or Clustered). This applies within the FirstNet NPSBN, Canadian PSBN, and any locally operated BBDS. There are a variety of manual and automated processes to help manage interference between network nodes that have overlapping coverage. The reliability of NPSBN service and BBDS service is based on best practices to manage and minimize harmful interference.

7. During BBDS operation, a significant consideration involves the security of Data-at-Rest, meaning data resident onboard the BBDS that must be maintained in a highly safe and secure manner. This has physical security as well as data encryption components. A BBDS may house sensitive information, including registration and authentication data that must be protected from accidental or deliberate actions.

8. Additional research and public safety collaboration is needed to establish best practices for the provision of mission critical services via a BBDS. This includes an assessment of the impact of macro hosted mission critical services vs. BBDS local hosting of these services. Mission critical services include MC-PTT and other mission critical data applications deemed essential for incident response.

9. NPSBN management should support the evolution of 3GPP standards to enhance the capabilities of BBDS, including issues addressed in this report.

10. Work is needed to develop a nationwide standard for identification of LTE talkgroups and to address best practices for on-network usage (both macro network and BBDS) and off-network usage (direct mode).

11. Consideration should be given to update the National Incident Management System (NIMS) sections on Resource Typing to standardize the various form factors and capabilities of BBDS, providing uniformity during requests for service.

12. Further research and advocacy are needed regarding utilization of non-700 MHz spectrum to support backhaul from BBDS to the macro network and between BBDS operating in a cluster. There are a variety of other radio frequency bands that may be used to provide backhaul connectivity between the BBDS and the NPSBN macro network, including 4.9 GHz and other licensed spectrum.

13. Further research is needed regarding how to best manage the access and credentialing solution for BBDS, including how HSS database records are stored and secured on a local BBDS. First responders need rapid access to BBDS during an emergency incident and the BBDS may not yet be connected to the NPSBN macro network (or may be operating in Stand-Alone mode). Rapid access requires that credentialing data must be stored locally on the BBDS. There are a number of issues to resolve, including which records to store locally, and processes for the manual addition of new subscribers.

14. NPSBN management should place a high priority on development of strategies and solutions on effective management of the BBDS HSS database. In order for HSS databases to exchange information, it is necessary that the interface protocols and data models be

implemented the same way by all the parties that own the BBDS systems. This would likely require national guidance [34].

15. NPSBN management should continue to leverage knowledge gained from the Early Builder communities which are using BBDS technology. A number of trials are underway to examine how broadband LTE technology can support first responders. This includes the results and lessons learned from After Action Reports generated by public safety agencies following major incidents and events.

16. A set of Best Practices for the deployment of BBDS technology should be created to help ensure that the BBDS solution matching the needs of the incident is dispatched at the right time. There may be more than one BBDS in a region that can support public safety. First responders will need guidance on how to select the best BBDS solution based on mission requirements.

# LIST OF APPENDICES


APPENDIX A: Operational Capabilities List

APPENDIX B: Technical Challenges Chart

APPENDIX C: Use Cases

APPENDIX D: Deployable Systems Incident Commander Checklist

APPENDIX E: Working Group and Contributor List

APPENDIX F: Bibliography

APPENDIX G: Terminology and Definitions

APPENDIX H: Detailed Diagrams

# APPENDIX A: Operational Capabilities List

Fifty-four operational capabilities were identified throughout the various use cases created to examine BBDS deployments. These capabilities formed the basis for the public safety requirements identified in this report and helped define a number of technical challenges. This list includes all of the capabilities, including those which are noted to have technical challenges associated with them (see Chapter 12).

1. First responders from different jurisdictions can authenticate on more than one in range BBDS deployed at an incident scene.

2. First responders connected to the public safety broadband network domain can participate in talkgroups with other users, some of whom are in the public safety broadband network domain and others in the LMR network domains.

3. First responders are able to connect through the BBDS to remote facilities including PSAPs, hospitals, EOCs, Fusion Centers, etc.

4. First responders from different jurisdictions can authenticate on BBDS used by other agencies. During an incident, personnel from other areas (counties, localities) should be able to authenticate on the deployable systems in use.

5. The first responders' voice and data sessions remain active during the handover of service between a BBDS and the NPSBN macro network with no noticeable degradation of service.

6. First responders can use BBDS to access or upload information that must be protected for confidentiality, privacy, and integrity, according to security policies of the operator of the NPSBN.

7. An authorized administrator of the public safety enterprise network is able to control access to the local application functions of the BBDS by the first responders.

8. First responders from the U.S. and Canada may authenticate on the BBDS of the other country and access local information networks.

9. An authorized network administrator is alerted if a denial of service attack is detected at the radio interface level of the BBDS.

10. First responders in the vicinity of two emergency vehicles that both contain BBDS can communicate wirelessly using either BBDS.

11. Public safety agencies, including PSAPs, may use the BBDS connectivity to manage applications that track the location of first responders, receive sensor data, and transmit voice and data information.

12. Users along the Canada-U.S. border can be served by BBDSs or macro PSBN sites on either side of the border and be able to access their information networks.

13. COML, or other trained personnel, can introduce Core-Ready BBDS into an existing network of BBDS with minimum human intervention.

14. First responders are able to connect to their agency information networks from any location in and around the building that is served by the BBDS or the in-building system.

15. The first responders' voice and data sessions remain active during the handover of service between the indoor serving network and the outdoor BBDS with no noticeable degradation of service.

16. First responders are able to use their UE devices for voice communications carried over a WiFi radio access network in the absence of LTE coverage from the BBDS.

17. First responders are able to experience similar priority and QoS treatment when they are connected to a WiFi network as when they are connected to the BBDS' LTE radio access network.

18. The first responders' voice and data sessions remain active during the hand-over of service between the BBDS' LTE domain and the Wi-Fi domain with no noticeable degradation of service.

19. The First Responders' voice and data sessions remain active during the handover of service between the UE-to-BBDS connected state and the UE- UE relay connected state, or the UE-network relay state.

20. First responders are able to communicate with other users in their assigned talkgroups when all or some of the users, in any combination, are connected to the macro network, the deployable system, or in device-to-device mode.

21. First responder’s communications sessions will maintain the Quality of Service Priority and Preemption (QPP) levels during the handover processes between the NPSBN macro network and the BBDS.

22. First responders encrypted communications sessions will maintain session persistence during the handover of service from the macro network to the deployable system, deployable system to device-to-device, and vice-versa.

23. First responders unencrypted communications sessions will maintain session persistence during the handover of service from the macro network to the deployable system, deployable system to device-to-device, and vice-versa.

24. First responders are notified when their communications sessions toggle from encrypted to unencrypted communications, and vice-versa.

25. First responders are able to know which other users they can communicate with when in device-to-device connected mode.

26. First responders are able to communicate with authorized users from other jurisdictions (local, mode/provincial, territorial, federal, international) in device-to-device connected mode.

27. First responders are able to communicate with users outside the incident area when they are connected in device-to-device mode.

28.First responders using direct mode communications can establish ad hoc communication with other user devices that are not preconfigured in the same manner (e.g., access a common interoperable LTE talkgroup)

29. The First responders' voice and data sessions remain active during the handover of service from one BBDS to the other with no noticeable degradation of service.

30. First responders and their support teams can receive information on the status of the incident, (e.g., the Common Operating Picture)

31. First responders are able to bring BBDS to incidents by different means of transport such as over paved roads, by 4x4 vehicles, air-drop, and hand-carry.

32. First responders operating on a BBDS are able to exchange data at broadband speeds in the absence of backhaul to the Internet or to remote information networks.

33. First responders can exchange data at broadband speeds on a one-to-one basis or one-to-many basis within the area served by the isolated BBDS.

34. First responders in manned aerial platforms can receive broadband service from terrestrial BBDS.

35. An authorized network administrator is able to assert suitable controls to mitigate a denial of service attack at the BBDS radio interface level.

36. First responders in the vicinity of an emergency vehicle that contains a BBDS can communicate wirelessly using that BBDS.

37. Sensors (machines) in the vicinity of an emergency vehicle that contains a BBDS can transmit and receive data wirelessly using that BBDS.

38. Sensors (machines) in the vicinity of two emergency vehicles that both contain BBDS can transmit and receive data wirelessly using either BBDS.

39. First responders can determine the quality of service that their devices are receiving from the BBDS.

40. First responders can turn up a Core-Ready BBDS with minimal intervention and with minimal support from specialized technical resources.

41. First responders can turn up a Core-Enabled BBDS with some support from specialized technical resources, depending on the complexity of the BBDS.

42. First responders are able to connect to their information networks from any location that is served by BBDS.

43. First responders are able to transition from the coverage area of one BBDS to that of any other BBDS without having to re-initiate the session or re-authenticate during the handover.

44. First responders are able to engage in one-to-one and group voice communications when connected to a BBDS.

45. Authorized administrators can exercise local monitoring and control actions on vehicular BBDS.

46. First responders are able to engage in voice communications with each other when connected to either the LTE network or the WiFi network, regardless of which access network they are connected to.

47. The first responders' voice communications session or the emergency alert notification is not interrupted when users transition between the UE-to-BBDS connected state and the UE-UE relay connected state, or the UE-network relay state.

48. First responders are able to communicate with other users when they are connected via the deployable system or the macro network. Communication services may include voice, video, and data.

49. First responders are able to maintain active communication sessions with other users in their assigned talk groups when users are randomly transiting to and from macro, BBDS, and device-to-device connection modes

50. First responders are notified if their devices are disconnected from a serving network and transitioned to device-to-device mode.

51. First responders are notified of network availability while operating in direct mode.

52. Agency administrators can select the manner by which their first responders are notified for the different connected modes as well as a totally disconnected mode (e.g., visual, audible, or tactile).

53. First responders can control their LTE device to operate in either device-to-device mode (i.e., off-net mode) or network connected mode (i.e., on-net mode).

54. First responders are able to engage in one-to-one or one-to-many for PTT voice.

# APPENDIX B: Technical Challenges Chart

This chart includes a listing of all operational capabilities in which an associated technical challenge was identified.

| Operational Capability | Technical Challenges |
|---|---|
| 1. An aerial BBDS SHALL be capable of coordinating with the terrestrial macro NPSBN to minimize mutual interference. | a) Tethered aerial platform: no significant technical challenges.<br><br>b) Untethered stationary aerial platform: no significant technical challenges.<br><br>c) Moving aerial platform: maintaining high-speed, low-latency connectivity between the NPSBN macro network and the aerial BBDS over its operating range. |
| 2. First responders from different jurisdictions can authenticate on more than one in range BBDS deployed at an incident scene. First responders from different jurisdictions can authenticate on BBDS used by other agencies. During an incident, personnel from other areas (counties, localities) should be able to authenticate on the deployable systems in use. | a) Connected mode: no significant technical challenges.<br><br>b) Limited connected mode: no significant technical challenges if using the HSS from the macro network.<br><br>c) Disconnected mode: provisioning the services (device keys, subscriber data, etc.) on a local HSS for the subscribers that need to be served at the incident; securing the HSS. |
| 3. First responders' voice and data sessions remain active during the handover of service between a BBDS and the NPSBN macro network with no noticeable degradation of service.<br><br>Assume that coverage of BBDS partially overlaps with NPSBN. | a) Connected mode: no significant technical challenges if the eNBs pertain to same PLMN.<br><br>b) Connected mode, Core-Enabled BBDS and macro network pertain to different PLMNs:<br><br>(i) if possible to use only the eNB of the BBDS: technical interoperability challenges for IPsec at S1, network IDs and IP addresses, OAM, etc.; BBDS eNB must broadcast PLMN ID of the macro network.<br><br>(ii) if application servers of BBDS are to be used as well as macro network application servers: S10 must be interconnected between the MMEs; all devices must be configured with all implicated PLMN IDs in |

| | |
|---|---|
| | the Equivalent-to-Home PLMN list.<br><br>c) Disconnected mode (no interconnection with macro network): no service continuity is possible.<br><br>d) Limited connectivity between the Core-Enabled BBDS and the macro core network: insufficient bandwidth in the backhaul to support user plane traffic. Sessions will end. It may not be possible to re-establish sessions with application servers of the network to which the UE was previously registered.<br><br>e) ARP and QCI settings must be the same in both systems. |
| 4. An authorized administrator of the public safety enterprise network is able to control access to the local application functions of the BBDS by the first responders. | a) Connected mode: no significant technical challenges.<br><br>b) Limited connected mode: no significant technical challenges<br><br>c) Disconnected mode:<br><br>(i) if authorized administrator is remote to the BBDS: only pre-configured permissions are possible. Dynamic assignment or revocation of permissions is not possible to do.<br><br>(ii) if authorized administrator is local to the BBDS: no significant technical challenges. |
| 5. First responders from the U.S. and Canada may authenticate on the BBDS of the other country and access local information networks. | a) Connected mode: no significant technical challenges<br><br>b) Limited connected mode: no significant technical challenges.<br><br>c) Disconnected mode: technical challenge associated with locally provisioning the UE devices to operate on the other country's BBDS, and granting access privileges for the local (to the BBDS) information networks. |
| 6. An authorized network administrator is alerted if a denial of service attack is detected at the radio interface level of the | No mechanism in LTE can do this. |

| | |
|---|---|
| BBDS. | |
| 7. First responders in the vicinity of two emergency vehicles that both contain BBDS can communicate wirelessly using either BBDS. | a) Connected mode: no significant technical challenges. eICIC could be used to minimize interference.<br><br>b) Limited connected mode: A UE may attach to the strongest source BBDS, but it would not be possible to dynamically optimize the interference environment at the areas of coverage overlap. A user attached to one BBDS may not be able to communicate with a user attached to the other BBDS. If both users are attached to the same BBDS they can communicate with each other.<br><br>c) Disconnected mode: same as (b). |
| 8. Users along the Canada-U.S. border can be served by BBDSs or macro PSBN sites on either side of the border and be able to access their information networks. | Introducing a BBDS from one PLMN into an area that is served by a BBDS or the macro network of the other country may create interference issues. It can be mitigated by connecting the inserted BBDS into the network that receives it and enabling interference control mechanisms. The tech challenge for interference mitigation is to provide local interconnection of the BBDS to the adjoining eNBs of the other network since interference control requires low latency and high bandwidth connection.<br><br>The capability would not be achievable in disconnected mode. |
| 9. COML, or other trained personnel, can introduce Core-Ready BBDS into an existing network of BBDS with minimum human intervention. | The Core-Ready BBDS must be connected with the adjoining BBDS. Tech challenge will be to establish such connectivity. Ad hoc deployments of BBDS could most readily be accommodated by a wireless backhaul – either microwave or satellite. Multiple nodes of BBDS would significantly complicate the microwave backhaul option. Satellite backhaul introduces high latency for interference control. The latency could also impact the closed-loop operation of SON algorithms. Another backhaul option is to use the UE Relay function. But this reduces the |

| | |
|---|---|
| | available capacity of the radio resources.<br><br>SON function should be enabled and previously verified to operate with all the implicated BBDS. This presents a considerable challenge to manage interoperability over time with a changing pool of qualified BBDS equipment and vendors. |
| 10. First responders are able to connect to their agency information networks from any location in and around the building that is served by the BBDS or the in-building system. | a) The in-building communications system is connected to the BBDS system: no significant technical challenge<br><br>b) No connection between the in-building system and the BBDS: not possible to reach the agency information networks from both systems. |
| 11. First responders are able to experience similar priority and QoS treatment when they are connected to a WiFi network as when they are connected to the BBDS' LTE radio access network. | a) The WiFi network is not HotSpot2 or NextGen HotSpot: the capability is not possible to achieve.<br><br>b) Technical challenges are:<br><br>(i) mapping of QoS parameters (QCI) onto the relevant Differentiated Services Code Point (DSCP) value to be used in the transport layer;<br><br>(ii) mapping LTE QoS parameters to the Wi-Fi QoS parameters (Wi-Fi Multimedia Extensions)<br><br>Mapping must be done a priori and all implicated systems must be configured to support the QoS mapping. |
| 12. First responders' voice and data sessions remain active during the hand-over of service between the BBDS' LTE domain and the Wi-Fi domain with no noticeable degradation of service. | a) The WiFi network is not HotSpot2 or NextGen HotSpot: the capability is not possible to achieve.<br><br>b) The WiFi system and the BBDS are not connected: the capability is not possible to achieve.<br><br>c) Ensuring that the Core-Enabled BBDS is equipped with the necessary functions that allow WiFi-LTE roaming (Automatic Network Discovery and Selection Function, AAA server, |

| | |
|---|---|
| | etc.).<br><br>d) Ensuring that the WiFi network is equipped with a AAA proxy server.<br><br>e) Ensuring that S2-based Mobility over GPRS Tunneling Protocol (SaMOG) is supported in the BBDS.<br><br>f) For un-trusted WiFi: the capability is not supported by current standards. |
| 13. First responders' voice and data sessions remain active during the handover of service between the UE-to-BBDS connected state and the UE- Relay Node connected state, or the UE-network relay state. | a) Relay Node and UE-Network Relay are synchronized with the BBDS: no significant technical challenge.<br><br>b) Relay Node and UE-Network Relay are not synchronized with the BBDS at time of the handover: the capability would not be supported. |
| 14. First responders are able to communicate with other users in their assigned talk groups when all or some of the users, in any combination, are connected to the macro network, the deployable system, or in device-to-device mode. | a) Significant technical challenges to include isolated UEs in the same talkgroups as those UEs connected to the macro network or the BBDS.<br><br>b) BBDS and macro network are connected: no significant technical challenges for UEs connected to either system to participate in the same talkgroup.<br><br>c) Multicast must be supported in direct mode. |
| 15. First responders encrypted communications sessions will maintain session persistence during the handover of service from the macro network to the deployable system, deployable system to device to device, and vice-versa. | a) BBDS connected to macro network: no significant technical challenges.<br><br>b) Limited connection or no connection: the capability is not supported.<br><br>c) ProSe Key Management server in the macro network is not synchronized with the ProSe Key Management server in the Core-Enabled BBDS: high risk of incompatible encryption between UEs.<br><br>d) If MVPN is used as an additional encryption layer: technical challenge is ensuring that all the VPN clients at the incident are associated |

| | |
|---|---|
| | with the same VPN server. |
| 16. First responders unencrypted communications sessions will maintain session persistence during the handover of service from the macro network to the deployable system, deployable system to device to device, and vice-versa. | a) BBDS connected to macro network: no significant technical challenges.<br><br>b) Limited connection or no connection: the capability is not supported.<br><br>c) ProSe Key Management server in the macro network is not synchronized with the ProSe Key Management server in the Core-Enabled BBDS: high risk of incompatible encryption between UEs. |
| The following technical challenges were noted regarding how a BBDS may support Pro Se direct mode communications. | |
| 17. First responders are able to communicate with authorized users from other jurisdictions (local, mode/provincial, territorial, federal, international) in device-to-device connected mode. | ProSe application clients are configured from different ProSe function servers: technical challenge to synchronize the ProSe function servers.<br><br>ProSe servers in the BBDS and the macro network would have to be synchronized before the UEs disconnected in order for the UEs from different jurisdictions to establish D2D communications |
| 18. First responders are able to communicate with users outside the incident area when they are connected in device-to-device mode. | a) No UE-Network relay is within the communications range of any of the isolated UEs: the capability would not be supported.<br><br>b) WiFi Direct: significant technical challenges to realize the capability. |
| 19. First responders using direct mode communications can establish ad hoc communication with other user devices that are not preconfigured in the same manner (e.g., access a common interoperable LTE talkgroup) | a) ProSe: this capability would not be supported.<br><br>b) WiFi Direct: UE devices capable of communicating directly with each other using WiFi Direct would be able to establish direct-mode communications without pre-configuration. MC-PTT would not be supported. |

# APPENDIX C: Use Cases

The use cases listed in this appendix were created by the Working Group to review operational considerations for Broadband Deployable Systems and to facilitate discussion on operational, technical, and standards issues.

These use cases are not meant to represent the complete list of capabilities, features, or uses of BBDS technology. These should be viewed in the context in which they were created, to provide a platform for discussion among Working Group members.

## Use Case 1: Wildland Fire in Isolated Area

**Baseline Use Case Description**: [This is a narrative of the use case that exemplifies how the deployable systems are expected to be used.]

Lightning has ignited a fire in a remote forested region. The weather conditions and state of the fire indicate a potential threat to power generation facilities, recreational sites, and natural resource extraction operations. The containment zone is estimated to be 2500 hectares. Deployable systems (DS) are required to deliver broadband communications to firefighters and support teams due to lack of existing PSBN and commercial wireless infrastructure.

Study of topographic maps shows two deployable LTE/LMR systems with 30m/100ft telescopic masts can provide 95% coverage to the planned operating zone. Planners propose three possible sites for each of the two locations, both of which are reachable by broadband satellite. Both locations have line-of-sight between them with sufficient clearance to establish a high-capacity microwave link. Both locations have minimal fire hazard risk within the foreseeable weather prediction horizon.

Fire crews use ruggedized broadband communications devices to receive situational awareness on weather conditions, fire line movement, temperature and hot spot data, location of fire crews and planned water bomber drops, location of food and supply caches, etc. The fire crews also use the broadband devices to upload information to the data fusion center and to participate in video conferencing sessions. Water bomber crews receive the common operational picture (COP) and upload data to the data fusion center. Land mobile radios are used for voice communications according to the established communications protocol.

As fire crews move from one sector to another they remain in contact with the Incident Command Centre and continue to receive COP updates from the data fusion center.

**Actors**: [This is list of the participants in the use case and their role.]

1. Firefighters
2. Incident command team
3. Communications specialists
4. Logistics support team
5. Water bomber crews
6. Air traffic controllers

**Pre-Conditions**: [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- Road access to the fire zone is sparse. Airlift is necessary to access key locations. Local power and telecommunications services are generally not available.
- The fire zone is not near the Canada-USA border. Mutual aid is from neighboring jurisdictions but is not international.
- Both DS are sourced from the same vendor and are identically configured at the time of deployment.
- The throughput of the satellite channel does not present a bottleneck for traffic that is backhauled.
- Both DS are configured with the same PLMN ID.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- Emergency responders from different jurisdictions can authenticate on both DS.
- The bearer sessions are persistent during the handover from one DS to the other.
- The emergency responders are authorized to connect to the data fusion center.
- The DS can be turned up with minimal human intervention.
- The broadband devices can participate in talk groups with LMR users.
- The COP is broadcast to all emergency responders and support teams.

**Parameters**

**Users and Devices**[50]

| User, Device | Location |
|---|---|
| Fire crews: a) handheld ruggedized broadband communications devices; b) vehicular broadband modems; c) land mobile radios. | Incident area |
| Water bomber crews: a) airborne data terminals; b) multiband radio terminal. | Water bomber aircraft |
| Incident command team: a) broadband | Incident Command Post |

[50] In this table, list the users and devices with their status relative to the location of the incident described (i.e. within the incident area, Emergency Operations Center, tactical command center, shipborne, airborne, etc.)

| | |
|---|---|
| communications devices; b) land mobile radios; c) access to other communications not pertinent to deployable systems. | |

### Type of Data[51]

| Data Source | Type |
|---|---|
| Data collected from unmanned sensors | TCP/IP |
| Video streams from portable devices | RTSP |
| COP | Interactive |
| Digital audio | UDP |
| Still images | TCP/IP |

### Data Sensitivity[52]

| Data Source | Sensitivity |
|---|---|
| Data collected from unmanned sensors | Some may be confidential; other info may be made public. |
| Video streams from portable devices | Some may be confidential; other info may be made public. |
| COP | Confidential |
| Digital audio | Confidential |

[51] List all of the information transmitted in the use case and what type it is, (i.e., bulk files, database info, interactive, etc.)

[52] This table should list the data sources and the sensitivity of the data, i.e., medical information, criminal information, secret, etc.

## Use Case 1 A: Wildland Fire in Isolated Area

**Variant A: No connection between deployable systems**

**Description**: [This is a narrative of the use case that exemplifies how the deployable systems are expected to be used.]

Lightning has ignited a fire in a remote forested region. The weather conditions and state of the fire indicate a potential threat to power generation facilities, recreational sites, and natural resource extraction operations. The containment zone is estimated to be 2500 hectares. Deployable systems (DS) are required to deliver broadband communications to firefighters and support teams due to lack of existing PSBN and commercial wireless infrastructure.

Study of topographic maps shows two deployable LTE/LMR systems with 30m/100ft telescopic masts can provide 95% coverage to the planned operating zone. Planners propose three possible sites for each of the two locations, both of which are reachable by broadband satellite. Both locations have minimal fire hazard risk within the foreseeable weather prediction horizon.

Fire crews use ruggedized broadband communications devices to receive situational awareness on weather conditions, fire line movement, temperature and hot spot data, location of fire crews and planned water bomber drops, location of food and supply caches, etc. The fire crews also use the broadband devices to upload information to the data fusion center and to participate in video conferencing sessions. Water bomber crews receive the common operational picture (COP) and upload data to the data fusion center. Land mobile radios are used for voice communications according to the established communications protocol.

As fire crews move from one sector to another they remain in contact with the Incident Command Centre and continue to receive COP updates from the data fusion center.

**Actors**: [This is list of the participants in the use case and their role.]

1. Firefighters
2. Incident command team
3. Communications specialists
4. Logistics support team
5. Water bomber crews
6. Air traffic controllers

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- Road access to the fire zone is sparse. Airlift is necessary to access key locations. Local power and telecommunications services are generally not available.
- The fire zone is not near the Canada-USA border. Mutual aid is from neighboring jurisdictions but is not international.
- Both DS are sourced from the same vendor and are identically configured at the time of deployment.
- The throughput of the satellite channel does not present a bottleneck for traffic that is backhauled.
- Both DS are configured with the same PLMN ID.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- Emergency responders from different jurisdictions can authenticate on either DS.
- The bearer sessions are persistent during the handover from one DS to the other.
- The emergency responders are authorized to connect to the data fusion center.
- The DS can be turned up with minimal human intervention.
- The broadband devices can participate in talkgroups with LMR users.
- The COP is broadcast to all emergency responders and support teams.

**Parameters**

**Users and Devices**

| User, Device | Location |
|---|---|
| Fire crews: a) handheld ruggedized broadband communications devices; b) vehicular broadband modems; c) land mobile radios. | Incident area |
| Water bomber crews: a) airborne data terminals; b) multiband radio terminal. | Water bomber aircraft |
| Incident command team: a) broadband communications devices; b) land mobile radios; c) access to other comms not pertinent to deployable systems. | Incident Command Post |

### Type of Data

| Data Source | Type |
|---|---|
| Data collected from unmanned sensors | TCP/IP |
| Video streams from portable devices | RTSP |
| COP | Interactive |
| Digital audio | UDP |
| Still images | TCP/IP |

### Data Sensitivity

| Data Source | Sensitivity |
|---|---|
| Data collected from unmanned sensors | Some may be confidential; other info may be made public. |
| Video streams from portable devices | Some may be confidential; other info may be made public. |
| COP | Confidential |
| Digital audio | Confidential |
| Still images | Some may be confidential; other info may be made public. |

## Use Case 1 B: Wildland Fire in Isolated Area

**Variant B: No connection between deployable systems. Deployable systems are sourced from different vendors.**

**Description:** [This is a narrative of the use case that exemplifies how the deployable systems are expected to be used.]

Lightning has ignited a fire in a remote forested region. The weather conditions and state of the fire indicate a potential threat to power generation facilities, recreational sites, and natural resource extraction operations. The containment zone is estimated to be 2500 hectares. Deployable systems (DS) are required to deliver broadband communications to firefighters and support teams due to lack of existing PSBN and commercial wireless infrastructure.

Study of topographic maps shows two deployable LTE/LMR systems with 30m/100ft telescopic masts can provide 95% coverage to the planned operating zone. Planners propose three possible sites for each of the two locations, both of which are reachable by broadband satellite. Both locations have minimal fire hazard risk within the foreseeable weather prediction horizon.

Fire crews use ruggedized broadband communications devices to receive situational awareness on weather conditions, fire line movement, temperature and hot spot data, location of fire crews and planned water bomber drops, location of food and supply caches, etc. The fire crews also use the broadband devices to upload information to the data fusion center and to participate in video conferencing sessions. Water bomber crews receive the common operational picture (COP) and upload data to the data fusion center. Land mobile radios are used for voice communications according to the established communications protocol.

As fire crews move from one sector to another they remain in contact with the Incident Command Centre and continue to receive COP updates from the data fusion center.

**Actors:** [This is list of the participants in the use case and their role.]

1. Firefighters
2. Incident command team
3. Communications specialists
4. Logistics support team
5. Water bomber crews
6. Air traffic controllers

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- Road access to the fire zone is sparse. Airlift is necessary to access key locations. Local power and telecommunications services are generally not available.
- The fire zone is not near the Canada-USA border. Mutual aid is from neighboring jurisdictions but is not international.
- Both DS are sourced from different vendors.
- The throughput of the satellite channel does not present a bottleneck for traffic that is backhauled.
- Both DS are configured with the same PLMN ID.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- Emergency responders from different jurisdictions can authenticate on both DS.
- The bearer sessions are persistent during the handover from one DS to the other.
- The emergency responders are authorized to connect to the data fusion center.
- The DS can be turned up with minimal human intervention.
- The broadband devices can participate in talkgroups with LMR users.
- The COP is broadcast to all emergency responders and support teams.

**Parameters**

**Users and Devices**

| User, Device | Location |
|---|---|
| Fire crews: a) handheld ruggedized broadband communications devices; b) vehicular broadband modems; c) land mobile radios. | Incident area |
| Water bomber crews: a) airborne data terminals; b) multiband radio terminal. | Water bomber aircraft |
| Incident command team: a) broadband communications devices; b) land mobile radios; c) | Incident Command Post |

| | |
|---|---|
| access to other communications not pertinent to deployable systems. | |

### Type of Data

| Data Source | Type |
|---|---|
| Data collected from unmanned sensors | TCP/IP |
| Video streams from portable devices | RTSP |
| COP | Interactive |
| Digital audio | UDP |
| Still images | TCP/IP |

### Data Sensitivity

| Data Source | Sensitivity |
|---|---|
| Data collected from unmanned sensors | Some may be confidential; other info may be made public. |
| Video streams from portable devices | Some may be confidential; other info may be made public. |
| COP | Confidential |
| Digital audio | Confidential |
| Still images | Some may be confidential; other info may be made public. |

## Use Case 1 C: Wildland Fire in Isolated Area

**Variant C: No connection between deployable systems. Deployable systems are sourced from different vendors. Satellite backhaul is not available.**

Description: [This is a narrative of the use case that exemplifies how the deployable systems are expected to be used.]

Lightning has ignited a fire in a remote forested region. The weather conditions and state of the fire indicate a potential threat to power generation facilities, recreational sites, and natural resource extraction operations. The containment zone is estimated to be 2500 hectares. Deployable systems (DS) are required to deliver broadband communications to fire fighters and support teams due to lack of existing PSBN and commercial wireless infrastructure.

Study of topographic maps shows two deployable LTE/LMR systems with 30m/100ft telescopic masts can provide 95% coverage to the planned operating zone. Planners propose three possible sites for each of the two locations, both of which are not reachable by broadband satellite services. Both locations have minimal fire hazard risk within the foreseeable weather prediction horizon.

Land mobile radios are used for voice communications according to the established communications protocol. Notwithstanding the absence of backhaul to the Internet or to remote information networks, users are nonetheless able to exchange some data between them. Typically, this data would be text messages, streaming video, and still images. Location information and vital signs of fire fighters are also exchanged.

**Actors:** [This is list of the participants in the use case and their role.]

1. Firefighters
2. Incident command team
3. Communications specialists
4. Logistics support teams

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- Road access to the fire zone is sparse. Airlift is necessary to access key locations. Local power and telecommunications services are generally not available.
- The fire zone is not near the Canada-USA border. Mutual aid is from neighboring jurisdictions but is not international.

- Both DS are sourced from different vendors.
- Both DS are configured with the same PLMN ID.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- Emergency responders from different jurisdictions can authenticate on both DS.
- The bearer sessions are persistent during the handover from one DS to the other.
- The DS can be turned up with minimal human intervention.
- The broadband devices can participate in talkgroups with LMR users.
- The COP is broadcast to all emergency responders and support teams.
- The network of DS is able to scale to support from 10s to 1,000s of users.
- The DS must be usable in different types of terrain – accessible by paved roads, by 4x4 vehicles, by air-drop, and hand-carried.
- The DS must allow users to exchange data at broadband speeds between them in the absence of backhaul to the Internet or to remote information networks.
- Users can exchange data at broadband speeds on one-to-one basis or one-to-many basis within the area served by the isolated DS.

**Parameters**

**Users and Devices**

| User, Device | Location |
|---|---|
| Fire crews: a) handheld ruggedized broadband communications devices; b) vehicular broadband modems; c) land mobile radios. | Incident area |
| Delete row | |
| Incident command team: a) broadband communications devices; b) land mobile radios; c) access to other communications not pertinent to deployable systems. | Incident Command Post |

**Type of Data**

| Data Source | Type |
|---|---|
| Data collected from unmanned sensors | TCP/IP |
| Video streams from portable devices | RTSP, SCTP |
| COP | Interactive |
| Digital audio | UDP |
| Still images | TCP/IP |
| Text messages | TCP/IP |
| Location information | TCP/IP |
| Vital signs information | TCP/IP |

**Data Sensitivity**

| Data Source | Sensitivity |
|---|---|
| Data collected from unmanned sensors | Some may be confidential; other info may be made public. |
| Video streams from portable devices | Some may be confidential; other info may be made public. |
| COP | Confidential |
| Digital audio | Confidential |
| Still images | Some may be confidential; other info may be made public. |
| Text messages | Confidential |
| Location information | Confidential (not for public disclosure). |
| Vital signs information of fire fighters | Confidential (not for public disclosure). |

## Use Case 2: Sporting Event in Urban Area

**Baseline use case**

**Description:** [This is a narrative of the use case that exemplifies how the deployable systems are expected to be used.]

A stadium-class sporting event elicits strong feelings between fans of opposing teams. Spurred on by a few instigators, rioting crowds engage in violence while also causing extensive property damage. Public safety personnel need to contain those fans who are committing crimes, expedite the evacuation and clearing of the stadium, identify and rescue injured persons, and gather information to develop a full situational awareness of the entire incident.

Deployable systems (DS) are brought in from their staging areas to pre-determined locations around the stadium in order to have additional broadband capacity serving the emergency responders. Deployables are being used to enhance the capacity of existing on-site systems that are not likely able to support the number of public safety users.

In order to augment the fixed coverage around the stadium external deployable vans with 40-foot masts are positioned at five locations. One van acts as the incident command and data fusion vehicle, and the others are used as eNBs. A previously installed fiber backhaul connection is available to the IC van and all others link to it using short range microwave.

The external vehicles have access to all security camera feeds throughout the stadium. Based on decisions from the incident commander, selected feeds may be passed on to public safety personnel who are using tablets and small wearable cameras. This capability allows real-time video streaming of any incidents occurring inside and outside the stadium. Voice capability is available through the same network, and public safety personnel can also be patched to stadium security officials using voice applications.

**Actors:** [This is list of the participants in the use case and their role.]

1. Law enforcement personnel
2. National security personnel
3. Incident command team
4. Communications specialists
5. Logistics support team
6. Stadium support staff

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- Stadium existing communications consist of active and passive Distributed Antenna Systems (DAS) for commercial cellular, public safety broadband, and land mobile radio (LMR). There are WiFi access points throughout the stadium.
- All DS are sourced from the same vendor and are identically configured at the time of deployment.
- All DS are configured with the same PLMN ID.
- Sites for deployable systems are pre-determined and pre-configured to be able to interface with the stadium security command center.
- All DS are backhauled to the core fabric EPC.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- Emergency responders from different jurisdictions can authenticate on all DS. During the incident personnel from other areas (counties, localities) should be able to authenticate on all deployable systems.
- The bearer sessions are persistent during the handover from one DS to the other and from any DS to any Public Safety Macro. Sessions should be handed off and maintained.
- The emergency responders are authorized to connect to the data fusion center.
- The DS can be turned up with minimal human intervention.
- The broadband devices can participate in talk groups with LMR users.
- The COP is broadcast to all emergency responders and support teams.

**Parameters**

**Users and Devices**

| User, Device | Location |
|---|---|
| LE personnel: a) handheld ruggedized broadband communications devices; wearable cameras | Incident area |
| Incident command team: a) broadband communications devices; b) land mobile radios; c) access to other communications not pertinent to deployable systems. | Incident Command Post |

| | |
|---|---|
| Stadium support personnel: a) FM handheld radio systems – voice only | Stadium |

**Type of Data**

| Data Source | Type |
|---|---|
| Data collected from unmanned sensors | TCP/IP |
| Video streams from portable devices | RTSP |
| COP | Interactive |
| Digital audio | UDP |
| Still images | TCP/IP |

**Data Sensitivity**

| Data Source | Sensitivity |
|---|---|
| Data collected from unmanned sensors | Some may be confidential; other info may be made public. |
| Video streams from portable devices | Some may be confidential; other info may be made public. |
| COP | Confidential |
| Digital audio | Confidential |
| Still images | Some may be confidential; other info may be made public. |

## Use Case 3: Visit of Senior U.S. Government Officials to Canada

**Description**: [This is a narrative of the use case that exemplifies how the deployable systems are expected to be used.]

Senior U.S. government officials are visiting Canada for a security summit and they are accompanied by a number of senior Canadian officials. The U.S. delegation includes U.S. Secret Service agents and VIPs. Canadian and U.S. security agents are responsible for security for the VIPs and their entourage. Unless stated otherwise, all U.S. and Canadian personnel responsible for security are collectively termed "officers." The delegation will travel by road from Ottawa, Ontario, to Montebello, Quebec.

A mobile command center (MCC) has been set up and is part of the convoy of vehicles. A helicopter that is assigned to track the convoy is equipped with a UE, which acts as the point of presence for on-board sensors and video cameras. It also provides access to broadband communications for agents on board the helicopter. Land-based PSBN deployable systems are located outside the meeting venue in Montebello. Small cells that are part of the PSBN are located inside the meeting venue.

The MCC receives live video streams from aerial surveillance platforms, as well as from fixed locations and from tactical cameras. The video streams are uploaded to a server at a Canadian secure facility which hosts facial recognition analytics for possible identification of persons of interest. By agreement, the video feeds are also sent to servers in the U.S. for facial recognition against U.S. databases of persons of interest. The video feeds are accessible by all the authorized officers on the ground, including U.S. officers.

The MCC can assign authority to any officer to control the PTZ functions of any camera. The camera control application would prevent more than one person from controlling the same camera at the same time.

The handheld broadband devices and vehicle-mounted devices are reporting position information of the officers and their vehicles. The MCC hosts a Blue Force Tracking application and the location and identity of all the officers is accessible by the officers on their handheld devices and mobile data terminals.

The facial recognition software returns a hit. The last location of the person of interest and the photo of the person is sent to all officers. The MCC issues orders by way of text and multimedia messages to specific agents with tasking to investigate and intercept.

The MCC detects a denial of service attack at the air-interface by way of RF interference in the operating band of the PSBN. The MCC initiates action to maintain communications with officers, and to identify and remove the source of the RF interference.

**Actors:** [This is list of the participants in the use case and their roles.]

1. U.S. Secret Service agents
    - Provide security for the US delegation.

2. Canadian security agents, RCMP
    - Provide security for the visiting and local delegations.

3. Mobile Command Centre
    - Coordinate security for the event.

4. Ottawa Police, Gatineau Police, Ontario Provincial Police, Québec Provincial Police
    - Control road closures.
    - Provide law enforcement support.

5. Threat agents
    - Attempt to deny communications services between the MCC and officers.

**Pre-Conditions:** *[This* is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- The route between Ottawa and Montebello is served by the PSBN and commercial wireless carriers.
- U.S. agents have been pre-authorized to access Canadian criminal information networks.
- An agreement has been entered into between Canada and the USA to allow some personal information of citizens of both countries to be exchanged.
- Canada has allowed U.S. agents to use their communications devices in Canada.
- Small cells operating on the PSBN frequency band have been installed in the meeting venue in advance of the event.
- Land-based PSBN deployable systems have been installed at key locations outside the meeting venue.

- Backhaul between deployable systems and the MCC is in place.
- The deployable systems may have been sourced from different vendors, but are configured such that they are all interoperable at the time of deployment.
- Roaming agreements are in place between FirstNet, Canadian commercial wireless carriers, and the Canadian operator of the PSBN.
- The small cells rely on the DS coverage to provide backhaul.

**Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- Deployable systems can be configured as an eNB or a full-up RAN+EPC for resilience and back up.
- The airborne UE has been certified to be used on helicopters.
- The airborne UE can maintain connection to the PSBN over its entire route without interruption of data sessions.
- Sensitive user information is protected for confidentiality, privacy, and integrity.
- Sensitive mission information (e.g., location of agents) is protected for confidentiality, privacy, and integrity.
- Control of access to information is asserted locally.
- Users from the U.S. can be authenticated on the Canadian PSBN using the U.S. subscriber database (FN HSS) and may access local information networks.
- The PSBN is able to detect denial of service attacks at the radio interface and alert authorized personnel.
- The PSBN offers authorized personnel the means to thwart denial of service attacks.
- The small cells, terrestrial deployable systems, and fixed PSBN sites are able to inter-operate without interfering with each other.

**Parameters**

**Users and Devices**

| User, Device | Geographical Location |
|---|---|

| | |
|---|---|
| Officers and police forces; vehicle MDT | With the delegation while stopped and while moving. |
| Officers and police forces; body worn detachable tactical cameras. | Along the route of the delegation and at event venue. |
| Officers: hand-held terminal for graphics display, viewing video streams, PTZ camera control, data capture, gateway for body sensors and tactical cameras. | Along the route of the delegation and at event venue. |
| Mobile Command Centre: vehicle MDT. | Along the route of the delegation and at event venue. |
| Officers: aerial UE-based modem/router. | On board the helicopter. |

**Type of Data**

| Data Source | Type |
|---|---|
| Officers' devices: video | UDP streaming |
| Officers' devices: sensor information | TCP/IP interactive |
| Officers' devices: camera control commands | TCP/IP interactive |
| Officers' devices: location information | TCP/IP interactive |
| Surveillance cameras: video | UDP streaming |
| MCC: video | Multicast streaming |
| MCC: location information | TCP/IP interactive |
| Criminal information | Bulk files |
| Conversational Voice | IMS SIP |
| MC PTT | IMS SIP |

**Data Sensitivity**

| Data Type | Sensitivity |
|---|---|
| Video collected from cameras | Tactical information |
| Officers' sensor data | Medical and tactical information |
| Person-of-interest information | Criminal information |
| Location information | Secret |

## Use Case 4: EMS Monitoring of Victims at the Scene of a Mass-Casualty Event

**Description**: [This is a narrative of the use case that exemplifies how the deployable systems are expected to be used.]

A mass-casualty event has occurred with many victims. The event has disrupted the terrestrial PSBN service and commercial cellular service in the incident area to the extent that they have been rendered unusable. Mission-critical LMR voice communications has not been affected.

Bob, Bill, and Mary are EMS first responders who comprise one of the several EMS teams that are dispatched to the incident. Their EMS team is assigned to an EMS vehicle. The magnitude of the incident, having caused a large number of casualties, overwhelms the capacity of the local emergency medical services and therefore a call goes out to a neighboring jurisdiction to dispatch additional EMS teams.

Each team member has a multimedia emergency services (MMES) device with voice and broadband data capability. The EMS team members are assigned an incident talkgroup to communicate by voice with each other, their EMS Public Safety Communications Center, and to standby doctors in two different Hospital Center Emergency Rooms (ER). The MMES devices can be used to capture video images of the victims.

At the scene of the incident, Bill and Mary place MMES-capable EKG sensors on victims in the field and collect identity and other information (fingerprints, photos, medic-alert bracelets, etc.) of the victims to upload to the ER. Meanwhile Bob remains with the EMS vehicle and uses his MMES-capable device to stream live video of the incident to the dispatcher. Anne and Larry, the two stand-by ER physicians, and Bob are monitoring the vital signs data that is collected by the MMES-capable sensors. The MMES-capable devices can operate on multiple radios access technologies (RATs), which can be LTE Band-14 and WiFi (license exempt or 4.9 GHz)

Two EMS supervisor vehicles (one from each jurisdiction) are each equipped with a small Band-Class-14 LTE Deployable System (DS) with a roof-top mounted omni-directional antenna. One of the DS is designated to provide broadband data service to the immediate vicinity of the incident area while the other is set to stand-by in case the designated DS fails. Alternatively, the second DS can be used to extend the range of the first DS if the incident area is broader than the usable range of the first DS. The EMS vehicles that host the DS are also equipped with compact satellite terminals, which allow them to connect to the fixed PSBN network.

The DS serve other emergency responders at the incident such as local law enforcement, firefighters, and federal investigators who are collecting evidence to help determine the cause of the incident.

**Actors**: [This is list of the participants in the use case and their role.]

1. EMS first responders
    - Place MMES-capable EKG devices on the victims.
    - Collect identity and other victim-specific information for upload to the ER.
    - Collect video of the incident area.
    - Receive personal medical information of the victims.

2. Law enforcement officials
    - Collect evidence.
    - Secure the incident area

3. Firefighters
    - Assist EMS technicians.
    - Prevent fire from erupting

4. Federal investigators
    - Collect evidence.

5. ER stand-by physicians
    - Receive vital signs information from the patients.
    - Receive medical records from the health records database
    - Provide verbal instructions and data to EMS personnel

6. Health records database administrators
    - Where are the databases located?
    - What information do the administrators use in order to determine whom to allow access to the health records?
    - How are the databases connected to the PSBN?

7. Victims
    - Numerous.

8. Dispatcher

- Receives video from the incident area that is captured by Bob's MMES-capable device.

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- The FirstNet network has a connection to the broadband satellite service provider.
- The agencies responsible for the emergency medical services have equipped a select number of their vehicles with DS and satellite terminals.
- All EMS vehicles that are equipped with vehicular modems that, as a minimum, have a UE BC-14 air interface.
- The MMES-capable sensors are certified to not interfere with electronic medical implants such as pacemakers.
- First responders from both jurisdictions can be authenticated and are able to access medical information of the victims as authorized.
- One DS is sufficient to serve the incident area.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- EMS Supervisor vehicles can serve as DS to connect dismounted EMS teams and sensors to the PSBN.
- MMES-capable devices and sensors can be served by either of the two vehicular DS regardless of which one is designated as the serving DS.
- The DS can be configured as an eNB or EPC or full-up RAN+EPC for resilience and back-up.
- The DS can be turned up and made fully operational with minimum human intervention and no specialized knowledge of the DS technology. This includes the satellite link.
- The two DS can operate without interfering with each other.

- The DS will not interfere with the terrestrial fixed PSBN network when the latter is functionally restored in the incident area.
- Deployable systems allow for sensitive medical and victim-identity information to be protected for confidentiality, privacy, and integrity.
- The EMS teams can determine the quality of service that their MMES-capable devices are receiving from the DS.
- The dispatcher can track the location of the EMS teams, receives telematics-related information on the state of the EMS vehicles, and can monitor the status of the equipment on board.
- The DS can interface with the PSBN core network using geo-stationary satellite backhaul.
- The EMS vehicles each contain an access point for a wireless local area network using WiFi protocol operating in the license exempt bands and/or in the 4.9 GHz public safety band.
- The user devices and sensors operate on, at least LTE Band-14 and WiFi. The WiFi could be in the license exempt bands and/or the 4.9 GHz public safety band.

**Parameters**

**Users and Devices**

| User, Device | Geographical Location |
|---|---|
| Vehicular modems | Inside the incident area. Contained within the EMS supervisor vehicles. |
| MMES-capable communications devices | Carried by the EMS personnel and the stand-by ER physicians.<br><br>Carried by emergency responders. |
| MMES-capable EKG sensors | Placed on the bodies of the victims. |
| Portable chemical sensors | Used by investigators. |

**Type of Data**

| Data Source | Type |
|---|---|

| | |
|---|---|
| Vital signs information of victims | UDP streaming |
| Identity information of victims | TCP/IP interactive |
| Video of victims | SCTP (streaming control transfer protocol) |
| Video of incident scene | SCTP (streaming control transfer protocol) |
| EMS vehicle telematics information | TCP/IP |
| Medical records of victims | TCP/IP |
| Chemical sensor data | TCP/IP |

**Data Sensitivity**

| Data Type | Sensitivity |
|---|---|
| Video collected from MMES devices | Possible evidence for criminal and/or insurance investigations. |
| Vital signs data | Medical information |
| Identity information | Personal information |
| Location information of EMS teams | Tactical mission information |
| Medical records | Personal information |
| Chemical sensor data | Evidence for criminal investigation. |

## Use Case 5a: Search and Rescue in a Forested Area

**Satellite backhaul is available.**

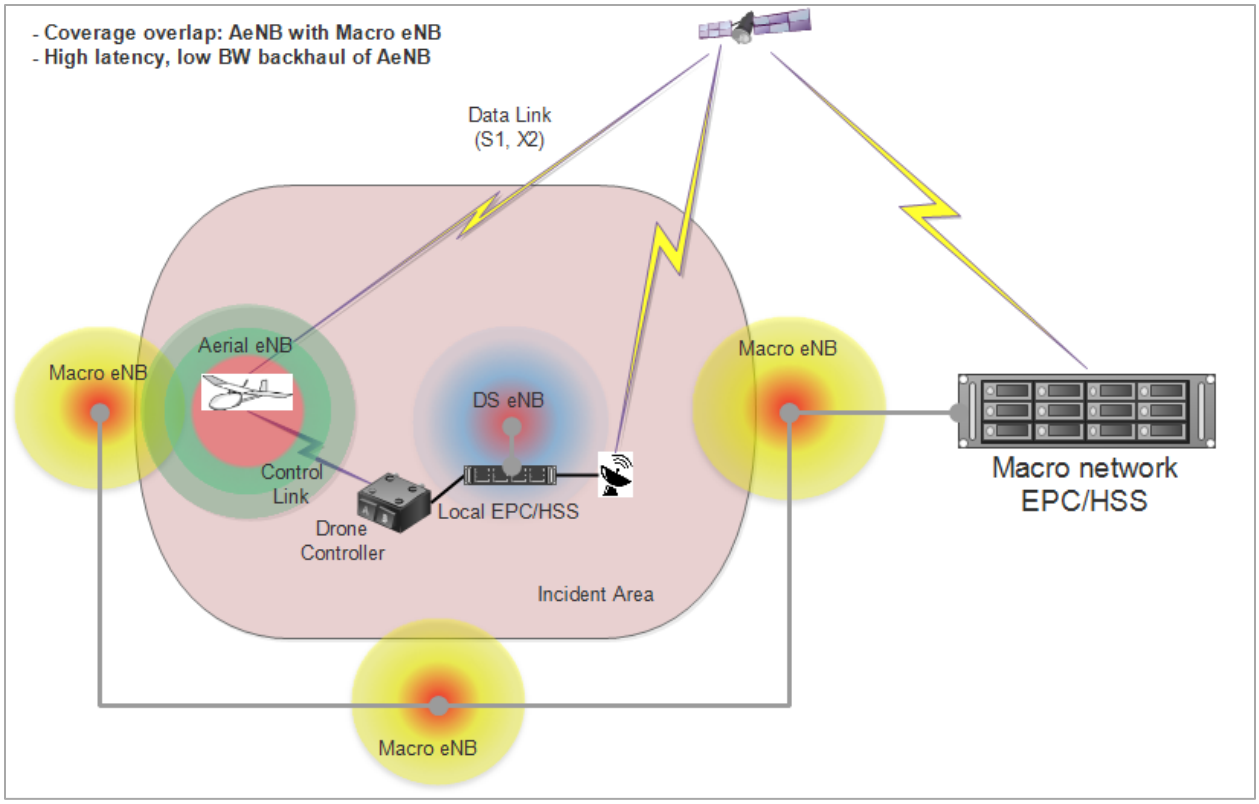
**Description**: [This is a narrative of the use case that exemplifies how an aerial platform would be used to extend an existing deployable system.]

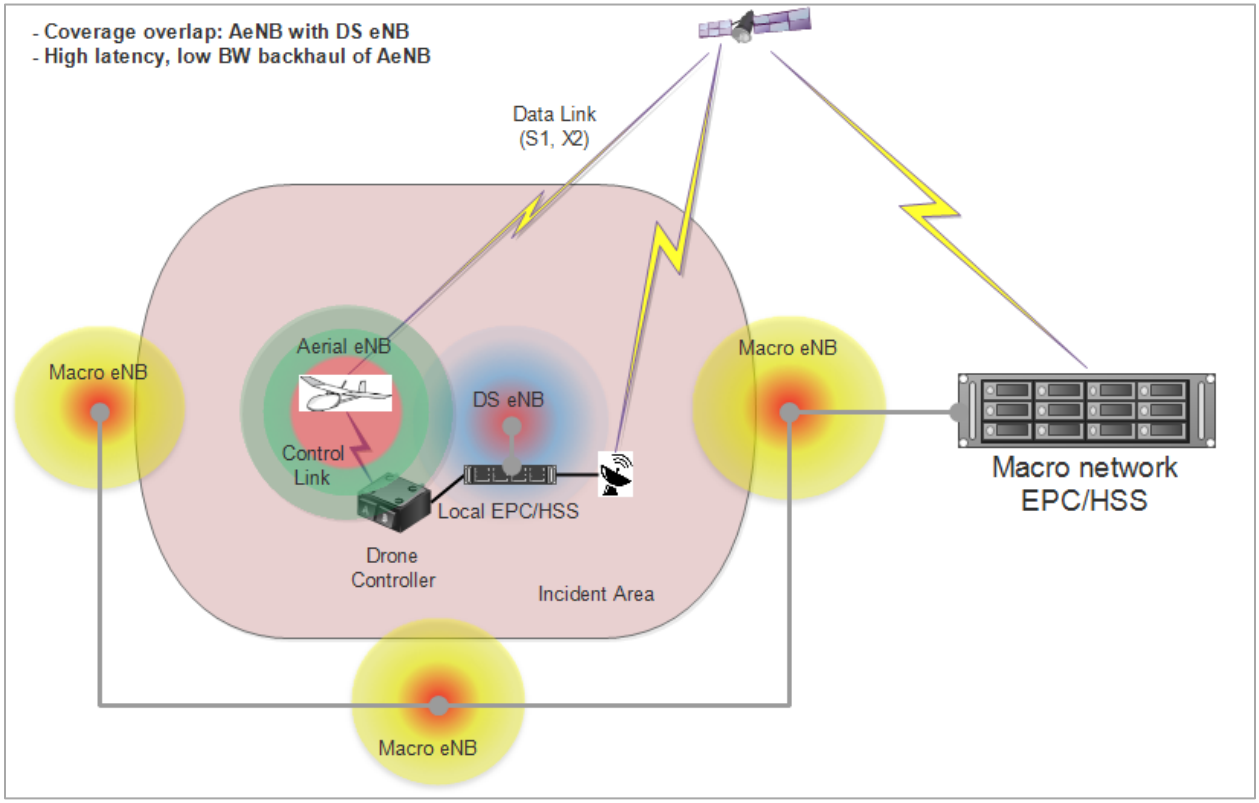
A child is reported lost in a forested area. The underbrush is not very dense and this increases the distance the child may have gone since last seen. The area is quite hilly which complicates coordination of the search. A few roads go through the area. The existing PSBN covers only 5% of the area.

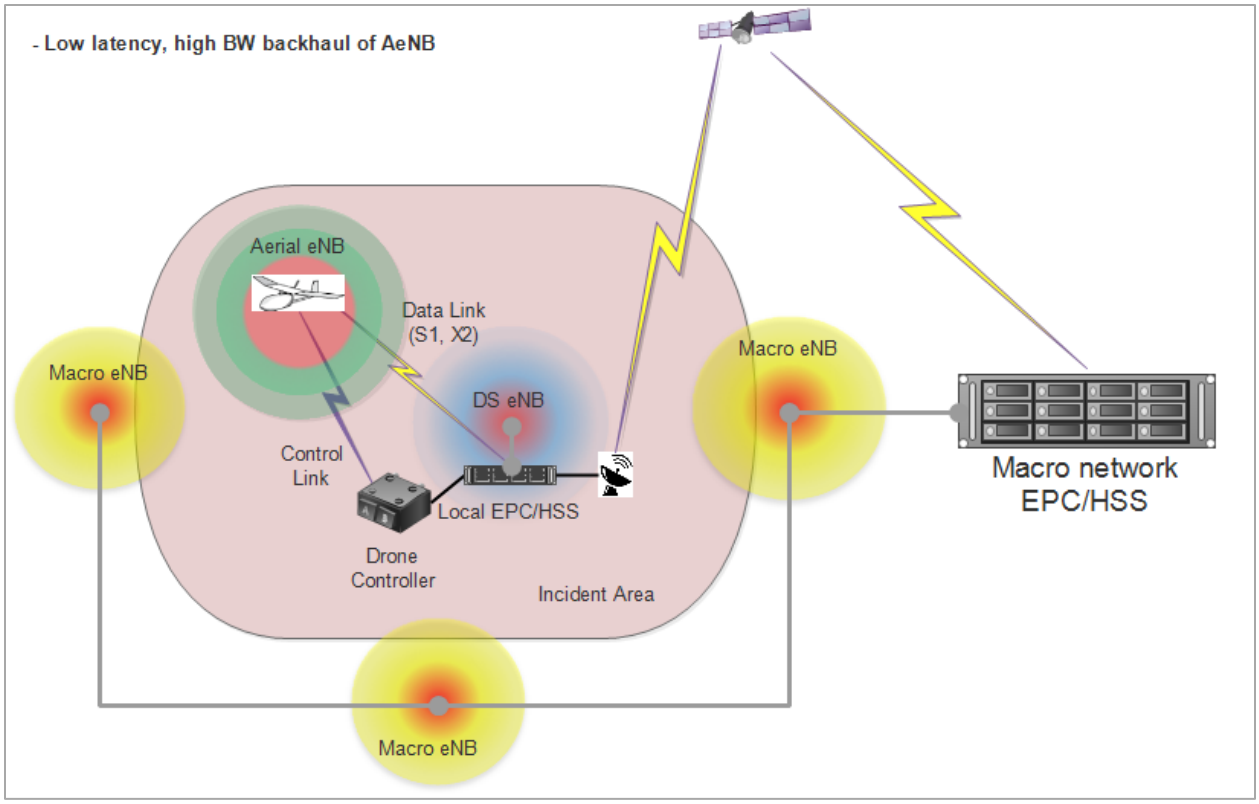
A search party gets organized, led by local law enforcement agencies. Many civilians and local organizations join the search which is expected to last at least a few days. A command post (CP) is set up out of PSBN coverage. It includes a deployable system (DS) which has a satellite backhaul that links it to the national PSBN. The DS has a local EPC/HSS associated with it.

The search party consists of a few hundred persons and is divided in many small teams of 8 -20 people. Each team leader has a multimedia emergency services (MMES) device with voice and broadband data capability. They use it to sporadically exchange maps, weather info, a few still pictures of the terrain with the CP.

Soon during the search the incident commander on site realizes that the combination of existing PSBN plus the DS can cover only a portion of the search area due to the local topography. An airborne platform carrying an eNB (AeNB) is ordered and arrives in the area several hours later. This platform consists of a drone with long flight autonomy and high maneuverability.


- Coverage overlap: AeNB with Macro eNB
- High latency, low BW backhaul of AeNB
Data Link
(S1, X2)
Aerial eNB
Macro eNB
DS eNB
Control
Link
Drone
Controller
Local EPC/HSS
Macro eNB
Macro network
EPC/HSS
Incident Area
Macro eNB


- Coverage overlap: AeNB with DS eNB
- High latency, low BW backhaul of AeNB
Data Link
(S1, X2)
Aerial eNB
Macro eNB
DS eNB
Control
Link
Drone
Controller
Local EPC/HSS
Macro eNB
Macro network
EPC/HSS
Incident Area
Macro eNB




**Actors**: [This is list of the participants in the use case and their role.]

1. Law Enforcement officers
    - Organize and lead the search teams

2. Civilian organizations and individuals
    - Conduct search.

3. Incident Commander
    - Coordinate the search efforts.
    - Requisition the resources.
    - Report on progress of the search

4. Drone Operator
    - Operate the drone
    - Configure the eNB payload

5. Terrestrial deployable system operator

- Configure the terrestrial deployable system
- Coordinate with the drone operator to provide backhaul to the drone's eNB
- Call up the satellite backhaul

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- The fixed PSBN, DS, and aerial eNB have been tested for interoperability and their hardware/firmware revision levels are managed to ensure that they remain interoperable.
- The DS is within an acceptable coverage footprint of a communications satellite.
- The DS is equipped with local servers with the applications needed by the search teams and incident command.
- The drone is requisitioned by the Incident Commander and is piloted under the authority of the Incident Commander.
- The Incident Commander has the sole authority to authorize the deployment of drones in the incident area.
- The control link to the AeNB is persistently connected throughout the incident area.
- The satellite is geo-stationary and terrestrial satcom equipment allows broadband connection.
- The satellite is geo-stationary and the small size of the aerial satcom antennas allow less than 512Kbps downlink (DL) and less than 128Kbps uplink (UL).
- The terrestrial data link to the drone is able to achieve more than 5Mbps DL and more than 1Mbps UL, when the drone is within range of the DS that allows the link to be established.
- The AeNB is actively transmitting and receiving on Band-14 while it moves.
- Assume onboard satellite switching to minimize path latency.
- There is a trained drone operator that is part of the incident command team.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- The aerial eNB extends the coverage of the DS and also serves as a sensor platform.
- The capacity of the Macro eNB is minimally affected when the AeNB's coverage overlaps with it.
- Session Continuity is maintained when the users' sessions are handed over between the AeNB, DS-eNB, and Macro-eNB wherever there is contiguous coverage between them.
- The DS can be configured as an eNB or eNB+EPC/HSS.
- The DS can be turned up and made fully operational with minimum human intervention and no specialized knowledge of the DS technology. This includes the satellite link.
- The mobile AeNB requires minimal human intervention to be usable as described in this use-case.

**Parameters**

**Users and Devices**

| User, Device | Geographical Location |
|---|---|
| Search team leaders: MMES handheld devices | Inside the incident area. Carried by the search team leaders. |
| Law enforcement officers: MMES handheld devices | Inside the incident area. Carried by the law enforcement officers. |
| Drone: sensor integration bridge | Carried by the drone. |

**Type of Data**

| Data Source | Type |
|---|---|
| Topographic maps with land use layers. | TCP/IP |
| Situational awareness information, including weather, accessed on Virtual USA or MASAS.[53] | DNS requests. |
| Video collected by search team leaders' MMES devices and the drone's sensors. | SCTP (streaming control transfer protocol) |
| Still images collected by search team leaders' | TCP/IP |

[53] MASAS: Multi-Agency Situational Awareness System. https://www.masas-x.ca/en

| | |
|---|---|
| MMES devices and the drone's sensors. | |
| MMES devices GPS tracking information. | |

**Data Sensitivity**

| Data Type | Sensitivity |
|---|---|
| Video ad still images collected from MMES devices and the drone's sensors | Evidence for possible criminal investigation. |
| Identity information | Personal information |
| Location information of search teams | Tactical mission information |

## Use Case 5b: Search and Rescue in a Forested Area

**Satellite backhaul is not available.**

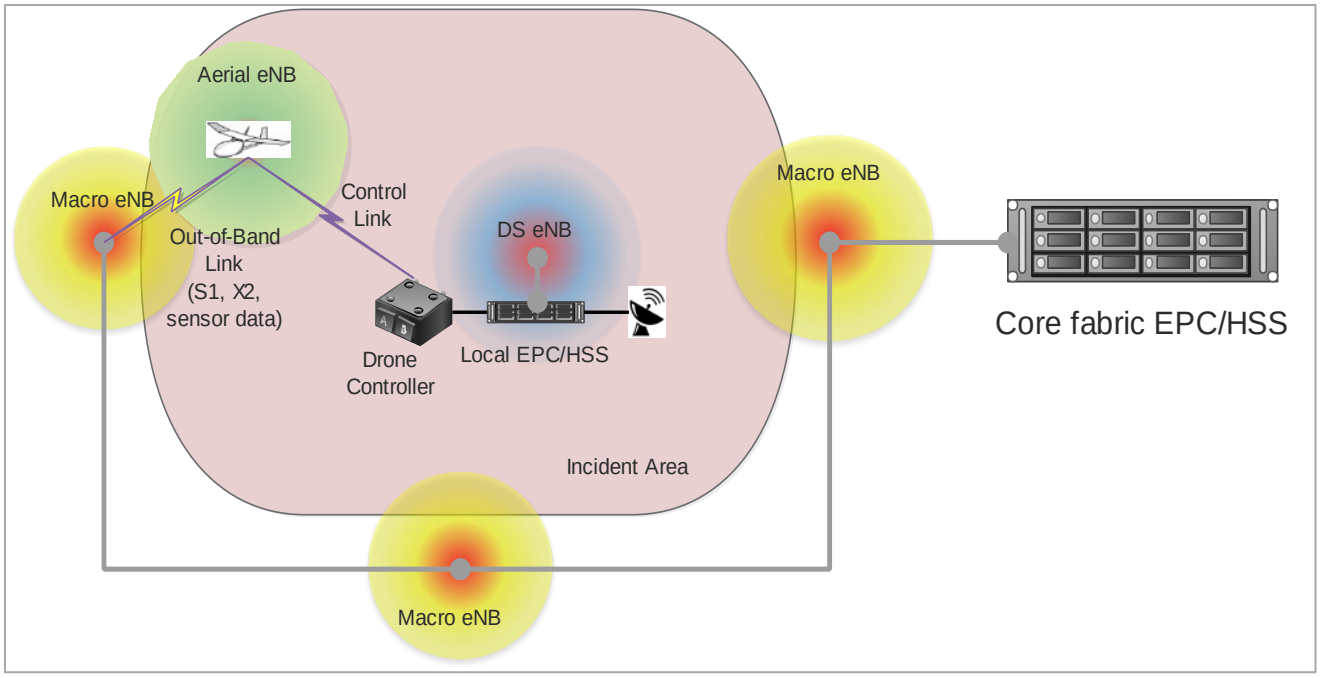
**Description**: [This is a narrative of the use case that exemplifies how an aerial platform would be used to extend an existing deployable system.]

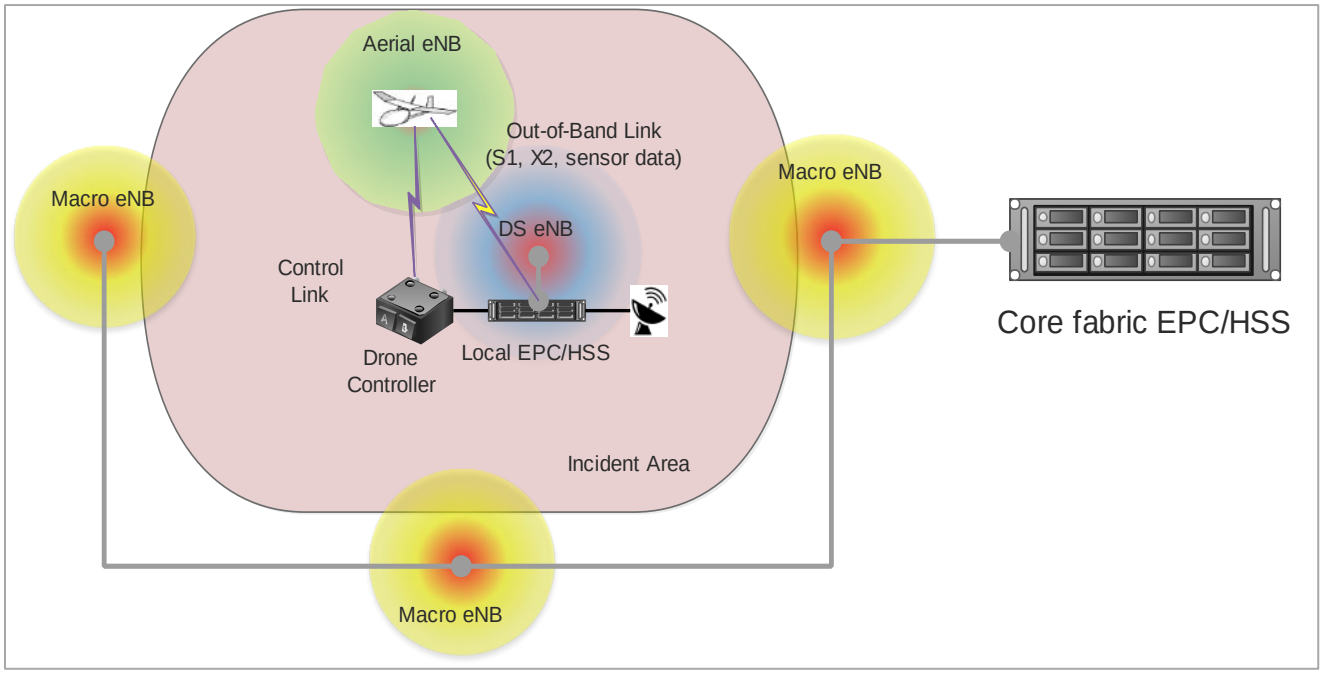
A child is reported lost in a forested area. The underbrush is not very dense and this increases the distance the child may have gone since last seen. The area is quite hilly which complicates coordination of the search. A few roads go through the area. The existing PSBN covers only 5% of the area.

A search party gets organized, led by local law enforcement agencies. Many civilians and local organizations join the search which is expected to last at least a few days. A command post (CP) is set up out of PSBN coverage. It includes a deployable system (DS), which has a local EPC/HSS associated with it. There is no satellite backhaul available for the DS.

The search party consists of a few hundred persons and is divided in many small teams of 8 -20 people. Each team leader has a multimedia emergency services (MMES) device with voice and broadband data capability. They use it to sporadically exchange maps, weather info, a few still pictures of the terrain with the CP.

Soon during the search the incident commander on site realizes that the combination of existing PSBN plus the DS can cover only a portion of the search area due to the local topography. An airborne platform carrying an eNB (AeNB) is ordered and arrives in the area several hours later. This platform consists of a drone with long flight autonomy and high maneuverability.




**Actors**: [This is list of the participants in the use case and their role.]

1. Law Enforcement officers
   - Organize and lead the search teams

2. Civilian organizations and individuals
   - Conduct search

3. Incident Commander

- Coordinate the search efforts
- Requisition the resources
- Report on progress of the search

4. Drone Operator

- Operate the drone.
- Configure the eNB payload.

5. Terrestrial deployable system operator

- Configure the terrestrial deployable system.
- Coordinate with the drone operator to provide backhaul to the drone's eNB.
- Call up the satellite backhaul.

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- The fixed PSBN, DS, and aerial eNB have been tested for interoperability and their hardware/firmware revision levels are managed to ensure that they remain interoperable.
- The DS and AeNB do not have the facility to connect to a satellite for backhaul.
- The AeNB to local EPC link can be in band or out of band of LTE for the radio access network.
- The DS is equipped with local servers with the applications needed by the search teams and incident command. This is to minimize traffic carried over the satellite link.
- The drone is requisitioned by the Incident Commander and is piloted under the authority of the Incident Commander.
- The Incident Commander has the sole authority to authorize the deployment of drones in the incident area.
- The control link to the AeNB is persistently connected with the ground controller throughout the incident area.

- The terrestrial data link to the drone is able to achieve more than 5Mbps DL and more than 1Mbps UL, when the drone is within range of the DS that allows the link to be established.
- The AeNB is actively transmitting and receiving on Band-14 while it moves.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- The aerial eNB extends the coverage of the DS.
- The capacity of the Macro eNB is minimally affected when the AeNB's coverage overlaps with it.
- Session Continuity is maintained when the users' sessions are handed over between the AeNB, DS-eNB, and Macro-eNB wherever there is contiguous coverage between them.
- The DS can be configured as an eNB or eNB+EPC/HSS.
- The DS can be turned up and made fully operational with minimum human intervention and no specialized knowledge of the DS technology.
- The AeNB requires minimal human intervention to be usable as described in this use-case.
- The aerial platform also serves as a sensor platform.

**Parameters**

**Users and Devices**

| User, Device | Geographical Location |
|---|---|
| Search team leaders: MMES handheld devices | Inside the incident area. Carried by the search team leaders. |
| Law enforcement officers: MMES handheld devices | Inside the incident area. Carried by the law enforcement officers. |
| Drone: sensor integration bridge | Carried by the drone. |

**Type of Data**

| Data Source | Type |
|---|---|

| | |
|---|---|
| Topographic maps with land use layers. | TCP/IP |
| Situational awareness information, including weather, accessed on Virtual USA or MASAS.[54] | DNS requests. |
| Video collected by search team leaders' MMES devices and the drone's sensors. | SCTP (streaming control transfer protocol) |
| Still images collected by search team leaders' MMES devices and the drone's sensors. | TCP/IP |
| MMES devices GPS tracking information. | |

**Data Sensitivity**

| Data Type | Sensitivity |
|---|---|
| Video ad still images collected from MMES devices and the drone's sensors | Evidence for possible criminal investigation. |
| Identity information | Personal information |
| Location information of search teams | Tactical mission information |

[54] MASAS: Multi-Agency Situational Awareness System. https://www.masas-x.ca/en

## Use Case 5c: Search and Rescue in a Forested Area

### Aerial eNodeB has no backhaul

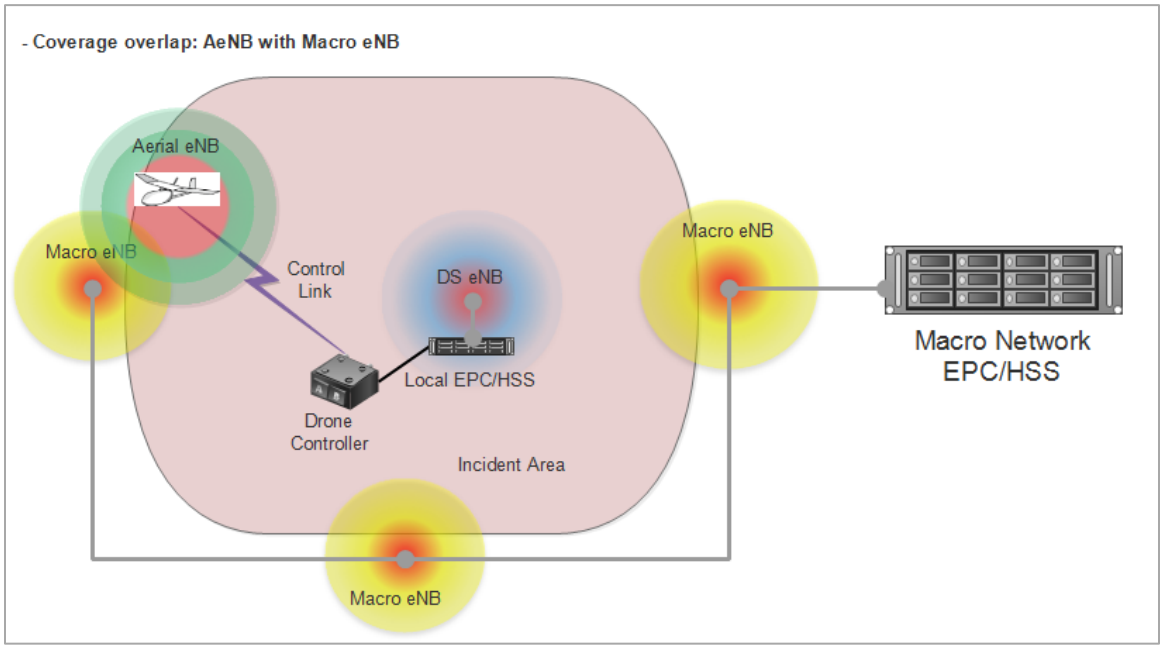
**Description**: [This is a narrative of the use case that exemplifies how an aerial platform would be used to extend an existing deployable system.]

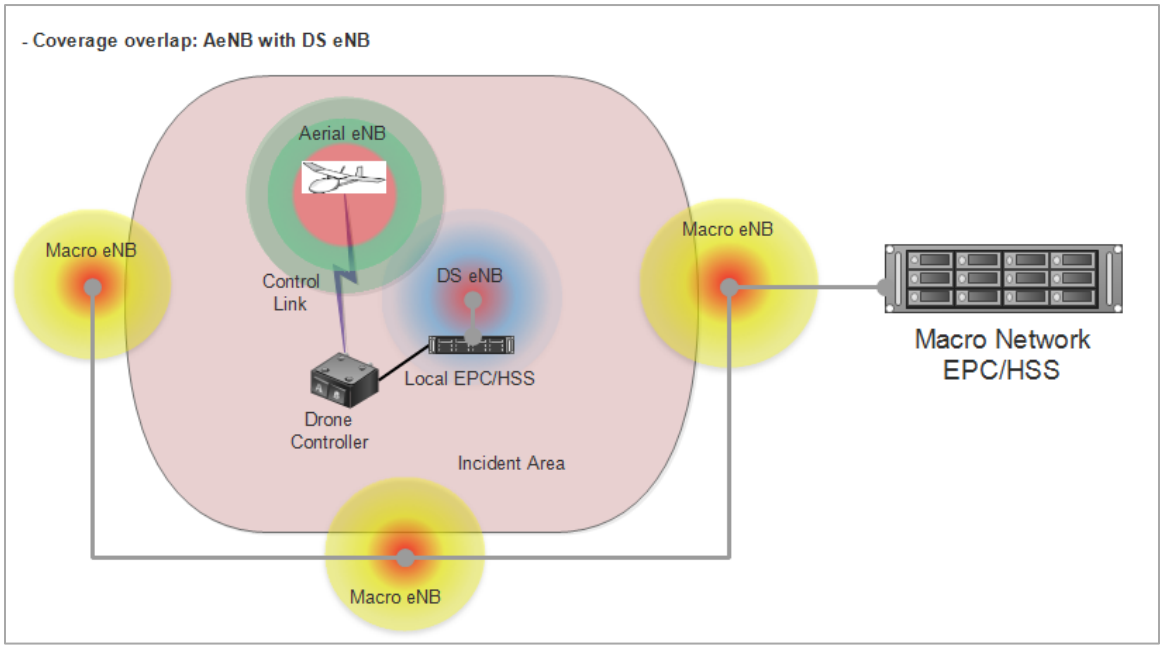
A child is reported lost in a forested area. The underbrush is not very dense and this increases the distance the child may have gone since last seen. The area is quite hilly which complicates coordination of the search. A few roads go through the area. The existing PSBN covers only 5% of the area.

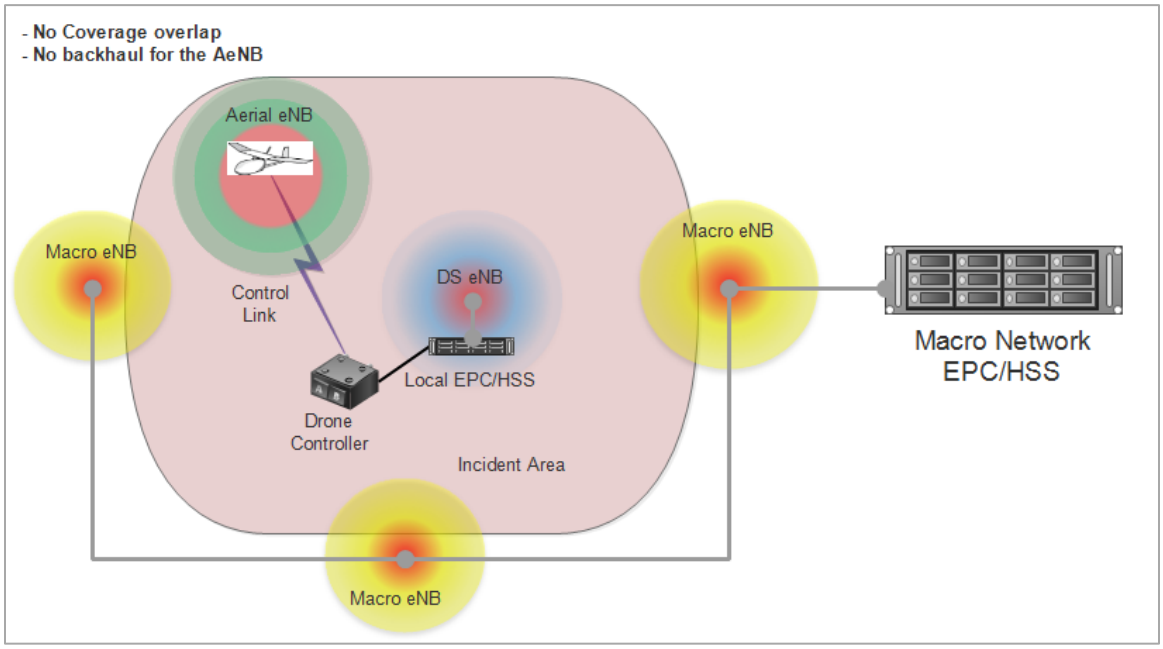
A search party gets organized, led by local law enforcement agencies. Many civilians and local organizations join the search which is expected to last at least a few days. A command post (CP) is set up out of PSBN coverage. It includes a deployable system (DS), which is only configured with an eNB. There is no satellite backhaul available for the DS. Hence, the DS is isolated. Local public safety agencies have configured their DS with IOPS functionality because of the possibility that there would be no backhaul in these remote rural environments.

The search party consists of a few hundred persons and is divided in many small teams of 8 -20 people. Each team leader has a multimedia emergency services (MMES) device with voice and broadband data capability. They use it to sporadically exchange maps, weather info, a few still pictures of the terrain with the CP.

Soon during the search the incident commander on site realizes that the combination of existing PSBN plus the DS can cover only a portion of the search area due to the local topography. An airborne platform carrying an eNB (AeNB) is ordered and arrives in the area several hours later. This platform consists of a drone with long flight autonomy and high maneuverability. The AeNB is also IOPS-enabled.


- Coverage overlap: AeNB with Macro eNB
Aerial eNB
Macro eNB
Control Link
DS eNB
Local EPC/HSS
Drone Controller
Incident Area
Macro eNB
Macro eNB
Macro Network EPC/HSS


- Coverage overlap: AeNB with DS eNB
Aerial eNB
Macro eNB
Control Link
DS eNB
Local EPC/HSS
Drone Controller
Incident Area
Macro eNB
Macro eNB
Macro Network EPC/HSS




**Actors:** [This is list of the participants in the use case and their role.]

1. Law Enforcement officers
    - Organize and lead the search teams

2. Civilian organizations and individuals
    - Conduct search

3. Incident Commander
    - Coordinate the search efforts
    - Requisition the resources
    - Report on progress of the search

4. Drone Operator
    - Operate the drone
    - Configure the eNB payload

5. Terrestrial deployable system operator
    - Configure the terrestrial deployable system
    - Coordinate with the drone operator to provide backhaul to the drone's eNB
    - Call up the satellite backhaul

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- The fixed PSBN, DS, and AeNB have been tested for interoperability and their hardware/firmware revision levels are managed to ensure that they remain interoperable.
- The DS and AeNB do not have the facility to connect to a satellite for backhaul.
- The DS and AeNB are configured with IOPS functionality.
- The drone is requisitioned by the Incident Commander and is piloted under the authority of the Incident Commander.
- The Incident Commander has the sole authority to authorize the deployment of drones in the incident area.
- There is no S1 and X2 connectivity between the aerial eNB and the macro eNB and DS eNB.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- The aerial eNB extends the coverage of the DS and also serves as a sensor platform.
- The capacity of the Macro eNB is minimally affected when the AeNB's coverage overlaps with it.
- Session Continuity is maintained when the users' sessions are handed-over between the AeNB, DS-eNB, and Macro-eNB wherever there is contiguous coverage between them.
- The DS can be configured as an eNB or eNB+EPC/HSS.
- The DS can be turned up and made fully operational with minimum human intervention and no specialized knowledge of the DS technology.
- The AeNB requires minimal human intervention to be usable as described in this use-case.

**Parameters**

### Users and Devices

| User, Device | Geographical Location |
|---|---|
| Search team leaders: MMES handheld devices | Inside the incident area. Carried by the search team leaders. |
| Law enforcement officers: MMES handheld devices | Inside the incident area. Carried by the law enforcement officers. |
| Drone: sensor integration bridge | Carried by the drone. |

### Type of Data

| Data Source | Type |
|---|---|
| Topographic maps with land use layers. | TCP/IP |
| Situational awareness information, including weather, accessed on Virtual USA or MASAS [35]. | DNS requests. |
| Video collected by search team leaders' MMES devices and the drone's sensors. | SCTP (streaming control transfer protocol) |
| Still images collected by search team leaders' MMES devices and the drone's sensors. | TCP/IP |
| MMES devices GPS tracking information. | |

### Data Sensitivity

| Data Type | Sensitivity |
|---|---|
| Video ad still images collected from MMES devices and the drone's sensors | Evidence for possible criminal investigation. |
| Identity information | Personal information |
| Location information of search teams | Tactical mission information |

## Use Case 6: Response to a Disaster Caused by a Major Earthquake

**Description:** [This is a narrative of the use case that exemplifies how the deployable systems are expected to be used.]

A major earthquake along the Cascadia fault and accompanying tsunami cause widespread destruction of property, transportation, and communications infrastructure. The damage and casualties are concentrated in the major urban centers of Victoria, BC, Vancouver BC, and Seattle, WA. Other population centers are also affected.

Local emergency responders are the first ones to mobilize to evacuate the devastated areas, begin rescue operations, administer first aid, and contain fires that ignite from broken gas lines. Utility workers are dispatched to shut off gas, water supply, and electrical power in the damaged areas.

Since the communications infrastructure is damaged, local agencies set up their PSBN Deployable Systems (DS) at those strategic locations, still reachable by road that were pre-defined during simulated exercises for such an event. Those DS that are configured as Systems on Wheels (SOW) are equipped with satellite backhaul and a telescopic mast to enable a high-capacity microwave connection to a facing site. The Incident Command vehicle (ICV) is similarly equipped with DS and satellite and microwave backhaul capability. Supervisor emergency vehicles are equipped with DS but no satellite capability. These DS essentially operate as small cells within the footprint of a donor DS-eNB. The COML team configures the ICV as the anchor for the other DSs. Satellite connectivity is established at the ICV, which also hosts application servers, caching servers, and security gateway.

The RF footprint of the $DS_{SOW}$ and $DS_{ICV}$ could potentially overlap into service areas of the PSBN that are still operating as well as across the Canada-U.S. border. The Self-Organizing Network application coarse-tunes the radio parameters of each DS and the COML team adjusts the settings to help train the SON algorithm.

County, state, and provincial resources arrive next to set up temporary shelter, medical, and morgue facilities. Environmental protection staff set up unmanned chemical/radiological, and seismic sensors at various sites. The State of Washington and Province of British Columbia activate their Emergency Operations Centers. Logistics and security for fuel distribution to DS is established. EOC coordinates with Red Cross to set up food/water distribution centers, establish logistics and security for the staff and supplies, and set up “missing persons” registration sites. These agencies are equipped with their own DSs to set up communications. The COML team determines which DSs from all the various agencies get tuned up and where. As they get tuned up the COML

staff monitors how the SON tunes the radio parameters to accommodate the newly inserted DSs. They intervene as required.

Military and reserve forces are deployed to assist local and state/provincial agencies to conduct search and rescue (SAR) operations and liaise with international SAR teams. The heat-sensing and RF emissions-sensing equipment can operate over WiFi as well as the public safety band, but the international SAR teams come from countries that use the Asia-Pacific Telecommunity (APT) band plan and so each team is supplied with PSBN Band-14 user equipment (UE) that also contains a WiFi Access Point.

Heavy equipment is brought in to assist SAR and recovery operations and to clear sites that are deemed to have no more living or deceased persons. They also remove structures that have been determined to be hazardous and to clear debris.

The COML staff must ensure that the lines of communications are enabled for voice and the exchange of data. They face numerous interoperability challenges listed below:

- Instantiate a wireless broadband communications service with DSs that are owned by different agencies, who in turn have independently sourced them from vendors of their choosing.
- Interface the network of DSs with the PSBN.
- Accommodate DSs that are inserted into the original network of DSs as other agencies arrive over the course of days and weeks and who offer their DSs to be inserted within the first group of DSs.
- Coordinate with U.S. and Canadian counterparts to avoid causing harmful interference across the border.
- Determine who is authorized to access the PSBN radio resources and with what priority and QoS privileges. Then, once that is determined, configure the access privileges accordingly for each user or groups of users.
- Balance the loading of traffic demands among the DSs.

**Actors:** [This is list of the participants in the use case and their role.]

1. First responders
    - Evacuate citizens from the disaster areas
    - Provide first aid
    - Search for victims
    - Provide security for fuel and food distribution

- Enforce curfews
- Prevent and contain fires

2. Utility workers
    - Locate downed power lines and gas breaks
    - Locate gas valves and electrical breakers
    - Locate water valves
    - Turn off gas, water, and electrical supplies to damaged areas

3. COML staff
    - Install and configure the DSs
    - Configure the SON overlay
    - Set access control privileges for users
    - Coordinate with international partners

4. State/provincial/county officials
    - Provide temporary shelter and medical services
    - Provide temporary morgue services
    - Monitor environmental conditions
    - Staff the EOCs

5. Federal agencies
    - Provide “boots on the ground” and aerial resources for SAR
    - Supply and operate earth movers and cranes
    - Coordinate the SAR efforts

6. Red Cross
    - Feed displaced persons and responders
    - Operate temporary shelters
    - Enable citizens to register missing persons in the Family Links database

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- The key locations for DSs have been identified as part of the outcome of an exercise to simulate a Cascadia subduction zone earthquake.

- Agencies procure DSs from a qualified list of products that have been tested for interoperability by an independent test organization.
- Agencies coordinate the upgrades and changes to the hardware, firmware, and software configurations of the DSs with a central authority to ensure ongoing interoperability.
- Agencies operate DSs as authorized by the spectrum licensees and/or regulatory agencies.
- COML staff are trained to set up and configure the different DSs. They are sufficiently knowledgeable to train the SON algorithm.
- Canadian and U.S. DS are configured with different PLMN IDs.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- Users are able to connect to their information networks from any location that is served by DSs. This includes staff of non-governmental organizations (NGO).
- Users are able to travel from the coverage area of one DS to that of any other DS without having to re-initiate the session or re-authenticate during the handover.
- Users along the Canada-U.S. border can be served by DSs or fixed PSBN sites on either side of the border and are able to access their information networks.
- COML staff can introduce DSs into an existing network of DSs with minimum human intervention.
- The vehicular PSBN LTE small cells can be served by any donor DS-eNB.
- DSs contained in transit cases can be powered from 120-240VAC or 12-48VDC sources.
- Generator fuel levels, unmanned sensors, vehicle telematics, UE location, fuel/food/water and other cargo locations, and responder and patient biometric sensors are monitored over the PSBN.

**Parameters**

**Users and Devices**

| User, Device | Geographical Location |
|---|---|

| | |
|---|---|
| Sensors: purpose-built devices. | Inside the incident area. |
| Utility workers: handheld devices | Inside the incident area. |
| Command staff: handheld devices; vehicular mobile data terminals. | Inside the incident area. |
| First responders: patient biometric sensors; handheld devices; vehicular mobile data terminals. | Inside the incident area. |

**Type of Data**

| Data Source | Type |
|---|---|
| GPS data from user devices | TCP/IP |
| Civil infrastructure information from municipal and utilities databases. | TCP/IP |
| Vital signs information collected from bio-sensors. | TCP/IP |
| Video from search teams' tactical cameras. | SCTP (streaming control transfer protocol) |
| Situational awareness information, including weather, accessed on Virtual USA or MASAS. | DNS requests. |
| Real-time voice and video | UDP |
| Sensor data for logistics (ex. fuel levels, water supplies, etc.) | TCP/IP |

**Data Sensitivity**

| Data Type | Sensitivity |
|---|---|
| Location of critical civil infrastructure components, ex. Valves, conduits, etc. | Critical infrastructure location. |
| Location of users | Situational awareness. |
| Vital signs associated to individuals | Personally identifying information. |
| Information on casualties and victims | Information for death certificates. |
| Location of food, water, medicine and fuel stores | Mission-sensitive information. |

## Use Case 7: Service Continuity During Transitions Between the Interior and Exterior of a Large Building

**Description:** [This is a narrative of the use case that exemplifies how the deployable systems are expected to be used.]

This use case describes a set of operational scenarios where emergency responders are able to access their application servers and information networks as they transition between outside and inside buildings that impair radio propagation.

A deployable LTE system (DS) is set up outside a LEED-certified 55 building in order to provide additional capacity to the emergency responders inside and outside the building. However, due to the large attenuation of the radio signal, power levels in deeper areas of the building are below the receiver threshold of user devices. Hence, there is no signal reception from the DS at some locations inside the building. As emergency responders emerge from inside the building the LTE signal level increases. Conversely, as emergency responders enter the building the LTE signal level decreases.

The building is served by a third party WiFi provider. A variation of the use case includes a Distributed Antenna System (DAS) that extends the PSBN service indoors, in addition to the WiFi service.

Five variations of the use case are examined. Scenarios 1 and 2 assume that the building is equipped with WiFi service that is accessible to emergency responders. The intent is to provide emergency responders an alternate access network to reach their information networks. Scenarios 3 and 4 assume that an alternative access network is not available and the emergency responders are equipped with device-to-device enabled devices. Scenario 5 assumes that the building is served with a DAS consisting of passive coaxial distribution.

During the transitions and through to re-attachment onto other radio domains, while either leaving or entering the building, emergency responders are able access their data networks without having to re-authenticate. The access privileges remain unaffected, including priority and QoS assignments. One-to-one and group call voice sessions are also maintained during the transitions.

**Scenario 1:** The building's WiFi network is powered up and connected to the Wide Area Network (WAN) through the Broadband Gateway. The DS is connected to the PSBN core network via satellite backhaul.

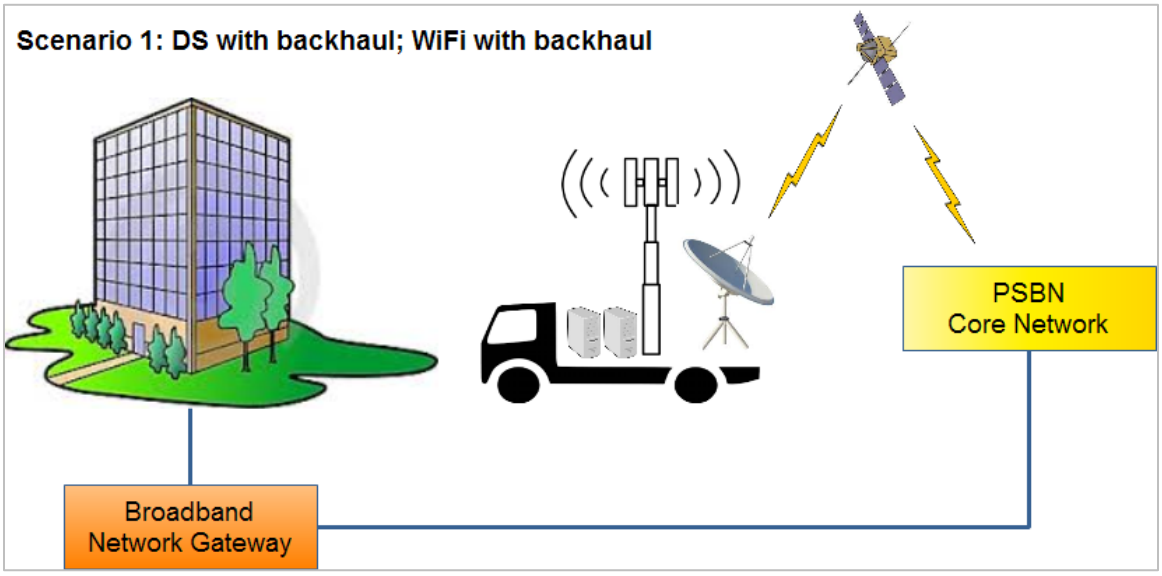
[55] Leadership in Energy and Environmental Design (LEED).

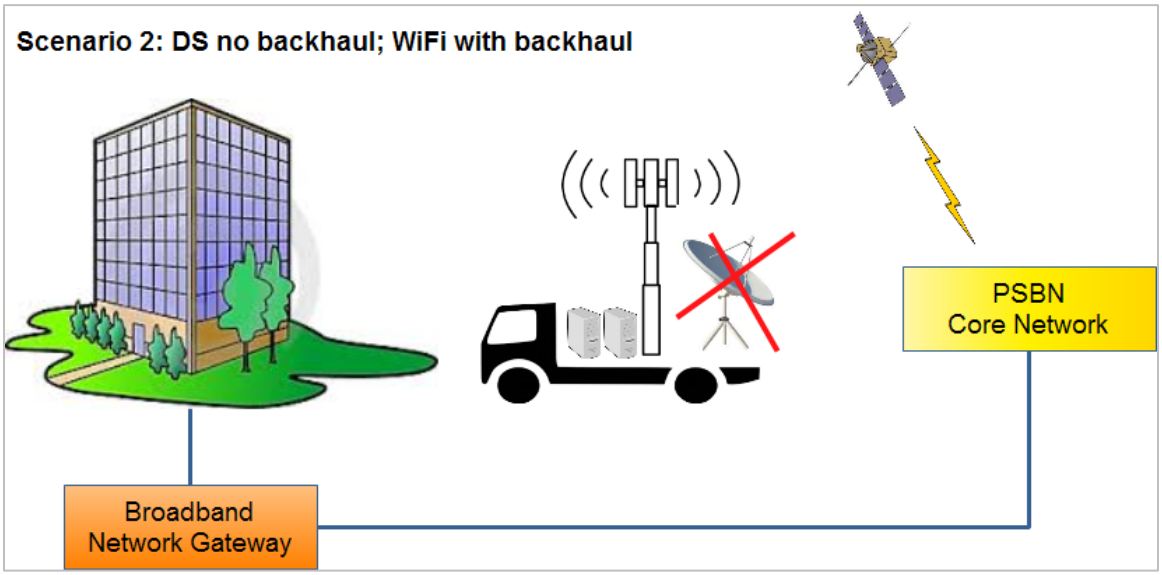
**Scenario 2:** The building's WiFi network is powered up and connected to the Wide Area Network (WAN) through the Broadband Gateway. The DS is isolated due to the failure or absence of the backhaul network.

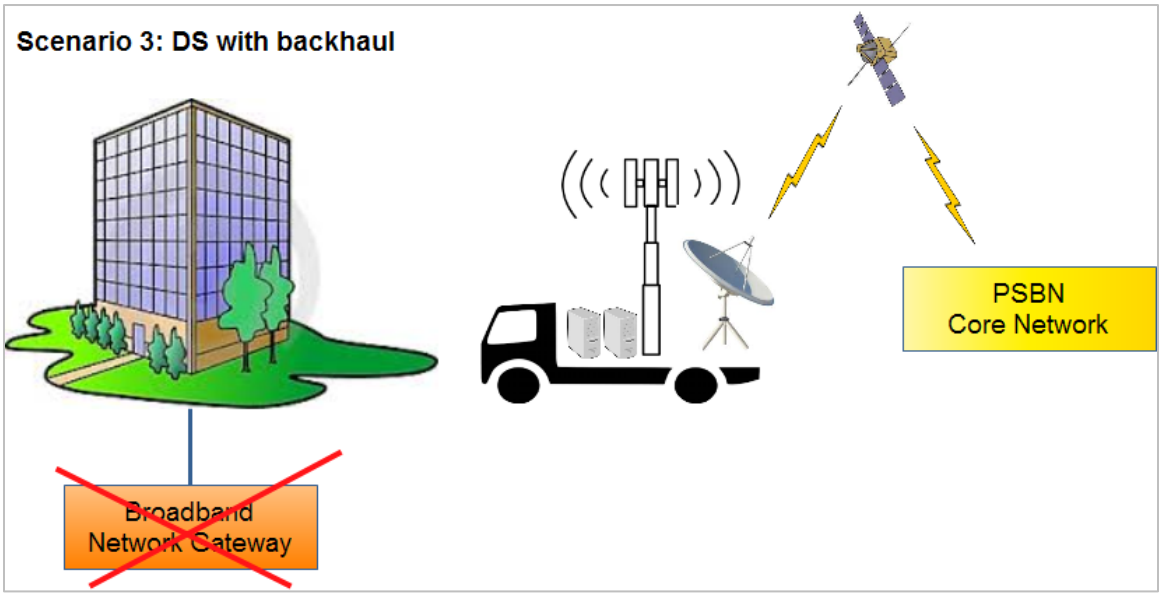
**Scenario 3:** A disaster has struck and the building's power supply is cut off and there is no connection to the WAN. The DS is connected to the PSBN core network via satellite backhaul.

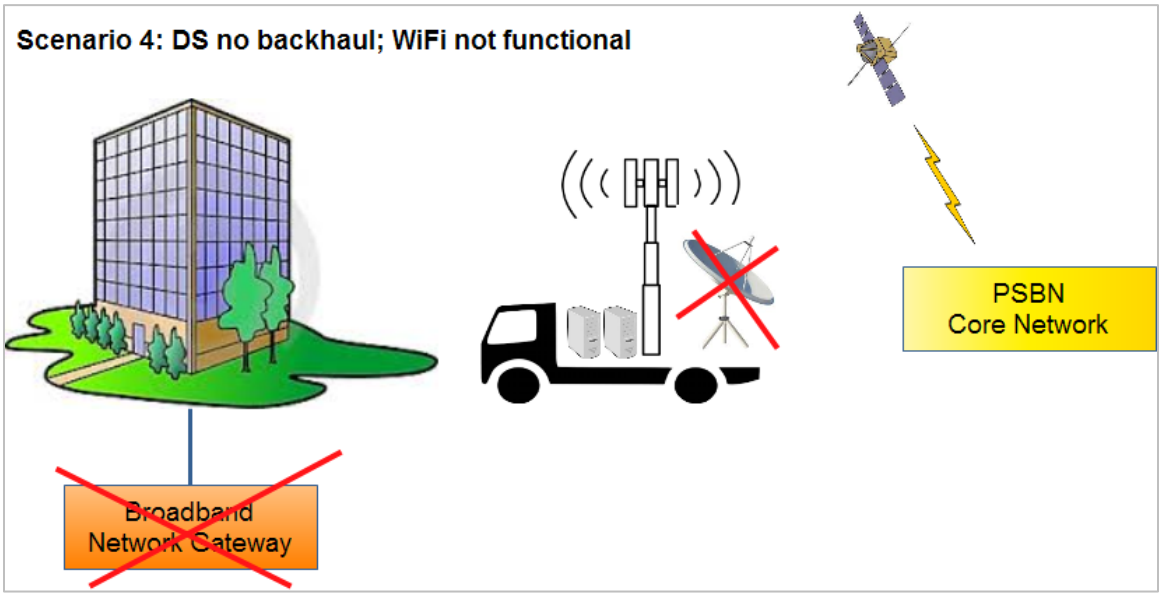
**Scenario 4:** A disaster has struck and there is no power to the building and the DS s satellite backhaul is inoperative.

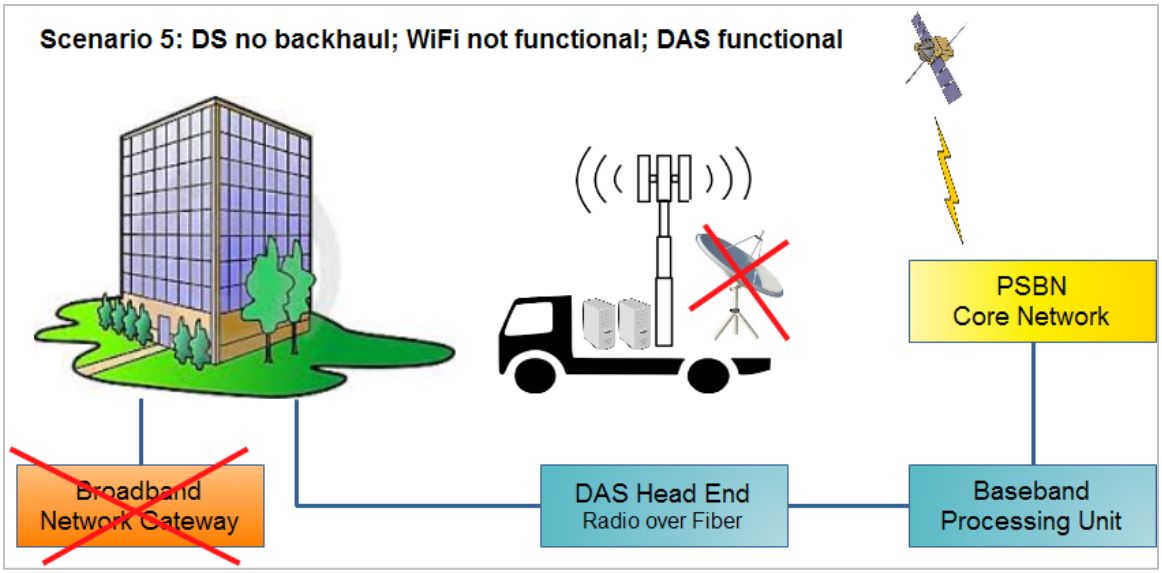
**Scenario 5:** A disaster has struck and there is no power to the building and the DS's satellite backhaul is inoperative. The DAS remains powered from a battery back-up system in the communications room.




Scenario 2: DS no backhaul; WiFi with backhaul
PSBN
Core Network
Broadband
Network Gateway


Scenario 3: DS with backhaul
PSBN
Core Network
Broadband
Network Gateway




**Actors:** [This is list of the participants in the use case and their role.]

1. Emergency responders
   - Access various areas inside and around the building in question
   - Access home information networks
   - Access local information networks
   - Engage in one-to-one and group call voice communications

2. WiFi service provider
   - Maintain WiFi access points in the building
   - Allow emergency responders to access the building's WiFi access network

- Connect the building's WiFi network to the PSBN core network
- Comply with the terms of the agreement with local public safety agencies allowing emergency responders to access its WiFi network.

3. Building owner
    - Maintain the in-building DAS and the battery back-up system.

4. Owner/operator of the PSBN (FirstNet)

    - Enable connection of the PSBN core network with the building's WiFi network
    - Drive the in-building DAS from a sector of the eNB

5. Owner/operator of the Deployable System
    - Install and configure the DS.

6. Local public safety agencies
    - Comply with the terms of the agreement with the WiFi service provider allowing emergency responders to access the building's WiFi network
    - Determine which emergency responders can access LTE DS radio resources
    - Equip emergency responders with ProSe-enabled user devices.

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- The user devices contain both WiFi and Band-Class 14 Radio Access Technologies (RAT).

- The in-building DAS is powered from conditioned DC power with battery back-up. There are no active components in the distribution system.

- There is an agreement between the WiFi service provider and public safety agencies that allows emergency responders to obtain wireless broadband service throughout the building from the many WiFi access points that are inside.

- The WiFi service provider and the owner/operator of the public safety broadband network (FirstNet) have connected the building's WiFi access network to the PSBN core network.

- The WiFi network is able to support priority and QoS.

- There is an agreement on harmonizing priority and QoS policies between the PSBN network operator (FirstNet), the owner/operator of the DS, and the WiFi hosting service.
- The WiFi network is able to support Voice-over-WiFi.
- The DS hosts local information and application servers.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

| Operational Capabilities | | Scenarios | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 4.1 | Users are able to connect to their agency information networks from any location in and around the building. | X | X | | | X |
| 4.2 | Users are able to connect to local information networks from any location in and around the building. | X | X | X | X | X |
| 4.3 | Users are able to access any information network, as authorized. | X | X | X | X | X |
| 4.4 | Users are able to access local information networks in the event that the LTE DS is isolated from the PSBN. | | X | | X | X |
| 4.5 | Users are able to engage in voice communications with each other indoors or outdoors, regardless of which access network they are connected to. | X | X | X | X | X |
| 4.6 | Priority and QoS policies are asserted according to PSBN operator's policies. | X | X | | | X |
| 4.7 | Active voice and data sessions are maintained when users transition between indoor and outdoor. | X | X | | | |
| 4.8 | There is no interruption of voice communications or of emergency alert notification when users transition between indoors and outdoors. | X | X | | | |
| 4.9 | Users are able to engage in one-to-one and group voice communications. | X | X | X | X | X |
| The term "Users" refers to home-based users and visiting (roaming) users. | | | | | | |

*Note: TS 22.278 "Service requirements for the Evolved Packet System (EPS), (Release 12)" contains requirements for inter-working and service continuity for fixed mobile convergence between 3GPP and non-3GPP networks and for ProSe.*

### Parameters

## Users and Devices

| User, Device | Geographical Location |
|---|---|
| Emergency responder; handheld devices | In and around the building. |

### Type of Data

| Data Source | Type |
|---|---|
| Handheld devices | Voice |

| | |
|---|---|
| Handheld devices | Data |

**Data Sensitivity**

| Data Type | Sensitivity |
|---|---|
| Voice – incident specific | Protected |
| Data – incident specific | Protected |

## Use Case 8: Bring-Your-Own-Coverage: BYOC for Every Day Public Safety Incident Area Operations

**Description:** [This is a narrative of the use case that exemplifies how the deployable systems are expected to be used.]

This use case describes a “day in the life” of a Bring-Your-Own-Coverage (BYOC) Deployable System (DS) and set of operational scenarios where first responders during the normal course of most incidents could improve the safety and operations efficiency within the area of incident. In today’s LMR based System/networks, many agencies bring a mission critical “suitcase” repeater(s) to a scene for communications support. Today LMR BYOC-enabled Deployable Systems are utilized to provide tactical scene of incident coverage. These are used to increase coverage for depth of building operations, span communication between multiple floors as well as extending coverage into tunnel systems and basements, and used to expand portable outdoor coverage. The notion of immediate usability upon turn on is implied.

Fire/EMS/LE agencies in rural, suburban, and urban settings will face coverage challenges from roll out through the expansion phases of the NPSBN. Coverage will be limited and will require some type of BYOC. This BYOC-enabled device that is in the vehicle will function as their LTE modem for in-vehicle terminal and also supply coverage (e.g., LTE Relay) when not in the vehicle. This device would provide “bubble” coverage into a stick built single family dwelling that represents the majority of the structures public safety enters. First responders would not consider this a problem requiring an “in-building” solution like a commercial structure. We expect our carrier devices to function in our own homes and expect FN UEs to function there as well. The BYOC portion would be turned off until the unit is parked. Most public safety items that need to be turned on and off tie into the park/brake set for activation or deactivation. This would handle the nomadic issue where it is off when mobile but on when parked.

BYOC devices may be installed in Fire/EMS/LE units where on-street and limited depth of building coverage is available for most of their **j**urisdiction. Coverage is required in framed wood stick built structures which match coverage on street. Thus, when the first responder parks/sets the brake for the vehicle with the BYOC device, a BYOC enabled-device turns on “Bubble coverage” at all locations, keeping in mind the home area for the unit is in an area where the majority of the jurisdiction has on street macro network coverage. These units will travel throughout the day in different settings from rural, suburban, and urban locations; i.e., EMS units travel daily in all three settings as an example, multiple times a day with patient transports thus their “bubble” will be activated when parked in all settings.

Many agencies respond daily to a wide array of calls covering a wide geographic area. Many locations within geographic area will include rural, suburban, and urban areas that may require BYOC bubble. As with law enforcement response, most calls are of short duration and range from major roadways to rural settings. Most EMS calls average 20 minutes with coverage required upon arrival.

Many times, law enforcement/Fire/EMS units will all be on the same scene simultaneously. There could be three to five or more BYOC devices present, all within a small overlapping

coverage area provided by different BYOC device vendors each providing “bubble” coverage simultaneously. These separate “bubble” coverage areas will need to be coordinated and interoperable with each other.

For response to large fire incidents, responders start off from a “still alarm” and migrate to a “full still” which will bring in neighboring departments for auto/mutual aid assistance comprised of up to ten outside fire companies. At the “full still” responders also start to move mobile command centers and other support units. Requests for additional resources will bring a 2-11 box which will add another 6 fire companies. This type of call typically can last 3 hours. Depending on the incident type, based on the requested alarm responders begin to move equipment and stage it until needed. Many times responders return some units en route. Many of these alarms are pulled based on information provided in the dispatch even before responders arrive.

During any of the scenarios above, the BYOC-enabled Deployable System will support the non-disruptive handover between public safety subscribers that access a BYOC-enabled vehicle’s coverage area and then are able to get handed over to/from the FirstNet Band 14 NPSBN, or possibly to a commercial carrier’s 4G LTE Macro network or possibly to Canadian public safety networks.

**Actors:** [This is list of the participants in the use case and their role.]

1. Emergency responders
    - Access various areas inside and around the building in question
    - Access home information networks
    - Access local information networks
    - Engage in one-to-one and group call voice communications

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- FirstNet has allowed B14 usage for BYOC bubble coverage for rural, suburban, and urban scenarios.
- The user devices contain both WiFi and Band-Class 14 Radio Access Technologies (RAT).
- The user devices are ProSe enabled and they support UE-to-network relay and UE-to-UE relay mode.

- There is an agreement between the BYOC operator and public safety agencies that allows emergency responders to obtain wireless broadband service throughout the coverage area. If a WiFi service is expected to be available within the BYOC LTE coverage area, then the BYOC in-vehicle system will support a WiFi hotspot for additional coverage in the incident area.
- The WiFi network, PSBN, and the BYOC networks are separate security domains. The WiFi network is considered to be an un-trusted network relative to the PSBN.
- The BYOC WiFi network is able to support priority and QoS.
- There is an agreement on harmonizing priority and QoS policies between the PSBN network operator (FirstNet), the owner/operator of the BYOC DS, and the BYOC WiFi Access Point service.
- The authorized use/access to the BYOC enabled-DS has been included in the negotiated Coverage Leasing Agreement (CLA) and also in the Service Level Agreement (SLA) between PSE and partner.
- System management has been updated to manage the system and network aspects of the BYOC-enabled Deployable System.
- There exists consistency of user experience when first responder accesses BYOC enabled-DS in a rural area or urban area.
- In the case where there is a MVNO/MNO configuration, there needs to be CLAs and SLAs agreed upon between the two operators involved.
- BYOC are only accessable by public safety users.
- Services and applications have to be standardized.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- The BYOC enabled DS supports multi-vendor or single vendor multi-DS interoperability when multiple BYOC enabled DS are used in a single incident (e.g. Police, Fire, EMS).
- FirstNet has allowed B14 usage for BYOC bubble coverage for Rural, Suburban and Urban scenarios.

- It should be well known how Primary and Secondary Users are affected when BYOC enable DS arrives on incident scene. There will exist mechanisms for Interference Mitigation and prevent disruption of the Macro network coverage.
- The BYOC WiFi network is able to support Voice-over-WiFi.
- The BYOC enabled DS will be under the Local Control of the DS Operator as well as the FN operator.
- Users are able to connect to their agency information networks from any location in and around the building.
- Users are able to connect to local information networks from any location in and around the building.
- Users are able to engage in voice communications with each other on both the LTE network and WiFi network, regardless of which access network they are connected to.
- Priority and QoS policies are asserted for users similarly on the LTE network as on the WiFi network.
- Active voice and data sessions are maintained when users transition between the LTE network and the WiFi network.
- Active voice and data sessions are maintained when users transition between the UE-to-DS connected mode and the UE-(UE) relay connected mode, or the UE-(network)relay mode.
- There is no interruption of voice communications or of emergency alert notification when users transition between the UE-to-DS connected mode and the UE-(UE)relay connected mode, or the UE-(network)relay mode.
- Users are able to engage in one-to-one and group voice.
- LTE-Unlicensed (LTE-U) should be added as a possibly for available device capabilities.
- Public safety operator could be serving as a Mobile Virtual Network Operator (MVNO)and Commercial carrier could be serving as Managed Network Operator (MNO). In this case it could be possible that either the MNO or MVNO could be using BYOC enabled DS to extend the coverage needed by a specific agency.
- The BYOC enabled Deployable System operating environment could be implemented using the ETSI Network Function Virutalization (NFV) model that implements Virtual

Network Functions (VNFs) on top of system hypervisor that serves as the base operating environment of the BYOC enabled DS.

**Parameters**

**Users and Devices**

| User, Device | Geographical Location |
|---|---|
| Emergency responder: handheld devices | In and around the BYOC incident area. |
| Emergency responder; in-vehicle BYOC system | Within vehicle that is located at the Incident area. |

**Type of Data**

| Data Source | Type |
|---|---|
| Handheld devices | Voice |
| Handheld devices | Data |
| In-vehicle System | Signaling information and backhaul traffic |

**Data Sensitivity**

| Data Type | Sensitivity |
|---|---|
| Voice – incident specific | Protected |
| Data – incident specific | Protected |
| Signaling – incident specific | Protected |

## Use Case 9: Use of Device-to-Device Communications

**Description:** [This is a narrative of the use case that exemplifies how the deployable systems are expected to be used.]

The Lake Town Fire Department is dispatched to a report of a building fire in an apartment complex. Three engines arrive to find several cars on fire in an underground parking garage. Thick smoke has risen into the building requiring all floors of the apartment complex to be evacuated. Several residents are suffering from smoke inhalation and are in need of medical treatment. The heavy construction design of the apartment building is preventing LTE coverage from the macro network and a Deployable System (DS) has arrived on scene to support incident operations. The DS was dispatched at the same time as the fire apparatus based on known coverage issues with buildings of this type.

The LTE devices used by the firefighters connect to the DS system and network coverage is maintained as the firefighters move to a lower level of the garage where the vehicles are on fire. After reaching the third level of the parking garage, several firefighters receive an alert message from their LTE device notifying them that they are out of coverage of the DS network. The LTE devices sense a loss of network connectivity and automatically switch to device-to-device direct mode communications. Other firefighters are at the top of the third level of the parking structure placing them at the edge of DS network coverage. Their devices are switching between the DS network and device-to-device mode. Those firefighters direct their device to lock on device-to-device mode allowing uninterrupted communications with the other firefighters. The fire department lieutenant, who is in charge of this fire attack crew, positions himself in an area where he maintains communications with the DS network. The lieutenant is able to communicate with the firefighters who are operating in device-to-device mode as well as with the incident commander and other personnel who are on the macro network.

**Actors:** [This is list of the participants in the use case and their role.]

1. Emergency responders
    - Incident commander who is in charge of the emergency scene
    - Fire lieutenant who is in charge of the fire attack group
    - A group of firefighters assigned to “fire attack” working as a team to extinguish the fire

**Pre-Conditions:** [This is a set of conditions that must exist before the use case unfolds. Pre-conditions may also be assumptions.]

- There is NPSBN macro network coverage in the area of the incident, excluding the interior of the apartment complex.

- The Deployable System used at the scene is operating in connected mode and has a backhaul connection.
- The user devices are device-to-device enabled and they support UE-to-network relay and UE-to-UE relay mode.

**Operational Capabilities:** [This is a list of the capabilities that are expected of the deployable systems in order to make the use case possible.]

- Users are able to communicate with other users when they are connected via the deployable system or the macro network. Communication services may include voice, video, and data.
- Users are able to communicate with other users in their assigned talkgroups when all or some of the users, in any combination, are connected to the macro network, the deployable system, or in device-to-device mode.
- Users are able to rely on ad hoc communications between LTE direct enabled devices that are not preconfigured in the same manner to support LTE direct discovery and communications
- Users communications sessions will maintain the Quality of Service Priority and Preemption (QPP) levels during the handover processes.
- Users unencrypted communications sessions will maintain session persistence during the handover of service from the macro network to the deployable system, deployable system to device to device, and vice-versa.
- Users encrypted communications sessions will maintain session persistence during the handover of service from the macro network to the deployable system, deployable system to device-to-device, and vice-versa.
- Users are able to maintain active communication sessions with other users in their assigned talkgroups when users are randomly transiting to and from macro, DS, and device-to-device connection modes.
- Users are notified of network availability while operating in direct mode.
- Users are notified when their communications sessions toggle from encrypted to unencrypted communications, and vice-versa.
- Users can select the manner by which they are notified for the different connected modes as well as a totally disconnected mode (e.g., visual, audible, or tactile).

- Users are able to know which other users they can communicate with when in device-to-device connected mode.
- Users are able to communicate with authorized users from other jurisdictions (local, state/provincial, territorial, federal, international) in device-to-device connected mode.
- Users are able to connect with users outside the incident area when they are connected in device-to-device mode.
- Users can control their LTE device to operate in either device-to-device mode (i.e., off-net mode) or network connected mode (i.e., on-net mode).
- Users are able to engage in one-to-one or one-to-many for PTT voice.

**Parameters**

**Users and Devices**

| User, Device | Geographical Location |
|---|---|
| Emergency responder; handheld devices | In and around the BYOC incident area. |
| Emergency responder; handheld devices | Inside an underground concrete parking garage structure. |

**Type of Data**

| Data Source | Type |
|---|---|
| Handheld devices | Voice |
| Handheld devices | Data |

**Data Sensitivity**

| Data Type | Sensitivity |
|---|---|
| Voice – incident specific | Protected |
| Data – incident specific | Protected |
| Signaling – incident specific | Protected |

# APPENDIX D: Deployable Systems Incident Commander Decision Matrix

This decision matrix was created as a concept to provide incident commanders and other personnel with a quick assessment of their operational needs in order to request the correct type of BBDS solution with the capabilities and features necessary to support the incident.

The following information provides an overview of each element of the Deployment Checklist:

**Site Access.** Certain types of BBDS units, such as trailer/towed COW-SOW systems, require access to paved roads. Other units, including those mounted in vehicles, require a road that would support a standard SUV-sized vehicle. The first item on the checklist allows the incident commander to indicate the type of terrain surrounding the incident. These diverse communication environments include hazardous conditions, impaired infrastructure, impassable roads / bridges, and hostile weather situations. There are also geographically different nominal operating areas (i.e., rural vs urban, cold north vs hot south) which will result in different site access requirements. A 100 percent all access deployable environment is likely unfeasible. Aerial systems are significantly influenced by weather and airspace conditions, which may not be immediately evident to the incident commander.

The checklist attempts to organize the site access into the following categories:

- The location of the DS site is accessible by paved/improved roadway (can support a towed trailer solution).
- The location of the DS site is accessible by unimproved road (can support an SUV or public safety vehicle based solution).
- The location of the DS site is accessible by all-terrain vehicles only (no roadway).
- The location of the DS site is not accessible by vehicle (deep woods, carry to top of building, etc.).
- The location of the DS site is not accessible by foot (aerial solution needed).

**Site Location.** The next item on the checklist deals with the site location and expected operating conditions. Public safety agencies often operate in disadvantaged communication conditions which can be result of compromised infrastructure, remote locations with limited communications, or saturation of end-user devices. It is important to note that disadvantaged communication environments are caused by both routine and extraordinary events. In some cases, BBDS equipment may be located inside an environmentally controlled facility or within a shelter. In other scenarios, the BBDS equipment may be operating outside.

The checklist queries two pieces of information:

- The DS will be sited indoors (vs. outdoors).
- The DS site will be located in an unusually harsh operating environment (describe:____).

**Power Availability.** The next item deals with the availability of power to support the BBDS equipment. The expected length of the incident or disaster will drive power requirements. In some cases, power may be available to support the BBDS and in other cases the BBDS will need to provide its own power. BBDS systems that implement standard, non-propriety, power / charging interfaces maximize the ability to have access to a power source.

Aerial BBDS systems have unique requirements due to the nature of the aerial deployment. Depending on the power source (fuel based versus renewable) accommodations must be made for access for refueling or power equipment swaps.

The checklist asks two questions regarding power:

- The site of the DS has access to an available/reliable power source.
- The DS solution must provide its own power.

**Backhaul Connectivity.** The next item deals with the availability of backhaul to support the BBDS services. In most cases, access to the macro network is essential to allow first responders to access needed services. A variety of locally agency applications, cloud-based applications, and LTE core services exist. A BBDS needs to accommodate different backhaul solutions to enable these applications or services. Some of these backhaul solutions may be carried on the BBDS and in other cases the BBDS needs to support the connection to other backhaul modes. These include backhaul using Band 14, satellite, and other wireless and wired networks. Backhaul requirements may vary greatly between backpack, vehicle based, trailer/towed solutions and aerial configurations.

The checklist asks the following questions regarding backhaul:

- The DS will have access to on site backhaul (specify type and connection).
- The DS will not have access to backhaul to the PSBN and will need to provide this service.
- Backhaul is not possible or not needed due to mission requirements.

**BBDS Configuration.** The next section deals with the expected configuration of the BBDS equipment. It is important to understand the mission expectations of the first responder and the relationship between the BBDS service and the macro network. There are several technical

issues that must be addressed when BBDS equipment is activated within the footprint of the NPSBN macro network or within the footprint of an existing BBDS device.

The checklist asks the following questions regarding configuration:

- The DS must operate within an overlapping NPSBN coverage area.
- The DS is needed to function as a relay to extend coverage.
- The DS is needed to add capacity to another DS already on scene.

**Applications and Services and Backhaul.** Additional questions on the checklist seek to identify the specific applications and services that will be needed at the scene. In some cases, the BBDS service may support basic communications without the need for backhaul. These might include mission critical voice and some incident command applications running on servers within the BBDS system. In other cases, access may be required to remote databases and applications which are not available locally on the BBDS. It should be noted that there are tradeoffs between latency, reliability, throughput, and utility based on the type of backhaul selected. Public safety agencies will likely expect an information backbone that manages and distributes data, including real-time vehicle location feeds, weather, critical infrastructure, and terrain information. It is unclear to what extent these services can be provided locally. Complexities will exist for applications that are resident on the BBDS that may or may not be utilized cohesively across regional agencies or subscribers using the BBDS (e.g., can a state-owned BBDS support all applications required by all local jurisdictions?)

The checklist asks the following questions regarding applications and services:

- The DS must provide a backhaul connection to support access to remote databases and specialized applications and services.
- The DS does not need a backhaul connection; all required applications and services are locally available.
- The DS must operate locally; there is no backhaul coverage option.

**Speed of Deployment.** The next section speaks to the urgency of BBDS service provision. In some cases, first responders may need immediate access to mission critical voice services vs. the delayed arrival of a BBDS solution that provides expanded capabilities. Some requests for BBDS services may be based on an expanding incident and the arrival of mutual aid units in the next operational period. This section of the checklist is designed to let the incident commander communicate a time frame for service delivery.

The checklist asks the following questions regarding speed of deployment:

- The DS solution is needed to support immediate mission needs (deployable as fast as possible).
- The DS solution needs to be fully operational within 4 hours.
- The DS solution needs to be fully operational for the next operational period (4-12 hours).

**Technical Assistance.** The next section of the report deals with deployment assistance that may be needed. In some cases, appropriately trained technical personnel may already be on scene and can manage the activation of the BBDS service. In other cases, the BBDS equipment may need to be in a hazard zone which will be accessible only to firefighters. In some cases, remote management and configuration of the BBDS may be needed. While it may be possible to deploy BBDS equipment to a remote deep woods area, the incident commander may select a different solution based on the complexity and time necessary to activate the BBDS.

The checklist asks the following questions regarding technical assistance:

- The DS will be used by forward operating teams in hazardous conditions (technical staff cannot accompany the system).
- Technically qualified personnel will be needed to activate/support the DS.
- Technically qualified personnel are already on the scene and can support the DS.

**Site Location/Terrain and Access:** The next section of the checklist attempts to gather other pieces of information which are important to the BBDS deployment. Information regarding the terrain of the incident may impact the type of BBDS equipment that would be needed to provide coverage. A mountainous area has different coverage requirements than flat open terrain. The expected duration of the incident is also a key factor in how the BBDS equipment should be supported. It is also important to understand the expected duration of an incident, as this will impact staffing, fuel to support power systems, etc. The length of deployment will vary greatly between small-scale local incidents and large-scale disaster events. The length of expected deployment can also change. For example, a police response to a domestic disturbance call can turn into a long-duration stand-off with a barricaded suspect. A building fire can rapidly evolve into a more complex and dangerous event involving hazardous chemicals. BBDS units should be designed to support everyday use and need to gracefully scale to adapt to dynamic conditions. It should be acknowledged that a tradeoff exists between deployment speed and a BBDS unit's uptime or utility. Deployment speed should be sufficient to ensure acceptable uptime and system performance.

While there are many variables in BBDS deployment, public safety agencies need to have a basic expectation of how quickly the service can be provided. There is no reason for an incident commander to request BBDS service if a house fire incident will be resolved in 1 hour and it will take 3hours for the BBDS service to arrive. The expected deployment time, from time of request to the time equipment is "rolling," should be documented in an MOU between the BBDS owner/operator and the public safety agencies who will be receiving BBDS service.

There are also issues relating to security of the BBDS equipment. Systems should be safeguarded against unauthorized access. Standard physical and cyber security procedures and technologies should be leveraged. Physical security requirements can be related to the set of services on the BBDS. For example, a BBDS with a full LTE core may have different security considerations than a deployable with an eNB. Finally, international operations and DS access to foreign nationals will influence security requirements. A full discussion of the security implications is included in Chapter 9.

The checklist asks the following questions regarding these issues:

- Assess the type of terrain to be covered in relation to the area to be covered (mountains, valleys, flatlands, buildings).
- Assess the type of terrain to be covered in relation to the area to be covered (mountains, valleys, flatlands, buildings).
- The expected duration of DS deployment is XX hours/days (relates to logistics for fuel, technical staffing, etc.).
- The DS solution will have personnel continuously on site.
- The DS solution will be deployed in an area without continuous personnel presence.

**Broadband Deployable Systems**
**Incident Command/COML Decision Matrix**
**Draft Version: 10/7/2015**

This document is designed to assist an incident command or COML in selecting the proper deployable system resource. The answers to the matrix questions below would be coupled with additional information on the incident location, type of terrain, and other factors that would impact the use of a backpack, vehicular, towed-trailer COW/SOW, or aerial solution.

**User Group Size:**

The DS needs to support PS User Group Size "A"
(to be defined, large number of users) N= ____

The DS needs to support PS User Group Size "B"
(to be defined, medium number) N = _____

The DS needs to support PS User Group Size "C"
(to be defined, small group) N = _____

**Expected Coverage Area:**

The DS needs to support Geographic Coverage Mode "A"
(a large-sized outdoor area to be defined)

The DS needs to support Geographic Coverage Mode "B"
(a medium-sized out door area to be defined)

The DS needs to support Geographic Coverage Mode "C"
(a small-sized outdoor area, to be defined)

The DS needs to support Geographic Coverage Mode "D"
(coverage to include in building)

**Expected Applications Needed:**

The DS needs to support PS Application Package "A"
(to be defined; ex: HD video, sensors, and other high bandwidth capacity services)

The DS needs to support PS Application Package "B"
(to be defined…)

The DS needs to support PS Application Package "C"
(to be defined …)

**Voice Capability:**

The DS needs to support Push-to-Talk Voice Applications

The DS needs to support Conversational Voice

The DS needs to support dial tone/telephony voice

**Other Needed Capabilities:**

Supplemental equipment will be needed to support an IP connection gateway to a public safety LMR

Supplemental equipment will be needed to support an IP connection to non-public safety systems (e.g., military, critical infrastructure, civil support teams, etc.)

The DS needs to support specialized information security needs, beyond baseline DS configuration

The DS solution needs to support WiFi and other wireless connections (specify _____)

The DS solution needs to support BYOC (Bring Your Own Coverage) devices (MCU/VNS solutions)

| DEPLOYMENT ISSUES |
|---|
| **Site Access:** |
| The location of the DS site is accessible by paved/improved roadway (can support a towed trailer solution) |
| The location of the DS site is accessible by unimproved road. (can support an SUV or public safety vehicle-based solution) |
| The location of the DS site is accessible by all-terrain vehicles only (no roadway) |
| The location of the DS site is not accessible by vehicle (deep woods, carry to top of building, etc.) |
| The location of the DS site is not accessible by foot (aerial solution needed) |
| **Site Location:** |
| The DS will be sited indoors (vs. outdoors) |
| The DS site will be located in an unusually harsh operating environment (describe: _____) |
| **Power:** |
| The site of the DS has access to an available/reliable power source |
| The DS solution must provide its own power |
| **Backhaul:** |
| The DS will have access to on-site backhaul (specify type and connection) |
| The DS will not have access to backhaul to the PSBN and will need to provide this service |
| Backhaul is not possible or not needed due to mission requirements |
| **Configuration:** |
| The DS must operate within an overlapping NPSBN coverage area and manage interference |
| The DS is needed to function as a relay to extend coverage |
| The DS is needed to add capacity to another DS already on scene |
| **Connected/Stand Alone Operations:** |
| The DS must provide a backhaul connection to support access to remote databases and specialized applications and services |
| The DS does not need a backhaul connection; all required applications and services are locally available |
| The DS must operate locally; there is no backhaul coverage option |
| **Deployment Speed Requirement:** |
| The DS solution is needed to support immediate mission needs (deployable as fast as possible) |
| The DS solution needs to be fully operational within 4 hours |
| The DS solution needs to be fully operational for the next operational period (4-12 hours) |
| **Deployment Assistance Requirements:** |
| The DS will be used by forward operating teams in hazardous conditions (technical staff cannot accompany the system) |
| Technically qualified personnel will be needed to activate/support the DS |
| Technically qualified personnel are already on the scene and can support the DS |
| **Additional Decision Points:** |

| |
|---|
| Assess the type of terrain to be covered in relation to the area to be covered<br>(mountains, valleys, flatlands, buildings) |
| Assess the type of terrain to be covered in relation to the area to be covered<br>(mountains, valleys, flatlands, buildings) |
| The expected duration of DS deployment is XX hours/days<br>(relates to logistics for fuel, technical staffing, etc.) |
| **Security/Vulnerability:**<br>The DS solution will have personnel continuously on site<br>The DS solution will be deployed in an area without continuous personnel presence |

# APPENDIX E: Working Group and Contributor List

NPSTC wishes to thank the Working Group Chairs and the following members of the **Public Safety Review Team** who helped conduct the final editing and review of the document.

Claudio Lucente, Senior Technical Advisor, Defence Research and Development Canada –Centre for Security Science (DRDC CSS), Working Group Chair
Robert Stafford, PSCR, Working Group Co-Chair

Chris Kindelspire, Director, Electronic Operations, Grundy County, IL
Barry Fraser, General Manager, BayRICS Authority
John Lenihan, LA County Fire Department (retired)
Kim Coleman-Madsen, Public Safety Broadband Manager, State of Colorado FirstNet Program
Tom Sorley, Deputy Director Information Technology, City of Houston

NPSTC also wishes to thank all the public safety, commercial, and industry participants who participated in the development of this report.[56]

**Writing Group Team Leaders**

Stephen Braham, Simon Fraser University PolyLAB
Tewfik Doumi, Nokia
Chris Kindelspire, Grundy County 911
Claudio Lucente, DRDC CSS
Walt Magnussen, Texas A&M University
Hien Nguyen, NIST, Public Safety Communications Research (PSCR)
Jerry Quenneville, Space Data Corporation
Mark Raczynski, General Dynamics Mission Systems
Dean Skidmore, IoT+LTE Consulting Group

[56] NPSTC wishes to note that persons identified in this list are displayed to acknowledge their participation in the process and does not automatically indicate their support, or absence of support, for information contained in this report.

**Working Group Participants**[57]

Karen Allen, AZ FirstNet
Simon Arcand, Communications Security Establishment Canada
Amir Basri, Communications Research Centre
Rob Berezowski, SaskTel
Michael Britt, State of Arizona
Wim Brouwer, Alcatel-Lucent
Billy Carter, Radio Communications Coordinator, Illinois Department of Public Health
Kim Coleman-Madsen, State of Colorado, Governor's Office of Information Technology
Bruce Cox, NextNav
Mike Dixon, RedMobile Consulting
David Eierman, Motorola Solutions
JJ Farnan, III, Good Will Fire Company of New Castle Delaware
Joe Fournier, DRDC CSS
Joe Hanna, Directions
Robert Janusaitis, Harris County Emergency Services District #9
Steve Kropper, Parallel Wireless
John Lenihan, Los Angeles County Fire Dept. (Retired)
Tad Matheson, NW-Regional Interoperability Coordinator, WI
Ed Mills, State of Colorado
Gary Monetti, Monetti and Associates, LLC
John Moyers, State of Tennessee
Doug Mummert, Phoenix Fire Department
John O'Connor, Memphis Police Department
Ben Posthuma, NIST/PSCR
John Potocki, Pepro LLC
Mel Samples, CADSTAR, INC.
Douglas Sharp, Oceus Networks
Robert Stafford, NIST PSCR
Gregory Sundie, Project Manager - Contractor | Arizona FirstNet
Bill Worger, General Dynamics Mission Systems

[57] Working Group Participants were actively involved in conference call meetings and contributed to the development and review of the report.

**Working Group Members**:[58]

David Adsit, FEMA - Spectrum Manager
Simon Arcand, Communication Security Establishment Canada
Dominick Arcuri, DVA Consulting
Frank Baier, Commonwealth of Pennsylvania
Michael Barker, Motorola Solutions Canada Inc.
Mike Barney, State of Texas (retired) Kodiak Networks
Edgardo Barreto, CODECOM
Jeffrey Billon, XG Technology
James Bitting, Veterans Enterprise Systems Technology
Yvonne Bond, California Governor's Office of Emergency Services
Irem Bor, Carleton University
Joe Boucher, Mutualink
Kathy Brand, Tower Safety & Instruction
Don Brittingham, Verizon
Curtis Brochu, Alberta, Justice and Solicitor General
Patti Broderick, Orange County Sheriff's Office, Orlando Fl-retired
Jeff Brooks, County of Lambton Emergency Medical Services
David Buchanan, Retired, NPSTC Spectrum Management Chair
Alicia Burns, The Digital Decision, LLC
Andrew Bussey, MONOC
Ferdinand Cedeno, All Professional Consulting, Commonwealth of Puerto Rico
Jim Coates, Santa Clara County Communications Department
John Contestabile, John Hopkins University/APL
Rodney Cooper, Sprint
Michael Cornwell, City of Hoover, Alabama
Rodney Cronin, Redline Communications
Afeite Dadka, Televate
John Davie, State of Colorado
Donald Denning, DELTAWRX, LLC
Stephen Devine, State of Missouri (retired)
Wim Dhondt, IBB Consulting
Vickie Diaz, Jacksonville FL Sheriff's Office
William Drew, NJ Office of Homeland Security and Preparedness
Arnold D'Souza, MTS, Inc.
Nicholas Emmerling, 49th Military Police Brigade

[58] Working Group Members monitored the progress of the Working Group and reviewed distributed documents.

Dan Ericson, Harris
Jeffrey Fenton, 908 Consulting, LLC
Thomas Fleck, Space Data Corporation
Donald Fortin, Ministère de la Sécurité, Québec
Ben Garvey, DragonCo Consulting
Chantal Gazaille, Innovation Science and Economic Development - Canada
Lee Gopadze, BBI, LLC
Bruce Grandy, Province of New Brunswick, Dept. of Transportation
Mylene Grenon, Ministère de la Sécurité Publique – Québec
Laslo Gross, Global Wireless Technologies
David Gross, Global Wireless Technologies
Semra Gulder, Innovation Science and Economic Development - Canada
Sid Gupta, Codan Radio Communications
Jacob Gurnick, Communications Research Centre, Innovation Science and Economic Development Canada
Nader Haghighat, City of Los Angeles
Gina Harrison, NTIA
Joe Heaps, DOJ/NIJ
Domingo Herraiz, Director, Programs at IACP
Steve Irving, Elara Networks
Vihang Jani, PSCR
Xiaowei Jin, Motorola Solutions
Craig Johnson, FEMA
Reid Johnson, Harris
Keith Kaczmarek, inPhase Wireless
Ramu Kandula, Kodiak Networks
Peter Kim, DHS
Justin Koval, Collier County Sheriff's Office
Eric Lafond, Communications Research Centre, Innovation Science and Economic Development Canada
Jean Lajoie, Centre de services partagés du Québec, Gouvernement du Québec
Thomas Lampe, Iowa Dept. of Public Safety
Rick Lange, Dane County Emergency Management
Lisa Leahy, ConnectME Authority
John Leitch, Province of Saskatchewan
Kenneth Link, Monroe Township NJ Fire / State of NJ OEM
William (Grant) Lohsen, Georgia Tech Research Institute
Chris Lougee, 5x9 Communications

Myles Lu, Star Solutions International, Inc.
Masif Manzoor, University of Regina, Canada
Chris McGaffey, Alcatel-Lucent
Richard McKinnon, DVBE Technology Group
Jim McMillan, Harris County
Christian Militeau, Intrado
Brian Moore, IAEM/Kelowna Fire Department
Yasser Morgan, University of Regina
Tim Moynihan, XG Technology
Darrin Mylet, Runcom
Narasimha Nagubhai, Kodiak Networks
Kamesh Namuduri, University of North Texas
Rohit Nerlikar, Kodiak Network
Paul Nikfarjam, Altaeros
Bryce Nordgren, Mineral County Disaster & Emergency Services
Erik Org, GWT
Mike Page, Motorola Solutions
Ted Pao, County of Los Angeles
Ben Pearce, Codan Radio
Tim Pierce, FirstNet
Alex Pourian, Star Solutions
John Powell, State of California OES
Prtihu Prakash, General Dynamic MS
Mike Quann, Government of Alberta, Canada
Michael Rohrbacher, State of New Mexico
Joe Ross, Televate
John Rowe, Telecom Bird Dogs LLC
Phil Royce, State of Florida Division of Emergency Management
Gino Scribano, Motorola Solutions
Bill Springer, Illinois Law Enforcement Alarm System
Stephen Surfaro, ASIS International
Alan Swain, Wavefront
Michael Swaney, Ohio EMS
Patrick Tabourin, Radio IP Software
Mohan Tammisetti, VirtualNetCom
Keller Taylor, Princeton University Dept of Public Safety
Gaétan Trépanier, Centre de services partagés du Québec, Gouvernement du Québec
Joe Troiano, CommScope

Dharmesh Tyagi, Nokia
Ajit Vanniamparampil, Inmarsat Government
David Warner, Virginia Information Technologies Agency (VITA)
Andrew Weinert, MIT Lincoln Laboratory
Paul West, Rhyzome Networks
Shelley Westall, Washington OneNet
Ronald Williscroft, Winnipeg Fire Paramedic Service
Halim Yanikomeroglu, Carleton University
Virgil Young, The Office of the Chief Technology Officer (OCTO)
Peter Zwagerman, NYSTEC

# APPENDIX F: Bibliography


[1] 3GPP, "TS 23.335, “User Data Convergence (UDC); Technical realization and information flows; Stage 2,” Release 12,," October 2014.

[2] FirstNet, "CTO Blog: Vehicular Network System (VNS)," 13 July 2015. [Online]. Available: http://www.firstnet.gov/newsroom/blog/cto-blog-mobile-communications-unit-mcu.

[3] GSMA, "IR.65 IMS ROAMING AND INTERWORKING GUIDELINES V23.0," 19 December 2016. [Online]. Available: http://www.gsma.com/newsroom/all-documents/ir-65-ims-roaming-interworking-guidelines-v23-0/.

[4] I. Source, "http://www.koreaherald.com."

[5] Codan Radio Communications, [Online]. Available: https://www.codanradio.com/wp-content/uploads/hivenet_001-v2.jpg.

[6] Mass Live, "http://www.masslive.com," 2011. [Online]. Available: http://media.masslive.com/republican/photo/2011/12/10315332-standard.jpg.

[7] NOMAD, "http://nomadgcs.com/," [Online]. Available: http://nomadgcs.com/wp-content/uploads/2015/01/towable-communications-trailer.jpg.

[8] The Times of India, "http://timesofindia.indiatimes.com/," [Online]. Available: http://timesofindia.indiatimes.com/thumb/msid-51210989,width-400,resizemode-4/51210989.jpg.

[9] Canadian Coast Guard, "http://www.ccg-gcc.gc.ca/," [Online]. Available: http://www.ccg-gcc.gc.ca/folios/00617/images/mspv-charles.jpg.

[10] Editor, "National Interagency Fire Center," [Online]. Available: NIFC: https://www.nifc.gov/fireInfo/nfn.htm.

[11] Editor, "NIFC Report for November 23, 2016," NIFC, 23 November 2016. [Online]. Available: https://www.predictiveservices.nifc.gov/IMSR/2016/20161123IMSR.pdf.

[12] Editor, "Stadiums of Pro Football - NFL Stadium Comparisons," [Online]. Available:

http://www.stadiumsofprofootball.com/comparisons/.

[13] D. Greenwald, "The Oregonian/Oregon Live - The 23 best and worst things about the Sasquatch! 2016 festival," 02 June 2016. [Online]. Available: http://www.oregonlive.com/music/index.ssf/2016/05/the_23_best_and_worst_things_sasquatch_festival_2016.html.

[14] J. ROBINSON, "nw news network - Rural Hospital Frustrated With Role As Sasquatch Festival's Emergency Room," 20 May 2014. [Online]. Available: http://nwnewsnetwork.org/post/rural-hospital-frustrated-role-sasquatch-festivals-emergency-room.

[15] NPSTC/CITIG, "NPSTC - Cross Border Communications Report Barriers, Opportunities, and Solutions for," 11 March 2015. [Online]. Available: http://npstc.org/download.jsp?tableId=37&column=217&id=3360&file=CrossBorder_Communications_FINAL_20150311.pdf.

[16] GSMA, "GSMA IR.65, "IMS Roaming and Interworking Guidelines v23.0," 19 December 2016. [Online]. Available: http://www.gsma.com/newsroom/wp-content/uploads//IR.65-v23.0.pdf.

[17] 3GPP ETSI, "Universal Mobile Telecommunications System (UMTS); LTE; Network sharing; Architecture and functional description (3GPP TS 23.251 version 11.4.0 Release 11".

[18] D. Jackson, "IWCE Urgent Communications - Mexico seeks bids for nationwide 700 MHz wholesale LTE network to serve competitive market, public safety," 10 February 2016. [Online]. Available: http://urgentcomm.com/long-term-evolution/mexico-seeks-bids-nationwide-700-mhz-wholesale-lte-network-serve-competitive-mar.

[19] Motorola, "Motorola Solutions - Motorola Solutions Demonstrates How Public Safety Broadband Solutions Can Contribute to a Safer Mexico," 17 November 2016. [Online]. Available: https://newsroom.motorolasolutions.com/news/motorola-solutions-demonstrates-how-public-safety-broadband-solutions-can-contribute-to-safer-mexico.htm.

[20] 3GPP, "3GPP TS 36.300 version 13.2.0 Release 13 - LTE Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 Page 39," January 2016. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/136300_136399/136300/13.02.00_60/ts_136300v

130200p.pdf.

[21] A. Apostolaras, "www.eurecom.fr," 2015. [Online]. Available: http://www.eurecom.fr/en/publication/4596/download/cm-publi-4596.pdf.

[22] NPSTC Broadband Emerging Technologies Working, "Considerations for the FirstNet Local Agency Information Homepage," 2016.

[23] 3GPP, "3GPP TS 23.303 version 12.2.0 Release 12 - Universal Mobile Telecommunications System (UMTS); LTE; Proximity-based services (ProSe); Stage 2," 2014.

[24] 3GPP, "3GPP - SA6 - Mission-critical applications," 2017. [Online]. Available: http://www.3gpp.org/specifications-groups/sa-plenary/sa6-mission-critical-applications.

[25] DHS First Responders Group , "Advanced Communications Video Over LTE: Efficient Network Utilization Research," 2015.

[26] 3GPP, "www.3GPP.org," [Online]. Available: http://www.3gpp.org/news-events/3gpp-news/1455-Public-Safety.

[27] NPSTC - Broadband Working, "Mission Critical Voice Communications Requirements for Public Safety ," 2011.

[28] NPTSC - Broadband Working, "Public Safety Broadband Push-to-Talk over Long Term Evolution Requirements," 2013.

[29] FirstNet RFP, "Federal Business Opportunities - FirstNet RFP," [Online]. Available: https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=33106ecc75222458a6e4405b0f66bd2e&_cview=0.

[30] Jeffrey Cichonski et al, "DRAFT NIST Special 1 Publication 800-187 - Guide to LTE Security," 2016. [Online].

[31] FirstNet RFP, "Federal Business Opportunities - FirstNet RFP," 2016. [Online]. Available: https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=7806696f4340f16474647ccc57805040&_cview=0.

[32] U.S. Department of Homeland Security - SAFECOM, "Interoperability Continuum Chart,"

2006.

[33] NPSTC and NRPC, ""700 MHz Nationwide Deployable Trunked Solutions" A Report by NPSTC and the NRPC," 2015.

[34] 3GPP, "3GPP TS 23.335, User Data Convergence (UDC); Technical realization and information flows; Stage 2, Release 12," September 2014.

[35] "Canadian Public Safety Operatons Organization (CanOps)," [Online]. Available: https://www.masas-x.ca/en.

[36] OPEN Process Framework (OPF), "Interoperability Requirements," [Online]. Available: http://www.opfro.org/index.html?Components/WorkProducts/RequirementsSet/Requirements/InteroperabilityRequirements.html~Contents.

[37] U.S. Department of Homeland Security,, "US DHS, Developing Operational Requirements – A Guide to the Cost-Effective and Efficient Communications of Needs version 2.0," 2008.

[38] NPSTC - Public Safety Grade Task Group, "NPSTC - Defining Public Safety Grade Systems and Facilities, Final Report," 2014.

[39] National Insititue of Standards and Technology - NIST, "Managing Information," 2011.

[40] National Institute of Standards and Technology (NIST)/Department of Commerce Joint Task Force, "NIST SP800-53 “Security and Privacy Controls for Federal Information Systems and Organizations” .," 2013.

[41] National Insitute of Standards and Technology - NIST, "Security and Privacy Controls for Federal Information Systems and Organizations," 2011.

[42] National Institute of Standards and Technology (NIST), "NIST SP 800-137Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," 2011.

[43] Open Security Architecture , "IT Security Requirements," [Online]. Available: http://www.opensecurityarchitecture.org/cms/definitions/it_security_requirements. [Accessed February 2017].

[44] Common Criteria, "Common Criteria for Information Technology Security Evaluation,"

July 2009. [Online]. Available:
https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf.

The following documents were reviewed by the Working Group but did not result in specific citations within the report. They are listed here as supplemental reports.

a) FirstNet, "FirstNet Deployables Request For Information,"8 July 2013.

b) ABSOLUTE Project Newsletter, 02/2015

c) Jim Strother (Editor), “ABSOLUTE End Users’ Requirements D2.2.2,” 09/30/2013

d) Macia Mut (Editor), Philippe Charpentier (Editor), “ABSOLUTE System Requirements D2.4.2 v.1.0,” 01/31/2014

*e)* The Los Angeles Regional Interoperable Communications System (LA-RICS), "Request for Proposals for a Public Safety Broadband Network (PSBN)," RFP No. LA-RICS 008, August 13, 2013

f) New Jersey Broadband Technology Opportunity Program (BTOP) Appendix A - Statement of Compliance.

g) UK Emergency Services Mobile Communications Programme, summary of requirements for Mobile Base Stations and Gateway Solutions and Devices.

h) Defence Research and Development Canada - Centre for Security Science, "PSBN Operational Requirements," October 2013, unpublished.

i) ibid, "PSBN Security Requirements," November 2013, unpublished.

j) ibid, "PSBN Interoperability Requirements," August 2014, unpublished.

k) Next Generation Mobile Network Alliance, "Recommended Practices for Multi-vendor SON Deployment,",28 January 2014.

l) Technical Advisory Board for First Responder Interoperability, "Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network,"22 May 2012.

m) Federal Communications Commission - Public Safety and Homeland Security Bureau, "White Paper: The Role of Deployable Aerial Communications Architecture in Emergency Communications and Recommended Next Steps," September 2011.

# APPENDIX G: Terminology, Definitions, and Acronyms

This Appendix includes terminology and definitions which were used by the Working Group in order to standardize technical discussions. This list was adapted from the report "Integrated Dictionary of Terms and Acronyms for a Canadian Public Safety Broadband Network," published in September of 2014. Please note that the attached list may include terms which are not included in this report.

**Left Application Programming Interface (API):** An Application Programming Interface (API) is a particular set of rules and specifications that a software program can follow to access and make use of the services and resources provided by another particular software program that implements that API. It serves as an interface between different software programs and facilitates their interaction, similar to the way the user interface facilitates interaction between humans and computers.

**Catastrophic Failure**: The inability of the NPSBN to deliver the required communications services at or above a minimum level of acceptable quality due to failure of connectivity, equipment, software, or capability for which there is no working stand-by or automatic recovery within a time period that is deemed to be acceptable by authorized entities. This may result from simultaneous failures of the main and redundant systems. Recovery from a catastrophic failure requires a manual intervention to repair the fault to a sufficient level that the capability is restored, even if initially it is without back-up.

**Deployable Systems**: Deployable systems refer to transportable communication systems composed of specific physical and logical configurations that render them operable in tactical environments of different degrees of harshness. Deployable systems may operate autonomously or assisted by fixed communications infrastructure. They may be hardened to operate in adverse environmental conditions, or they may be sheltered in controlled physical environments.

**Emergency Operations Centre (EOC**): The Emergency Operations Centre is strategic command and control function that does not typically engage in the tactical decision-making of the incident response, which is the role of the ICC. The EOC gathers and analyzes data and provides a decision-support function to the ICC. The EOC may liaise with media and external agencies. There would be typically, one EOC plus a redundant EOC, per region.

**Public Safety Entity Administrator**: The person(s) responsible for administering the user profiles of the users within the jurisdiction of his/her public safety agency. The administrator may monitor the Key Performance Indicators (KPI) of the NPSBN within prescribed limits. The administrator can control some configurable parameters of the NPSBN, such as priority and QoS, within prescribed limits. The administrator would have the authority to configure some parameters of the deployable systems under their jurisdiction. The division of responsibilities and range of authority for the administrator with respect to configuration control of deployables and priority and QoS assignments would be by agreement between the public safety entities and the network operator.

**First Responder**:Those individuals who are federal, state/provincial/territorial, tribal, and local emergency public safety, law enforcement, emergency response, firefighters, and emergency medical personnel. The definition may be used more broadly to include those who are responsible for the protection and preservation of life, property, evidence, and the environment, as well as emergency management, public health, clinical care, public works, and other skilled support personnel, such as equipment operators, who provide immediate response or related support services during prevention, response, and recovery operations.

**Immediate Peril Situation:** Indicates an immediate threat to human life and a responder's need for immediate assistance. This function may also be used, for example, when the destruction of property or other events may imminently endanger human life. Immediate Peril should be rarely used. Examples: forest fire about to circle campers, tanker truck about to explode near school, paramedic video consultation required with a doctor regarding a poisoned patient.

**Incident Area Network (IAN):** The IAN is the communications network that serves the geographic area that encompasses the users that are engaged in the response to an incident.

**Information Network:** In the context of the NPSBN, refers to public safety databases, services, and applications.

**Interoperability:** Wireless communications interoperability refers to the ability of users to share information via voice and data applications – on demand, in real time, when needed, and as authorized. The Communications Interoperability Continuum is shown in Figure 1. Each lane in the Continuum represents a pillar of communications interoperability and illustrates that the state of interoperable communications is a matter of degree. The leftmost states typify the lowest state of interoperable communications, whereas the right-most states represent a high degree of interoperability.

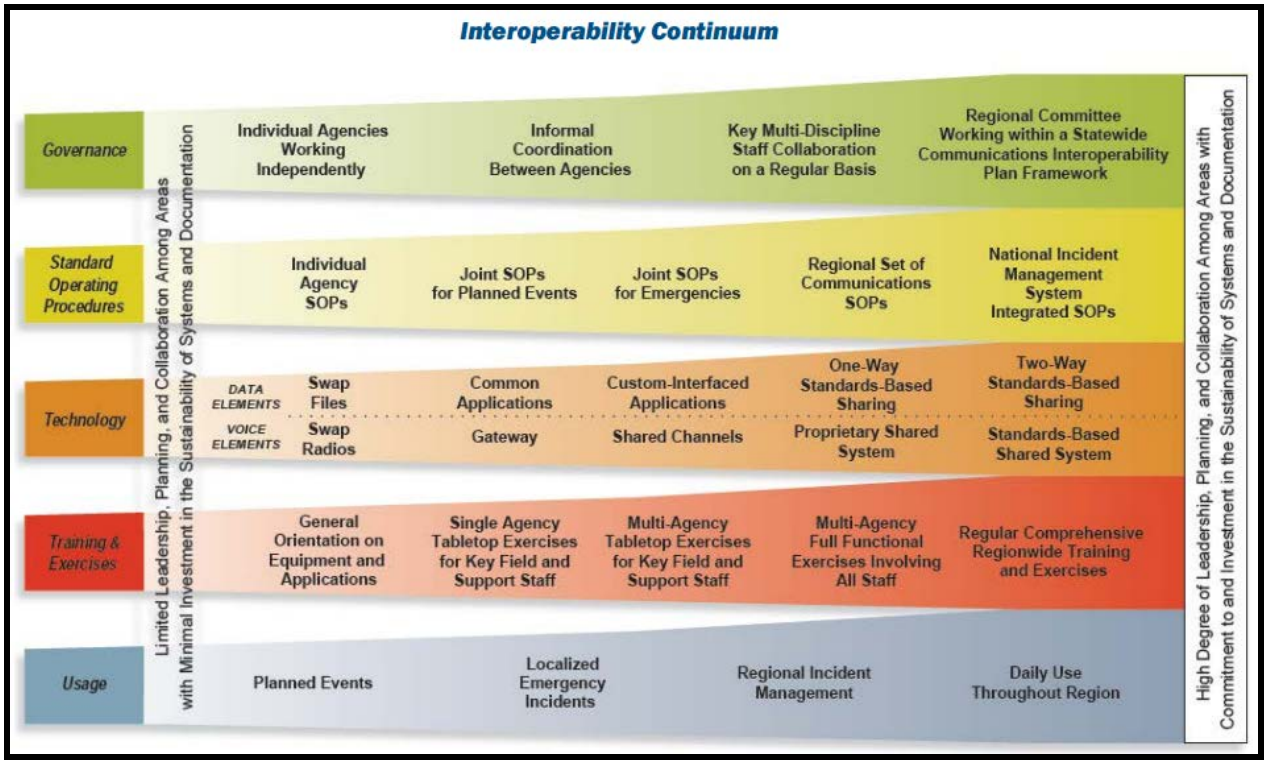



*FIGURE 1: Communications Interoperability Continuum [32]*

**Interoperability Requirement**: An *interoperability requirement* is a user-oriented requirement that specifies the degree to which something is connected to and operates with others. [36] The typical objectives of an interoperability requirement are to ensure the application or component interoperates with other specified applications and components in the following manner:

- Can pass necessary data to the other applications and components.
- Can receive necessary data from the other applications and components.
- Can use the data it receives.
- Can request the public services of the other applications and components.
- Can have its public services requested by the other applications and components.

**Location Information**: Location information typically describes the latitude, longitude, bearing, speed, time, height and other location information related to a UE device and/or end user.

**Mission Critical**: Refers to a system, device, service, or activity whose failure or disruption will result in the immediate inability of a person or entity to fulfill his/her/its mission.

**Mobile Command Centre (MCC):** A Mobile Command Center would have a similar function as the ICC, but is contained within a vehicle or trailer. The MCC may be used to enhance emergency preparedness or function as a backup to the ICC.

**Mobile Data Terminal (MDT):** A device which is typically within a vehicle, that provides a visual representation of information with a capability of entering information. The MDT has connectivity to the LTE network through some mechanism (integrated LTE radio or interface to a local LTE device through wired or wireless means). An MDT may be a laptop, heads-up display, tablet, LTE dash-mount radio, or similar device.

**Network Administrator**: The person(s) responsible for overseeing the set-up, operation, provisioning services, and maintenance of the PSBN. The network administrator interacts directly with the PSBN as an administrative user and has higher levels of authorized access to the PSBN. There may be a hierarchy of authorization levels within the network administration function. Network Administrators are members of the Network Operator's organization.

**Operational Requirements**: Operational requirements represent the problem space of the requirements hierarchy as illustrated in the US Transportation Safety Administration example of Figure 2. Whereas Technical Requirements represent the solution space, Operational Requirements are typically qualitative statements that describe a needed capability.

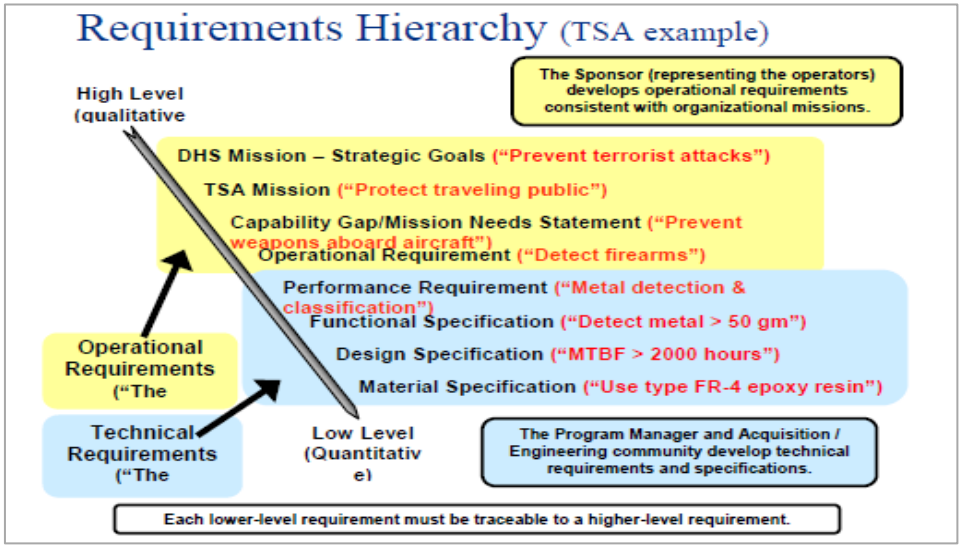



*Figure 2: The requirements hierarchy – U.S. Dept. of Homeland Security example. [37]*

**Over-The-Top (OTT):** Over-The-Top (OTT) refers to content such as video, images, audio, and other media that is managed and controlled by a service that is not the Internet service provider (ISP). Whereas the ISP provides the connectivity between the user and the content servers, it is the OTT provider that is responsible for controlling access to the content and collecting revenues, if any, from subscriptions to the content. An example of an OTT provider is

Netflix. Netflix uses the ISPs to deliver its content, but retains the rights to the contents and owns the relationship with the consumers of its contents. Another example of an OTT provider is Google. The chat and messaging applications from Google use the ISPs to connect users, but Google owns and operates the messaging service.

**Nationwide Public Safety Broadband Network (NPSBN):** The NPSBN is an LTE-based communications network operating on the 3GPP Band Class-14 frequency band, or a portion thereof, as well as any other radio access technologies and core network elements that are used to serve the intended user base, under the control of the NPSBN operator. It is the collection of the regional and national components, physical facilities, applications, user equipment, and other devices. The NPSBN can be functionally partitioned as follows: a) LTE core and RAN infrastructure, b) user devices, c) backhaul network, d) deployable systems, e) alternative access and networking technologies such as other 3GPP and non-3GPP technologies, f) operations support systems applications, g) end-user applications that are hosted by the operators of the PSBN, h) networking appliances such as routers and servers, and i) security appliances and applications such firewalls and intrusion detection probes. Not included in the NPSBN are customer premise equipment that reside in End User Agency networks such as databases and servers. Client-hosted applications such as computer-aided dispatch and records management systems are also excluded from the NPSBN.

**Public Safety Grade:** The definition of "Public Safety Grade" (PSG) has been published in the NPSTC report by the same title [38]. PSG designates a degree of robustness of the PSBN in light of anticipated threats and risks such that it can remain operational during and immediately following natural or man-made disasters. NPSTC has defined "public safety grade" for the following characteristics:

- Reliability and resiliency
- Coverage
- Push-To-Talk services
- Application
- Site hardening
- Installation
- Operations and Maintenance

In addition, the PSG report recommends best practices where appropriate, since the attributes of PSG are not the sole purview of the network itself.

**Public Safety Multimedia Emergency Services (MMES):** Public Safety MMES are next generation emergency services utilizing real-time session – and non-session-based text and other multimedia, in addition to voice that are based on trusted applications in support of non-voice communications amongst responders and command centers. Public Safety MMES

provides secure transport of messaging and media content, and location information of the reporting device.

**Redundancy:** Redundancy is the property of duplicating functions such that one or more failures do not cause a catastrophic failure. This is achieved by having the PSBN switch to the duplicate, i.e., redundant functions, in less time than would cause a catastrophic failure. A redundancy strategy would be derived from a failure mode and effects analysis that typically, would uncover single points of failure and the impacts of those failures.

**Resiliency:** The ability to withstand stress or adversity. In the context of the PSBN, resiliency can be considered to be the degree of hardening of the infrastructure to withstand environmental forces. In the event of catastrophic failure, resiliency is also determined by the speed with which the PSBN service is restored. The property of resiliency encompasses the supply chain, maintenance procedures, diagnostic properties, skill level of maintenance resources, ease of repair, and sparing strategy.

**Roaming:** ”Roaming” refers to the hand-off of connectivity from the PSBN to a partner’s network with whom the PSBN operators have roaming agreements in force. Roaming means connecting to an alternative carrier in the home location or outside of the home location.

**Security Controls:** A management, operational, or technical high-level security requirement prescribed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls are implemented using various types of security solutions that include security products, security policies, security practices, and security procedures. [39].

**Security Gateway:** The network domain control plane of a Network Domain Security/IP (NDS/IP) network is sectioned into security domains and typically these coincide with operator borders. The border between the security domains is protected by Security Gateways (SEGs). The SEGs are responsible for enforcing the security policy of a security domain towards other SEGs in the destination security domain. The network operator may have more than one SEG in its network in order to avoid a single point of failure or for performance reasons. A SEG may be defined for interaction towards all reachable security domain destinations or it may be defined for only a subset of the reachable destinations.

**Security Posture:** A characteristic of an information system that represents its resilience to a specific set of deliberate attacks and accidental and natural hazards (i.e., selected threats). [40]

- Level of assurance that adequate technical security controls have been implemented to meet the information protection needs, as defined by Federal Information Processing Standard (FIPS) 200, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. [41]

- The security status of an organization's networks, information, and systems based on Information Assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the organization and to react as the situation changes. [42]

**Security Requirements:** There are two types of security requirements. [43]

- Functional Security Requirements: These are security services that need to be achieved by the system under inspection. Examples could be authentication, authorization, backup, server-clustering, etc. This requirement artifact can be derived from best practices, policies, and regulations.

- Non-Functional Security Requirements: These are security related architectural requirements, like "robustness" or "minimal performance and scalability." This requirement type is typically derived from architectural principals and good practice standards.

Alternative definition: A requirement, stated in a standardized language, which is meant to contribute to achieving the security objectives for a Target Of Evaluation, i.e. a set of software, firmware and/or hardware possibly accompanied by guidance. [44]

**"Shall":** The attribute, which is the object of the sentence with "shall" as the auxiliary verb, is essential or necessary to ensure the operability, interoperability, or security of the PSBN. Alternatively, the non-adoption of the attribute which is the object of the sentence would present a high risk for non-operability, non-interoperability, or security vulnerability of the PSBN.

**"Should":** The attribute, which is the object of the sentence with "should" as the auxiliary verb, is proffered as guidance or as a recommendation for the standards that apply to the attribute. In light of other standards which may exist, the sentence conveys the recommendation of the authors for what standards to apply to the PSBN. The use of other standards could impede attaining the recommended operating state, increase the risk of non-interoperability, or increase the security vulnerability of the PSBN due to lack of significant adherents to the alternative standards, or pending obsolescence, or other similar risks.

**Untrusted Network:** Any type of access network that is not under control of the operator (public open hotspot, subscriber's home Wireless Local Area Network [WLAN], etc.) and which does not provide sufficient security (authentication, encryption, etc.).

**User:** A user is a person or machine authorized to access the resources available on the NPSBN and to communicate with other users on the network, or subscribers of other services globally. The users are deemed to belong to the following user groups:

**Front-line users/end-users:**

- Police, Fire, Emergency Medical Services; from local, state/provincial/territorial, tribal and federal agencies.
- Forestry, public works, public transit, dangerous chemical clean-up, customs, and other agencies contributing to public safety.
- Other government and certain non-governmental organizations, agencies, or entities,
- Commercial subscribers.

**Back-office users**

- Network administrators: interface with the network via a dashboard; able to configure service-affecting and non-service-affecting parameters according to hierarchical levels of authorization.
- Security officer: monitor usage; policies and procedures.

**Operations support users**

- Field technicians with access to physical facilities: may or may not be authorized to perform service-impacting maintenance actions.
- Network engineers: conduct performance evaluations and tests; take action related to expansion or optimization of the network; likely to impact service.
- Value-Added Services staff: bring new applications on-line.

**Machines**

- Mobile access routers: gateway to dismounted officers' handheld devices, vehicle telemetry, dashboard cameras, license plate readers, vehicle-mounted computers.
- Portable sensors: tactical optical and infra-red cameras.

**User Equipment (UE):** User equipment refers to the mobile equipment that is on the client side of the LTE radio access network. It may be a handheld device such as a smartphone, a dongle that connects to a computer or laptop, it may be embedded in sensors, or it may have other form factors. The UE is a functionally integrated unit and, typically can be assigned a stock keeping unit (SKU). For example, if the UE is a dongle that is attached to a laptop, the laptop is not part of the UE. If the laptop has an embedded Band-14 LTE modem allowing it to connect to the PSBN, then the laptop is the UE.

# List of Acronyms

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| AAA | Authentication, Authorization and Accounting |
| AC | Admission Control |
| ACC | Access Control Class |
| ACL | Access Control List |
| ADMF | Administrative Function |
| AES | Advanced Encryption Standard |
| AF | Application Function |
| AF | Authentication Framework |
| AFIS | Automated Fingerprint Identification System |
| AH | Authentication Header |
| ALPR | Automated License Plate Reader |
| AMBR | Aggregate Maximum Bit Rate |
| AMR | Adaptive Multi-Rate |
| AN | Access Network |
| ANDSF | Automatic Network Discovery Function |
| A-NOC | Agency Network Operations Centre |
| APB | All-Points Bulletin |
| APCO | Association of Public-Safety Communications Officials International |
| API | Application Programming Interface |
| APN | Access Point Name |
| ARP | Allocation Retention Priority |
| AS | Application Server |
| ASP | Application Service Provider |
| ATP | Acceptance Test Procedure |
| AVL | Automatic Vehicle Location |
| BB | Broadband |
| BBDS | Broadband Deployable System |
| BBF | Broadband Forum |
| BCAST | Broadcast Services Enabler Suite |
| BCCH | Broadcast Control Channel |
| BCF | Border Control Function |
| BCGF | Border Control Gateway Function |
| BCM | Business Continuity Management |
| BGCF | Breakout Gateway Control Function |

| | |
|---|---|
| BGF | Border Gateway Functions |
| BM-SC | Broadcast Multicast Service Center |
| BS | Base Station |
| BSS | Business Support System |
| BTB | Beyond the Border |
| BYOD | Bring-Your-Own-Device |
| CAD | Computer-Aided Dispatch |
| CALEA | Communications Assistance for Law Enforcement Act (USA) |
| CAN-US | Canada – USA |
| CAZAC | Constant Amplitude Zero Autocorrelation Codes |
| CBC | Cell Broadcast Centre |
| CBE | Cell Broadcast Entity |
| CBS | Cell Broadcast Service |
| CC | Content of Communication |
| CCBG | Critical Communications Broadband Group |
| CCIRC | Canadian Cyber Incident Response Centre |
| CCTV | Closed Circuit Television |
| CDF | Charging Data Function |
| CDMA | Code Division Multiple Access |
| CDR | Call Detail Record |
| CDR | Charging Data Record |
| CGF | Charging Gateway Function |
| CGW | Charging Gateway |
| CIRTEC | Communications Interoperability Research Test and Evaluation Centre (Canada) |
| CM | Congestion Management |
| CM | Configuration Management |
| CMAS | Commercial Mobile Alert System (USA) |
| CODEC | Coder-Decoder |
| COLT | Cell On Light Truck |
| CoMP | Coordinated MultiPoint |
| COPS | Community Oriented Policing Service |
| COW | Cell On Wheels |
| CPE | Customer Premise Equipment |
| CPIC | Canadian Police Information Centre |
| CSCF | Call Session Control Function |
| CSEC | Communications Security Establishment Canada |
| CSP | Credential Service Provider |
| CSS | Centre for Security Science (Canada) |

| | |
|---|---|
| CSSP | Canadian Safety and Security Program |
| CTIA | Cellular Telecommunications Industry Association (USA) |
| D2D | Device to Device |
| DASH | Dynamic Adaptive Streaming over HTTP |
| DCH | Data Clearing House |
| DDoS | Distributed Denial of Service |
| DEA | Drug Enforcement Agency |
| DHCP | Dynamic Host Configuration Protocol |
| DHS | Department of Homeland Security (USA) |
| DHS OEC | DHS Office of Emergency Communications (USA) |
| DL | Down-Link |
| DM | Device Management |
| DMR | Digital Mobile Radio |
| DMRS | Demodulation Reference Signal |
| DMZ | De-Militarized Zone |
| DND | Department of National Defence |
| DNS | Domain Name System |
| DoJ | Department of Justice (USA) |
| DoS | Denial of Service |
| DRA | Diameter Routing Agent |
| DRDC | Defence Research & Development Canada |
| DRDKIM | Defence Research & Development Knowledge & Information Management |
| DRII | Disaster Recovery Institute International |
| DS | Deployable Systems |
| DSCP | Differentiated Services Code Point |
| DSMIP | Dual Stack Mobile IP |
| DTN | Disruption Tolerant Networking (for Space Operations) |
| DUT | Device Under Test |
| E911 | Enhanced 9-1-1 |
| EAP | Extensible Authentication Protocol |
| ECG | Electrocardiogram |
| ECGI | E-UTRAN Cell Global Identifier |
| ECI | E-UTRAN Cell Identifier |
| ECM | Electronic Counter Measure |
| EDACS | Enhanced Digital Access Communication System |
| EDXL | Emergency Data Exchange Language |
| eICIC | enhanced Inter-Cell Interference Coordination |
| EM | Element Manager |

| | |
|---|---|
| eMBMS | enhanced Multimedia Broadcast Multicast Services |
| EMS | Emergency Medical Services |
| eNB | evolved Node-B |
| eNB ID: | e-Node-B Identifier |
| ENUM | (ITU-T) E.164 Number Mapping |
| EOC | Emergency Operations Centre |
| EPC | Evolved Packet Core |
| ePDG | enhanced Packet Data Gateway |
| EPS | Evolved Packet System |
| EPWS | Emergency Public Warning System |
| ER | Emergency Room |
| ESINet | Emergency Services IP NETwork |
| ESP | Encapsulating Security Payload |
| ETA | Estimated Time of Arrival |
| eTOM | enhanced Telecommunications Operations Map |
| EUA | End-User Agency |
| EUA-A | End-User Agency Administrator |
| E-UTRA | Evolved Universal Terrestrial Radio Access |
| E-UTRAN | Evolved UMTS Terrestrial Radio Access |
| EV-DO | EVolution Data Optimized |
| F/P/T/M | Federal/Provincial/Territorial/Municipal |
| FBI | Federal Bureau of Investigation |
| FCAPS | Fault, Configuration, Accounting, Performance, and Security |
| FCC | Federal Communications Commission (USA) |
| FDD | Frequency Division Duplex |
| FEMA | Federal Emergency Management Agency (USA) |
| FICAM | Federated Identity, Credentials, and Access Management |
| FIM | Federated Identity Management |
| FIPS | Federal Information Processing Standard (USA) |
| FLUTE | File Delivery over Unidirectional Transport |
| FMC | Fixed Mobile Convergence |
| FRS | Facial Recognition System |
| FTP | File Transport Protocol |
| GBR | Guaranteed Bit Rate |
| GCS | Ground Control Station |
| GCSE | Group Communications System Enablers |
| GFIPM | Global Federated Identity and Privilege Management |
| GHz | gigahertz |

| | |
|---|---|
| GIS | Geographic Information System |
| GoS | Grade of Service |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| GSM | Global System for Mobile Communications or Groupe Spécial Mobile |
| GSMA | GSM Association |
| GTP-C | GPRS Tunneling Protocol for the Control plane |
| GTP-U | GPRS Tunneling Protocol for the User plane |
| GUI | Graphical User Interface |
| GUMMEI | Globally Unique Mobility Management Entity Identifier |
| GW | Gateway |
| HazMat | Hazardous Materials |
| HetNet | Heterogeneous Networks |
| HF | High Frequency |
| HLR | Home Location Register |
| HPMN | Home Public Mobile Network |
| HSPA | High Speed Packet Access |
| HSS | Home Subscriber Server |
| HTRA | Harmonized Threat, Risk Assessment Methodology |
| HTTP | Hypertext Transfer Protocol |
| IAN | Incident Area Network |
| I-BCF | Interconnection Border Control Function |
| IBET | Integrated Border Enforcement Team |
| I-BGF | Interconnection Border Gateway Function |
| IC | Incident Command |
| ICAM | Identity, Credentials, and Access Management |
| ICC | Incident Command Centre |
| ICIC | Inter-Cell Interference Coordination |
| ICM | Identity and Credentials Management |
| ICS | Incident Command System |
| ICT | Information and Communications Technology |
| ID | Identifier |
| ID | Identity |
| IdM | Identification Management |
| IDS | Intrusion Detection System |
| IETF | Internet Engineering Task Force |
| IFOM | IP Flow Mobility |
| IKE | Internet Key Exchange |

| | |
|---|---|
| IMEI: | International Mobile Equipment Identity |
| IMPI | IP Multimedia Private Identity |
| IMPU | IP Multimedia Public Identity |
| IMS | Incident Management System |
| IMS | IP Multimedia Subsystem |
| IMS-AGW | IP Multimedia Sub-system – Access Gateway |
| IMSI | International Mobile Subscriber Identity |
| IM CN | IP Multimedia Subsystem Core Network |
| IOT | Interoperability Test |
| IP | Internet Protocol |
| IPAWS | Integrated Public Alert and Warning System |
| IPsec | IP security |
| IPX | IP eXchange |
| IRD | Interoperability Requirements document |
| IRI | Intercept Related Information |
| IRP | Integration Reference Point |
| ISC | IP Multimedia Service Control |
| I/S-CSCF | Interrogating/Serving Call Session Control Function |
| ISDN | Integrated Services Digital Network |
| ISIM | IP Multimedia Service Identity Modules |
| ISO | International Organisation for Standardisation |
| ISUP | ISDN User Part |
| IT | Information Technology |
| ITS | Information Technology Security |
| ITU | International Telecommunication Union |
| IWLAN | Integrated/Interworked WLAN |
| JTF2 | Joint Task Force 2 |
| KPI | Key Performance Indicator |
| LAN | Local Area Network |
| LBS | Location Based Services |
| LEMF | Law Enforcement Monitoring Facility |
| LI | Lawful Intercept |
| LIPA | Local IP Access |
| LMR | Land Mobile Radio |
| LTE | Long Term Evolution |
| MAC | Media Access Control |
| MAG | Mobility Access Gateway |
| MANET | Mobile Ad-hoc Network |

| | |
|---|---|
| MASAS | Multi Agency Situational Awareness System |
| MBMS | Multimedia Broadcast Multicast Services |
| MBMS GW | Multimedia Broadcast Multicast Services Gateway |
| MBR | Maximum Bit Rate |
| MCC | Mobile County Code |
| MCC | Mobile Command Centre |
| MCE | Multi-cell/multicast Coordination Entity |
| MCS | Modulation and Coding Scheme |
| MCV | Mobile Command Vehicle |
| MCV | Mission Critical Voice |
| MDT | Mobile Data Terminal |
| MDT | Minimization of Drive Tests |
| ME | Mobile Equipment |
| MGCF | Media Gateway Control Function |
| MGW | Media Gateway |
| MHz | megahertz |
| MIB | Management Information Base |
| MIME | Multipurpose Internet Mail Extensions |
| MIMO | Multiple Input Multiple Output |
| MIP | Multilateral Interoperability Programme |
| MITS | Management of Information Technology Security |
| MME | Mobility Management Entity |
| MMEGI | MME Group Identifier |
| MMES | Multi-Media Emergency Services |
| MMS | Multimedia Messaging Service |
| MNC | Mobile Network Code |
| MOCN | Multi-Operator Core Network |
| MPEG | The Moving Picture Experts Group |
| MRFP/C | Media Resource Function Processor/Controller |
| MS | Mobile Station |
| MSF | Multi Service Forum |
| MSISDN | Mobile Station International Subscriber Directory Number |
| MT | Maintenance Technician |
| MVPN | Mobile Virtual Private Network |
| NA | Network Administrator |
| NAAD | National Alert Aggregation & Dissemination |
| NaaS | Network as a Service |
| NAD | Network Architecture Description |

| | |
|---|---|
| NAPT | Network Address and Port Translation |
| NAS | Non-Access Stratum |
| NAT | Network Address Translation |
| NDS | Network Domain Security |
| NE | Network Element |
| NENA | National Emergency Numbering Association |
| NG 911 | Next Generation 911 |
| NGN | Next Generation Network |
| NGO | Non-Governmental Organization |
| NGOSS | Next Generation Operations Support System |
| NI | Network Identifier |
| NIEM | National Information Exchange Model |
| NIMS | National Incident Management System (USA) |
| NIST | National Institute of Standards and Technology (USA) |
| NLOS | Non-Line-Of-Sight |
| NLP | Natural Language Processing |
| NM | Network Manager |
| NMC | Network Management Centre |
| NNI | Network-to-Network Interface |
| N-NOC | National Network Operations Centre |
| NOC | Network Operations Centre |
| NPSTC | National Public Safety Telecommunications Council (USA) |
| NRM | Network Resource Model |
| NTP | Network Time Protocol |
| O&M | Operations and Maintenance |
| OAM | Operations Administration and Maintenance |
| OAM&P | Operations, Administration, Maintenance, and Provisioning |
| OASIS | Organization for the Advancement of Structured Information Standards |
| OCS | Online Charging System |
| OMA | Open Mobile Alliance |
| OR | Operational Requirement |
| ORD | Operational Requirements Document |
| OS | Operating System |
| OSA SCS | Open Services Access Service Capability Server |
| OSS | Operations Support Systems |
| OTA | Over-The-Air |
| OTT | Over-The-Top |
| PC | Personal Computer |

| | |
|---|---|
| PCC | Policy Charging Control |
| PCEF | Policy Charging and Enforcement Function |
| PCFICH | Physical Control Format Indicator Channel |
| PCI | Physical Cell Identity |
| PCM | Pulse Code Modulation |
| PCRF | Policy Charging and Rules Function |
| P-CSCF | Proxy Call Session Control Function |
| PDCP | Packet Data Convergence Protocol |
| PDN | Packet Data Network |
| PDN ID: | Packet Data Network Identifier (same as APN) |
| PGS | Policy on Government Security |
| PGW | Packet Gateway |
| PGW ID: | Packet Data Network Gateway Identifier |
| PHB | Per-Hop Behavior |
| PIA | Privacy Impact Assessment |
| PIN | Personal Identification Number |
| PIV | Personal Identification Verification |
| PKI | Public Key Infrastructure |
| PLMN | Public Land Mobile Network |
| PLMN ID | PLMN Identifier |
| PLR | Packet Loss Rate |
| PMIP | Proxy Mobile IP |
| PMN | Public Mobile Network |
| PMR | Professional Mobile Radio |
| PoC | Push-To-Talk over Cellular |
| PPP | Public Private Partnership |
| P/QoS | Priority and Quality of Service |
| PRACH | Physical Random Access Channel |
| PS | Public Safety |
| PSAC | Public Safety Advisory Committee (USA) |
| PSAP | Public Safety Answering Point |
| PSBN | Public Safety Broadband Network |
| PSE | Public Safety Enterprise |
| PSS | Primary Synchronization Signal |
| PSST | Public Safety Spectrum Trust |
| PSTN | Public Switched Telephone Network |
| PTT | Push To Talk |
| PTZ | Pan Tilt Zoom |

| | |
|---|---|
| PWS | Public Warning System |
| QCI | Quality of Service Class Indicator |
| QoE | Quality of Experience |
| QoS | Quality of Service |
| R&D | Research and Development |
| RAN | Radio Access Network |
| RAP | Random Access Procedure |
| RAP | Returned Accounts Procedure |
| RAT | Radio Access Technology |
| RB | Resource Blocks |
| RBAC | Role-Based Access Control |
| RCMP | Royal Canadian Mounted Police |
| REGS | Resource Element Groups |
| REST | Representational State Transfer |
| RF | Radio Frequency |
| RFC | Request For Comments |
| RFI | Request For Information |
| RFID | Radio Frequency Identification |
| RFP | Request For Proposal |
| RLC | Radio Link Control |
| RMS | Records Management System |
| R-NOC | Regional Network Operations Centre |
| RPO | Recovery Point Objective |
| RRC | Radio Resource Control |
| RSDE | Regional Service Delivery Entity |
| RTO | Recovery Time Objective |
| RTP | Real-time Transfer Protocol |
| RTU | Remote Terminal Unit |
| SAE | System Architecture Evolution |
| SAML | Security Assertion Markup Language |
| SCADA | Supervisory Control and Data Acquisition |
| SCPS-TP | Space Communications Protocol Specification – Transport Protocol |
| SCTP | Stream Control Transmission Protocol |
| SDM | Service Delivery Model |
| SDO | Standards Development Organization |
| SDP | Session Description Protocol |
| SEG | Security Gateway |
| SGSN | Serving GPRS Support Node |

| | |
|---|---|
| SGW | Serving Gateway |
| SID | Shared Information Data model |
| SIP | Session Initiation Protocol |
| SIPTO | Selected IP Traffic Off-load |
| SKU | Stock Keeping Unit |
| SLA | Service Level Agreement |
| SMS | Short Message Service |
| SNMP | Simplified Network Management Protocol |
| SOA | Service Oriented Architecture |
| SOAP | Simple Object Access Protocol |
| SOC | Security Operations Centre |
| SON | Self Organizing Network |
| SOP | Standard Operating Procedure |
| SOT | Security Operations Team |
| SPR | Subscriber Profile Repository |
| SRD | Security Requirements Document |
| SRS | Sounding Reference Signal |
| SSO | Single Sign-on |
| SSS | Secondary Synchronization Signal |
| SUV | Sport Utility Vehicle |
| SWAT | Special Weapons and Tactics |
| TAC | Tracking Area Code |
| TAG | Technical Advisory Group (Canada) |
| TAI | Tracking Area Identifier |
| TAP | Transferred Account Procedure |
| TCCA | Tetra and Critical Communications Association |
| TETRA | Terrestrial Trunked Radio |
| THIG | Topology-Hiding Inter-network Gateway |
| TIA | Telecommunications Industry Association |
| TMC | Transportation Management Center |
| TMF | TeleManagement Forum |
| TRVA | Threat, Risk, Vulnerability Assessment |
| TS | Technical Specification |
| UDR | User Data Repository |
| UE | User Equipment |
| UICC | Universal Integrated Circuit Card |
| UL | Up-Link |
| UL-RS | Up-Link Reference Signals |

| | |
|---|---|
| UMTS | Universal Mobile Telecommunications System |
| URL | Uniform Resource Locator |
| USAT | USIM Applications Toolkit |
| USIM | UMTS Subscriber identity Module |
| UTC | Coordinated Universal Time |
| VANET | Vehicular Ad hoc Network |
| VLAN | Virtual Local Area Network |
| VoIP | Voice-over Internet Protocol |
| VoLTE | Voice over LTE |
| VPMN | Visited Public Mobile Network |
| VPN | Virtual Private Network |
| VQiPS | Video Quality in Public Safety (DHS OIC Working Group) |
| VSAT | Very Small Aperture Terminal |
| WAN | Wide Area Network |
| WCDMA | Wideband Code Division Multiple Access |
| Wi-Fi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |
| WPAS | Wireless Public Alerting System |
| WPS | Wireless Priority Service |
| XDMS | XML Document Management Server |
| XML | Extensible Mark-up Language |
| ZC | Zadoff-Chu |

# APPENDIX H: Detailed Diagrams

The following information is adapted from the "*Field Operational Test Facility for Next-Generation Interoperable Mission-Critical Communications – Final Analysis (D13)"* Report, 2015, funded by the Canadian Safety and Security Program. Some additional diagrams and drawings were created by the Working Group for illustration purposes to aid in the discussion.

The general remote network architecture concept for a Core-Enabled field-based deployed/tactical implementation of a BBDS is shown in **Figure H-1** and indicates the corresponding Long Term Evolution (LTE) interfaces (protocols and methods) operating over each connection.

The basic functions in an LTE network are based on Third Generation Partnership Program (3GPP) standards ("3G" and "4G" networking) and are as follows:

**User Equipment (UE):** The UE is the basic user device in LTE. It may be a smartphone, an in-vehicle LTE modem, an LTE dongle, or any other device that connects to the LTE radio frequency (RF) network. It is expected that UEs may be carried by humans, by vehicles (air, land or sea), or may even be in robotic and Unmanned Aerial Vehicle (UAV) systems.

**Evolved Node B (eNodeB):** The eNodeB is the "cell tower" or base station of an LTE network. The UE and eNodeB communicate with each other over a 3GPP RF standard network called the Evolved Universal Terrestrial Radio Access Network (E-UTRAN). This is often designated by the Uu interface name. This is the primary component of any deployed network. But, to function, it must communicate with an Evolved Packet Core (EPC) that runs the entire network – this includes the deployable and fixed nodes for the entire PS LTE network. The combination of UE, eNBs, and EPC is the Evolved Packet System (EPS).

**Mobility Management Entity (MME):** The MME provides support for UE mobility management and access to the EPC. The MME provides for handover (HO) between the public safety LTE network eNBs that are different networks (whereas eNBs on the same local network can support HO directly). This is different from roaming, which refers to movement between two different networks, such as a potential Canadian PSBN and the planned U.S. public safety broadband network to be operated by FirstNet. In LTE, a network is identified by a Public Land Mobile Network Identification Number (PLMID). Thus, HO occurs between eNBs with the same PLMN IDs. Roaming is between two different networks which have unique PLMNIDs. A user's usual home network is referred to as the H-PLMN and the visited network is called the V-PLMN.

**Home Subscriber Server (HSS):** The HSS provides information to the EPC on access rights and priority for UEs, and provides all authentication services and credentials (e.g., keys).

**Serving Gateway (SGW):** The SGW provides a *mobility anchor* – an apparent fixed point in the network for moving users - for User Plane traffic from a UE, even as they HO from one eNodeB to another. The SGW passes traffic between the PDN Gateway and the eNodeB. A UE is only represented by one SGW at a time but it is possible to move from one SGW to another during HO.

**Packet Data Network Gateway (PDN GW/PDG):** The PDN GW (or PDG) is the path for User Plane traffic from or destined to a UE, to or from a network external to the EPS, respectively. The PDN GW also provides for access to EPC via non-3GPP accesses via a range of mechanisms incorporating other servers. The EPC can support more than one external network by the use of multiple PDN GW servers. Additionally, the PDN GW is the user plane anchor for mobility between 3GPP access and *non-3GPP access*. Non-3GPP access can be other standards such as WiFi, WiMAX, or other alternative methods of *offload* of traffic from the usual 700 MHz E-UTRAN PS LTE network.

**Policy and Charging Rules Function (PCRF):** The PCRF communicates with the three components of the network that handle routing of User Plane traffic, and established a through-network set of Quality of Service (QoS) values for each network traffic flow, while also providing charging rules and services.

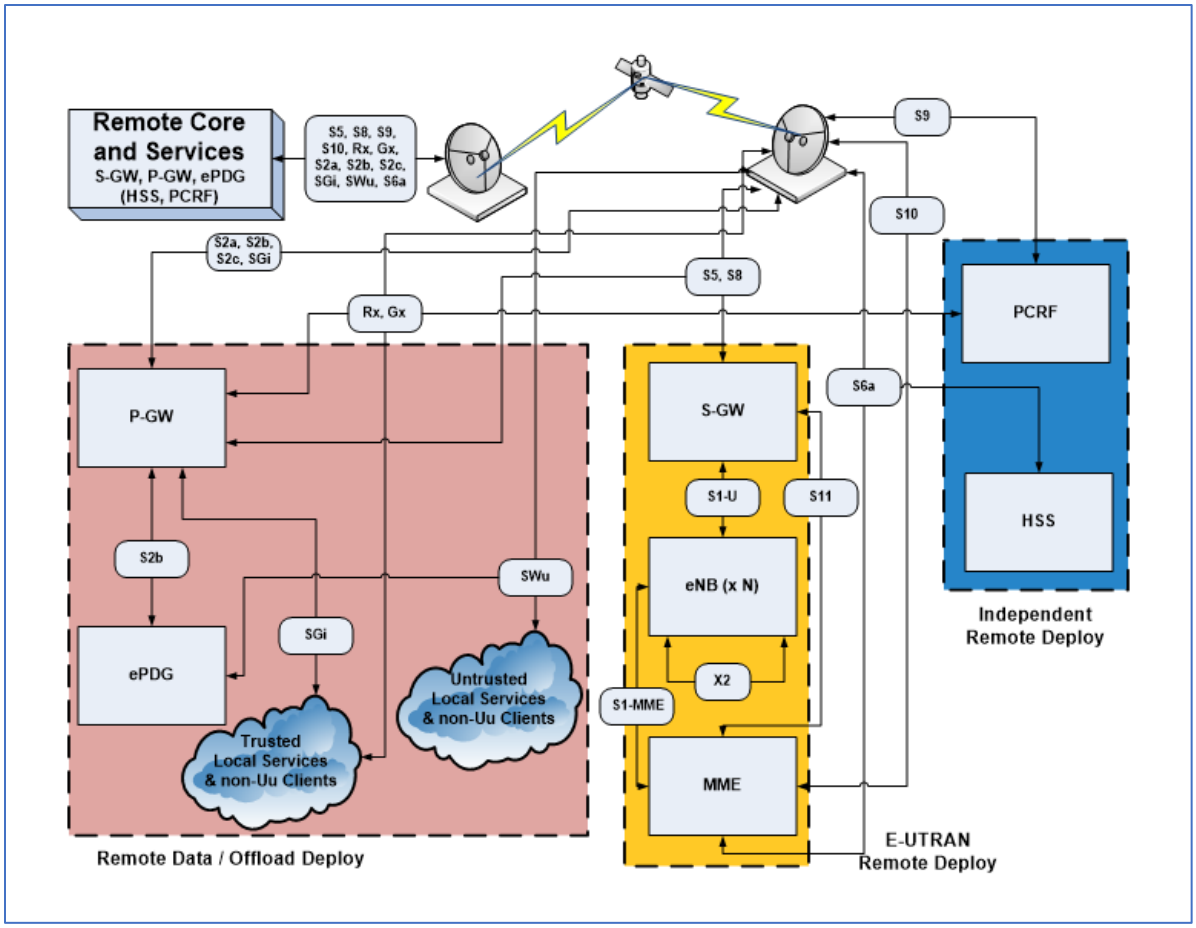



*Figure H-1: General Remote Network Architecture for a Core-Enabled BBDS.*

Figure H-1 contains illustrates a network with various field components providing the following functionalities:

- E-UTRAN Remote Deploy: Support of Band 14 700 MHz E-UTRAN UEs. A local MME is used to avoid the use of the S1-MME LTE interface over the remote communications link, due to expected performance problems with high-latency and potentially high packet-loss links. The X2 interface and multiple eNBs are allowed as a solution, to allow for larger coverage areas in complex terrains and increased network capacity when required;

- Remote Trusted / Untrusted Data / Offload Deploy: Two potentially independent components providing access to trusted and untrusted networking components. These can include both services and client systems. An *Evolved Packet Data Gateway* (ePDG) is a special gateway that allows for a secure IPSec-based (SWu) interface between authenticated clients and services on the untrusted network and the PS LTE network.

Non-700 MHz PS LTE network wireless clients can be connected into the network, as offload capability, at the trusted and untrusted levels;

- Independent Remote Deploy: Extra user database components to allow other deployed components to operate without an external remote connection, or when the remote connection cannot support both user- and control-plane traffic.

The outgoing connection can be a satellite connection, as indicated, or some other remote communications technology providing connectivity to primary national/agency components. Required interfaces passing over this connection are marked, as are corresponding services that are not located in the field. It is assumed that this connection is relatively compromised, and has increased latency and lower data rate than urban-deployed backhaul infrastructure. It may also have a higher packet loss rate (PLR). Additional information on the role of backhaul connections is included in Chapter 5.

**Usage Architectures for Remote Deployed Network (Interface Delineation):** The various components indicated in **Figure H-1** can be added to or removed from a given remote network to support different requirements for a deployed environment. With all components, the network supports roaming, localized services, alternate communication technologies, and 700 MHz UEs, plus a localized HSS and PCRF. Interface delineation is provided by the components, and corresponding connecting interfaces, indicated.

**Independent Remote and External Remote Network Support** Initial response teams will often need to deploy a local communications capability before an external communication link can be established, especially in mountainous regions. The network architecture shown in **Figure H-2** demonstrates the topology required if a space segment connection does not exist. The deployed system can operate in a fully self-contained fashion, and provides full, localized, data services, alternate localized communication technologies, and Band 14 700 MHz UE access. The HSS and PCRF must contain the information for all of the UEs in the field. The untrusted network may be located on un-secured local communication links away from other deployed components, with protection provided via the ePDG. A reduced version of this configuration is one without untrusted (IPSec authenticated and encrypted) services and clients, shown in **Figure H-3**.

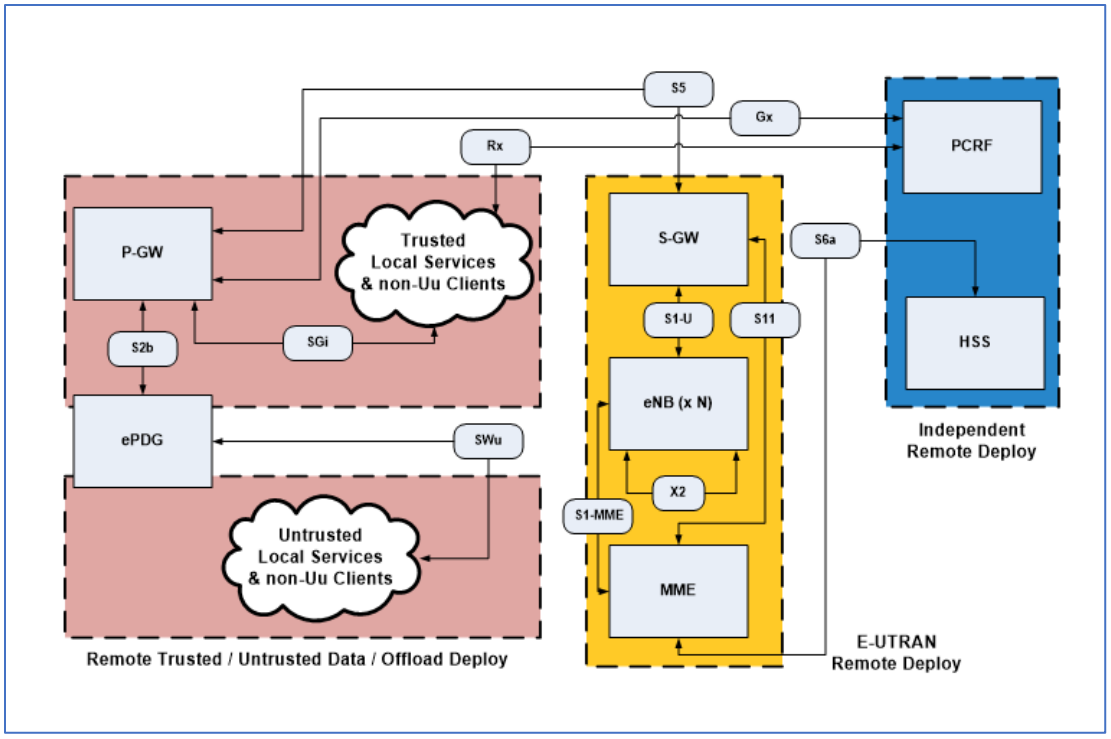



*Figure H-2: Independent Remote Deployed Core-Enabled BBDS Architecture.*

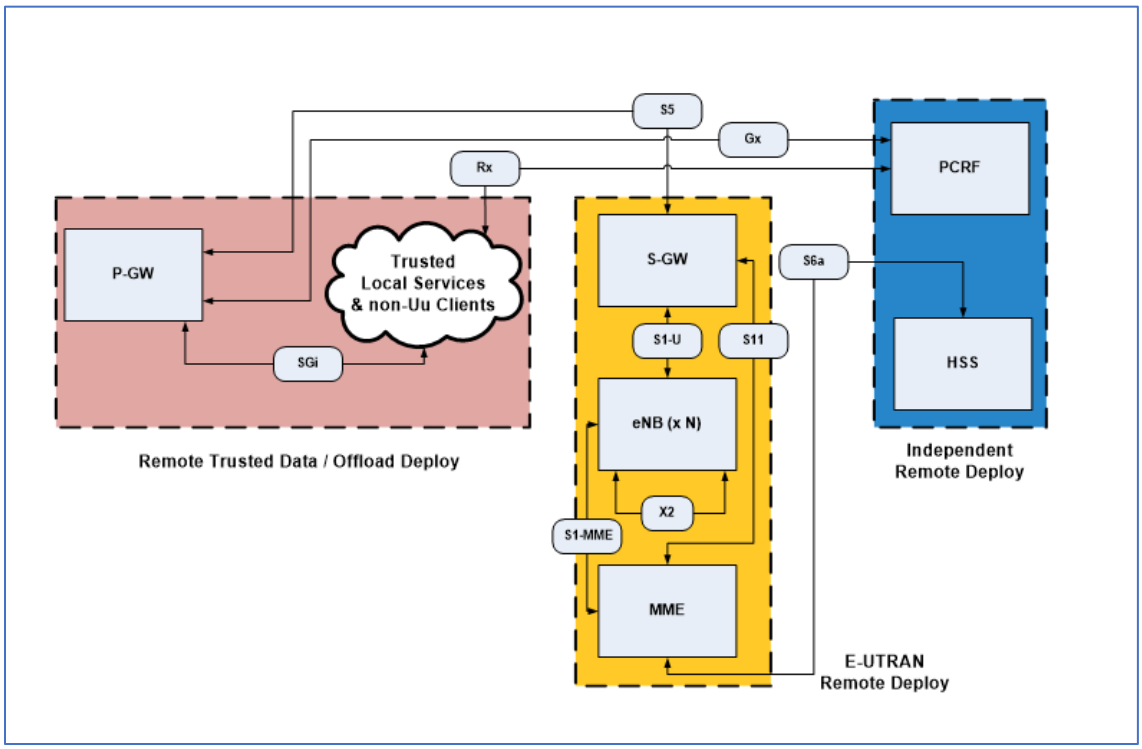



*Figure H-3: Independent Remote Core-Enabled BBDS architecture with no Untrusted Components*

**Fully Connected Emergency or Remote Community PS LTE network:** The network architecture in Figure H-4 is appropriate to a deployed system in which a high-performance satellite connection is available, either for a drop-in emergency deployment scenario, or to support a remote rural community without fiber-optic or high-performance microwave backhaul. This latter situation may arise when the BBDS is used to replace a community's emergency management backhaul network, or when a community's network is used to transport sensitive emergency response data across a region. All HSS and PCRF services are supplied by the national networks, with corresponding interfaces and protocols traversing the satellite / remote link. Additionally, a case in which only 700 MHz PS LTE network UEs are supported in a connected remote deploy or rural remote community is indicated in Figure H-5. All cases include full roaming interfaces over the satellite/remote link.

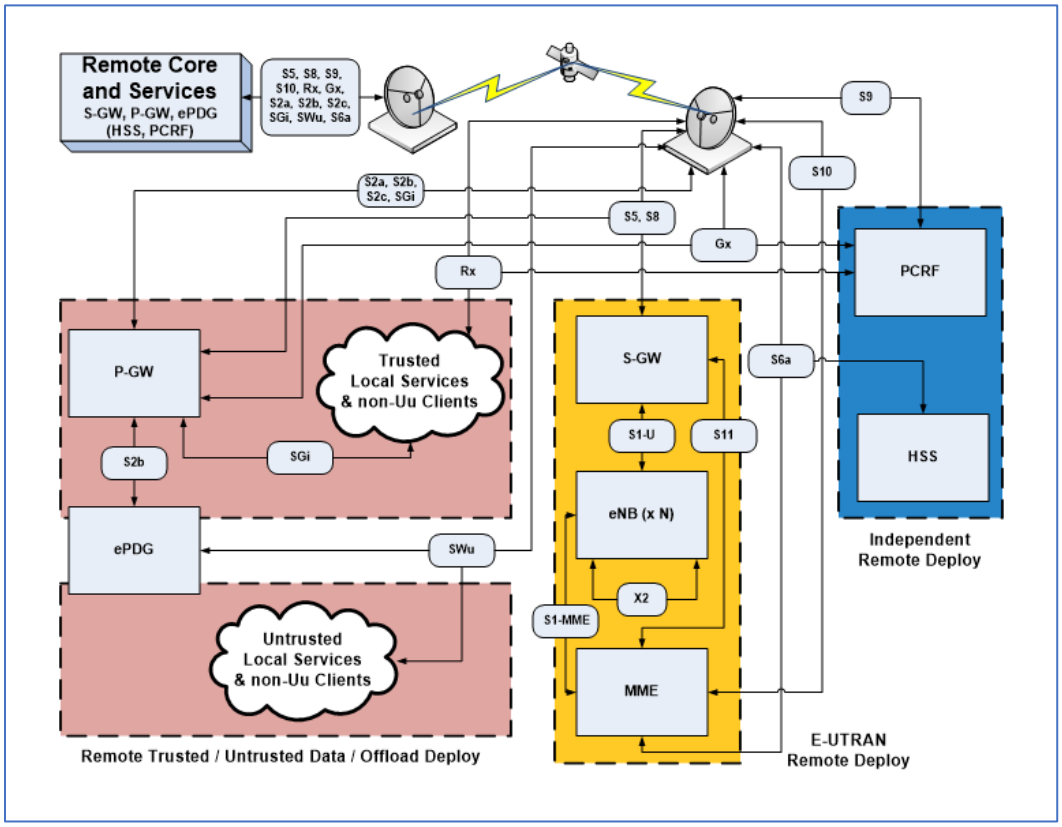



*Figure H-4: Core-Enabled BBDS architecture for Connected Emergency Deployment or Remote Community*

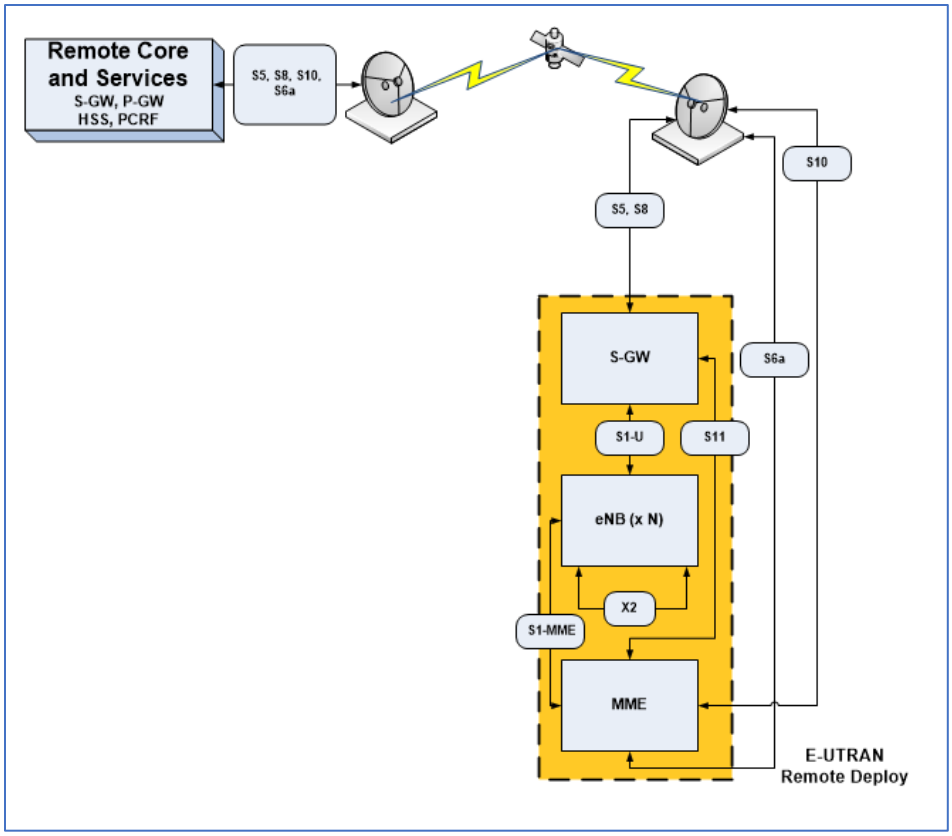



*Figure H-5: Core-Ready BBDS architecture for Connected UE-Only Deployment*

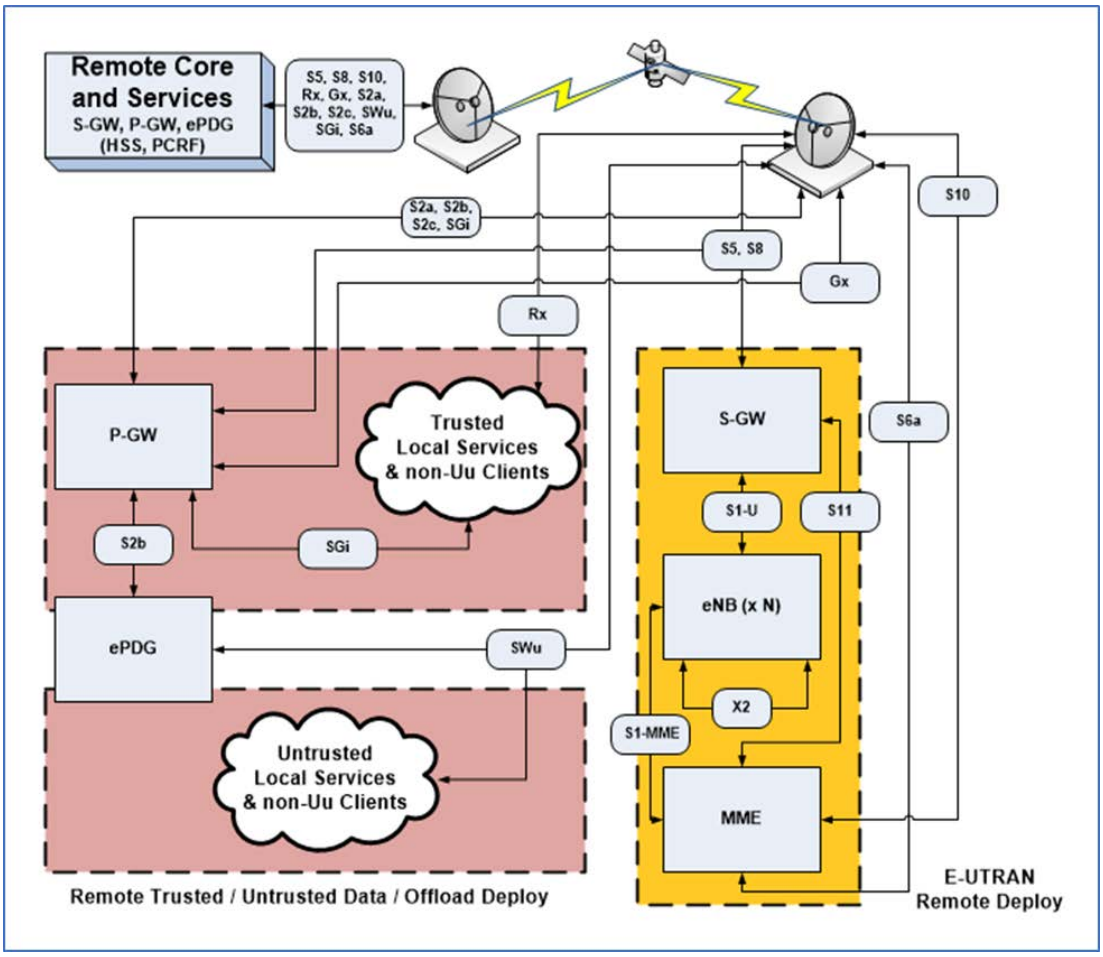



*Figure H-6: Service Connection Interfaces in a BBDS.*

**Figure H-6** shows various service connections involving a BBDS. This diagram was used to facilitate discussion on various components, information flows, and security considerations for BBDS usage