Nationwide Public Safety Broadband Network (NPSBN) QoS Priority and Preemption (QPP) Framework

FirstNet CTO Whitepaper

Version 0.9 draft
11/18/2015

Table of Contents

Table of Figures and Tables

1 Executive Summary

Reference to the Middle Class Tax Relief and Job Creation Act of 2012

The establishment of the FirstNet authority was a mandate in the Middle Class Tax Relief and Job Creation Act of 2012 [1].

Upon being established, FirstNet (the Authority) was instructed to establish consultation, define the objectives and characteristics, and ultimately build and operate a NationwidePublic Safety Broadband Network (NPSBN).

The Act also requires FirstNet to establish network policies that assign priority to local users. This requirement can be satisfied with the establishment of a Quality of Service, Priority and Preemption (QPP) Framework for the NPSBN. In order for the NPSBN to support Public Safety, QPP is a fundamental principal.

FirstNet's vision of QPP in the NPSBN

Quality of Service, Priority and Preemption concepts define the user's interaction with the FirstNet NPSBN, namely in terms of receiving prioritized access to network resources, maintaining a secure and communication link, and a guaranteed level of service performance. QPP policies are essential requirements for FirstNet's mission critical users, and are most impacting when network traffic levels rise and precious wireless resources become strained.

Quality of Service (QOS) is needed to ensure that Public Safety users have access to their services and applications at the required level of quality, corresponding to their individual needs (e.g. telephony, mission critical voice/data, medical telemetry, etc.). This requires discriminatory assignment of properties such as but not limited to bandwidth, bandwidth guarantees, usage limits, latency, accuracy, accessibility and retention.

Priority is the property by means of which users, applications, traffic streams or individual packets take precedence over others in setting up a service session or forwarding packets during periods of congestion in the network. Public Safety users will require priority access to the NPSBN resources to make their communications (at the required level of QOS) an effective tool in their management of incidents and emergencies.

Preemption is used together with priority to control use of resources by removing active sessions of lower priority users to allow allocation of resources to higher priority users when network resources are scarce or fully occupied.

A comprehensive QPP framework is needed to ensure that,

- Quality of Service, Priority and Preemption capabilities can be established and managed (statically and dynamically) in the NPSBN,
- Public Safety users can have different services, applications and usage profiles,

- Public Safety users can have default QPP properties, and
- Public Safety users QPP properties can be modified in real-time:
    - When they acquire an active role in the management of an incident
    - According to their role in the management of the incident, and
    - According to the severity and scale of the incident

FirstNet's Public Safety Advisory Committee QPP Framework Task Team

The Middle Class Tax Relief and Job Creation Act of 2012 [1] also requires the establishment of the Public Safety Advisory Committee (PSAC) to advise FirstNet on Public Safety matters. FirstNet asked the PSAC, in December of 2014, to establish a task team to define a QPP Framework. This work was completed over the next six months with the support of FirstNet Staff and Public Safety Communications Research staff.

3GPP LTE QPP capabilities

The Middle Class Tax Relief and Job Creation Act of 2012 [1] required that the NPSBN was developed using standard Long Term Evolution (LTE) technology.

3GPP has standardized various LTE capabilities for the support of QOS, Priority and Preemption. These capabilities range from,

- Subscriber Profiles in the HSS, to differentiate services, applications and some QOS, Priority and Preemption characteristics at User level
- Configuration settings in the User Equipment (UE) and Universal Integrated Circuit Card (UICC)
- Policy Control and Charging in the Evolved Packet Core
- Special Features in the Evolved Universal Terrestrial Radio Access Network (E-UTRAN), for example Dedicated versus Default Bearers, Quality of Service Class Indicators (QCI) for the established bearers, Guaranteed Bit Rate bearers, Allocation Retention Priority.
- Application profiles in the Application Layer (including the IP Multimedia Subsystem and third party hosted or cloud subscriptions)
- Support for Emergency Communications (e.g. 911 calling)

QOS and Priority capabilities can also be established in ancillary network subsystems such as Backhaul and Transmission (e.g. MPLS), IP Layer (e.g. Differentiated Services, Default/Preferred Routes), SS7 and Diameter Signaling (e.g. Default/Preferred Routes).

The aforementioned 3GPP LTE capabilities associated to QPP are available today by the majority of LTE Equipment Providers, and are used or exploited by commercial Service Providers according to their targeted business requirements and regulatory obligations.

Utilization of the 3GPP QPP features and additional capabilities required in support of the Authority mandate

As was mentioned above, QPP is a fundamental characteristic in the NPSBN. FirstNet seeks to exploit the available capabilities in LTE technology and further develop towards a comprehensive QPP solution that attends the needs of Public Safety users, importantly,

- Dynamic designation of QPP profiles, aligned with users' roles, application types, and incident types
- Ability to control or designate QPP profiles by means of user action, automated controls and Local Control (incl. manual override),
- Assign priority levels to applications based on QPP profiles as opposed to using pre-established priorities (e.g. favor QCI 1 VOLTE over a QCI 9 File Transfer only if telephony is relevant to the First Responder).

FirstNet DOES NOT expect that the NPSBN will be developed by using the QPP capabilities existing in LTE technology ONLY. In addition to the capabilities defined by 3GPP for core and RAN components, FirstNet envisions that a holistic QPP solution will also require device, applications, Local Control, operations, and policy elements.

Objective, intended audience, disclaimer and structure of this document

FirstNet has developed this technical white paper on the QOS, Priority and Preemption Framework to be included in the Vendors Library and serve as a guiding reference to potential NPSBN offerors.

This white paper is organized in five sections:

(1) Executive Summary (this section),
(2) Explains the framework of QPP Requirements/Objectives mentioned in the Act,
(3) Explains the FirstNet vision for a QPP framework in greater detail,
(4) Explains QPP capabilities that require further study,
(5) Provides a summary of our conclusions and final notes.

2 QPP Requirements/Objectives in the Act

Summary of the requirements in the Act

As was mentioned in the introductory section, the Middle Class Tax Relief and Job Creation Act of 2012 [1] tasked the FirstNet Authority to provide consultation, define objectives and characteristics, and ultimately build and operate a NationwidePublic Safety Broadband Network (NPSBN).

Quality of Service, Priority and Preemption (QPP) capabilities are mentioned in the Act in four different sections. See the following table and explanations further below:

No.	Section	Subsection	Page(s)	Directive
1	6206 Powers, Duties and Responsibilities of the First Responder Network Authority	(c)(2)(A)(v) (c)(2)(A)(vi)	15-18	In developing requests for proposals and otherwise carrying out its responsibilities under the Act, the First Responder Network Authority shall consult with regional, State, tribal, and local jurisdictions regarding the distribution and expenditure of any amounts required to carry out the policies established under paragraph 1 (Establishment of Network Policies), including with regard to, (i) Construction of a core network and any radio access network build out; (ii) Placement of towers; (iii) Coverage areas of the network, whether at the regional, State, tribal, or local level; (iv) Adequacy of hardening, security, reliability, and resiliency requirements; (v) Assignment of priority to local users; (vi) Assignment of priority and selection of entities seeking access to or use of the nationwide public safety interoperable broadband network established under subsection b (duty and responsibility to deploy and operate a Nationwide Public Safety Broadband Network); and (vii) Training needs of local users.
3	6206 Powers, Duties and Responsibilities of the First Responder Network Authority	(c)(5)	18	The First Responder Network Authority shall negotiate and enter into, as it determines appropriate, roaming agreements with commercial network providers to allow the nationwide public safety broadband network to roam onto commercial networks and gain prioritization of public safety communications over such networks in times of an emergency
4	6211 Public Safety Roaming and Priority Access	(3)	22	The Commission may adopt rules, if necessary in the public interest, to improve the ability of public safety networks to roam onto commercial networks and to gain priority access to commercial networks in an emergency if such access does not preempt or otherwise terminate or degrade all existing voice

No.	Section	Subsection	Page(s)	Directive
				conversations or data sessions
5	6302 State and Local Implementation	(e)(3)(D)(iii)	24-25	In order to obtain grant funds and spectrum capacity leasing rights for the submission and approval of alternative plan, a State shall demonstrate comparable security, coverage, and quality of service to that of the nationwide public safety broadband network
6	6303 Public Safety Wireless Communications Research and Development	(e)(3) (e)(4)	25-26	The Director of NIST, in consultation with the First Responder Network Authority and the public safety advisory committee, shall, (1) Document public safety wireless communications technical requirements; (2) Accelerate the development of the capability for communications between currently deployed public safety narrowband systems and the nationwide public safety broadband network; (3) Establish a research plan, and direct research, that addresses the wireless communications needs of public safety entities beyond what can be provided by the current generation of broadband technology; (4) Accelerate the development of mission critical voice, including device-to-device ‘‘talk-around’’ capability over broadband networks, public safety prioritization, authentication capabilities, and standard application programing interfaces for the nationwide public safety broadband network, if necessary and practical; (5) Accelerate the development of communications technology and equipment that can facilitate the eventual migration of public safety narrowband communications to the nationwide public safety broadband network; and (6) Convene working groups of relevant government and commercial parties to achieve the requirements in paragraphs (1) through (5)

Table 1 – Requirements for Quality of Service, Priority and Preemption listed in the Act

The directives in Section 6206 of the Act establish the basic requirement to designate priority access to the users of the NPSBN (NPSBN-U), and carry over that priority when these users roam onto commercial networks.

Section 6211 makes a disclaimer regarding the priority access under roaming scenarios, where the requested priority cannot preempt, terminate or degrade stable communications.

Section 6302 instructs the States that chose to build their own Radio Access Networks to develop their alternative State Plans while complying with the QOS definitions of the NPSBN.

Section 6303 establishes the mission in the National Institute of Science and Technology (NIST) to direct research and development towards (a) public safety prioritization, (b) features needed in Public Safety beyond what standard/current broadband technology supports today, and (c) to consult with the FirstNet Public Safety Advisory Committee in address this mission.

The directives outlined in the Act as listed above were taken as the input to the FCC Technical Advisory Board for First Responder Interoperability to develop the Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network [2] (the *Minimum Technical Requirements*).

The Minimum Technical Requirements establish,

- The use of QPP features standard to LTE networks (section 1.3.6, page 11),
- The concepts of QOS Profile Templates, Public Safety vs Secondary Users, Default vs Dynamic Prioritization, and QOS and Priority Management API (section 1.4.7, pages 14-15)
- Section 4.7 expands on the explanations introduced in 1.3.6 and 1.4.7

The following section 3 in this white paper on QPP expands on the concepts introduced in [2], and explains the FirstNet QPP framework in greater detail.

3 Detailed Framework of QPP Capabilities – NPSBN Vision

Influence from US standards on Emergency Management and Preparedness

While LTE networks provide features that partially provide QOS, Priority and Preemption capabilities, a more comprehensive QPP solution is needed to align with the specifications and best practices from agencies. These various agencies provide a framework of emergency management standards and guidelines addressing prevention, mitigation, preparedness, response and recovery.

Relevant to FirstNet's objectives on QPP, FEMA provided the Incident Command System (ICS) and the Communications Unit (COM-U) specifications, as a part of the National Incident Management System (NIMS).

The ICS [3] provides criteria to classify incidents by type and severity, and defines standardized roles within a given incident organizational chart.

The COM-U [3, 4] develops the communications plan, to make the most effective use of the communications equipment and facilities assigned to incidents.

NIMS also highlights the importance of well integrated and effective emergency management and incident response operations, when they depend on the involvement of multiple jurisdictions, levels of government, functional agencies, and/or emergency responder disciplines.

FirstNet's Public Safety Advisory Committee QPP Framework Task Team

The Middle Class Tax Relief and Job Creation Act of 2012 [1] also requires the establishment of the Public Safety Advisory Committee (PSAC) to advise FirstNet on Public Safety matters. QPP has long been discussed in the Public Safety Community however the practitioners and the engineers often spoke different languages. Public Safety users want it work when they need it but engineers want to describe that in terms of Quality of Service Class Indicators, Guaranteed Bit Rates and Access Class Barring. Clearly the two sides of the equation need a way to communicate needs and solutions.

In order to create this common language for discussion, FirstNet asked the PSAC, in December of 2014, to establish a task team to define a QPP Framework. This work was completed over the next six months with the support of FirstNet Staff and Public Safety Communications Research staff.

The task team defined a process to establish the framework that contained the following steps:

1. Define Usage Scenarios for the NPSBN
2. Document actual and created incidents in Use Cases that would utilize the Usage Scenarios

3. Walk through the Use Cases, utilizing the Usage Scenarios and define how QPP should be modified to ensure that the appropriate public safety users have the appropriate level of QPP to manage the incident at each time interval

Complementary to and in support of the framework, Local Control provides the methodology for public safety to interact with the framework and perform the following (not an exhaustive list):

- Be able to define QPP profiles (static and dynamic) based on users' roles, application types, and incident types,
- Provide management tools aligned and in support of the incident Communications Unit, Dispatch function or Public Safety Answering Point, and
- Provide management tools that assign QPP properties across PSE jurisdictions.

The above framework requires a comprehensive ecosystem of network capabilities, data that triggers those capabilities when needed, subscription databases that allow the provisioning of user data as pertaining to public safety (e.g. incident type, user role, etc.), applications whose QPP properties are dynamically defined (e.g. VOLTE is not always highest priority), and systems and tools (Local Control) that allow the dynamic designation of QPP properties between users, applications and network sections.

The result of this exercise was the QPP Framework that is the subject of this white paper.

The following section introduces and develops the visualization of the QPP framework in each of the areas discussed above.

3.1 Visualization of the NPSBN QPP framework

FirstNet, with the support of the PSAC, has visualized a comprehensive ecosystem of systems, applications and parties, all contributing towards the QPP framework:

- Users
- Network
- Applications
- Data, static and dynamic
- Triggers and thresholds
- The Dynamic Controller

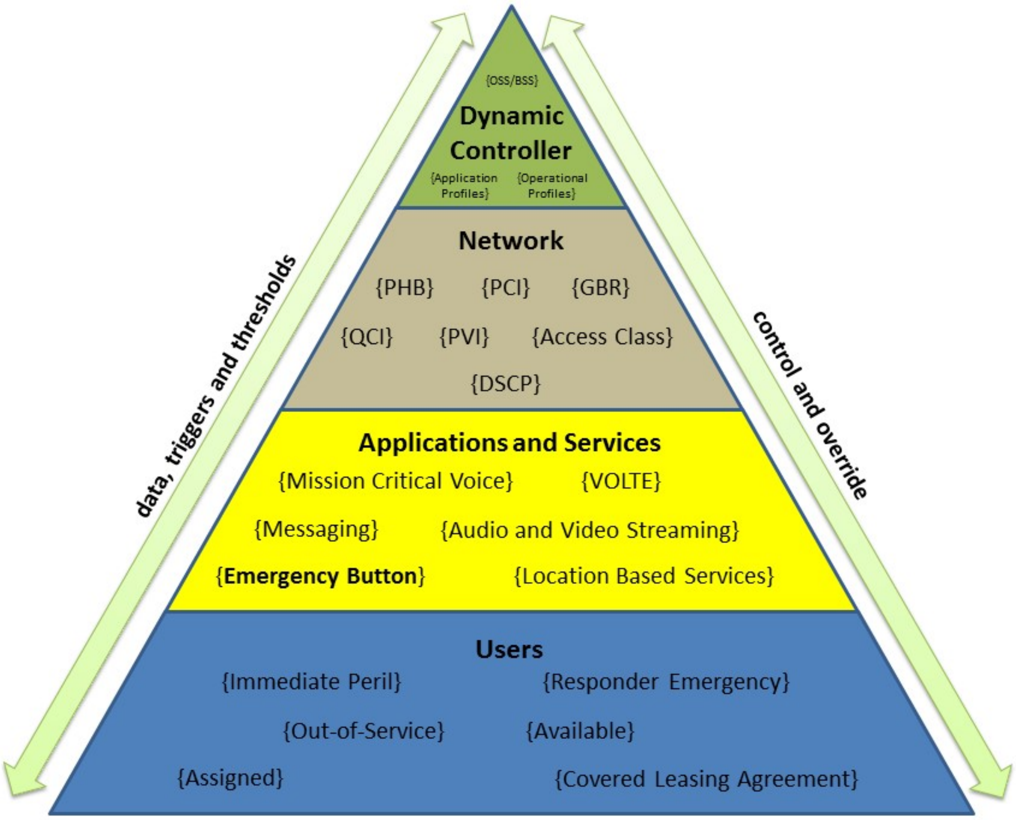


Figure 1- QPP Framework Visualization

Users play a role in the QPP Framework, as their unique characteristics demand specific QOS, Priority and Preemption features depending on their role in the management of incidents. They can also invoke a change in their QPP attributes (e.g. pushing an emergency button).

Applications play their role in the delivery of services (e.g. MCV and Messaging), but can also be used as a mechanism to trigger a change in user or network state (e.g. emergency button or entering a code).

The *Network* is where the QPP attributes assigned to users influence their experience in their use of the NPSBN. It comes in the form of special settings and features in the UE/USIM, E-UTRAN, EPC and other peripheral network subsystems (e.g. Transmission, IP Layer).

Data is the key in defining when changes in user or network status are needed.

Triggers and thresholds are settings in the network systems for the purpose of analyzing data and invoking changes in user or network status accordingly, manually or in an automated manner. For instance, the rules engine in the Policy Charging and Rules Function (PCRF) uses the input data from the Subscription Profile Repository (SPR) and the Operations and Maintenance Center (OMC) to make policy control decisions.

Finally, the *Dynamic Controller* allows the NPSBN, in real-time, to manage, operate and command QPP properties in the NPSBN during incidents.

In the following sections, components in the QPP framework are discussed in more detail.

3.2 QPP Network Model

QPP should primarily come into play on the NPSBN when there is congestion in the network. The NPSBN can be broken down into a few basic parts in order to consider where congestion might occur.

- User Device – Inside the User Device
- Air Interface – Between the User Device and the Cell Tower or LTE Base Station (most likely source of congestion)
- eNodeB – Internal to the LTE Base Station at the Cell Tower
- Backhaul – Connectivity between eNodeB and the Core Network
- Core Network – Inside the Core Network and the connectivity between Core Network physical sites
- Public Safety Enterprise Network Connectivity – The physical network connectivity between the Core Network and the Public Safety Entity
- Public Safety Enterprise Networks – Inside the Public Safety Entities network
- Other Networks – Additional networks like the Internet

The modern User Device should have sufficient processing power to not become a bottleneck. Proper engineering and growth planning should ensure that the eNodeB, Backhaul, Core Network, Public Safety Enterprise Network Connectivity and Other Networks have enough capacity to handle potential overload situations. However there are numerous controls available to ensure that any QPP treatment is carried and enforced across all network connections and in all elements of the network.

If the NPSBN is properly engineered, then the single most likely point of congestion is the Air Interface. The capacity of the Air Interface defined in Megabits per second of Uplink and Downlink, is limited by the 10MHz + 10MHz assigned to the NPSBN and the implementation of LTE standards. Uplink is the connectivity from the device to the eNodeB and downlink from the eNodeB to the device. The NPSBN's assigned spectrum provides a theoretical maximum bit rate of 74Mbps in the downlink and 36Mbps in the uplink, assuming a 2X2 MIMO deployment. This capacity is shared by all users using that spectrum on that eNodeB.

Furthermore, the capacity can vary across the cell site's geographical area. A user at the edge of a cell may only be able to achieve 256kbps of data transfer rate, which may demand a majority of wireless network resources and reduce the average cell capacity.

Typical deployments divide each cell site into three cell-sectors. From the cellular tower and antennas, each cell-sector radiates in a 120-degree pattern from the cell site. Depending on the capacity and coverage model for the cell site the cell-sector can extend out for 20 miles but typically extends 3-5 miles. A cell-section on one side of the tower could be at full capacity and the other two sectors could be virtually un-used.

Each cell-sector therefore typically provides the following capacity

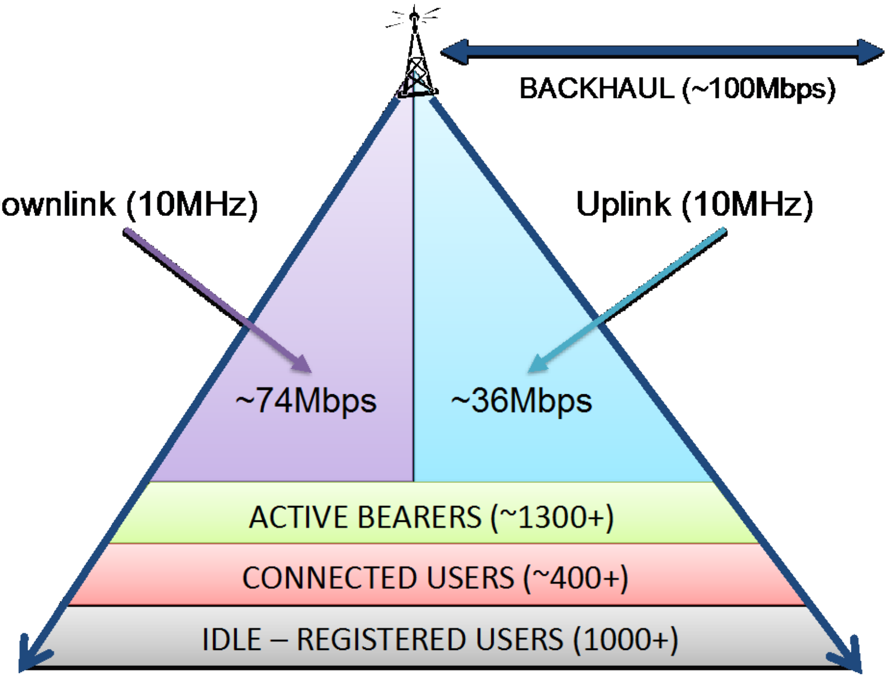


Figure 2- Cell-Sector Capacity

- 74Mbps of Downlink from the tower to the device
- 36Mbps of Uplink from the device to the tower
- ~1300 active user sessions
- ~400 connected users (assuming each user has two sessions on average)
- ~1000 idle users who are connected but not doing anything

Note: The above figures are provided as a reference of typical capacity in a cell.

3.3 Network

3.3.1 Network States

The QPP of the network will always be in one of three states, as illustrated in the following Figure 3. Since the primary point of congestion is the cell-sector as described above, the QPP Network State must also be defined as a particular geographical area of the NPSBN. The area could be a single cell-sector/cell site or a group of cell sites and cell-sectors. The NPSBN is a nationwide network and must support many simultaneous incidents across the country therefore there may be many parts of the network that are in different Network States.

Static
Dynamic
Controlled

Figure 3- Network States

Static State is the network operational mode that utilizes the QoS, Priority and Preemption properties that were statically defined when users were provisioned in the network and the network was configured, to manage the QPP of the network.

Dynamic State is the network operational mode when the network begins to see congestion that cannot be relieved through the static QPP configuration utilized in the *Static State*. This state uses dynamic information, triggers, real-time network performance data and utilization data to begin making dynamic decisions in real-time to vary the QPP parameters of the network, individual users and groups of users.

Controlled State is the network operational mode when QPP properties can be directly influenced by an authorized individual who has specific operational or incident knowledge through a controlled override process.

Movement of a geographical portion of the NPSBN between these states is done through a combination of triggers, network usage data, incident severity, data and a QPP / Local Control portal. Static, Dynamic and Controlled states can coexist in the overall NPSBN, in different geographical areas (e.g. a fire in a residence in Virginia, an earthquake in California and a hurricane in Florida).

3.4 Users

Users of the NPSBN can be Primary and Secondary users.

Primary users are Public Safety responders and other authorized public safety personnel, whereas secondary users are those users using the NPSBN under a Covered Leasing Agreements (CLA) established between FirstNet and an entity utilizing the capacity of the NPSBN when Public Safety is not using it.

3.4.1 Primary User States

In order to ensure that the NPSBN can react to specific Primary User situations, First Responders may be temporarily mapped into the following user states (see Figure 4 below):

- Immediate Peril
- Responder Emergency
- Relayed User

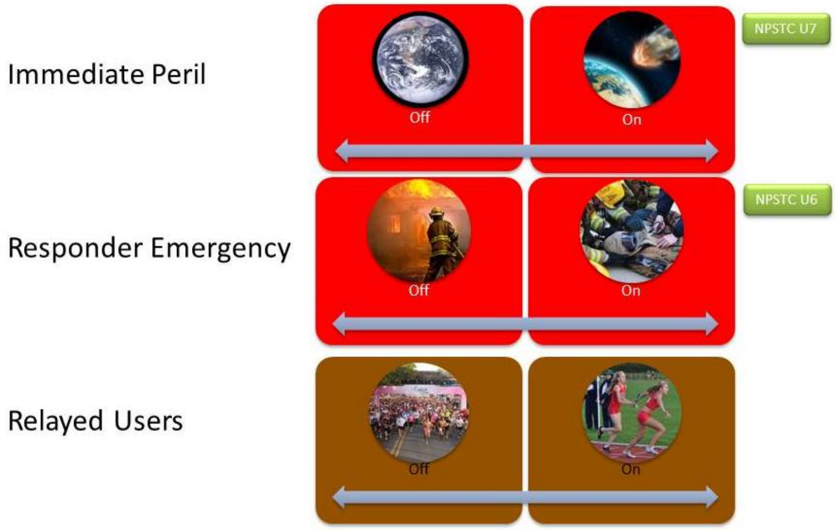


Figure 4- Primary User States

Immediate Peril is a primary user state where there is an immediate threat to human life. That could be a paramedic whose patient has suffered a cardiac arrest while en-route to the hospital.

Responder Emergency is a primary user state where the first responder is in a life-threatening situation. That could be a firefighter who has become trapped inside a burning building.

Relayed User is a primary user that is not assigned a role in the management or operations of an incident, and yet his/her UE can be used as a relay of the air interface for other UEs that may have lost coverage. This Relayed User shall preserve the same QPP characteristics as those of the UEs that it is serving.

Each of these states can be initiated by the user, on behalf of the user by a dispatcher, through Local Control, for example. Each temporary user state can also be used as a trigger to move a geographic portion of the network between the Static and Dynamic network states. A primary user who has declared a responder emergency state could move the affected geographic portion of the NPSBN to a Dynamic State. Once the responder emergency state has been cleared, the affected geographic portion of the network would be returned to a static state.

3.4.2 Secondary User States

As was mentioned above, Secondary Users are those using the network under a Covered Leasing Agreements (CLA).

Based on the requirements in the Act, secondary users exist in the NPSBN under the assumption that their access to the network will always receive the lowest priority, as compared to primary users and will only have access to the capacity that primary users are not currently using. Under normal circumstances (Static State of the network) the NPSBN will have excess capacity to attend both, primary and secondary users.

Based on the above, a secondary user can be in three different states:

- Free Range,
- Restricted, and
- Preempted.

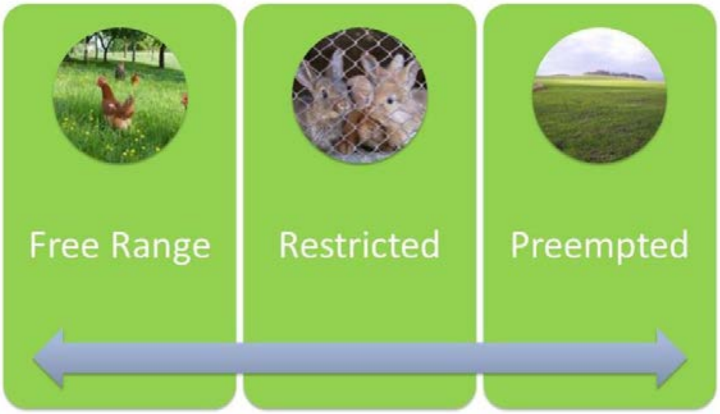


Figure 5- Secondary User States

A secondary user in *Free Range State* is one that has full and unrestricted access to any network capacity not in use by primary users as well as his/her services (provided by the holder of the Covered Leasing Agreement), without being subject to blocking or preemption.

A secondary user in *Restricted State* is one whose access to the NPSBN is limited because the network has entered into a dynamic or controlled state, requiring priority access to primary users. The user should be restricted to a portion of the unused capacity that primary users are not using thus reserving capacity for primary users.

A secondary user in *Preempted State* is one who's established communications on the NPSBN are subject to being terminated, as a means to freeing network resources required by primary users, when the network has entered into a dynamic or controlled state.

3.5 User and Incident Data

It is quite difficult for any system to understand what is actually going on the world. The NPSBN is no exception and must understand as much as possible about the users and the incident in order to make QPP decision to ensure that the users are able to utilize the NPSBN when they need it. The information required - user and incident data - can be both static and dynamic. As incidents grow in complexity and user's roles and activities change, the network must be made aware of these changes.

3.5.1 User Data

When primary users are provisioned onto the NPSBN they will be assigned a series of settings and attributes that define who they are and what they do. This data includes default QOS, Priority and Preemption values in the Home Subscriber Server and within the User Device, and their default leadership or functional role within Public Safety. These data are considered as *Static*.

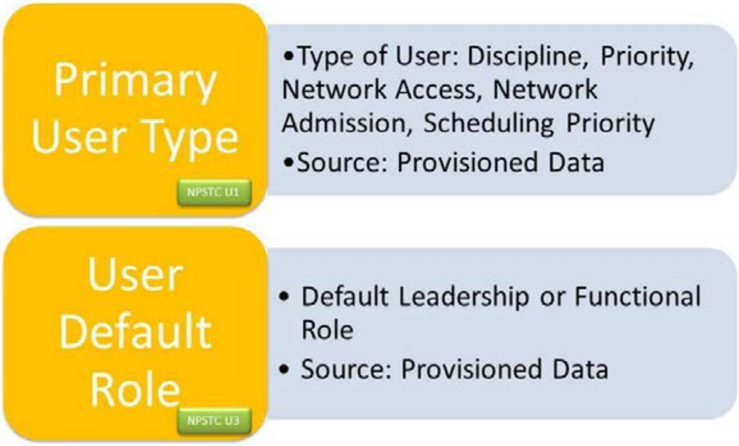

Primary User Type
NPSTC U1
•Type of User: Discipline, Priority, Network Access, Network Admission, Scheduling Priority
•Source: Provisioned Data
User Default Role
NPSTC U3
• Default Leadership or Functional Role
• Source: Provisioned Data

Figure 6- Primary Users Static Data

First Responders and other public safety personnel will attain other data or attributes that change based on their location, operational status and incident role. These data are considered as *Dynamic*.

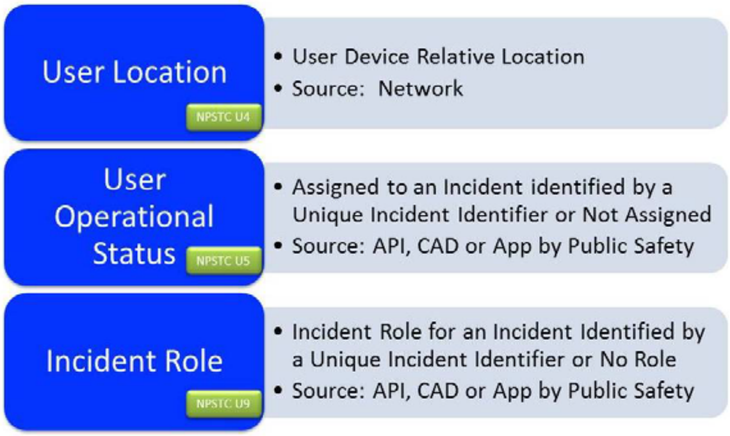

User Location
NPSTC U4
• User Device Relative Location
• Source: Network
User Operational Status
NPSTC U5
• Assigned to an Incident identified by a Unique Incident Identifier or Not Assigned
• Source: API, CAD or App by Public Safety
Incident Role
NPSTC U9
• Incident Role for an Incident Identified by a Unique Incident Identifier or No Role
• Source: API, CAD or App by Public Safety

Figure 7- Primary Users Dynamic Data

User location is the user device's relative location to an incident. This, when combined with an Incident location ensures that the network is providing QPP for users that are within the geographic area of the incident rather than extending the incident location to a very large geographic area for a single responder that might be traveling a long distance to an incident.

The User Operational Status defines if a user is actively participating in an incident. This can be used to ensure that a user who might be sleeping for operational period or has self-deployed and is not assigned to the incident is not provided the same level of QPP that an active participant is assigned.

Incident Role defines the role that the user is performing on the incident. This enables the NPSBN to provide varying levels of QPP based on the user's actual role during the incident. The user can be elevated above or below their User Default Role for the incident and returned to their User Default Role after the incident has concluded.

The dynamic data will either come from the network in the case of user location or via a set of Application Programming Interfaces (API) utilized by a computer aided dispatch terminal or other public safety application.

3.5.2 Incident Data

User dynamic data is needed to determine a change in a primary user state, but information about the incident is also needed. Incident data is dynamic in nature and if there is no incident, there is no data. There are three attributes that constitute the incident dynamic data:

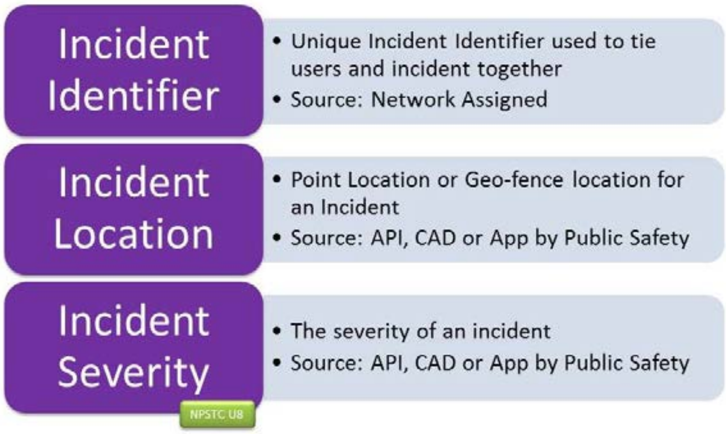

Incident Identifier
• Unique Incident Identifier used to tie users and incident together
• Source: Network Assigned
Incident Location
• Point Location or Geo-fence location for an Incident
• Source: API, CAD or App by Public Safety
Incident Severity
• The severity of an incident
• Source: API, CAD or App by Public Safety
NPSTC UB

Figure 8- Incident Data

The Incident Identifier is required because the NSPBN can have multiple incidents occurring nationwide simultaneously. This must be a unique value and serves as the key value to tie all of the users to an incident.

The Incident Location is critical to define the area that an incident occupies so that, if required, a Network State change can cover the incident without changing areas that are part of the incident. This could be defined by a point and radius or a Geofence.

]

The Incident Severity is both a trigger that may signal a Network State change as well as a method to prioritize overlapping or adjoining incidents.

The dynamic incident data will come from a set of Application Programming Interfaces (API) utilized by a computer aided dispatch terminal or other public safety application.

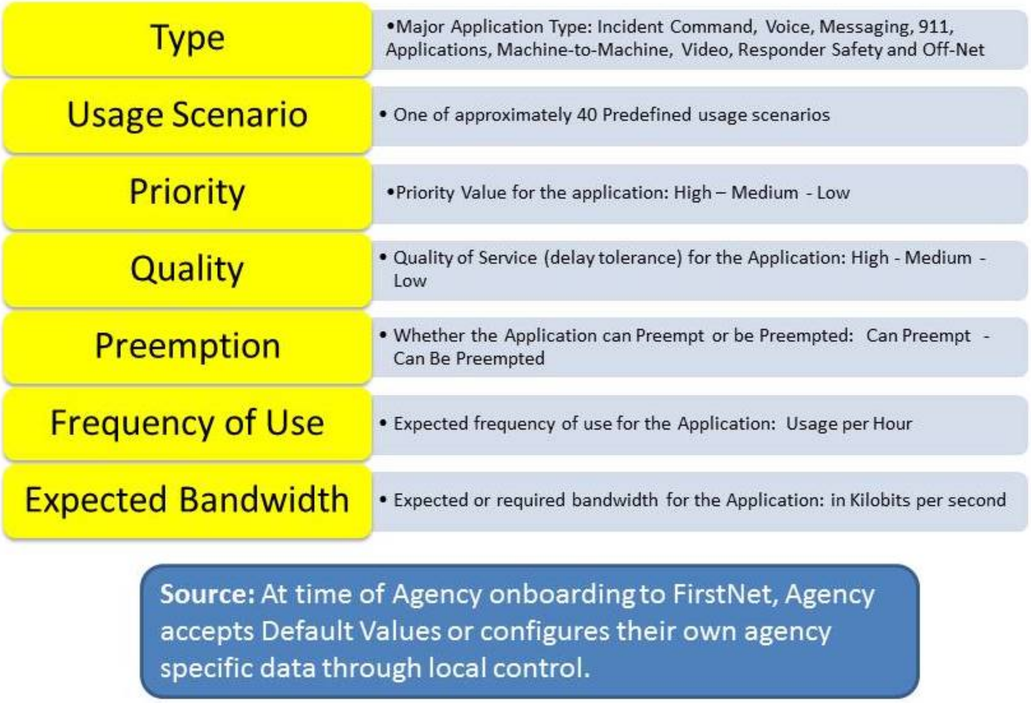
3.6 Application Data

In the introductory section we mentioned how QPP-related data needed to be applied differently at the application level. For instance, a medical telemetry application may be considered of lesser importance to a firefighter, as opposed to a paramedic transporting a critical patient in an ambulance. Application data is broken into two areas, static application profiles and operational profiles.

3.6.1 Static Application Profile

The term application has many different definitions depending on how it is used. In this context application refers to a usage scenario of the NSPBN. This might include using a mobile data terminal to access computer aided dispatch information or making a telephone call. It does refer to just the software running on a device. Each usage scenario will require a profile to be defined.

In order to create this profile, QPP framework has identified the following data as relevant to the implementation of diverse applications with the necessary QPP parameterization in the network systems:



Type	•Major Application Type: Incident Command, Voice, Messaging, 911, Applications, Machine-to-Machine, Video, Responder Safety and Off-Net
Usage Scenario	• One of approximately 40 Predefined usage scenarios
Priority	•Priority Value for the application: High – Medium - Low
Quality	• Quality of Service (delay tolerance) for the Application: High - Medium - Low
Preemption	• Whether the Application can Preempt or be Preempted: Can Preempt - Can Be Preempted
Frequency of Use	• Expected frequency of use for the Application: Usage per Hour
Expected Bandwidth	• Expected or required bandwidth for the Application: in Kilobits per second

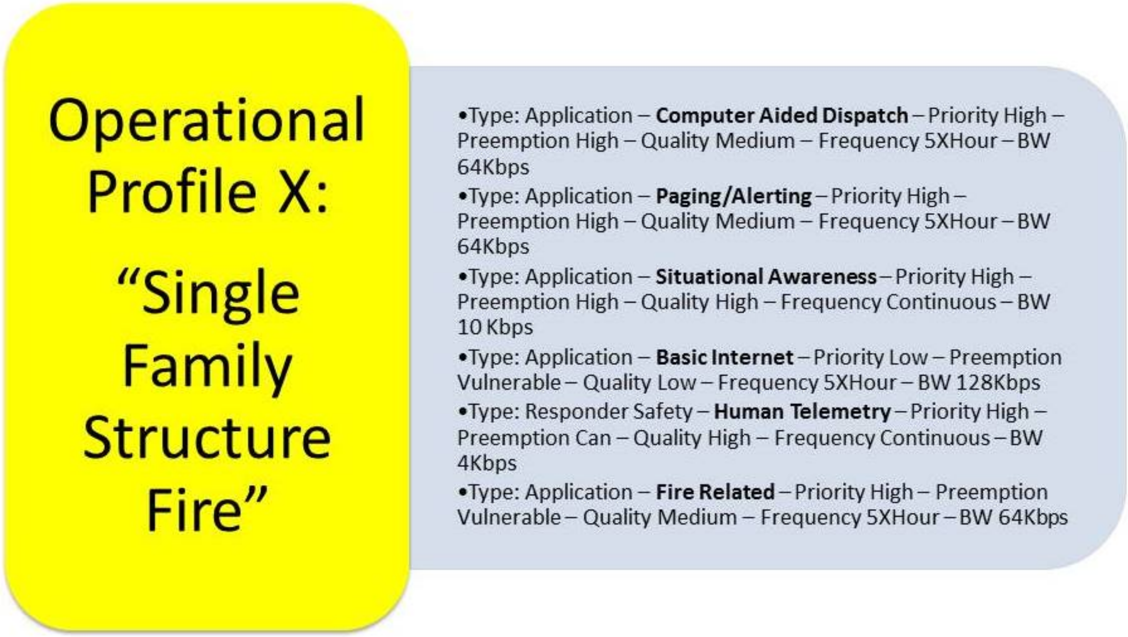
Source: At time of Agency onboarding to FirstNet, Agency accepts Default Values or configures their own agency specific data through local control.

Figure 9- Application Data

Note that this application data is not necessarily mapped to QOS, Priority and Preemption parameters standard to LTE networks (i.e. QCI, AC, ARP, etc.), but it is expected that a combination of LTE parameters, Apps and network management capabilities will provide the required QPP behavior at the application level.

3.6.2 Operational Profiles

Application Profiles can be grouped into Operational Profiles which describe a predefined set of applications that a first responder would use during an incident. Figure 10 below illustrates a sample Operational Profile that can be assigned to a First Responder with an active role in a single family structure fire incident.



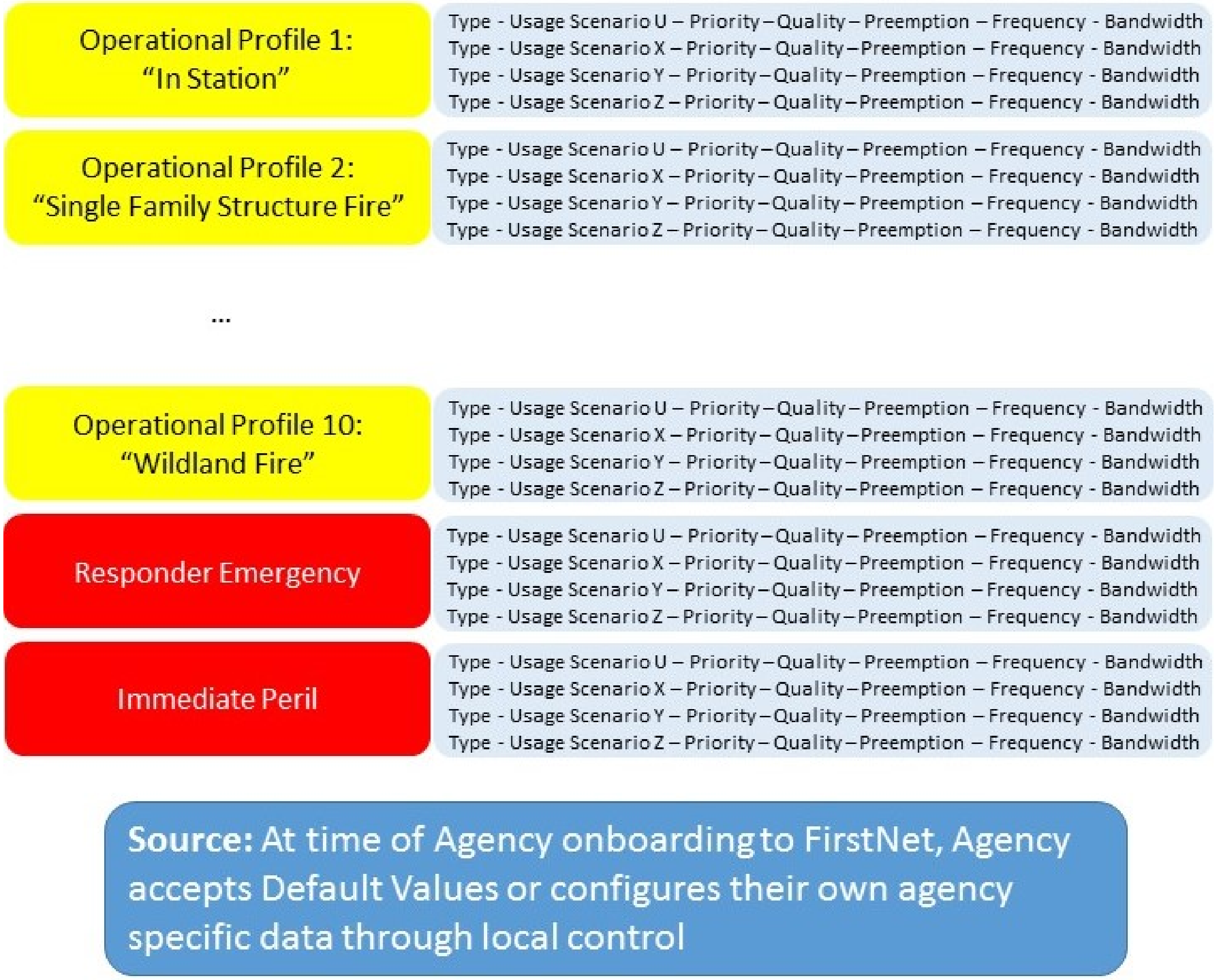
Operational Profile X: “Single Family Structure Fire”

- •Type: Application – **Computer Aided Dispatch** – Priority High – Preemption High – Quality Medium – Frequency 5XHour – BW 64Kbps
- •Type: Application – **Paging/Alerting** – Priority High – Preemption High – Quality Medium – Frequency 5XHour – BW 64Kbps
- •Type: Application – **Situational Awareness** – Priority High – Preemption High – Quality High – Frequency Continuous – BW 10 Kbps
- •Type: Application – **Basic Internet** – Priority Low – Preemption Vulnerable – Quality Low – Frequency 5XHour – BW 128Kbps
- •Type: Responder Safety – **Human Telemetry** – Priority High – Preemption Can – Quality High – Frequency Continuous – BW 4Kbps
- •Type: Application – **Fire Related** – Priority High – Preemption Vulnerable – Quality Medium – Frequency 5XHour – BW 64Kbps

Figure 10- A sample Operational Profile

Operational Profiles can be considered as the basic unit of application provisioning, available to PSE Administrators. Different Operational Profiles can be configured to reflect the requirements specific to individual PSEs.

Figure 11 below illustrates a sample PSE-specific Operational Profile framework, with 10 Operational Profiles for this PSE:


Operational Profile 1:
"In Station"
Type - Usage Scenario U – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario X – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario Y – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario Z – Priority – Quality – Preemption – Frequency - Bandwidth
Operational Profile 2:
"Single Family Structure Fire"
Type - Usage Scenario U – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario X – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario Y – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario Z – Priority – Quality – Preemption – Frequency - Bandwidth
...
Operational Profile 10:
"Wildland Fire"
Type - Usage Scenario U – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario X – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario Y – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario Z – Priority – Quality – Preemption – Frequency - Bandwidth
Responder Emergency
Type - Usage Scenario U – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario X – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario Y – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario Z – Priority – Quality – Preemption – Frequency - Bandwidth
Immediate Peril
Type - Usage Scenario U – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario X – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario Y – Priority – Quality – Preemption – Frequency - Bandwidth
Type - Usage Scenario Z – Priority – Quality – Preemption – Frequency - Bandwidth

Source: At time of Agency onboarding to FirstNet, Agency accepts Default Values or configures their own agency specific data through local control

Figure 11- A sample PSE Operational Profile framework

Note that,

- PSEs should be able to define their own Operational Profile framework,
- Users of the NPSBN (in a PSE context) should be assigned a default Operational Profile during initial provisioning, and
- Users of the NPSBN (in a PSE context) should be able to change their Operational Profile when they acquire an active role in incident's management or operations.

The ability to change Operational Profiles is referred as dynamic Profile selection, which is illustrated in Figure 12 below.

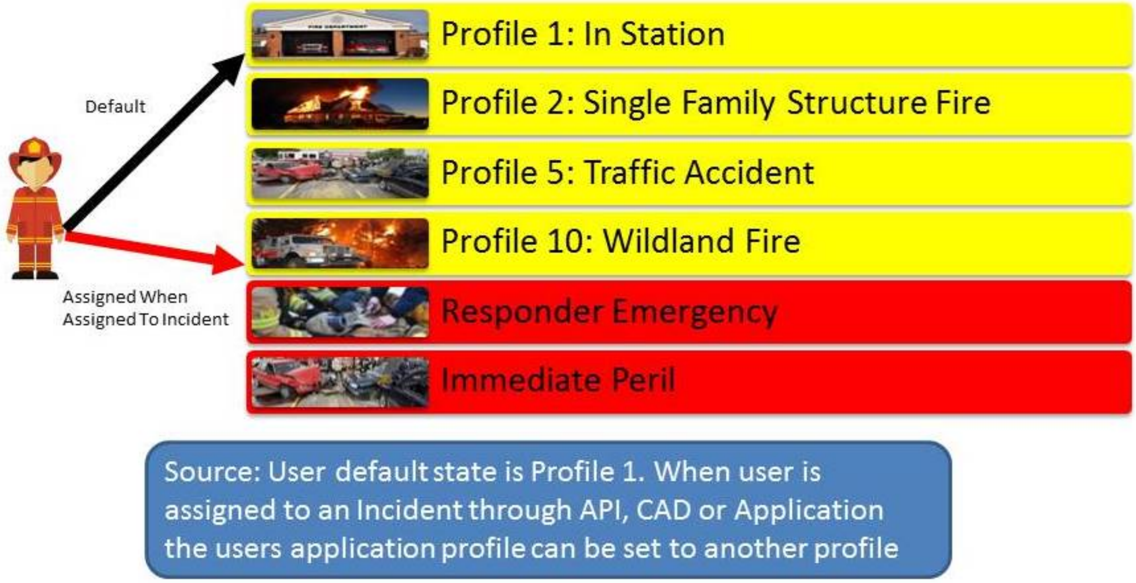

Profile 1: In Station
Profile 2: Single Family Structure Fire
Profile 5: Traffic Accident
Profile 10: Wildland Fire
Responder Emergency
Immediate Peril
Default
Assigned When
Assigned To Incident
Source: User default state is Profile 1. When user is assigned to an Incident through API, CAD or Application the users application profile can be set to another profile

Figure 12- Dynamic selection of Operational Profiles

The User default application profile is selected at the time of provisioning for the user. Changes to a user’s application profile will come from via a set of Application Programming Interfaces (API) utilized by a computer aided dispatch terminal or other public safety application when that user is assigned to an incident.

3.7 The Comprehensive QPP framework

In the previous sections we explained the network and user states, user, incident and application data, as well as the application and operational profiles.

This complete ecosystem is what constitutes the QPP Framework, which is comprehensibly illustrated in Figure 13 below:

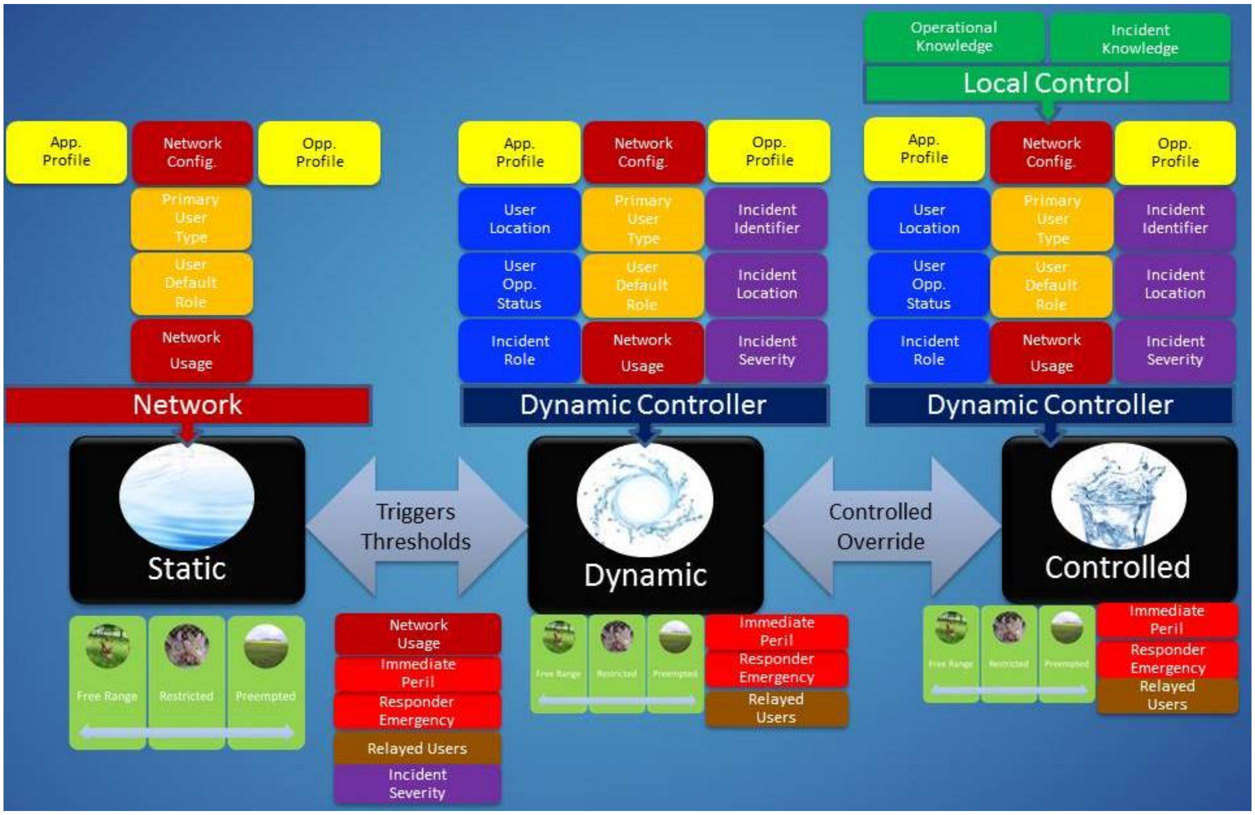


Figure 13- Comprehensive FirstNet QPP Framework

3.7.1 The Static State

In the Static State, the configuration of the network will determine how the QPP of the network is managed. The users will have default profiles and default application profiles defined in the Home Subscriber Server (HSS) and enforced both by the Policy Charging and Rules Function (PCRF), the Policy Control Enforcement Function (PCEF) and the Packet Data Network Gateway (PGW). The scheduler within the eNodeB will manage the air interface based on the static profiles. Secondary Users under a Covered Leasing Agreement can be in either one of their three states depending on network configuration; however they must only have access to unused portions of the capacity in free-range or restricted states.

Movements from the Static to the Dynamic State occur based on triggers or thresholds when:

- If network usage for a particular cell sector reaches a pre-defined threshold of utilization, e.g. 70%
- An Immediate Peril User State is declared
- A Responder Emergency State is declared
- There are relayed uses in a cell-sector
- An incident is created and transmitted via API to the NPSBN with Incident Severity that is above a pre-defined threshold

It is expected that the NPSBN will operate in a Static State a majority of the time.

3.7.2 The Dynamic State

An optimized *Static State* operational mode is crucial for network performance. Significant efforts should be spent in advance to verify the rules defined in this state are correct. An intelligent Static State mode will reduce the need and frequency of performing dynamic changes to the QPP policies, hence reducing the probability of errors.

Once the NPSBN has been triggered into a Dynamic State, the Dynamic Controller for the defined Incident Location or affected area, will assess the current network utilization situation and any dynamic user or incident data that has been sent to the NPSBN in order to begin making real-time dynamic QPP changes to ensure that primary users receive the QPP they require to manage their incidents. User States will also directly trigger the Dynamic Controller if they occur within an area under the control of the Dynamic Controller.

The most widely deployed LTE configurations today enable the network to elevate a user's QPP values and the network elements react to that user's elevated QPP state. However, these deployments are typically not able to reduce the QPP values for other users. In order to ensure that multiple differing users can be granted QPP, significant headroom must be left in the network to enable users to be prioritized over other users. These decisions are also typically made without knowledge of the user's context, only triggers from the Rx interface on PCRF for example.

The Dynamic Controller is a concept that sits above the PCRF and has access to considerable additional details such as network utilization, static and dynamic user data, triggers and the static data contained in the HSS. It will, once triggered, assess the user and incident data available, the network usage, the users in a given Incident Location and other data in order to begin making real-time decisions. These decisions could include:

- Restricting or Preempting Secondary Users
- Increasing the QPP treatment of specific users based on role or location
- Decreasing the QPP treatment of a user or users that are not involved in a defined incident
- React to User State changes like Immediate Peril or Responder Emergency

Movement from the Dynamic State back to the Static state will occur when the triggers and thresholds that triggered the Dynamic State are cleared.

Movement from the Dynamic State to the Controlled State will occur when a controlled override action is performed.

It is expected that the NSPBN will seldom operate in a Dynamic State and only for the time period that thresholds have been exceeded and triggers have been activated.

3.7.3 The Controlled State

When an incident has reached a very high level of severity or complexity and an authorized individual who has specific incident or operational knowledge, has decided to initiate a controlled override action, the Incident Location defined subset of the NPSBN will move into a Controlled State. That authorized individual will be able to provide additional high-level input to the Dynamic Controller in order to directly affect how QPP is managed for that Incident Location. This high-level input may be done via an application or API but is not expected to directly change network QPP parameters but rather influence additional rules and policies available to the Dynamic Controller.

Movement from the Controlled State back to the Dynamic State will occur when the Controlled Override action is completed.

3.8 User, Application, Network and Dynamic Controller Views

Our final topic in the description of the QPP framework is how QPP is seen from different views, relevantly Users, Application Developers and Product Engineers, Network Engineers and PSE Administrators.

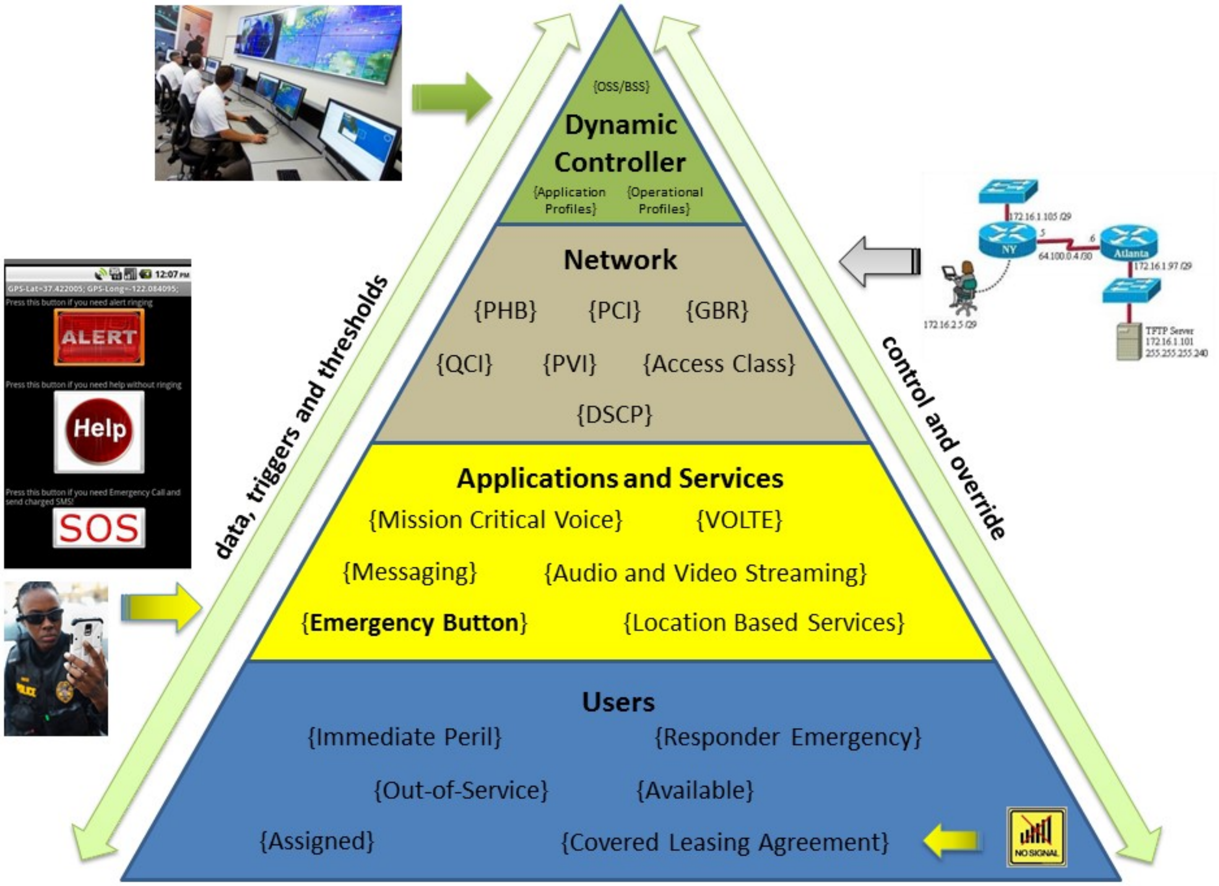


Figure 14- User, Application, Network and Dynamic Controller Views

At the User level, Primary Users will see their QPP properties reflected in better QOS and access to their applications, with the ability to influence those through special Apps such as Emergency Button.

Secondary Users may see their services being blocked when sharing the network in a geographical area where the network is in dynamic or controlled state.

At the Application level, Network and Product Engineers will provide flexible configuration APIs to allow specific QPP characteristics.

Application developers will use flexible configuration APIs to influence specific QPP characteristics.

At the Network level, Network engineers will configure their standard LTE QPP parameters and policies to implement the standard mechanisms associated to QOS, Priority and Preemption throughout the various network subsystems (including backhaul and IP networking), but will need to adapt their traditional understanding of how these mechanisms influence different applications. OSS and BSS interfaces will also need to be defined to facilitate the functions of the Dynamic Controller.

At the Dynamic Controller level, the PSE Administrator will have the ability to define default user profiles, default application and operational profiles and to interface their systems such as computer aided dispatch systems via API to the NPSBN in order to provide the data that the NSPBN needs to make QPP decisions.

4 QPP Capabilities for Further Study

In this section we provide a list of areas that require further study, to complement the QPP framework described in Section 3.

4.1 Groups

Traditional LMR or other communication systems dedicated to Public Safety offer the capability to define *groups* or fleets, a subset of subscribers that can communicate with each other with more flexible mechanisms (e.g. dial a short number), have the ability to conference and some other advantages.

In the context of the NPSBN, groups can be defined as well, for instance to receive broadcast data, and important to this discussion, be assigned similar QPP characteristics. The concept of QPP Operational Profiles can be exploited towards that purpose, but then (a) the QPP subscriber databases require the dimension of group as one additional configurable data, (b) the Dynamic Controller requires an integration with the NPSBN mission critical services infrastructure (e.g. IMS group list) for provisioning and operational QPP management, and (c) the network needs to provide those flexible dialing, conferencing, data broadcast and other characteristics to a group concept that doesn't exist in that form in the traditional LTE networks.

Standards work is being carried out in 3GPP to specify QPP management for group communications.

4.2 Relayed User Emergency

A Relayed User Emergency is a user in the NPSBN that may not be involved in the management and operations of an incident, and yet their UE could act as a communication relay in the Uu interface (UE-eNodeB) to sustain network availability in a case where a UE in Immediate Peril, Responder Emergency or other high priority User State has lost his/her connection (e.g. due to a lack of line of sight with the eNodeB).

The scenario described is one of the possible mechanisms to be implemented in the NPSBN, to enhance network coverage and availability, critical elements to First Responders.

As a consequence of this scenario, a Relayed User should be assigned a QPP Operational Profile that accommodates the QPP requirements of the User in Immediate Peril (or other high priority User State).

Note that a Relayed User could also be a secondary user.

4.3 QPP treatment of VPN/mVPN Traffic

If a public safety agency chooses to use a mobile virtual private network mVPN solution to encrypt traffic end-2-end, the NPSBN may not be able to differentiate that users differing traffic to provide QPP treatment. The QPP solution may not be able to determine if a user is sending an email or calling for help in a responder emergency.

4.4 QPP treatment on App Security Container Solution

Currently there are enterprise users that protect their application, data and identification with security containers for their customers, using a more encrypted end-to-end model. The QPP management for these applications and services during incidents needs to be explored.

4.5 QPP preserved in Roaming scenarios

It has been mentioned above that the QPP framework requires not only the features available in the network subsystems, but also the interactions between the network, applications and the dynamic controller to provide a comprehensive framework. That also includes the exchange of dynamic data and the implementation of triggers and thresholds.

Commercial networks from roaming partners may not only have different QPP features and configurations (e.g. preemption), but also may not be able to interact properly with applications and the dynamic controller as required by the comprehensive QPP framework.

Finally, although home policies and QPP relevant parameters (ARP, QOS) can be passed down from the home network (NPSBN) to the visited network (roaming partner´s), it is not clear what the visited network will do with those settings. This topic needs to be discussed with roaming partners.

4.6 QPP preserved in Opt-Out scenarios

From the perspective of QPP, an Opt-Out state that has chosen to build its own RAN must fully comply with QPP Framework to ensure end-2-end QPP.

4.7 QPP profiles preserved across PSE Network Domains

End-to-End QPP may not be possible with current technologies, unless there is interaction between the QPP framework and a public safety agencies enterprise network. For instance, the two networks must share DSCP information to ensure end-2-end QoS, Priority and Preemption.

4.8 Overlapping Jurisdiction QPP

This scenario is relevant when Incidents reach multiple jurisdictions, levels of government, functional agencies, and/or emergency responder disciplines, where the PSE Administrator may only have access to the QPP Operational Profiles framework under his/her domain, without mentioning that profile frameworks may differ across different jurisdictions.

There are technical capabilities that need to be investigated to support this objective, and there is also a requirement for a governance process that adjudicates conflicting requests based on geographical or jurisdictional overlaps.

5 Conclusion

Summary of major definitions, requirements and next steps

In this white paper the QPP framework, as envisioned by the FirstNet PSAC, has been introduced and explained.

The QPP framework responds to the mandate in the Act, to define, implement and operate a NPSBN network that provides mobile broadband service to the users in Public Safety (or First Responders), with sustained quality of service and priority access to those users assigned to management and operations during incidents. To support this sustained QOS and priority access, a preemption capability needs to be implemented as well.

Given the requirements in the Act, the QPP framework uses the features and configurations standard in LTE networks, but relies also on a comprehensive ecosystem of systems, parties and functions to provide the required QPP capability and maintain alignment to the requirements from agencies involved in Emergency Management, relevantly FEMA's NIMS.

The comprehensive QPP framework is explained in section 3. The architecture and design of the NPSBN shall take into consideration this framework, especially as it relates to data management, applications and the dynamic controller.

Finally, additional investigation is needed to understand how this QPP framework can expand towards scenarios of roaming and Opt-Out states, how groups can be managed, how relayed LTE users can be supported, how encrypted traffic can be applied priority and preemption rules, and how QPP characteristics can be ported across different PSE jurisdictions.

6 Glossary of terms

3GPP:	3rd Generation Partnership Project
AC:	Access Class
API:	Application Programming Interface
ARP:	Allocation and Retention Priority
BSS:	Business Support Systems
CDC:	Centers for Disease Control and Prevention
COM-U:	Communications Unit
CAD:	Computer Aided Dispatch
CLA:	Covered Leasing Agreement
DSCP:	Differentiated Services Code Point
ENodeB:	Enhanced Node Base Station
EPA:	United States Environmental Protection Agency
EPC:	Evolved Packet Core
E-UTRAN:	Evolved – Universal Terrestrial Radio Access Network
FCC:	Federal Communications Commission
FEMA:	Federal Emergency Management Agency
GBR:	Guaranteed Bit Rate
Geofence	A geofence is a virtual barrier. Programs that incorporate geo-fencing allow an administrator to set up triggers so when a device enters (or exits) the boundaries defined by the administrator, an action is executed, e.g. a text message or email alert is sent
HSS:	Home Subscriber Server
ICS:	Incident Command System
IP:	Internet Protocol
Kbps:	Kilo Bits Per Second
LOS:	Line of Sight

LTE:	Long Term Evolution
Mbps:	Mega Bits Per Second
MCV:	Mission Critical Voice
MIMO:	Multiple-Input and Multiple-Output
MPLS:	Multiprotocol Label Switching
mVPN:	Mobile Virtual Private Network
NIMS:	National Incident Management System
NIST:	National Institute of Standards and Technology
NPSBN:	Nationwide Public Safety Broadband Network
OMC:	Operations and Maintenance Center
OSS:	Operations Support System
PCEF:	Policy Control Enforcement Function
PCRF:	Policy Charging and Rules Function
PCI:	Pre-emption Capability Indicator
PCRF:	Policy Charging and Rules Function
PGW:	Packet Data Network Gateway
PHB:	Per-Hop Behavior
PSAC:	Public Safety Advisory Committee
PSE:	Public Safety Entity
PVI:	Pre-emption Vulnerability Indicator
QCI:	QOS Class Identifier
QOS:	Quality of Service
QPP:	QOS, Priority and Preemption
RAN:	Radio Access Network
SPR:	Subscription Profile Repository
SS7:	Signaling System 7

UE:	User Equipment
UICC:	Universal Integrated Circuit Card
UMTS:	Universal Mobile Telecommunications System
USIM:	Universal Subscriber Identity Module
UTRAN:	Universal Terrestrial Radio Access Network
VOLTE:	Voice Over Long Term Evolution
VPN:	Virtual Private Network

7 References

[1] Middle Class Tax Relief and Job Creation Act of 2012

[2] Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network

[3] Incident Command System (ICS) Communications Unit (COMU), Implementation and Best Practices, A Guide for Program Development, US Department of Homeland Security, OEC/ICTAP, December 2012

[4] National Incident Management System, Homeland Security, December 2008