Priority and Quality of Service in the Nationwide Public Safety Broadband Network

Rev. 1.4

August 2015

NPSTC Technology and Broadband Committee

Priority and QoS Working Group

National Public Safety Telecommunications Council

Revision History

Date	Version	Notes	Authors
10/28/11	0.1b	Original draft, prior to Task Group review.	Dave Buchanan, Cynthia Cole , Reid Johnson , Trent Miller, Ralph Parker
1/4/12	0.1c	Added Access Class Barring and discussion of initial system access (sections 2.1 and Appendix A). Resolved review comments PSCR-1, PSCR-3, PSCR-4, ALU1-ALU4.	Dr. Michael Britt, Wim Brouwer , Dave Buchanan, Reid Johnson, Brian Kassa, Patrick Kenealy, Trent Miller , Ralph Parker, Andrew Thiessen, Curt Wong
1/5/12	0.1d	Resolved review comments ALU-5, ALU-6, Harris-1, RJW1-3. Deleted "Magnitude of Incident" dynamic priority parameter per TG Meeting #14.	Wim Brouwer, Reid Johnson, Trent Miller, Robert Wilson
1/29/12	0.1e	Resolved review comments PSCR-2, RJW-4, RJW6-9. Added write-ups on Bandwidth Management and Immediate Peril.	Dr. Michael Britt, Wim Brouwer, Dave Buchanan, M. Jay Farr , Jeff Farris, Patrick Kenealy, Frank Kiernan (C, Jim Marocchi, Trent Miller (MSI), Pam Montanari , Val Oprescu , Ralph Parker, Robert Wilson
2/13/12	0.1f	Separated Home vs. Itinerant into static and dynamic portions. Clarified comparison of Responder Emergency vs. Immediate Peril. Added write-up on Group/Session priority.	Wim Brouwer , Dave Buchanan , Trent Miller, Ralph Parker
2/29/12	0.2	Updated "Responder Function" and "Responder Emergency" write-ups. Added Trasnport Priority, Priority and QoS Survey, Preemption write-ups.	Cynthia Cole, Jim Marocchi, Trent Miller
3/27/12	0.3	Updates from 3/21/12 task group review.	M. Jay Farr , Tom Hengeveld, Ajit Kahaduwe, Trent Miller, Ralph Parker, Robert Wilson
4/2/12	0.4	Additional clarification of 3/21/12 review issue HRS26. Version submitted for NPSTC Governing Board review.	Tom Hengeveld, Trent Miller
4/17/12	1.0	Removed watermark. Formal published version after NPSTC Governing Board review.	Trent Miller
5/18/15	1.1	Initial updated draft from NPSTC 2014-2015 Working Group.	NPSTC 2014-2015 Priority and QoS Working Group participants.
5/26/15	1.2	Integrated updates from chapter leads. Version distributed for formal Working Group review.	NPSTC 2014-2015 Priority and QoS Working Group participants.
6/27/2015	1.3	Updated document from formal working group review.	NPSTC 2014-2015 Priority and QoS Working Group participants.
7/20/2015	1.4	Updates on v1.3 rework.	NPSTC 2014-2015 Priority and QoS Working Group participants. Update from NPSTC requirements scrub.

Priority and QoS in the Nationwide Public Safety Broadband Network

Table of Contents

1 INTRODUCTION

1.1 ORIGIN

The purpose of this document is to outline public safety priority and quality of service (PQoS) needs and use cases for the 700 MHz Nationwide Public Safety Broadband Network (NPSBN). The document contains herein the requirements for the Nationwide Priority and QoS Framework, and it was developed by the Priority and QoS Working Group (PQoS Working Group) of the NPSTC Technology and Broadband Committee. This report was originally issued in 2012; however, this document represents a 2015 update of the same and was constructed by a collaborative effort between public safety users, government representatives, and members from industry. Unless explicitly noted, the document represents broad consensus of the material provided. This report is one in a family of National Public Safety Telecommunications Council (NPSTC) reports which provide recommendations and requirements for the NPSBN.

With substantial support from public safety, the U.S. Congress has identified 3GPP Long-Term Evolution (LTE) as the access network technology for the NPSBN. Although LTE represents a "how," this document assumes LTE as a constraint. As such, references to LTE will be used to enhance clarity of the public safety need description. Where there is broad consensus on an LTE feature that is appropriate to a given need, this paper identifies that feature and suggests an approach that meets the need; however, specific implementation details are intentionally omitted.

The Working Group views the NPSBN as a private network, distinct from public (commercial) networks. It is therefore assumed that the NPSBN will not be subject to the same regulatory regimen as public networks. For the purposes of this document, the relevant constraint is the LTE technology.

Public safety presents a number of unprecedented prioritization challenges for the NPSBN. First, the NPSBN will be simultaneously shared by many different types of users (e.g., police, fire, EMS, secondary use, etc.) and these various User Entity types have, in many cases, overlapping jurisdictional areas (e.g., federal, state, county, local). Second, all types of applications (e.g., voice, data, video) now share a common packet-based network. Third, public safety operations are dynamic and it is difficult to assign a single priority to a responder that will meet all their operational needs. These challenges necessitate a disciplined and rigorous approach to the definition of a PQoS Framework suitable for nationwide interoperability and public safety.

1.2 SCOPE

Items explicitly included in the scope of this document are the priority and quality of service aspects of:

- Nationwide interoperability
- Nationwide PQoS Framework for the NPSBN
  - "Default" day-to-day prioritization and QoS capabilities
  - "Dynamic" prioritization and QoS capabilities to meet special incident situations, such as a responder emergency
- Needs pertaining to devices (UEs) and infrastructure supporting the NPSBN

- Specific references to LTE technology for enhancing the description of a public safety need
- Specific needs of public safety applications as they interface with the NPSBN
- Usage of preemption on the NPSBN, which immediately discontinues certain sessions in favor of allowing other sessions to proceed
- Rate limiting and bandwidth management, controls which can manage how much bandwidth a responder can consume at one time

Items explicitly excluded from the scope of this document include:

- Discussions of how to implement or realize stated needs
- Settings, configuration, or profile descriptions
- Prioritization and Quality of Service of NPSBN devices as they roam to commercial or other networks
- Multi-national Priority and QoS interactions (e.g., Canada-U.S.)

Application level prioritization and QoS pertains to what may be achieved at the application layer above the LTE bearer plane. For example, a push-to-talk handset application could communicate with a centralized server that multiplexes and forwards the voice communications with various users within the system based on a talk group identifier. In this case, the centralized server could provide varying priorities and QoS based on user profile as identified within the push-to-talk application itself. These prioritization and QoS parameters would be separate from those established at the bearer plane within the LTE network, but ultimately need to be translated into parameters established at the bearer plane.

Experience shows that the needs of various public safety agencies are unique and can vary over both long and short time horizons (e.g., over months or years at the long end, and over minutes and hours within an incident at the short end). Therefore, flexibility must be built into any plan regarding priority and QoS. Use of the framework described herein must not eliminate a User Entity's flexibility to meet their needs, and must allow agencies to adjust their operations and procedures as experience is gained in using the broadband network. More specifically, many of the needs and requirements reflect the nearer term network and device capabilities, therefore the Priority and QoS requirements will need to be modified as the network and devices evolve.

1.3 Areas for Further Analysis

This section enumerates topic areas that the Working Group identified as requiring further analysis outside the scope of the Working Group's charter.

1. The relationship between FirstNet, and any regional or statewide networks or network operations requires further definition. The technical interworking between NPSBN Opt-In and Opt-Out scenarios are not addressed herein and requires further study.

2. Specific end-user controls (such as, in a mission critical voice system, the ability to control "remote monitor" and similar functions) is not addressed herein. If, as expected, standards organizations begin to develop interoperable application standards, the detailed control needs of each application should be clearly addressed.

1.4 REFERENCES

- Public Law 112-96: The Middle Class Tax Relief Act of 2012, US GPO, 2012. (INFORMATIVE).
- Priority and QoS in the Nationwide Broadband Network. National Public Safety Telecommunications Council. Rev 1.0, National Public Safety Telecommunications Council, April 2012. (INFORMATIVE).
- Local Control in the Nationwide Public Safety Broadband Network. National Public Safety Telecommunications Council. Rev F, National Public Safety Telecommunications Council, March 2012. (INFORMATIVE).
- 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture, 3GPP, 2015, 3GPP TS 23.203. (NORMATIVE).
- 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service accessibility, 3GPP, 2015, 3GPP TS 22.011. (NORMATIVE).

2 Use Cases

The PQoS Working Group developed a detailed set of use cases which cover a variety of law enforcement, fire, and EMS scenarios with a focus on priority and quality of service elements. These use cases were closely examined to determine required functionality to support a Priority and Quality of Service framework for the NPSBN. The resulting requirements were vetted with other operational requirements documents, including work being done in the Local Control and Broadband Deployable Systems Working Groups, to ensure alignment and to confirm that public safety operational needs were met.

The Working Group also evaluated other functional actions taken by telecommunicators and first responder personnel. Actions in the use cases relating to priority service were then extracted and developed further to address system features and requirements identified elsewhere in this report.

Additional information was derived from a gap analysis of the existing broadband requirements documents. Each of the PQoS requirements identified in the use cases will be required for implementation of the NPSBN.

The use cases listed below have been organized to demonstrate the public safety requirements that were derived from them.

2.1 General Use Case #1

Any-City Police Department has multiple units participating in a training exercise. Any-City Fire Department units respond to a house fire in the same cell sector. Without PQoS management, units at the training exercise may negatively impact units at the house fire.

2.2 General Use Case #2

A firefighter working inside a burning building gets separated from his crew and calls for assistance using a mission critical voice application. The network in the firefighter's cell sector is congested from multiple units and another firefighter's helmet camera video feed. The firefighter's voice message takes priority over the helmet camera feed because the LTE system has been programmed that *mission critical voice* applications have higher priority than mission critical video applications.

2.3 General Use Case #3

A fire dispatcher assigns multiple units to a report of a warehouse fire which is located near other responders in the same cell sector conducting a training exercise. Congestion is occurring in this cell sector. Dynamic PQoS can automatically elevate the priority of units assigned to the warehouse fire. A CAD system interface notified the PQoS that specific units (devices) were assigned to a high-priority incident, and their priority should be set to a new value.

2.4 General Use Case #4

Dispatch Center personnel receive a Responder Emergency alert automatically generated by a police officer's body sensor. "Responder Emergency" elevates the priority of a set of agency-configured applications (and their associated LTE bearers) on all of the officer's LTE devices to the highest level on the network. This allows voice, data, and video to flow to the dispatch center – even during periods of network congestion.

2.5 General Use Case #5

A paramedic needs to establish a video telemedicine session using a video application with a physician at the hospital regarding treatment options for a pediatric asthma patient who is not responding to medication. The video application is denied due to network congestion. The paramedic activates the Immediate Peril option from the user's authorized device, which increases the priority of this video application. The LTE system then preempts (or slows) resources (bearers) associated with other applications to allow this video application to commence. The elevated priority created by the Immediate Peril feature is only assigned to this paramedic's selected video application.

2.6 General Use Case #6

Multiple units and agencies arrive at the scene of a passenger jet crash at a local airport. Two hundred public safety personnel are operating in the immediate vicinity of the crash site covered by a single cell sector. Dynamic priority parameters in the PQoS allow designated applications and users to have higher priority. This may include non-traditional first responders (i.e., airport security director).

2.7 Use Case – Shared Equipment among multiple users

Prior to leaving the station, Alice, a city police officer, selects an available broadband device from a charging bay. The charging area has over 50 devices available and responders can use any of the devices. Alice notes that the device she selected today is different than the broadband device she used yesterday, but proceeds with the sign-in process. After successful sign-in, Alice's priorities and defaults are applied to the device she is currently using.

2.8 Use Case – Shared Equipment

A city fire station is alerted to a blaze at a nearby chemical plant involving multiple hazardous materials. Steve, the fire captain, validates the inventory of essential equipment on his ladder truck and joins his crew to respond to the call. Steve is already signed into the fire truck's data terminal and because of Steve's assignment to the hazmat fire, he receives elevated priority on the NPSBN. The data terminal is able to receive building plans and map files while en route to the scene.

2.9 Use Case – Users with Multiple Devices

John is serving as the incident commander at the scene of a warehouse fire. He currently has a command tablet that shows the location of three engine and two ladder companies in his operations group. He also is using a broadband portable and broadband mobile for push-to-talk. The warehouse fire happens to be served by a congested FirstNet cell. Other activities in the cell are video surveillance of gang members and heavy telephony usage by commercial users. Because John and his operations team have been identified as serving a high-priority incident, his command and push-to-talk applications receive priority and are not disrupted.

2.10 Use Case – Type of User

Laura is a citizen using her commercial cellular phone at the scene of a warehouse fire. Her phone is using NPSBN spectrum under a roaming lease agreement. Laura is streaming a video session to her husband who is at work in another state. The cell sector in this area is congested and additional resources are needed to support the public safety mission. The NPSBN PQoS recognizes that Laura is not a public safety user and assigns lower PQoS parameters to her resources (bearers) than are assigned to the emergency personnel resources (bearers). This action discontinues the dedicated NPSBN resources (bearers) associated with her video streaming session. Consequently, her video becomes choppy and the image quality is reduced.

2.11 Use Case – Type of Application

A multi-vehicle accident has taken place during a snow storm and has involved more than 40 vehicles. Numerous police, fire, and EMS units are on-scene. Ted, an EMS technician, attempts to establish a video telemedicine session with his home hospital, but the session is denied due to insufficient resources. Ted then tries to initiate a push-to-talk voice session with his home hospital and that call goes through. Ted consults with hospital staff. This use case illustrates that certain applications on the NPSBN, e.g., push-to-talk, can be configured to have higher priority, by default, than other applications.

2.12 Use Case – Responder Emergency

Jerrod, a police officer, is shot after approaching a vehicle during a traffic stop. The vehicle drives away as Jerrod falls to the ground, unconscious. His automatic health monitoring system detects his condition and activates the Responder Emergency condition through Jerrod's broadband device. Jerrod's agency has preconfigured full-duplex PTT, health monitoring, and location reporting to be activated when a Responder Emergency is activated. Because Jerrod's agency pre-configured these applications with the NPSBN, they are given emergency priority on the NPSBN. Jerrod's dispatcher and shift supervisor can listen in and monitor his vitals as they call for EMS, despite congestion in Jerrod's cell.

2.13 Use Case – Immediate Peril #1

Ryan is an EMS paramedic at the scene of an unconscious teenager. Ryan believes that the teenager has ingested some type of poison and needs to establish a video telemedicine session with a hospital. Network congestion is preventing the video session from being established. Ryan long-presses the icon[1] for the telemedicine video application in order to trigger Immediate Peril priority. The telemedicine video session then initiates successfully and Ryan can share data and video with the physician in the Emergency Department. The act of initiating Immediate Peril caused NPSBN resources associated with a nearby utility worker's meter-reading application to be lowered in priority. This results in the slowing of the application's network access.

2.14 Use Case – Immediate Peril #2

A windswept brush fire is rapidly approaching a gas station. A tanker truck is at the station refilling the underground tanks and is blocked in by multiple vehicles that are attempting to get fuel before evacuating the area. Lieutenant Williams, assigned to a fire truck, is approaching the scene and attempts to send a streaming video session to the Incident Commander (IC) to communicate the extreme danger of the situation. The video session does not initiate due to congestion from multiple users in the immediate area. Williams activates Immediate Peril and re-attempts his video streaming session. The license plate reading application on a nearby police car is slowed and the streaming video of the gas station is initiated.

2.15 Use Case – Operational Status

Dave, an EMT, has finished his shift. He uses his device for both work and personal communications. Using his device, Dave signs out of his workforce management system. This informs the NPSBN Dave is off-duty and the

[1] This is one of many possible implementations to activate Immediate Peril. This use case is not attempting to prescribe a specific method. This example is purely explanatory.

NPSBN now uses off-duty PQoS for Dave. Dave attempts to initiate a video call to his wife to let her know he's on his way home, but the call fails due to congestion from other incidents in the area. Dave pulls over and sends his wife a text message indicating he'll be home at 6:15 PM. The text message successfully goes through.

2.16 Use Case – Incident Command System (ICS) using Incident Severity

At the scene of a large Western wildfire, 15 active engine companies are attempting to prevent the spread of the blaze. The fire spans a large geographic area (multiple NPSBN cells). Each of the firefighters is equipped with a real-time health array, which tracks location, temperature, pulse, SCBA air volume, and a helmet-mounted video camera. The IC calls dispatch to ask for additional engine companies to relieve several companies that have been on duty nearly 12 hours. Because the IC is assigned to a high-priority incident, the IC's call causes traffic from commercial users who have roamed to band class 14 and who are sharing the same cell to be pre-empted. The IC's call goes through. In another band class 14 cell, commercial users attempt to initiate a real-time video session of the blaze, but the session is blocked by the NPSBN because telemetry data from several engine companies is consuming site resources.

2.17 Use Case – Incident Command System (ICS) using Incident Role

A passenger jetliner crashes in a suburb shortly after takeoff. Hundreds of responders [Federal Emergency Management Agency (FEMA) Type 2] are dispatched to the scene to create a perimeter, extinguish fires from the crash, and search for survivors. This area is served by two NPSBN eNodeB (eNB) sites. A federal evidence-gathering team arrives and begins capturing images and video. They also search for the flight recorder, cockpit voice recorder, and other evidence of the cause. As responders arrive, they show up on the IC's incident command application. The operations chief is also notified of arriving responders and directs each of them to designated staging areas. Responders assigned to the operations group of the incident (firefighters, search and rescue, perimeter) are prioritized over members from the finance/administration group assigned to the same incident. The head of the finance group attempts to initiate a video call to the IC to provide a plan to relieve responders that have been on shift for 10 hours. The video portion of the call does not successfully initiate due to congestion in the cell; however, the voice portion of the call does proceed.

2.18 Use Case – User Location

Tom, a police supervisor, is driving his agency-issued vehicle into another state to attend a training class. A malfunction in the vehicle's system has turned on Tom's front-facing dash camera and is streaming high-definition video over the NPSBN. Tom enters a congested cell, caused by multiple fire units working a traffic accident. The NPSBN analytics determine that Tom is not assigned to an incident and that he is out of his home jurisdiction. Resources for the streaming video from Tom's car are discontinued by the NPSBN and Tom receives an indication in his vehicle that the video session has been terminated.

2.19 Deployable System Use Case – Wildland Fire in isolated area

Lightning has ignited a fire in a remote forested region which is now threatening a power generation facility. A Deployable System (DS) will be required to provide broadband communications support in this remote area which has no NPSBN or commercial wireless coverage. A firefighter needs to communicate an urgent voice message to the IC; however, the deployable system is congested with multiple users including a firefighter who is streaming an update image to the IC. The firefighter's voice application successfully initiates and the video session is temporarily disrupted.

2.20 Use Case – End-to-End Priority and QoS #1

During the morning commute a gasoline tanker truck overturns on an elevated viaduct crossing through the city center, violently exploding and erupting into a massive fireball. The explosion is heard several miles away and local TV stations switch to aerial coverage from traffic helicopters. Thousands of area residents are instantly aware of a serious emergency and begin accessing information or attempting voice calls from their wireless devices. Less than 2 minutes after the crash commercial wireless networks and local landlines are heavily congested.

Public safety personnel, both on and off duty, are instantly aware of a major emergency. On-duty law enforcement, fire, and emergency medical personnel immediately check their NPSBN device for dispatch instructions via an automated dispatch application. Off-duty personnel follow a pre-established "check-in" procedure using various devices operating on either the NPSBN or a commercial network. The NPSBN becomes congested as a result of network traffic associated with the explosion. Users on the NPSBN network receive public safety priority based on the incident. Public safety users on commercial networks invoke priority using an available priority capability such as Next Generation Network Priority Service. End-to-end PQoS between the NPSBN, interconnected commercial networks, and Public Safety Enterprise Networks (PSEN) are essential in order to successfully distribute information and to mobilize public safety resources.

2.21 Use Case – End-to-End Priority and QoS #2

While transporting a severely injured patient to the hospital from the scene of the explosion, a paramedic determines the need for an immediate consultation with an emergency room physician due to the patient's deteriorating condition. Congestion on the NPSBN is preventing an outbound telephone call. Given the life-threatening circumstances, the paramedic invokes Immediate Peril on her NPSBN device to initiate a voice call to a pre-designated hospital ER telephone line operating on the Public Switched Telephone Network (PSTN). The elevated NPSBN priority now associated with the call carries through to the PSTN via an available priority capability such as Next Generation Network Priority Service in order to reach the hospital. The successful completion of this call will require the capability of end-to -end PQoS in both the NPSBN and interconnected commercial network(s).

2.22 Use Case – End-to-End Priority and QoS #3

The IC at the scene of the explosion is concerned that the intensity of the fireball may cause the elevated viaduct to collapse. Accessing his NPSBN device, he requests a consultation with an on-call State Department of Transportation engineer. An NPSBN application triggers an emergency consultation page over a commercial carrier to the on-call engineer. The engineer is carrying a non-NPSBN device operating on the commercial cellular network. Congestion on the commercial wireless network is preventing the engineer from placing a telephone call to the IC. The engineer then invokes an available priority capability such as Next Generation Network Priority Service on their outbound commercial network originated telephony call to reach the IC's NPSBN device. The elevated priority now associated with the cellular call on the commercial network carries through into the NPSBN to reach the IC's NPSBN device. The successful completion of this call requires the capability of end-to-end PQoS into the NPSBN.

3 Environment and Operations

Public Safety Entities (PSEs), cities, counties, and other local governments, state, and federal agencies, etc.) typically procure and deploy communications services based on operating conditions, established emergency response procedures, applicable state and federal requirements , mutual aid agreements, work rules, public-private partnerships, and citizen input. Affordability is a prime consideration, encompassing acquisition costs, installation, maintenance and management, training, and conversion costs. Other considerations include status of existing communications services, duration of service contracts, and availability of new communications services within the operational area.

These environmental and operational considerations form the basis for an entity's "communications plan."[2] To provide for both routine and emergency communications, a typical communication plan is likely to:

1. Prescribe communications services according to roles and responsibilities. For example, a local government entity such as a city or county might assign communications services based on the following roles and responsibilities:

    - First Responders: Law, fire, and emergency medical

    - Dispatch/EOC: Workstations in the centralized dispatch center and Emergency Operations Center (when activated)

    - Leadership: Senior management, essential department heads, Emergency Operations Director, Chief Public Information Officer, and, in some jurisdictions, senior elected officials

    - Key Responders: Personnel and functions within departments likely to be involved in an emergency response, such as Public Works, Water and Power, Building Inspection, Department of Health, etc.

    - Supporting Responders: Other departments and personnel providing emergency response support. May include departments such as Finance, Parks and Recreation, Social Services, District Attorney, Animal Control, and others

2. Define policies and guidelines for use of communications services.

    - Identifies the services and user equipment to be provided to departments, individuals or installed in vehicles, locations, and functions

    - Addresses "on-duty" and "off-duty" use of entity provided services and user equipment[3]

3. Establish processes and procedures for ongoing administration and management of communications:

    - Funding and budgeting

    - Inventory control, distribution, and installation for user equipment

[2] Entities may or may not have an all-inclusive communications plan; instead, an entity-wide plan might consist of a series of departmental policies and procedures that collectively constitute an entity-wide plan.

[3] Some entities have personnel obtain their own commercial cellular service, compensating them for official use through a monthly stipend.

- User training and support
- Drills and exercises
- Performance reviews and audits

PSE communications plans usually include a mix of communications services, including LMR radio systems (Land Mobile Radio), commercial cellular, landlines (Public Switched Network, Internet, leased lines, etc.), satellite, private networks (carrier provided and self-provisioned), and others. While these services can be made interoperable via interconnection, they are usually procured, deployed, assigned, and administered individually. For example, LMR is a freestanding system, physically separate from commercial cellular and landline services. Operationally, it is common practice for services to be associated with particular roles and responsibilities:

- First Responders: LMR systems are almost universally designated as the primary communications service, followed by commercial cellular, private networks, landlines, and satellite
- Dispatch/EOC: These critical functions require access to all services; LMR may be limited to a few EOC workstations
- Leadership: Commercial cellular and landline services are frequently the primary communications service, with LMR and satellite assigned individually where called for in the plan
- Key Responders: LMR systems are often assigned to individuals and/or vehicles in select departments having daily and/or emergency response roles and responsibilities. Otherwise, commercial cellular, private networks, and landlines are the primary communications services
- Supporting Responders: Commercial cellular, private networks, and landlines are the primary communications services for departments and individuals not having "full-time" response roles and responsibilities. Emergency response plans are likely to identify circumstances when these departments and individuals have a response role or responsibility, thus elevating their communications requirements on an as-needed basis

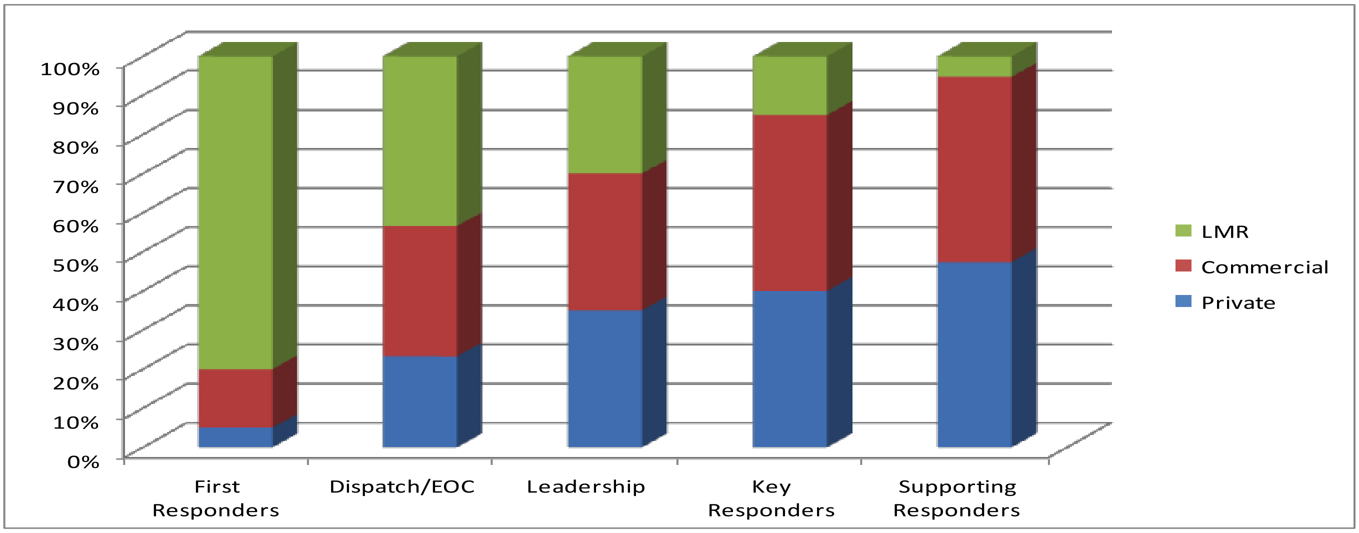


FIGURE 1. USERS AND COMMUNICATIONS SERVICES

The previous figure illustrates the relative mix of communications services that might be included in an entity's Communications Plan.

Priority capabilities have historically been bundled with the communications service(s) proscribed for each responder's role and responsibility. The highest level of priority has been usually accomplished by assigning and configuring LMR systems for primary use by first responders, select leadership, and key departments, so when an incident response threatens to congest or impair communications, these pre-identified responders are able to communicate. For instance, selected groups like SWAT or Rapid Response Teams have been given their own talk groups to avoid congestion and to provide assured communications. Priority in private networks (i.e. Public Safety Enterprise Networks) can be achieved by similarly controlling access according to roles and responsibilities. Satellite services are usually limited to mission critical functions due to cost. Per-call priority for commercial cellular voice is available by subscribing user devices to Wireless Priority Service (WPS), and per-call priority for voice calls originated on the Public Switched Network can be provided for functions and individuals through the Government Emergency Telecommunications Service (GETS). There really has not been an equivalent to the Quality of Service part of PQoS in the LMR or current commercial wireless world. The relative allocation of bandwidth and throughput has not been an option until 4G-LTE standards incorporated the capability and public safety has required the functionality within the NPSBN.

The NPSBN will present a number of opportunities and challenges for PSE, necessitating significant changes to existing entity-wide communications plans:

- First, the NPSBN will make available all types of applications (e.g., voice, data, and video) over a common packet-based network. Entities will have the opportunity to migrate from separate private and commercial services to a single network across all roles and responsibilities.

- Second, transition to the NPSBN may necessitate changes in policies, processes, and procedures for procurement, administration, and management of communications. Entities will need to evaluate which functions, capabilities, and applications provided within the NPSBN are appropriate for the various roles and responsibilities within their organization.

- Third, and most relevant to this report, is that the NPSBN will provide PQoS capabilities that can be applied across the entire organization according to role and responsibility. Instead of proscribing specific services to assure appropriate PQoS in the event of congestion or impairment, entities can apply different PQoS levels to meet both daily and emergency communications requirements according to their environment and operational situation.

3.1 Shared Spectrum and Congestion

In the 2012 Act, Congress introduced the concept of Covered Lease Agreements and the notion that Band 14 spectrum can be shared by not only public safety users but also agencies utilizing the same resources with non-public safety users. Shared spectrum takes into consideration the likelihood that at times of day spectrum remains idle if not lightly used across a particular geography hence the notion of monetizing that excess capacity. For example, if the average capacity of a NPSBN radio site is 30 Mbps and day-to-day first-responders traffic demand to that particular site averages to 10 Mbps, 20 Mbps becomes the excess capacity. This available capacity should not be compared to a user peak data rate which can largely exceed those figures. Therefore, it becomes clear that as the first responder traffic demand within a site footprint increases then the lower the available excess capacity.

As first responder traffic demand becomes high enough then lower-priority non first responders will experience delays and will possibly lose connectivity. As part of that sharing framework it may be that the commercial providers have spectrum bands towards which non first responders' traffic can be offloaded if those other bands are not congested.

With traditional or conventional LMR technologies, preemption leads to essentially dropping low-priority voice calls; however, the common usage of group communications, whereby one speaks while many listen or one video stream is viewed by many, lessens to some extent the need for preemption. With new technologies and multimedia services, the introduction of QoS which can distinguish between best effort and guaranteed service, an ongoing active call is not necessarily dropped completely but could be throttled to a best-effort service and/or to a lower bit rate; a user/device running multiple sessions across a mix of bearers may not experience the preemption of all its sessions. Therefore, since preemption in LTE was introduced to address management and admission of dedicated resources (so-called guaranteed bit rate bearers) it will not necessarily result in device disconnection from the network or to the termination of best-effort sessions. Best-effort sessions may remain 'active' up to the limit of the radio site resources capacity. There is an expectation that the NPSBN's PQoS policy control will rely on a set of rules designed to favor public safety users, devices, and applications over non-public safety usage of the network resources.

3.2 PQoS Coverage Options (terrestrial 700 MHz, Deployables, and Satellite)

In today's environment, many public safety agencies rely on commercial carriers to provide wireless broadband to run critical applications to provide mapping and location services, enhance situational awareness, query databases, and deliver many other services. The challenges with commercial wireless broadband for public safety are the constraints of available commercial carrier coverage in their respective areas and the lack of support for access, admission, and scheduling priority.

Commercial wireless broadband coverage is provided by a terrestrial network of towers, antennas, and backhaul infrastructure which is similar to current LMR networks. This network model creates coverage gaps where tower coverage footprints are not conjoined creating challenges for public safety to perform and sustain operations.

Commercial carriers have the ability to extend coverage or add capacity to their network via deployables. The most common commercial deployable is the CoLT or cellular on light truck which has RAN functionality with backhaul capabilities. CoLTs are limited resources provided by commercial carriers that have limited response areas nationwide which do not provide priority.

In tomorrow's environment, public safety will have access to the NPSBN. The NPSBN is anticipated to increase terrestrial coverage coupled with access, admission, and scheduling priority supplemented by deployable and satellite coverage.

During the build out of the NPSBN and during development of rural coverage requirements, it is likely that NPSBN service will be supplemented via roaming agreements with commercial wireless carriers.

Deployable coverage is an option that should extend or add capacity to the NPSBN network, much like the commercial deployable, but should have the ability to prioritize network traffic. Public safety requires this type of coverage to operate in areas with spotty to no coverage (e.g., remote areas, in-building) or at events with a high public safety presence.

Satellite coverage is an option that may be necessary to provide backhaul and/or UE device connectivity to the NPSBN. This type of connectivity should support prioritization of network traffic in a similar way as traditional NPSBN core functions.

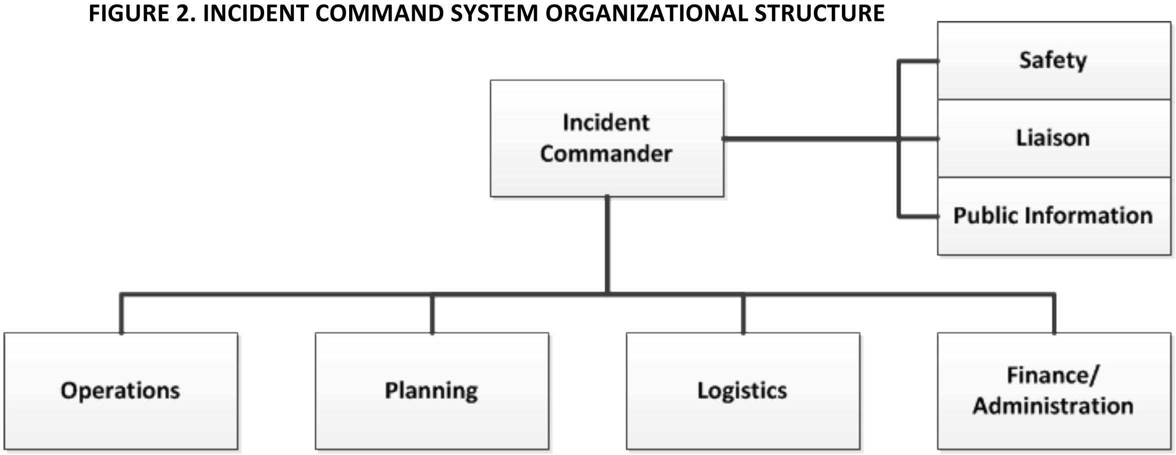
Other coverage options to consider are WiFi hotspots. These hotspots are used as a bridge to connect the NPSBN/commercial carrier network with UE devices using current 802.11 protocols. Public safety agencies are using this option to reduce equipment and device subscriber costs. Public safety agencies will need prioritization and QoS capabilities if using this band.

The traditional implementation of PQoS attributes and settings relate to a singular 4G LTE network system; however, when the additional options of commercial roaming, deployables, satellite or WiFi are factored in the question of how PQoS will be integrated into the overall schema becomes quite complex. The requirement would be to replicate and emulate the intended PQoS settings and attributes where possible.

3.3 Incident Command System[5]

The Incident Command System (ICS) is used by public safety agencies to manage emergencies. The full use of ICS depends upon the size and complexity of the incident. Functions and roles may be assigned to multiple individuals or a few persons may be assigned multiple responsibilities.

FIGURE 2. INCIDENT COMMAND SYSTEM ORGANIZATIONAL STRUCTURE



Not all of the ICS positions need to be active in each incident. The ICS structure is meant to expand and contract as the scope of the incident requires. For small-scale incidents, only the incident commander may be assigned. Command of an incident would likely transfer to the senior on-scene officer of the responding public agency when emergency services arrive on the scene.

An abbreviated summary of the roles and responsibilities of each ICS position are presented below.

INCIDENT COMMANDER

- In charge of the organization’s on-scene response

- Maintain command until public agencies arrive and assume command or when relieved at start of next operational period

- Assess the situation

- Order warning of persons at risk or potentially at risk to take appropriate protective actions

- Notify or verify internal teams, departments, public agencies, regulators, contractors, and suppliers have been notified

- Appoint others to incident command positions as needed

- Brief staff on current organization and activities; assign tasks; schedule planning meeting

- Determine the incident objectives and strategy; identify information needed or required by others; ensure planning/strategy meetings are held and attend as needed

- Coordinate activities with the EOC; identify priorities and activities; provide impact assessment for business continuity, crisis communications, and management

- Review requests for resources; confirm who has authority to approve procurement; approve all requests for resources as required

- Provide information to and coordinate with crisis communications or media relations team

- Terminate the response and demobilize resources when the situation has been stabilized

SAFETY

- Identify and assess hazardous situations; prevent accidents

- Prepare safety plan; ensure messages are communicated

- Stop unsafe acts; correct unsafe conditions

LIAISON

- Point of contact with outside agencies and companies

- Monitors operations to identify inter-organizational problems

PUBLIC INFORMATION

- Notify spokespersons and Crisis Communications Team

- Develop information for use in media briefings

- Obtain IC's and management approval for all news releases

- Conduct periodic media briefings

- Arrange for tours, interviews, and or briefings

- Monitor and forward useful information to the media

OPERATIONS

- Manage all tactical operations during the incident
- Assist in the development of the operations portion of the Incident Action Plan
- Ensure safe tactical operations for all responders (in conjunction with any assigned Safety Officer)
- Request additional resources to support tactical operations
- Expedite appropriate changes in the operations portion of the Incident Action Plan
- Maintain close communication with the Incident Commander

PLANNING

- Conduct and facilitate planning meetings
- Supervise preparation of the Incident Action Plan
- Determine need for technical experts as well as specialized resources to support the incident
- Compile and display incident status information

LOGISTICS

- Provides resources to stabilize the incident and support personnel, systems, and equipment:
    - Workspace or facilities for incident management staff
    - Media briefing center
    - Transportation
    - Communications equipment
    - Food, water, shelter, and medical care
- Ensures Incident Command Post and other facilities have been established as needed
- Estimates and procures resources for the next operational period

FINANCE/ADMINISTRATION:

- Manages all financial aspects of the incident
- Provides financial and cost analysis information as requested
- Create accounts for claims and costs; coordinates with Logistics
- Tracks worker time and costs for materials and supplies

- Documents claims for damage, liability, and injuries

The organizational hierarchies already established within the ICS structure can easily be translated into settings and assignment within PQoS attributes of the NPSBN.

4 VIEWS OF PQOS

This section attempts to identify the users that contribute information to the NPSBN's PQoS. Overall, this is a desired interaction model and it should be emphasized that every attempt is made to integrate PQoS interactions into existing public safety workflows. New manual interactions by a user with the NPSBN in order to support PQoS have been strongly minimized.

TABLE 1. USER INTERACTIONS WITH THE NPSBN PQOS SOLUTION

Type of User	How does the user interact with the NPSBN Priority and QoS Solution?
NPSBN (i.e., FirstNet) Administrator	• On boarding and configuring new agencies on the NPSBN • Provisioning (adding, deleting, changing) users and applications for agencies that don't have their own administrators (including configuring default priority attributes) • Defining NPSBN PQoS Policy (consulting with state and local planners) • Adding, deleting, and changing nationwide applications • Managing user authentication and authorizing access to the PQoS solution
State and Local Planner	No special interactions for PQoS; however, these actions are used by the NPSBN PQoS solution: • Consult with FirstNet on the definition of NPSBN PQoS Policy
PSE Administrator	• Provisioning (adding, deleting, changing) users and applications (including configuring default priority attributes) • Managing user authentication
User's (Responder's) View	• Activation and de-activation of dynamic priority controls (Responder Emergency and Immediate Peril)
Dispatcher's View	No special interactions for PQoS; however, these actions are used by the NPSBN PQoS solution: • Determination of incident type and severity • Assignment of users to an incident
Critical Infrastructure User's View	• Activation and de-activation of dynamic priority controls (Responder Emergency and Immediate Peril, if authorized) • Given elevated priority, if assigned as responder to an incident

5 Priority and QoS Model

Priority, QoS, and Preemption are essential attributes of a mission critical system. Responders must have the resources they need to complete their mission. A nationwide framework is necessary which balances the needs of all users sharing the NPSBN, yet the framework must not be too rigid so as to ignore the dynamic nature of incidents.

This section provides a conceptual framework model which helps clarify the PQoS needs of NPSBN users. References to LTE technology are included for the purposes of understanding the relationship between user needs and prioritization mechanisms provided by LTE.

Unless explicitly noted, all requirements in this chapter apply equally to the fixed NPSBN system and NPSBN deployables.

5.1 User-Device Relationship

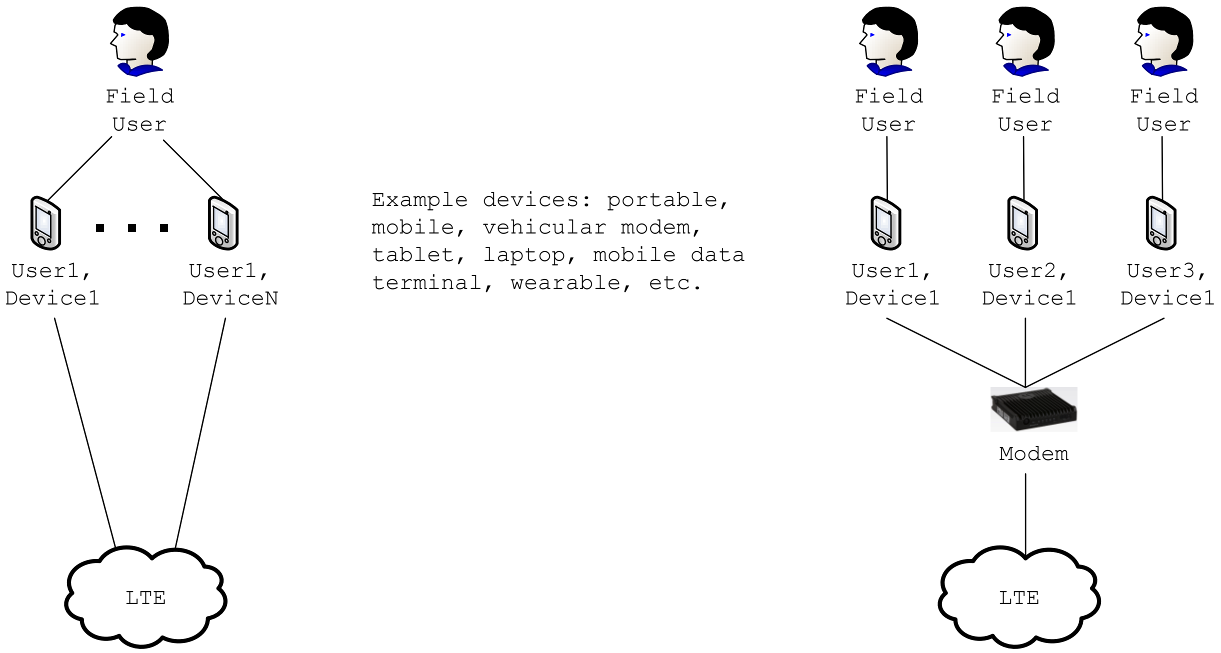
The NPSBN is anticipated to provide a favorable environment for device and equipment innovation. Specialized devices such as drones, sensors, wearable communications, and robotics aid in responder safety and response.

In the commercial world, a cellular device is typically issued to an individual. When you call the telephone number associated with that device, you expect to reach the individual. There is an implied one-to-one relationship between a user and his/her device. This is not the case for public safety. Responders may use different devices from shift-to-shift and incident-to-incident. Many agencies maintain a bank of devices that are re-used across shifts and thus it is not valid to assume a single device is always associated with exactly one user. Many responders suit up for the day and grab one or more devices from the User Entities' (agency's) charging bay. The NPSBN PQoS solution should not be cumbersome and require an administrator to provision a device for a user each time the user goes into the field. Responders should be able to utilize any authorized NPSBN device and receive their PQoS treatment.

Responders often use multiple devices simultaneously, as the mission dictates. For example, the Incident Commander at a warehouse blaze uses a portable device for mission critical voice communication, a laptop for situational awareness, a cellphone to keep the mayor and others informed, and a tablet for group situational awareness. All of the user's devices must receive consistent PQoS treatment from the NPSBN.

The following figure shows the user-device relationships for the NPSBN. The left side of the figure emphasizes that a single user may utilize multiple devices during their shift and those devices can be any authorized NPSBN device.

The right side of the figure is a more complicated scenario. In this case, multiple responders are sharing a single NPSBN device. For example, this is the case a fire truck vehicular modem would use. The responder's device would utilize WiFi to communicate with the vehicular modem, which acts as a broadband gateway to the NPSBN. In this scenario, different users share a single device and each user may have a different priority.



Example devices: portable, mobile, vehicular modem, tablet, laptop, mobile data terminal, wearable, etc.

FIGURE 3. USER-DEVICE RELATIONSHIPS

TABLE 2. USER-DEVICE RELATIONSHIP REQUIREMENTS

#	Requirement
1	It SHALL be possible for a single user to authenticate him/herself and be associated to one or more NPSBN devices simultaneously.
2	It SHALL be possible for an authorized NPSBN user to sign into **any** authorized NPSBN device and receive her/his PQoS treatment.
3	The PQoS solution SHALL provide consistent PQoS treatment to all of the devices to which the user has successfully signed in and been authenticated.
4	It SHALL be possible for the PQoS solution to provide user-specific priorities for multiple users sharing a single NPSBN authorized device. *Note: The intent of this requirement is to support, for example, the vehicular modem or relay case.*

5.2 PRIORITY GATES

As explained in the previous section, a user is associated with one or more NPSBN device(s). This section explains the sequential steps each of the user's devices must undergo in order to receive resources from the NPSBN.

In general, a user's LTE device (and hence an NPSBN user) must pass the three gates shown in Figure 4 before the device can transmit or receive user content:

1. **Step 1 - Access Priority Gate** – wherein a user's device determines that it is allowed to communicate with a particular eNodeB,

2. **Step 2 - Admission Priority Gate** – wherein an eNodeB determines that a user's device should be allowed to allocate system and air resources; and,

3. **Step 3 - Scheduling Priority Gate** – wherein the bandwidth allocated to a particular user's device is apportioned and regulated by the system.

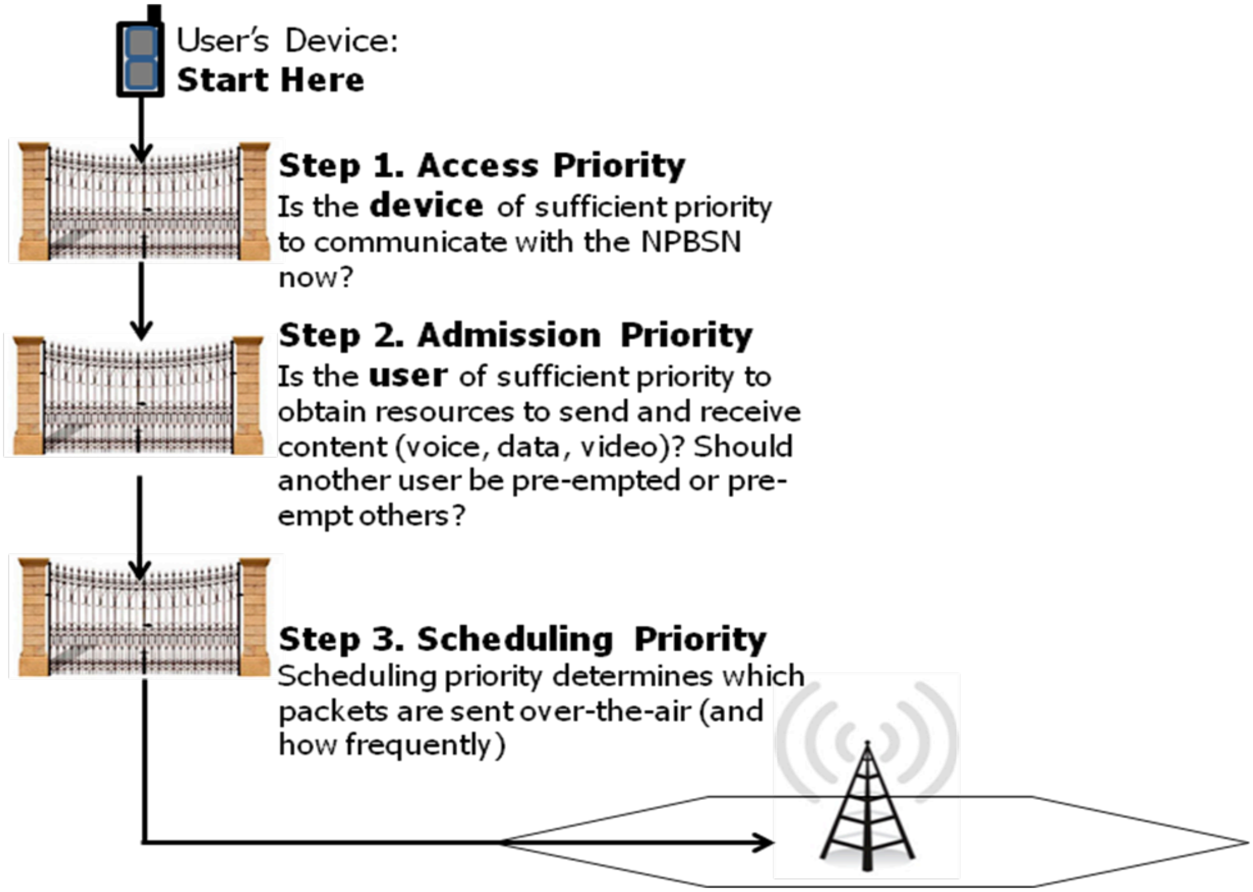

User's Device:
Start Here
Step 1. Access Priority
Is the device of sufficient priority to communicate with the NPBSN now?
Step 2. Admission Priority
Is the user of sufficient priority to obtain resources to send and receive content (voice, data, video)? Should another user be pre-empted or pre-empt others?
Step 3. Scheduling Priority
Scheduling priority determines which packets are sent over-the-air (and how frequently)

FIGURE 4. LTE PRIORITIZATION "GATES"

5.2.1 Access Priority

Various events such as earthquakes, large-scale medical emergencies, and the like will cause heavy system access. Such events frequently cause a concentration of responders in a given area. This concentration may result in a heavy load at a given cell, especially to the Random Access Channel (RACH), and the load may be so severe that a responder's device is prevented from accessing the NPSBN. While there are substantially fewer users on the NPSBN than a comparative commercial LTE system, care must be taken to prioritize initial system access for the NPSBN user community.

LTE technology provides methods which may address this need in the form of barring capabilities, such as "Access Class Barring." For more detail, see Appendix 0.

TABLE 3. ACCESS PRIORITY REQUIREMENTS

#	Requirement
5	It SHALL be possible for the PQoS solution for a user's device to consider the priority attributes identified in Table 25 (Access Priority column) when determining a user's Access Priority. *Note: In some cases, the device is not yet communicating with the NPSBN and thus the amount of information known to the user's device might be limited. For example, a device that is not yet attached to the NPSBN might not have information regarding an incident to which they were recently assigned.*
6	It SHALL be possible for the NPSBN PQoS solution to automatically enable and disable Access Priority based on cell congestion.
7	It SHALL be possible for the NPSBN PQoS solution to automatically manage LTE barring capabilities.
8	Secondary users SHALL be able to access the NSPBN so long as the act of connecting to the NPSBN does not interfere with or prevent a primary user from accessing the NSPBN.

5.2.2 Admission Priority

Admission priority refers to the behavior of the NPSBN as responders attempt to initiate (or receive) service. In light of congestion, admission priority determines whether or not a responder's application should be commenced on the NPSBN.

Admission priority policy is typically defined by an authorized administrator and is enforced directly by each LTE eNB, independently from other eNBs. Both LTE point-to-point (unicast) and point-to-multipoint (MBMS) resources utilize admission priority.

Admission priority is also used to determine whether or not preemption applies to the user and the user's application(s). This is discussed further in section 5.6.

TABLE 4. ADMISSION PRIORITY REQUIREMENTS

#	Requirement
9	It SHALL be possible for the NPSBN PQoS solution to influence LTE admission and retention capabilities.
10	The NPSBN SHALL be capable of determining which application flow a packet is associated with when MVPN or VPN technology is being used.

5.2.3 Scheduling Priority

Once a responder has a resource admitted to the NPSBN (i.e., the user's priority attributes of section 5.3 have been evaluated and the eNB has determined that resources should be granted), scheduling priority determines when traffic (e.g., packets/frames) should be sent to or received from the user's mobile device.

Like admission priority attributes, scheduling priority attributes are collected by the NPSBN PQoS solution and are ultimately enforced on a per-eNB basis.

Scheduling priority considers the following attributes in both the downlink and uplink directions:

- Packet latency and loss rate
- Whether a constant "guaranteed" bandwidth should be made available

The 3rd Generation Partnership Project (3GPP) has done considerable research into the scheduling priority needs of applications on LTE. Standardized combinations of the scheduling priority attributes have been defined in TS 23.203 [4] and are called "QoS Class Identifiers" (QCIs). A QCI is assigned to an LTE resource typically when a new application is added to the system and the QCI is likely not changed thereafter.

After the Working Group's review of the standard QCI values from 3GPP TS 23.203 [4], Table 6.1.7, Appendix 0), it has been determined that the standard QCI definitions are suitable and sufficient for public safety applications.

By adopting the industry standard QCI definitions, interoperability will be enhanced within the NPSBN and also simplify public safety's ability to roam for added coverage and capacity to non-NPSBN LTE systems.

Should the need arise, LTE does allow custom QCIs to be created.

LTE networks typically select the QCI based on the type of application being used and the particular protocol the application is using.

TABLE 5. SCHEDULING PRIORITY REQUIREMENTS

#	Requirement
11	It SHALL be possible for the NPSBN PQoS solution (using NPSBN PQoS policy) to select the scheduling priority (QCI) utilized by the NPSBN user for a given application flow.
12	On a per-application flow basis, it SHALL be possible for the NPSBN to assign and control the packet latency and packet loss characteristics.

5.3 User Priority Model

In order to address the highly varied needs identified by the user community, the NPSTC Priority and QoS Working Group has developed a logical model for NPBSN users. This model identifies *priority attributes* which are used by NPSBN PQoS policy to derive a user's priority on the NPSBN. NPSBN Administrators define NPSBN PQoS policy, which maps a user's aggregated priority attributes to specific LTE PQoS controls (i.e., the user's priority attributes are mapped to controls provided by LTE at each priority "gate").

It is essential that the priority attributes in this section be as transparent as possible to the NPSBN users. That is, a user should not have to log in to an LTE terminal during a high-stress incident and adjust technology controls to give a user priority. For example, a dispatcher using a Computer-Aided Dispatch terminal to assign a responder to an incident should not have to manually set the "Incident Severity" attribute. The act of the dispatcher choosing the incident type in the CAD terminal should automatically adjust the "Incident Severity" priority attribute for the assigned responder.

Figure 5 shows the user priority model.

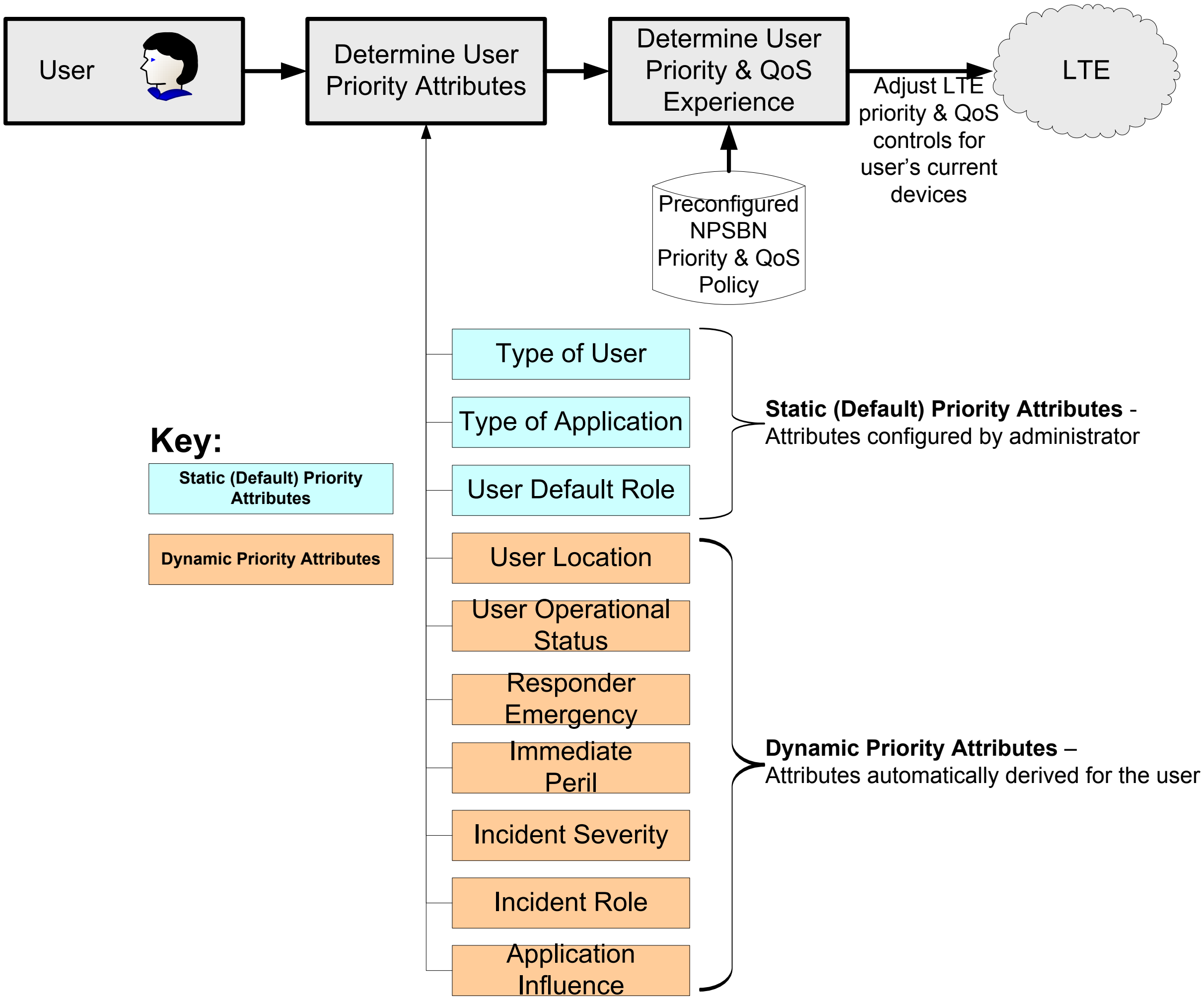

User
Determine User Priority Attributes
Determine User Priority & QoS Experience
LTE
Adjust LTE priority & QoS controls for user's current devices
Preconfigured NPSBN Priority & QoS Policy
Key:
Static (Default) Priority Attributes
Dynamic Priority Attributes
Type of User
Type of Application
User Default Role
Static (Default) Priority Attributes - Attributes configured by administrator
User Location
User Operational Status
Responder Emergency
Immediate Peril
Incident Severity
Incident Role
Application Influence
Dynamic Priority Attributes – Attributes automatically derived for the user

FIGURE 5. USER PRIORITIZATION MODEL

After determining the user's current priority attributes, NPSBN PQoS policy is used to map the user's priority attributes to specific LTE controls. That is, a change in one or more of the user's priority attributes (e.g., an assignment to an incident) will cause NPSBN PQoS policy to be evaluated, and if necessary will result in a change to the user's priority on the NPSBN. The user priority attributes are used to influence each of the user's sequential priority gates (see section 5.2).

TABLE 6. USER PRIORITY MODEL REQUIREMENTS

#	Requirement
13	It SHALL be possible for an authorized administrator to provision static priority attributes for a user.
14	It SHALL be possible for the NPSBN PQoS solution to track dynamic priority attributes for a user at run-time (i.e., while the NPSBN is operating and the user has active sessions).
15	It SHALL be possible for an authorized NPSBN Administrator to define NPSBN PQoS policy in the NPSBN PQoS solution. *Note NPSBN PQoS Policy adjusts LTE PQoS controls when a user priority attribute changes.*
16	It SHALL be possible for the NPSBN PQoS solution to provide capabilities to all NPBSN users. *Note: The intent of this requirement is to explain the scope of the NPSBN PQoS solution. The solution must be able to prioritize all FirstNet users (i.e., users that are considered subscribers of the FirstNet network).*

5.3.1 User Default Priority Attributes

This section focuses on “default” or “static” priority attributes, which would be utilized unless explicitly overridden by User Dynamic Priority Attributes (section 5.3.2). Default priority attributes provide a basic stratification of users on the NPSBN and are used to determine the day-to-day prioritization LTE will automatically provide to user devices barring special incidents or needs. Because congestion can occur at any moment, the default priority framework must be carefully designed to accommodate the widest range of responder activities.

Default priority is commensurate with the usual day-to-day functions of a user, as opposed to when that user serves under the ICS structure or other dynamic priority circumstances. When heavy congestion arises, less critical day-to-day communications of emergency response support responders will be subordinated to the typically more urgent traffic of first responders in their area of operation.

Typically, an authorized User Entity administrator would configure the LTE device with default priority attributes when a user is added to the overall NPSBN (i.e., when a user joins a User Entity). The attributes themselves are not usually changed and would remain in effect until special circumstances arise. After initial configuration, the responder would not have to take any action in the field to receive the priority identified in this section.

Table 7 lists the default priority attributes for the user.

TABLE 7. USER DEFAULT PRIORITY ATTRIBUTES

Attribute	Example Values (Values ultimately selected by NPSBN Administrator)	Explanation	Who can change?	How often does this attribute change?
U1 Type of User	“Primary User,”“Secondary	Used to provide default prioritization	User Entity Admin via Web Portal,	Rarely – Defined when user is added

	User,” …	separation between types of users and machines (e.g., to differentiate responders from commercial users).	NPSBN Admin via Web Portal.	to the system
U2 Type of Application	“GBR Mission Critical Voice,” “Non-GBR Mission Critical Data,” …	Used to distinguish priority for applications	User Entity Admin via Web Portal for User Entity Applications. NPSBN Admin via Web Portal for FN Applications	Rarely - Defined when application is added to the system
U3 Default Role	“Supervisor,” “Patrol,” “Support,” …	This is the user’s normal day-to-day role within the user’s User Entity.	Admin via Web Portal, NPSBN Admin via Web Portal.	Rarely – Defined when user is added to the system

TABLE 8. USER DEFAULT PRIORITY ATTRIBUTES REQUIREMENTS

#	Requirement
17	It SHALL be possible for an authorized administrator to provision the NPSBN PQoS solution with a user’s type (e.g., Primary User, Secondary User, etc.). *Note: See section 5.3.1.1*.
18	It SHALL be possible for an authorized administrator to provision the NPSBN PQoS solution with an application; identifying the “Type of Application.” *Note: See section 5.3.1.2*.
19	It SHALL be possible for an authorized administrator to provision the NPSBN PQoS solution with a user’s “Default Role.” *Note: See section 5.3.1.3.*

5.3.1.1 Type of User

The default priority attributes include a “Type of User” attribute. Differentiation of the different types of users ensures public safety users receive appropriate priority in the presence of NPSBN congestion. In heavy congestion, less-critical users, such as public works may receive fewer resources. This attribute also allows the NPSBN to support concurrent use of the system by many different types of users. For example, this attribute can support primary users (e.g., responders) and secondary use (e.g., utility workers, streets and sanitation, machine-to-machine, and other users). FirstNet should define a nationwide scheme for the values of this field to account for the specific classifications of users supported by the NPSBN.

TABLE 9. TYPE OF USER REQUIREMENTS

#	Requirement
20	It SHALL be possible for the NPSBN Priority and QoS solution to provide a differentiated PQoS experience to a user, based on the user's type (e.g., primary user, secondary user).

5.3.1.2 TYPE OF APPLICATION

Traditional LMR systems often maintain a distinction between resources for over-the-air push-to-talk and data services. This provides mission critical PTT services with a pool of guaranteed resources. With LTE, voice and data share a common transport, so this distinction could be removed and all applications share the same resources. Bandwidth-intensive video and multimedia services also share these resources. Because voice (PTT and telephony), data, and video all share a single set of LTE resources, it is important to distinguish the most important applications to help facilitate nationwide interoperability. The NPSBN needs to be able to determine the type of application a responder is using. As a general strategy, the Working Group has identified mission critical voice as the highest priority application to use the NPSBN. Every attempt is made to retain mission critical voice even in cases of heavy congestion. Application prioritization needs to also be consistently applied to all NPSBN sites.

An attempt is made to keep these definitions broad to account for new unforeseen applications. As the users develop experience with the technology, the framework needs to be flexible and support changes.

The Working Group studied the "Type of Application" attribute and made several changes from the 2012 Working Group report. The "Type of Application" attribute is intended to show the relative default importance of all applications on the NPSBN. The intent is that applications, other than non-mission critical data applications, receive heightened priority on the system. As congestion increases at a given NPBSN cell, lower priority applications will receive fewer NPSBN resources by default. Table 10 reflects these changes.

TABLE 10. TYPE OF APPLICATION – RELATIVE PRIORITIES[4]

Relative Priority	Applications
1 (Highest)	**Mission Critical Voice** – Example: Mission Critical Push-to-Talk Application
2	**Mission Critical Data** – Examples: Computer-Aided Dispatch Application, Location Service Application, User Health & Telemetry Application
3	**Mission Critical Video**[5] – Examples: Firefighter Helmet Camera Application, Two-way Video Application, License Plate Recognition Application
4	**Non-Mission Critical Voice –** Examples: Telephony Application, Secondary Push-to-Talk Application
5	**Non-Mission Critical Video** – Examples: Training and Quality Assurance Video Application
6	**Non-Mission Critical Data** – Examples: Text and Multimedia Messaging Application, File Transfers, Web Browsing, Email, Device Management

TABLE 11. TYPE OF APPLICATION REQUIREMENTS

#	Requirement
21	It SHALL be possible for the NPSBN PQoS solution to determine the type of application being used by an NPSBN user.
22	It SHALL be possible for the NPSBN PQoS solution to provide a differentiated PQoS experience to an application, based on the application's type (e.g., mission critical voice, mission critical data, etc.).
23	The NPSBN PQoS solution SHALL support the relative application priorities identified in Table 10.

5.3.1.3 DEFAULT ROLE

The "Default Role" attribute allows a User Entity to identify certain users as being of greater operational priority, by default, than other users. For example, the police chief is of higher default priority than the lieutenants.

[4] It is understood by NPSTC that this table mixes both Guaranteed Bit Rate (GBR) and non-GBR traffic in LTE. The exact assignment of GBR vs. non-GBR is assumed to be part of the NPSBN network implementation. In a congested system, GBR traffic is generally involved in preemption and non-GBR traffic would typically slow down. The NPSBN implementation team must consider all aspects of an application's needs, including but not limited to traffic bandwidth, latency, packet loss, etc. when choosing GBR vs. non-GBR.

[5] One factor raised by the PSCR is the nature of the video in use. For example, video can be used to view motion or video could be used for resolution and detail. This illustrates a trade-off of frame rate and resolution. Additionally, video applications often include adaptive bit-rate codecs. Specific video usage must be considered during NPSBN system design.

TABLE 12. DEFAULT ROLE REQUIREMENTS

#	Requirement
24	It SHALL be possible for the NPSBN PQoS solution to provide a differentiated PQoS experience to a user, based on the user's default role (e.g., police chief, detective, lieutenant, etc.)

5.3.1.4 Administering Default Priority

The NPSBN is expected to serve many different applications which can be provided locally, regionally, or even nationwide. The entity (e.g., NPSBN or local User Entity Administrator) managing each application may or may not be the same. For example, a specialized video application may be deployed by a local User Entity and telephony services may be provided by the NPSBN Administrator. Each entity providing applications (local, regional, state, NPSBN) must have the ability to establish priority of its applications and responders within bounds established by the nationwide framework on the NPSBN. Following the previous example, the User Entity would be able to assign default priority attributes for the specialized video application, whilst the NPSBN Administrator would assign default priority attributes for telephony services; however all assigned priority attributes would conform to the values outlined in the NPSBN nationwide framework.

The act of assigning default priority attributes is typically done by an authorized administrator, subject to the terms of governance, when any of the following are added to the NPSBN:

- Users
- Applications
- Agencies

As each of these entities is provisioned for use with the system, it is anticipated each would be assigned an appropriate configuration. For example, a new user being added to the system would have her/his "Type of User" attribute provisioned into the NPSBN PQoS solution.

The Working Group notes that an agreed upon set of administrative procedures should be established for the purpose of ensuring consistency among jurisdictions controlling default priority.

TABLE 13. ADMINISTERING DEFAULT PRIORITY REQUIREMENTS

#	Requirement
25	It SHALL be possible for an authorized NPSBN Administrator to onboard (add) a new User Entity to the NPSBN system.
26	It SHALL be possible for an authorized NPSBN or User Entity Administrator to add a new user to the NPSBN system, associate the new user with a User Entity, and configure the user's type (e.g., primary user, secondary user).
27	It SHALL be possible for the NPSBN PQoS solution to provide PQoS for User Entity-operated applications.
28	It SHALL be possible for the NPSBN PQoS solution to provide PQoS for NPSBN-operated applications.

5.3.2 User Dynamic Priority Attributes

PQoS for public safety users is *situational*. That is, the priority realized by a user's devices on the NPSBN must account for what the responder is doing at the moment. For example, an on-duty firefighter at a 4-alarm blaze should receive higher relative priority than an off-duty firefighter. Dynamic priority attributes are designed to identify the NPSBN user's current activities and are measured in real time. Dynamic priority attributes temporarily override the user's default priority attributes. Typically, human intervention is required to trigger a dynamic priority change, such as pressing a device's emergency button or being assigned to an incident.

Table 14 lists the dynamic priority attributes for the user.

TABLE 14. USER DYNAMIC PRIORITY ATTRIBUTES

Attribute	Example Values (Values ultimately selected by NPSBN Administrator)	Explanation	Who can change?	How often does this attribute change?
U4 User Location	1. Latitude + Longitude , or 2. Serving Cell	Used to prevent accidental resource usage for responders out of their home area who aren't performing in an official capacity. e.g., "In or Out of Jurisdiction,""Situational Awareness"	Provided to NPSBN PQoS solution automatically from user's device(s).	Frequently - User's device location is automatically calculated as user moves and NPSN needs to map user's location
U5 Operational Status	"On Duty," "Off Duty"	Needed to support BYOD for responder devices and other use cases.	Provided to NPSBN PQoS solution automatically from (a) user CAD sign-in, (b) workforce	Infrequently - approximately 1-2x per day

			management system sign-in, or (c) device sign-in	
U6 Responder Emergency	“Enabled,” “Disabled”	Broadband equivalent of LMR emergency button. Prioritizes **User Entity defined** applications for emergency user. May pre-empt other applications to get resources for the RE.	RE can be activated from user’s device(s) for himself/herself. An authorized user (e.g., incident commander) can initiate RE for another user via their device.	Rarely – as needed by situation
U7 Immediate Peril	“Enabled,” “Disabled”	Used to prioritize an application (e.g., video) so that it won’t get pre-empted or can’t get resources to start. Provides indication that a dangerous situation is in-progress. Prioritizes **application(s) selected by end-user**.	IP can be activated from user’s device(s) for himself/herself. An authorized user (e.g., incident commander) can initiate IP for another user via their device.	Rarely – as needed by situation
U8 Incident Severity	FEMA Incident Severity Classifications, CAD Incident Priority Types, …	Used to manage the PQoS of users assigned to incidents.	Received automatically from Dispatch (CAD), Incident Command application or the user.	Per incident
U9 Incident Role	“Command Staff,” “Operations,” “Finance,” “Planning,” “Logistics”	Used to ensure resources are available for the most tactically active responders within an incident.	Received automatically from Dispatch (CAD) or Incident Command application.	Per incident
U10 Application Influence	“High,”“Low”	Allows an application, e.g., PTT, to indicate that certain calls (e.g., scan calls) are less important than other calls (e.g., 1st responder talk group).	Received from application (e.g., PTT)	Varies

TABLE 15. USER DYNAMIC PRIORITY ATTRIBUTES REQUIREMENTS

#	Requirement
29	The NPSBN SHALL provide a 'Dynamic PQoS control service' to allow suitable PSE and mobile applications to override the default day-to-day priority assigned by the PSE administrator.
30	The NPSBN PQoS solution SHALL provide an electronic interface to NPSBN-deployed and PSE-deployed mobile and fixed applications so that they might change dynamic priority attributes.
31	NPSBN LTE users and non-LTE public safety users SHALL NOT be burdened by the NPSBN with PQoS control outside of their operational paradigms. It is understood that human intervention is required to initiate a dynamic PQoS change, but the act of performing this change should not significantly distract the responder. For example, the responder should be able to press an emergency button for a life-threatening condition and not have to enter an LTE terminal to adjust complex LTE PQoS parameters.

5.3.2.1 User Location

By virtue of today's LMR system coverage (e.g., each User Entity having their own LMR system) or by configuration of an existing LMR system, agencies have a well-defined operating area (e.g., jurisdiction). The definition of a User Entity's jurisdiction varies with the scope of the User Entity itself. For example, city, county, state, and nationwide functions can all overlap.

The NPSBN will combine many User Entity types onto a single network with a single spectrum allocation. It is desirable to retain the concept of a jurisdiction when discussing priority on the NPSBN. For some responders, their normal jurisdictional area is a suburb or part of a metropolitan area. For other responders, their jurisdiction is the entire state, and for others the entire country.

There are many reasons a responder may travel outside her or his jurisdiction. Some examples include:

- Incident-based Events: Mutual aid, pre-planned events (e.g., sporting events), inter-User Entity service agreement

- Non-incident-based Events: Training, traveling to court, on vacation with device, stopping for food, vehicular service

Aside from unintentional use of bandwidth outside a responder's home area (i.e., non-incident-based events), there are cases such as mutual aid where it is desirable for a responder to operate with priority outside her/his home area. Generally, responders can be classified in one of three states:

- Home User (i.e., responder in home area)

- Low Priority Itinerant User (i.e., responder out of home area, not supporting an incident-based event)

- High Priority Itinerant User (i.e., responder out of home area, supporting an incident-based event)

For these reasons, the NPSBN must be capable of changing (typically lowering) the priority of Low Priority Itinerant Users. For example, a responder exiting their home jurisdiction to travel to court (who isn't supporting an incident-based event) would automatically (i.e., without human intervention) be de-prioritized in favor of responders home to the area. Implementation must allow for cooperating agencies (e.g., mutual aid responders) to not incur degraded communications in fast-breaking incidents that cross jurisdictions.

In some cases, responders will pursue suspects outside their jurisdiction, while not assigned to an incident. For example, a narcotics officer working undercover may pursue a suspect to their pick-up point. Such cases are dangerous and volatile. For this reason, the Working Group felt that end-user dynamic priority controls, such as Responder Emergency (section 5.3.2.3) and Immediate Peril (section 5.3.2.4) be available at all times (i.e., whether the responder is 'in jurisdiction' or 'out of jurisdiction').

TABLE 16. USER LOCATION REQUIREMENTS

#	Requirement
32	It SHALL be possible for an authorized administrator to define the jurisdictional area of a User Entity.
33	It SHALL be possible for the NPSBN PQoS solution to identify whether or not a user is associated with an incident.
34	It SHOULD be possible for the NPSBN PQoS solution to adjust a user's priority and QoS experience based on whether the user is in or out of jurisdiction and based on whether the user is or is not associated with an incident.
35	It SHALL be possible for an authorized NPSBN user, when operating outside his/her jurisdiction, to utilize dynamic priority controls (such as Responder Emergency and Immediate Peril).

5.3.2.2 Operational Status

Some agencies choose to provide a device for a user and that device can be used for both professional and personal use (i.e., the user takes the device home after her/his shift is completed). Other agencies provide a stipend to a user with the expectation that her/his device is used on the job (in addition to personal use). Both of these situations give rise to the case of a user's equipment that can be utilized for both "on duty" official business and "off duty" personal activities.

When off duty and performing in an unofficial capacity, a responder's device should not receive the same level of NPSBN prioritization as an on-duty user. The Working Group noted, however, that certain applications, e.g., mission critical push-to-talk, may retain priority even in an off-duty capacity. The Working Group further noted that dynamic priority controls need to continue to be supported in an "off duty" situation when a dynamic, rapidly changing situation is present. For example, an off-duty responder needs to be able to activate Responder Emergency (rather than requiring the responder to transition to an on-duty state first). There are many cases where an off-duty responder comes to "lend a hand" when she/he sees a nearby incident.

TABLE 17. OPERATIONAL STATUS REQUIREMENTS

#	Requirement
36	It SHALL be possible for the NPSBN PQoS solution to support BYOD devices.
37	It SHALL be possible for an authorized NPSBN user to designate whether she/he is on duty or off duty.
38	It SHALL be possible for an authorized NPSBN application (e.g., an agency CAD system) to designate whether a user is on duty or off duty.
39	It SHALL be possible for the NPSBN PQoS solution to adjust a user's PQoS experience based on whether the user is "on duty" or "off duty."
40	It SHALL be possible for an authorized NPSBN user to activate dynamic priority controls, regardless of on-duty or off-duty state.

It is recommended that certain applications and functions (e.g., mission critical push-to-talk) should retain their normal priority assignments even if the user is in an off-duty status. The Working Group recognizes this is an NPSBN policy decision.

5.3.2.3 Responder Emergency

Traditionally, the responder can press the emergency button on their LMR device to affect the priority of their push-to-talk application. The emergency button is typically used to indicate a life-threatening condition.

Similarly, the NPSBN needs to support the ability for the NPSBN user to indicate a life-threatening condition from her/his broadband device and receive emergency prioritization. The enhanced capabilities of the NPSBN LTE network can offer more than just elevated priority for push-to-talk. While it is possible to emulate LMR PTT-based emergency calling, the definition of emergency application(s) should not be as strict on broadband. For example, a User Entity might choose to use full-duplex telephony with an enabled speakerphone and location services during an emergency. In this context, an emergency application is defined as any application (voice, video, or data) pre-configured by the User Entity for use when the responder initiates the Responder Emergency function. It is recognized that law enforcement, fire, and EMS agencies may require different applications when the Responder Emergency capability has been activated.

When the Responder Emergency capability is initiated from the responder's broadband device (e.g., responder presses the emergency button), all emergency application sessions (GBR and non-GBR traffic), as defined by the responder's User Entity for all of the responder's associated device(s) must receive elevated emergency priority from the NPSBN. This must take place automatically without an administrator having to manually adjust LTE parameters. If any of the User Entity-defined emergency applications are already in use by the responder when the responder initiates the emergency function, the priority of those applications must be changed to receive emergency priority. If any of the User Entity-defined emergency applications are not in use at the responder's device when the emergency function is initiated by the responder, those User Entity-defined applications must be initiated with emergency priority. This provides users in the emergency state with the greatest possibility for communication even during heavy congestion.

Similarly, the act of clearing the emergency condition must return the emergency applications' priority to their pre-emergency values. Typically, the user that activated the Responder Emergency capability is the user that clears the condition; however, any authorized user (e.g., the dispatcher) can also clear a user's Responder Emergency.

It is recommended that the priority of the Responder Emergency capability be as high as practically possible, however it is recognized that certain functions (e.g., system administration) may require higher priority to repair and administer the NPSBN. Further, activation of the Responder Emergency needs to have pre-emptive access to NPSBN resources. In other words, should the NPSBN be congested when a responder activates the capability, the NPSBN needs to discontinue lower priority applications in progress to allow the responder's emergency applications (and their associated resources) to be accepted by the NPSBN.

TABLE 18. RESPONDER EMERGENCY REQUIREMENTS

#	Requirement
41	It SHALL be possible for an authorized administrator (User Entity or NPSBN Administrator on behalf of a User Entity) to designate a set of one or more applications to receive emergency priority when a user activates the "Responder Emergency" capability. *Note 1: The set of applications to receive emergency priority can include NPSBN nationwide or User Entity applications (or both).* *Note 2: User Entity Administrators are assumed to be able to designate Responder Emergency applications for users associated with their User Entity.*
42	It SHALL be possible for each User Entity to select different applications to be used when the "Responder Emergency" capability is activated.
43	Applications that have been designated to receive emergency priority SHOULD receive top access, admission, and scheduling priority when the "Responder Emergency" capability is activated. *Note: it is understood this is an NPSBN PQoS policy decision; however, this requirement is provided to share the desired behavior from the user community.*
44	It SHALL be possible for an authenticated and authorized NPSBN user to initiate and clear the "Responder Emergency" capability for herself/himself. *Note: The PSAC is considering all issues associated with Identity, Credential, and Access Management (ICAM), including the use case of engaging a Responder Emergency without being signed in to the device.*
45	It SHALL be possible for an authenticated and authorized NPSBN user to initiate and clear the "Responder Emergency" capability for another NPSBN user. *Note: CAD operators, shift supervisors, Incident Commanders, and similar staff may witness or become aware of an emergency condition for another user. There are many cases in which a disabled user is unable to activate the emergency capability for herself/himself and this requirement supports remote activation of "Responder Emergency" for such a user.*
46	When the "Responder Emergency" capability is activated for a user, all applications pre-designated by an authorized administrator for use in an emergency on all of the user's active devices SHALL receive emergency priority (i.e., all applications designated for emergency use by the User Entity on all active user devices).
47	When the "Responder Emergency" capability is active for a user, a clear indication SHALL be present on all of the user's active devices. *Note 1: The intent of this requirement is to avoid a situation where a user forgets to clear an emergency condition. This requirement can be satisfied by visual indicators (such as a flashing icon) or audible indicators (such as a periodic beep) or other methods.* *Note 2: While user device form factors and other issues are out of the scope for this report, it should be noted that the safety of some first responders could be compromised by visual and*

	audible alerting. It is recommended that those display features be controlled by the PSE Administrator based on end user needs.
48	It SHALL be possible for an authorized administrator to designate the notifications a user's User Entity receives when the "Responder Emergency" capability is activated. Notifications SHOULD include, but are not limited to: a) Operations terminal (e.g., maintenance terminal) alarm b) Application Programming Interface (API) callback operation
49	It SHALL be possible for the PQoS solution to generate Usage Records each time the Responder Emergency capability is activated and provide the Usage Records to authorized User Entity Administrators. *Note: Usage Records can be used for a variety of purposes, including training, charging, and operations review.*

5.3.2.4 Immediate Peril

In cases of heavy congestion at a NPSBN cell, a responder may not be able to initiate (or continue) an application. For example, an in-progress video session may be pre-empted. In congestion, the default behavior of this prioritization framework is to favor voice services over video services.

In certain rare circumstances, responders in the field or authorized User Entity administrators may require the ability to override the default prioritization of the system.

The Immediate Peril function provides the end responder (or authorized User Entity administrator) with the ability to temporarily override the default prioritization of the system when there is an **immediate threat to any human life or property** (not just to responders themselves). For example, an EMS paramedic on scene may need to use video to consult with doctors regarding a patient trapped in machinery at an industrial accident.

Immediate Peril is a serious end-user control and must be used judiciously. Training and procedures must be developed and consistently applied for its use.

TABLE 19. IMMEDIATE PERIL REQUIREMENTS

#	Requirement
50	Applications that have been selected by the end user to receive Immediate Peril priority SHOULD receive elevated, admission, and scheduling priority when the "Immediate Peril" capability is activated. *Note: it is understood this is an NPSBN PQoS policy decision; however, this requirement is provided to share the desired behavior from the user community.*
51	It SHALL be possible for an authenticated and authorized NPSBN user to initiate and clear the "Immediate Peril" capability for herself/himself.
52	When activating the "Immediate Peril" capability, it SHALL be possible for an authorized NPSBN user to designate one or more applications to receive elevated priority.
53	It SHALL be possible for an authenticated and authorized NPSBN user to initiate and clear the "Immediate Peril" capability for another NPSBN user. *Note: The PSAC is considering all issues associated with Identity, Credential, and Access Management (ICAM), including the use case of engaging an Immediate Peril without being signed in to the device.*
54	When the "Immediate Peril" capability is activated for a user, the user-selected application(s) SHALL receive Immediate Peril priority on all of the user's active devices
55	When the "Immediate Peril" capability is active for a user, a clear indication SHALL be present on all of the user's active devices. *Note 1: The intent of this requirement is to avoid a situation where a user forgets to clear an Immediate Peril condition. This requirement can be satisfied by visual indicators (such as a flashing icon) or audible indicators (such as a periodic beep) or other methods.* *Note 2: While a police officer may require a "silent" call for help when using Responder Emergency, it should be noted that Immediate Peril is not intended to support the officer's own safety condition and thus notifications may not have to be as subtle.*
56	It SHALL be possible for an authorized administrator to designate the notifications a user's User Entity receives when the "Immediate Peril" capability is activated. Notifications SHOULD include, but are not limited to: a) Operations terminal (e.g., maintenance terminal) alarm b) Application Programming Interface (API) callback operation
57	It SHALL be possible for the PQoS solution to generate Usage Records each time the Immediate Peril capability is activated and provide the Usage Records to authorized User Entity Administrators. *Note: Usage Records can be used for a variety of purposes, including training, charging, and operations review.*

5.3.2.5 RESPONDER EMERGENCY AND IMMEDIATE PERIL COMPARISON

Responder Emergency and Immediate Peril are the two main PQoS controls available to end users. It is important to understand these capabilities and especially note where they are different.

TABLE 20. RESPONDER EMERGENCY AND IMMEDIATE PERIL COMPARISON

Description	Responder Emergency	Immediate Peril
What is the service intended to do?	Used by the public safety user when there is an immediate danger to their life or property.	Used by the public safety user when there is an urgent need to access a particular broadband application that is being denied due to network congestion. The urgent need is tied to a threat to human life or property, but not necessarily the responder themselves.
Can an authorized NPSBN user activate the service to apply priority for her/his own devices?	Yes Example: Police Officer activates Responder Emergency after shots are fired.	Yes Example: EMS technician activates IP to prioritize a telemedicine session for a patient he is treating.
Can an authorized user (e.g., dispatcher, console operator) activate the service to apply priority to another NPSBN user's devices?	Yes Example: A remote video dispatcher sees a responder fall unconscious and activates RE for the downed user.	Yes Example: In congestion, the Incident Commander wants to view video from a firefighter's body-worn camera.
How do you activate the service? (examples only – user experience cited is not intended to be a device requirement)	Examples: • Responder in the field presses their broadband device's emergency button • Responder's health-monitoring system automatically activates R# when a responder is horizontal for 5 minutes	Examples: • A long-press of a Smart Phone application icon • Voice activation from Smart Device
How do you de-activate the service?	The user activating the service normally de-activates the service. Additionally, an authorized user (e.g., console operator) can deactivate the service.	The user activating the service normally de-activates the service. Additionally, an authorized user (e.g., console operator) can deactivate the service.
Who chooses the application(s) that receive priority?	An authorized administrator (User Entity Administrator or NPSBN Administrator on behalf of a User Entity) configures applications that receive RE priority for user's within the administrator's User Entity prior to any users entering the field. Example: The PSE administrator signs into the NPSBN P QoS solution and configures the applications that are used by her/his User Entity when RE is activated.	The user initiating Immediate Peril chooses the applications that receive priority. Example: a paramedic long-presses a telemedicine icon on their smart tablet.
What priority should the user get	Users have requested the highest	Users have indicated either a similar

when the service is activated?	priority available, but this is understood to be an NPSBN Administrator policy decision.	priority as RE or slightly lower, but still elevated from norm.
Is the feature mandatory (i.e., must every user have the capability)?	No. The User Entity Administrator can disable this feature based on User Entity policy.	No. The User Entity Administrator can disable this feature based on User Entity policy.

5.3.2.6 Incident Severity and Incident Role

The National Incident Management System (NIMS) includes the Incident Command System (ICS) (see section **Error! Reference source not found.** for an introduction). ICS is a nationwide standard which provides common language, organization, and procedures for addressing any type of incident. ICS is applied on a per-incident basis and may be used by a single User Entity or multiple agencies performing mutual aid. ICS is especially beneficial in addressing large, complicated incidents.

Once a responder is assigned to an incident and under ICS, she/he is given a role in an incident-specific "organizational chart" with a specific function and well-defined command and control. The responder's ICS role exists for at least a portion of the duration of the given incident. This new role (e.g., logistics) may be different than the day-to-day function of the responder (e.g., firefighter).

The NPSBN PQoS Framework must accommodate the usage of ICS. The NPSBN must prioritize the responder according to the responder's assigned incident role. This may alter the responder's default priority on the NPSBN.

In an effort to limit technology distractions to dispatchers and command staff, it is desirable that the act of assigning a responder to an incident role automatically adjust the responder's priority on the NPSBN. Similarly, when the incident is completed, the responder is expected to automatically return to her/his day-to-day default priority.

FEMA has defined a means to identify the complexity, size, and severity of an incident according to the following figure:

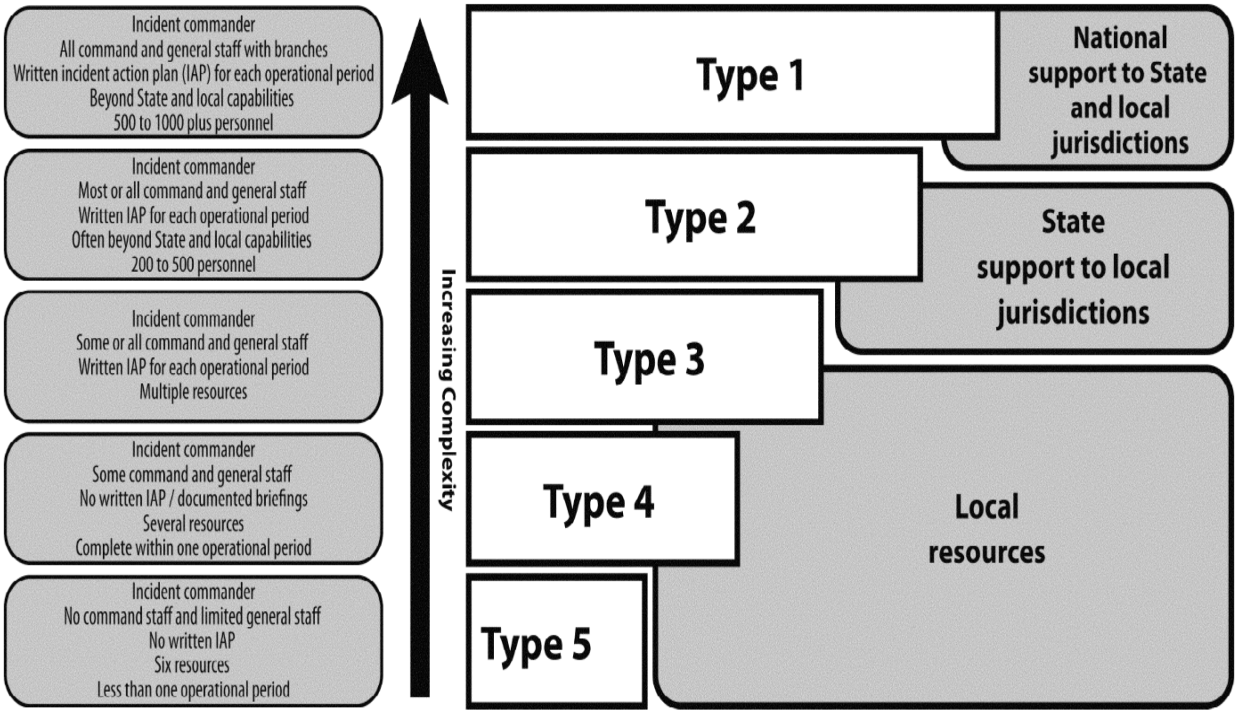

Incident commander
All command and general staff with branches
Written incident action plan (IAP) for each operational period
Beyond State and local capabilities
500 to 1000 plus personnel
Incident commander
Most or all command and general staff
Written IAP for each operational period
Often beyond State and local capabilities
200 to 500 personnel
Incident commander
Some or all command and general staff
Written IAP for each operational period
Multiple resources
Incident commander
Some command and general staff
No written IAP / documented briefings
Several resources
Complete within one operational period
Incident commander
No command staff and limited general staff
No written IAP
Six resources
Less than one operational period
Increasing Complexity
Type 1
Type 2
Type 3
Type 4
Type 5
National support to State and local jurisdictions
State support to local jurisdictions
Local resources

FIGURE 6. INCIDENT SEVERITIES

Type 5 incidents are the least complex and typically involve six or fewer responders. Examples include a police traffic stop, vehicle fire, or an injured person. Command staff (other than the Incident Commander) are not activated for a type 5 incident.

Figure 7 shows an example of a FEMA Type 4 incident.

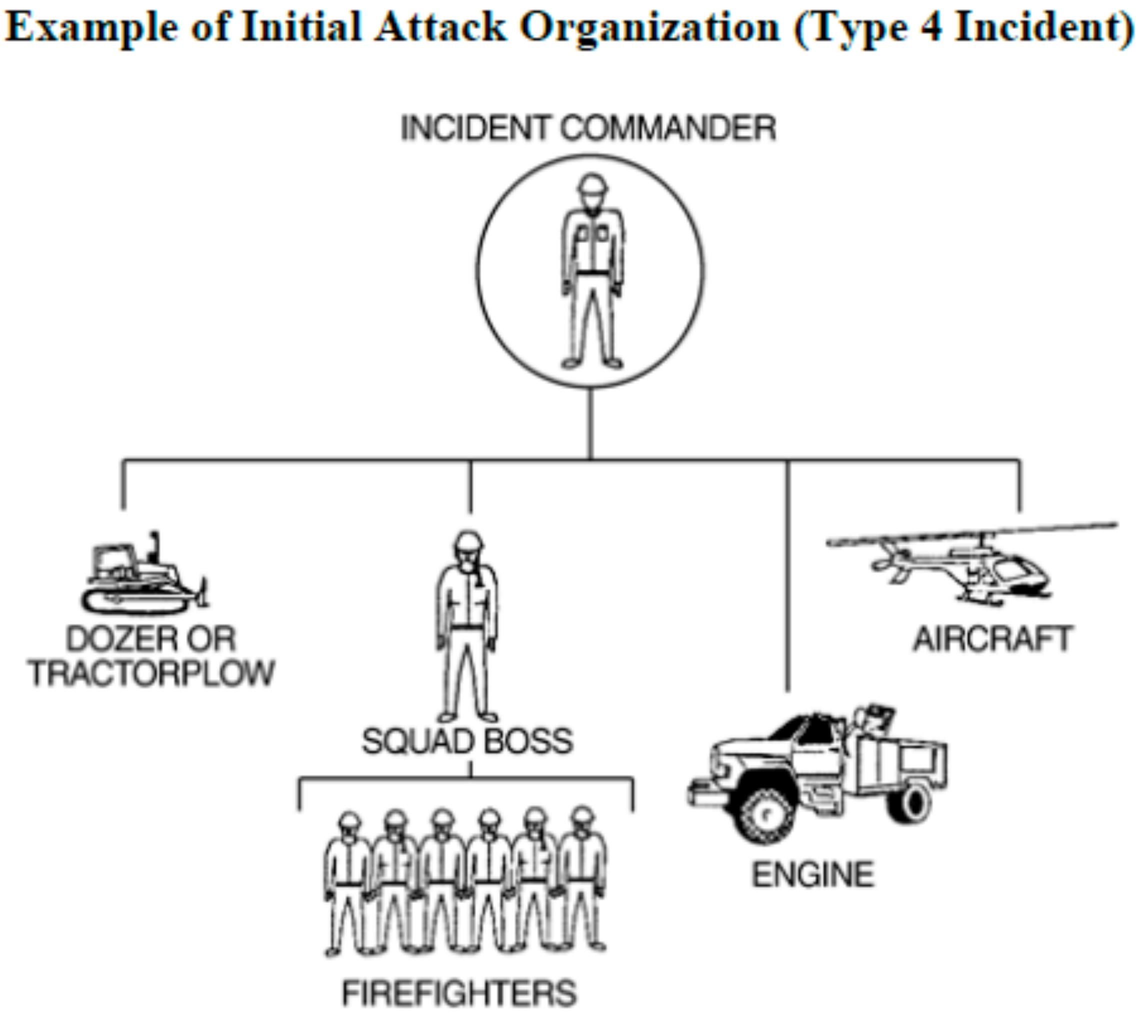


FIGURE 7. FEMA TYPE 4 (SMALL) INCIDENT

Type 1 incidents are the most complex, often involving 500 or more responders and federal support. All command positions are filled and activated. Figure 8 shows an example organizational template that is utilized for this type of incident:

Organization Chart for Type 1 and Type 2 Incidents

Remember: Fill only those positions needed.

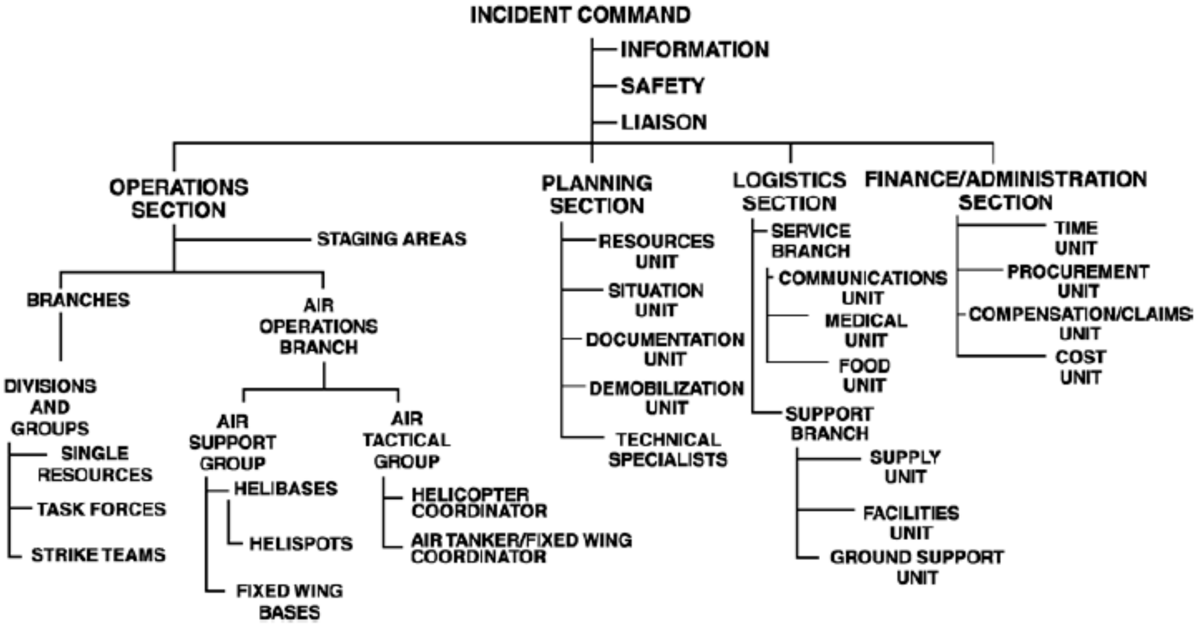


FIGURE 8. FEMA TYPE 1 (MOST COMPLEX) INCIDENT

The “Incident Severity” dynamic priority attribute is used to first differentiate the presence of an incident from normal operations. For example, a traffic stop would receive elevated priority when compared to a responder on patrol. Next, this attribute is used to differentiate the severity of different incidents themselves. For example, a FEMA Type 3 incident would typically receive higher priority than a FEMA Type 5 incident. It should be noted that incident size may influence whether or not FEMA types are used in incident classification. For smaller agencies, the CAD’s incident classification may be used instead.

Within a given incident, certain roles may be of higher relative priority than other roles. The “Incident Role” attribute is used to identify roles within the incident that have additional emphasis. For example, communications between Incident Command and Section Chiefs should receive elevated priority. Additionally, the Operations Section is typically the group of responders performing highly tactical real-time functions (i.e., the critical “boots on the ground”). It may be necessary to segregate the users in the operations section from other sections of the ICS structure, such as planning, logistics, and administration to provide the correct PQoS experience. Information regarding these assignments may come from the Incident Action Plan instead of the CAD system.

TABLE 21. INCIDENT SEVERITY AND INCIDENT ROLE REQUIREMENTS

#	Requirement
58	It SHALL be possible for an authorized NPSBN user, who is utilizing an authorized NPSBN application (e.g., CAD dispatcher, incident commander, etc.) to identify the following information and make that information available to the NPSBN PQoS solution: a) A new incident has been created, b) The type of the incident c) The severity of the incident d) Authorized NPSBN users assigned to the incident and the user's assigned incident role
59	The NPSBN PQoS solution SHALL provide an open interface to allow an authorized application to provide "Incident Severity" and "Incident Role" information.
60	It SHALL be possible for the NPSBN PQoS solution to adjust a user's PQoS experience based on the user's associated "Incident Severity" and "Incident Role."

5.3.2.7 APPLICATION INFLUENCE

The "Application Influence" attribute is a specific control provided to applications in order to differentiate priority within the application itself. For example, scan PTT calls (i.e., listening in on one or more group channels for situational awareness) are typically treated with lower priority than active PTT groups (i.e., groups where the user is an active PTT communicator) within the push-to-talk application.

TABLE 22. APPLICATION INFLUENCE REQUIREMENTS

#	Requirement
61	The NPSBN PQoS solution SHALL provide an open interface to allow an authorized application to provide "Application Influence" information.
62	It SHALL be possible for the NPSBN PQoS solution to adjust a user's priority and QoS experience based on the "Application Influence" information provided by an authorized application the user is currently using.

5.3.2.8 ADMINISTERING DYNAMIC PRIORITY

Users and administrators should not be encumbered with LTE prioritization details and prioritization methods, especially during time-sensitive incidents. The Working Group envisions dynamic priority changes occurring as part of the user's (or administrator's) normal activities. For example, rather than an Incident Commander having to directly program LTE admission priority, it may be adjusted automatically by a dispatch application assigning a responder to an incident (see "Incident Severity" and "Incident Role"). This means responders and administrators must have the ability, using an authorized application, to trigger dynamic priority changes, without being bothered by the exact details of the LTE technology. Authorized applications can be numerous, but are envisioned to include mission critical push-to-talk (MC-PTT), computer-aided dispatch (CAD), incident command application(s), mobile applications, and others. These applications are anticipated to interface to the NPSBN PQoS solution and provide a request (i.e., automatically signal to the PQoS solution) for the activation of dynamic priority capabilities, and these applications would hide LTE technology details.

Further, the exact dynamic priority attributes that are used must comply with the nationwide framework (i.e., a user cannot choose their own dynamic priority in the system). The criteria used to compute a user's dynamic priority is defined in section 5.3.2.

Generally, the entity requiring dynamic priority is the entity that must be allowed to trigger dynamic priority. This provides for the most prompt and expedient service to public safety. It is not desirable to call a central authority and provide device identifiers over the phone to adjust priority. This is both error prone and slow.

TABLE 23. ADMINISTERING DYNAMIC PRIORITY REQUIREMENTS

#	Requirement
63	User dynamic priority attributes SHALL automatically be provided to the NPSBN PQoS solution by applications. *Note: it is envisioned existing public safety applications can be enhanced to transparently and automatically provide dynamic priority attributes to the NPSBN PQoS solution. Examples:* • *User Location – Device application, LTE system* • *Operational Status – Workforce management application, CAD application* • *Responder Emergency, Immediate Peril – Device application, dispatch application* • *Incident Severity, Incident Role – Dispatch application, incident command application* • *Application Influence – Authorized application, such as PTT* *Public safety users should not have to directly interface with LTE-specific controls.*
64	The NPSBN PQoS solution SHALL supply an open interface to applications for the purpose of transmitting dynamic priority attribute values to the NPSBN PQoS solution.
65	A set of administrative procedures SHOULD be established for the purpose of ensuring consistency between user entities utilizing dynamic priority.

5.4 Group Priority Model

In addition to priority being associated with a user, certain applications provide the concept of a group. For the purposes of this document, a group is considered an association of two or more users sharing a common application. For example, LMR systems today associate priority of push-to-talk with a particular talk group. Thus, all users involved in the same group share a common group priority for the given application. This behavior must be supported on broadband as well, especially for broadband mission critical push-to-talk. As an example, police can be assigned to a SWAT group and that group needs to have the same priority when utilizing tactical data communication (e.g., building maps). Interoperability would be hindered if some of the SWAT users had different priorities than other members of the same voice SWAT group.

An LTE group can be constructed using:

- **Unicast resources** – These are uplink and downlink resources to/from the Application from/to a device. NPSBN PQoS policy may allow all unicast resources for a given group application to be aggregated together and treated with similar Admission and Scheduling Priority.

- **Broadcast resources** – LTE provides a downlink point-to-multipoint capability (i.e., single resource to distribute simultaneously to multiple receiving devices). Unicast uplink (device to infrastructure) resources are still required for each device. NPSBN PQoS policy may allow all unicast uplink and broadcast downlink resources for a given group application to be aggregated together and treated with similar admission and scheduling priority.

In LTE, each of these resources may be prioritized independently. This means it is possible to construct a group of two members with two unicast resources that are prioritized differently. In itself, this can cause a problem. If one of the responders has a substantially lower priority in the LTE system, it can reduce the probability the call or session will go through (because, for example, only one of the two responders acquires resources).

Figure 9 shows the group priority model, which is very similar to the user priority model:

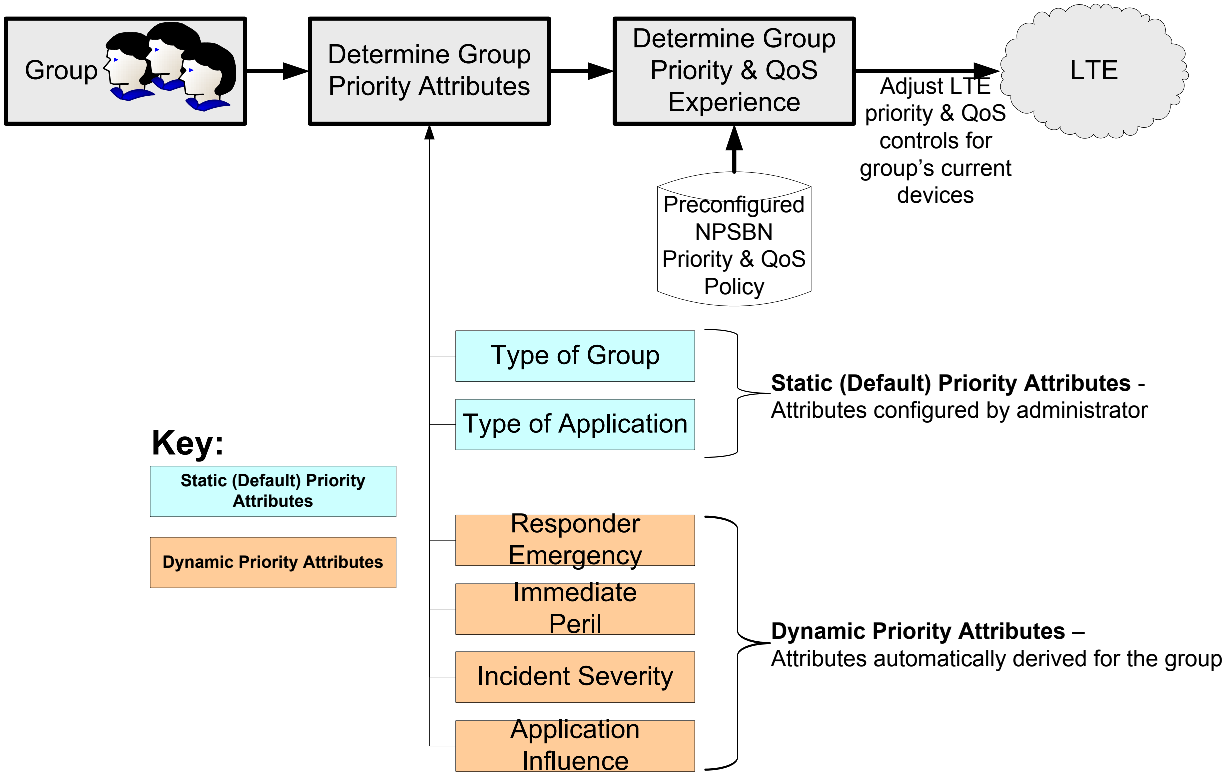

Group
Determine Group Priority Attributes
Determine Group Priority & QoS Experience
LTE
Adjust LTE priority & QoS controls for group's current devices
Preconfigured NPSBN Priority & QoS Policy
Type of Group
Type of Application
Static (Default) Priority Attributes - Attributes configured by administrator
Key:
Static (Default) Priority Attributes
Dynamic Priority Attributes
Responder Emergency
Immediate Peril
Incident Severity
Application Influence
Dynamic Priority Attributes – Attributes automatically derived for the group

FIGURE 9. GROUP PRIORITY MODEL

One notable difference between the user and group priority models is the change of "Type of User" to "Type of Group." Essentially, this priority attempts to stratify the group as predominantly serving different classes of user (e.g., first responder group, secondary user group, commercial user group). It is understood a first responder group may contain secondary users or other users as need dictates.

TABLE 24. GROUP PRIORITY MODEL REQUIREMENTS

#	Requirement
66	It SHALL be possible for an authorized administrator to designate an application as a group application.
67	It SHALL be possible for an authorized administrator to configure the following information for a group: • Type of Group • Type of Application
68	For a given group application, it SHALL be possible for a change in a group priority attribute to alter the PQoS experience for all NPSBN users associated with the group.
69	If a User Entity has designated a group application to be included in the list of applications used for the Responder Emergency capability, all users associated with the group will receive emergency priority when the capability is activated. *Note: This allows, for example, resources associated with a sending user and receiving user(s) to all receive priority. If only the originating user were prioritized, the priority of a session (e.g.,, call) completing is not necessarily improved. For example, an agency may have pre-configured a group health-reporting application to be used when a responder activates the Responder Emergency capability. This would allow all users in a rapid response group to receive health information for the user that activated Responder Emergency.*
70	If a user has activated the Immediate Peril capability for a given group application, all members of the group will receive Immediate Peril priority. *Note: Because mission critical voice is deemed the highest priority application (by default), this capability is most useful for group video or group data applications. For example, a SWAT team requiring tactical priority to view a real-time video feed to coordinate a response would use this capability.*
71	It SHALL be possible for the NPSBN PQoS solution to utilize LTE controls to prioritize groups consisting of 1:1 (unicast) and 1:N (broadcast) resources.

5.5 NPSBN PQoS Policy

Working with state and local agencies, the NPSBN Administrator defines common policies for managing PQoS functions and features. As described in section 5.3, NPSBN PQoS policy maps user and group priority attributes to specific LTE PQoS controls. When a user or group priority attribute changes, it can result in the change of one or more specific LTE PQoS controls.

- NPSBN policies provide a common implementation allowing users from all jurisdictions to operate efficiently on the same network.

- NPSBN policies should be relatively consistent across the U.S. in order to maximize operability and interoperability; and to ensure ***consistent behavior*.**

- Standardized consistency in priority assignments between adjoining jurisdictions is critical to ensure effective use of the network.

- NPSBN policies and functionality must provide a ***consistent*** and ***reliable*** user experience for public safety entities. This includes a common system for prioritizing voice, data and video applications among all users.

- NPSBN policies must be sufficiently ***flexible*** to meet local User Entity operational needs while also managing large scale incidents requiring multiple agencies.

- Priority determination made as a result of NPSBN policies should be automated and integrated with work-flow practices.

  - It is very difficult to make manual changes to LTE PQoS settings in real time.

  - Responders should not have to request priority; the system should understand what the responder is doing and automatically obtain the correct priority for the user.

  - The responder's attention cannot be pulled away from the mission to manage the technology.

It is anticipated that the NPSBN Administrator (with appropriate public safety user consultation) will define, configure, and manage these policies and the policies will generally be consistent across the entire NPSBN. It is highly desired that these policies be pre-configured into the PQoS solution so they can automatically be utilized by NPSBN users and groups. The Working Group strongly discourages the manual management of LTE priorities (i.e., by a human) because this can be slow or inaccurate (i.e., it is extremely difficult for one human to understand all the incidents taking place from all agencies in a single LTE cell).

If each User Entity were to define their own PQoS policies, it would likely hamper interoperability and operability. Consider the case when two agencies need to interoperate, and one User Entity prioritizes PTT while another User Entity prioritizes video. In the presence of congestion, the two agencies may not be able to easily communicate!

Table 25 defines which priority attributes can be used to influence access, admission, and scheduling policies.

TABLE 25. APPLICABILITY OF PRIORITY ATTRIBUTES TO EACH PRIORITY GATE

Priority Attribute	Influences Access Priority (Gate 1)?	Influences Admission Priority (Gate 2)?	Influences Scheduling Priority (Gate 3)?
U1: Type of User	Yes	Yes	Yes
U2: Type of Application	Yes	Yes	Yes
U3: Default Role	Yes	Yes	Yes
U4: User Location	Yes[6]	Yes	Yes
U5: Operational Status	Yes[6]	Yes	Yes
U6: Responder Emergency	Yes	Yes	Yes
U7: Immediate Peril	Yes	Yes	Yes
U8: Incident Severity	Yes[6]	Yes	Yes
U9: Incident Role	Yes[6]	Yes	Yes
U10: Application Influence	Yes[6]	Yes	Yes

TABLE 26. NPSBN PQOS POLICY REQUIREMENTS

#	Requirement
72	It SHALL be possible for an authorized NPSBN Administrator to pre-configure PQoS policy. This policy maps user and group priority attribute values to specific LTE access, admission, and scheduling controls.
73	It SHALL be possible for a user's device to be assigned priority attributes and for those priority attributes to result in the selection of Access Classes used by the device.

5.6 Preemption and Preemptability

Preemption refers to the immediate removal of resources, often without warning to the responder themselves. As of this writing, U.S. public carriers do not generally support preemption. Preemption is also avoided by most LMR system operators today. Instead, talk groups are prioritized and, at worst, responders experience an increased queuing delay during system access. The environment of the NPSBN is fundamentally different than that of public

[6] The intent of this table is to capture user need. It is understood that from the perspective of the device (user equipment) that the referenced attributes will likely not be available for Access Priority because the device is not yet communicating with the NPSBN. Presumably, static priority attributes can be downloaded to the device after a successful user sign on at the start of a shift (i.e., before the device lost communication with the NPSBN).

carriers and existing LMR systems. Unlike LMR, all applications share a single set of NPSBN resources. This means high bandwidth video applications and mission critical voice utilize the same set of resources.

Section 5.3 describes a series of default and dynamic attributes that are used by the NPSBN PQoS solution to automatically compute a user's priority. Ultimately, this user priority is associated with the user's devices and device resources. In LTE, device resources are associated with an Allocation and Retention Priority, ARP, and it contains a number from 1-15 with 1=highest priority. The user's ARP priority is not only used during Admission Priority (Gate 2), it is also used during the preemption process. Should a new responder resource request take place in the presence of congestion and have a higher ARP than an existing resource's ARP and assuming preemption is enabled, the existing resource will be discontinued (preempted).

Preemption on the NPSBN is required in order to:

- Preserve responder health and the lives of the public
- Insure all responders can operate and interoperate minimally through mission critical voice
- Satisfy the dynamic application needs of the incident (e.g., Is video required to save a life?)

The Working Group has identified the ordered preemption behaviors that should be seen as congestion increases on a particular NPSBN cell. These behaviors are captured in Table 27 below. Preemption must allow for open access to assure a top-priority application from a top priority user can be discerned; i.e., the emergency button.

In general, the Working Group has indicated that:

- Mission critical voice applications should not be pre-empted
- Applications associated with active Responder Emergency and Immediate Peril sessions should not be pre-empted

It should be noted that the requirements in Table 27 are intended to provide general guidance regarding preemption. The table is not intended to restrict usage of the system. For example, a low-priority user should be allowed to utilize a high-priority application if needed (See especially group priority in section 5.4).

TABLE 27. PREEMPTION AND PREEMTABILITY REQUIREMENTS

#	Requirement
74	Should congestion develop at an LTE cell, the following preemption behaviors SHALL be performed (in order): a) User non-GBR traffic should slow down based on user/application priority b) Preemption of low-priority applications of low-priority users c) Preemption of low-priority applications of higher priority users d) Preemption of low-priority users e) Preemption of higher priority users
75	The following authorized applications (NPSBN-provided or User Entity-provided) SHALL NOT be pre-empted: • Mission critical voice applications • Applications used during active Responder Emergency or Immediate Peril sessions.

5.7 Rate Limiting and Bandwidth Management

Rate limiting and bandwidth management provide public safety with the ability to control the amount of over-the-air resources that are made available to a given responder. Technical details of LTE's standard capabilities may be found in Appendix A.

Under normal circumstances, the amount of bandwidth that is available to a responder can be pre-configured into the NPSBN. When configuring a new device for use with the NPSBN, the User Entity must have the option to limit the maximum bit-rate for general data services (such as using the Internet/Intranet). This will prevent a single responder from dominating non-GBR resources at an eNB. Policies and profiles must be created to consistently apply rate limits per-user across the entire NPSBN. This allows general data usage (i.e., non-GBR traffic) to be fairly balanced for all NPSBN users and their associated devices. In the presence of congestion, the NPSBN must further provide a guaranteed minimum bandwidth for a device's non-GBR traffic (in order to prevent starvation).

When configuring a new streaming voice or video application for use with the NPSBN, the minimum and maximum bandwidth needs of the application are usually well-known (e.g., codec bandwidth needs). Real-time voice and video applications typically require dedicated NPSBN resources. Therefore, agencies must have the ability to configure application minimum and maximum bandwidth needs when commissioning new applications for use on the NPSBN.

Because of the high complexity involved, the Working Group has determined that real-time adjustment of NPSBN bandwidth controls should be strongly avoided for both devices and applications. The Working Group also noted that use cases could not be identified which require this capability.

TABLE 28. RATE LIMITING AND BANDWIDTH MANAGEMENT REQUIREMENTS

#	Requirement
76	The NPSBN administrator SHALL provide policies and profiles to consistently apply rate limiting for all NPSBN users.
77	User Entity administrators SHALL have the capability to select a rate limiting profile for a user's general data services (such as using the Internet/Intranet).
78	It SHALL be possible for an Authorized administrator to configure the PQoS solution with the guaranteed minimum bandwidth for an application.
79	When commissioning a new User Entity application, the User Entity administrator SHALL have the ability to specify the minimum and maximum bandwidth needs for the application.

5.8 Backhaul and Transport Priority

In order to provide consistent end-to-end treatment of public safety traffic, prioritization of NPSBN resources must be provided both over the air as well as within the network infrastructure. Backhaul and IP network priorities must be aligned to match the priority of over-the-air resources (i.e., the priority derived by the NPSBN PQoS solution). The IP transport that is used to carry public safety user traffic between the NPSBN infrastructure elements must be configured in a manner consistent with the assigned scheduling priority (section 5.2.3) of the NPSBN resource. This means a consistent mapping between NPSBN-assigned priority and transport/backhaul priority must be devised. Further, this mapping must be consistently applied to the entire NPSBN (nationwide system). This document does not attempt to require a specific mapping of NPSBN priority to the myriad of backhaul and IP technologies available; however, an illustrative example is provided in Appendix 0.

Failure to align NPSBN scheduling priority with IP network/backhaul priority will significantly reduce the quality of the end user's experience. For example, voice and video may be choppy (excessive packet loss or delay) or entire sessions may be lost.

TABLE 29. BACKHAUL AND TRANSPORT PRIORITY REQUIREMENTS

#	Requirement
80	NPSBN backhaul and transport network priorities SHALL be aligned with NPSBN PQoS solution scheduling priorities.

5.9 NPSBN User Roaming

Users provisioned on (i.e., home to) the NPBSN can, subject to roaming arrangements constructed by the NPSBN Administrator, roam to other LTE systems (such as commercial carriers). In this case, the commercial carrier may control prioritization when the NPSBN's device utilizes commercial spectrum. NPSBN negotiations with the commercial carriers will ultimately determine the treatment received by NPSBN users.

Even though a commercial carrier may constrain the exact LTE controls available to NPBSN users, it is still highly desirable to support user and group priority attributes. That is, the NPSBN Administrator should still be able to determine the relative priority of users and groups, even when the user is roaming on a commercial system.

Note 1: Roaming in to NPSBN spectrum by non-NPSBN users is out-of-scope of this document.

Note 2: The requirements in Table 30 *are subject to business negotiation between the NPSBN and commercial operators.*

TABLE 30. NPSBN USER ROAMING

#	Requirement
81	When an NPSBN user roams from the NPSBN system to a commercial system, it SHOULD be possible for the NPSBN PQoS solution to identify the relative priority of the user to the commercial system.
82	In general, primary NPSBN users SHOULD receive higher default priority than commercial users on the commercial system.
83	It SHOULD be possible for NPSBN PQoS solution to support default and dynamic priority for NPSBN users who have roamed to a commercial system. *Note: The intent of this requirement is for a user's dynamic priority capabilities (e.g., Responder Emergency) to be available while roaming.*

5.10 NPSBN PQoS for Deployables

This section is constructed in collaboration between the NPSTC Broadband Deployable Systems Working Group (BBDSWG) and PQoS Working Groups. The BBDS WG has considered a variety of use cases and this section has been constructed to provide PQoS guidance for those use cases. It should be noted that the BBDS WG is considering numerous RF technologies (not just LTE) to meet the needs of the user community.

Deployables are regularly utilized to extend existing fixed network coverage or provide coverage where none exists. As used herein, the term 'deployable' is used to include both of these scenarios. Wide Area Network (WAN)-connected deployables have an ability to communicate with the fixed NPSBN core network (often with wireless backhaul) and as a result require less configuration and maintenance. There is no need to replicate user database and policy information in the WAN-connected deployable because the deployable can utilize the databases of the wide-area NPSBN system. Conversely, a WAN-disconnected deployable does not have communication with the fixed NPSBN core network and thus must provide its own databases and policies.

NPSBN broadband deployables will utilize at least a portion of the NPSBN licensed spectrum to provide coverage for user devices. Like the nationwide fixed NPSBN, a deployable will support many different types of users (e.g., police, fire, EMS, and possibly other users). The exact type of users authorized to use a particular deployable is out of scope.

WAN-disconnected deployables bring coverage where none exists (e.g., for wildfires in the Western U.S. or for hurricane destruction in Florida). In this case, the deployable can be thought of as a self-contained LTE system. This type of deployable requires the LTE site (eNodeB), core network, and applications to be brought to the incident scene. Like the fixed NPSBN network, the Working Groups believe PQoS is required for a WAN-disconnected deployable. PQoS policies between the fixed NPSBN system and the deployable must be kept as consistent as possible in order to avoid a confusing user experience. Exact methods to achieve this, whether automatic or manual, are out of scope of this document. For example, a deployable system that prioritizes applications differently from the fixed NPSBN system can hinder interoperability and confuse users.

WAN-connected deployables can extend coverage or enhance the bandwidth provided by the fixed NPSBN and these deployables utilize priority and QoS policy information from the fixed NPSBN. As such, policies defined for the fixed NPSBN must include support for WAN-connected deployables.

Large incident scenes may require multiple deployables. In some cases, the deployables may have overlapping RF coverage. The Working Groups believe that all deployables at an incident scene must be capable of dynamically integrating to form a single broadband network, called a deployable cluster. Devices should be able to handover from one deployable to another and retain their PQoS experience.

PQoS for multi-national operations (e.g., along the Canada-U.S. border) are out of scope of this document.[7]

[7] As of this writing a bi-national task group is investigating the use cases for this scenario, including multi-national mutual aid.

TABLE 31. NPSBN PRIORITY & QOS FOR DEPLOYABLES REQUIREMENTS

#	Requirement
84	It SHALL be possible to apply the NPSBN PQoS solution to support a deployable system with no connection to the fixed NPSBN (i.e., support for "WAN-disconnected" deployables).
85	It SHALL be possible to apply NPSBN PQoS solution to support a deployable system with a wide-area connection to the fixed NPSBN (i.e., support for "WAN-connected" deployables).
86	It SHALL be possible for a deployable system to operate with the same NPSBN PQoS Policies as the wide-area NPSBN system. *Note: Exact methods to synchronize polices with the fixed NPSBN is out of scope, however automatic synchronization is desired.*
87	Emergency responders from different jurisdictions SHALL be able to authenticate on a deployable system.
88	It SHALL be possible for a deployable system to prioritize users from multiple NPSBN agencies and disciplines.
89	It SHALL be possible for a deployable system to support access, admission, and scheduling priority.
90	It SHALL be possible for a deployable system to support dynamic PQoS capabilities (see section 5.3.2).
91	It SHALL be possible for multiple independent deployable systems to come together, form a single interoperable cluster, and automatically create a PQoS experience consistent with the fixed NPSBN experience. *Note: PQoS must apply consistently to the LTE air interface, but also all interconnecting transport equipment (e.g., switches, routers, etc.).*
92	It SHALL be possible to prioritize user transport resources for deployable system interconnecting links (e.g., microwave) according to the scheduling priority (e.g., QCI) specified by the NPSBN PQoS solution.
93	It SHALL be possible for an authorized user (e.g., COML) to monitor deployable system load. *Note: the Deployables Working Group is recommending that human interaction with a deployable system be minimized, although manual controls are still desired, if needed.*
94	It SHALL be possible to support handoffs of an active user session, while maintaining user priority, from one deployable system to another deployable system. *Note: The Deployables Working Group is investigating multi-technology handover (e.g., In-building WiFi to NPSBN LTE).*
95	Resources (bearer sessions and their associated PQoS) SHALL be persistent during hand-offs from one deployable system to the other.
96	It SHALL be possible to support handoffs of an active user session, while maintaining user

	priority, from the fixed NPSBN and a WAN-connected deployable.

5.11 Inter-Network Interoperability

End-to-End PQoS Use Cases 2.20 – 2.21 describe scenarios where end-to-end priority and quality of service between the NPSBN, interconnected commercial networks, and PSEN) are essential to successfully distribute information and to mobilize and manage public safety resources. When the NPSBN, commercial networks, and/or PSENs are congested, the probability of a communication completing is diminished. It is therefore essential that when responders are simultaneously operating on the NPSBN, commercial networks, and PSENs (or other private networks), that communications "out of" and "in to" the NPSBN are able to send and receive a priority indication to engage end to end prioritization capabilities. A "communication," for the purposes of this section, should be considered any media (session based or otherwise) that must pass between users.

TABLE 32. INTER-NETWORK INTEROPERABILITY REQUIREMENTS

#	Requirement
97	NPSBN users operating on the NPSBN, when attempting to communicate with devices operating on other networks, SHALL be able to convey end-to-end priority needs to the interconnected IP-based system(s) in order to increase the probability of completing communications during periods of network congestion or impairment.
98	When an NPSBN user receives an incoming call from outside the NPSBN flagged with an appropriate priority message header, it SHALL be possible for the originating IP-based system to convey end to end priority needs to the NPSBN in order to increase the probability of completing communications during periods of network congestion or impairment. This is meant to include interconnected public safety, commercial, satellite, and other IP-based networks.

5.12 Priority and QoS Model Examples

5.12.1 Responder Emergency Activation

Use case: An officer is disabled and his automatic health monitoring system detects his condition and activates Responder Emergency through the officer's broadband device.

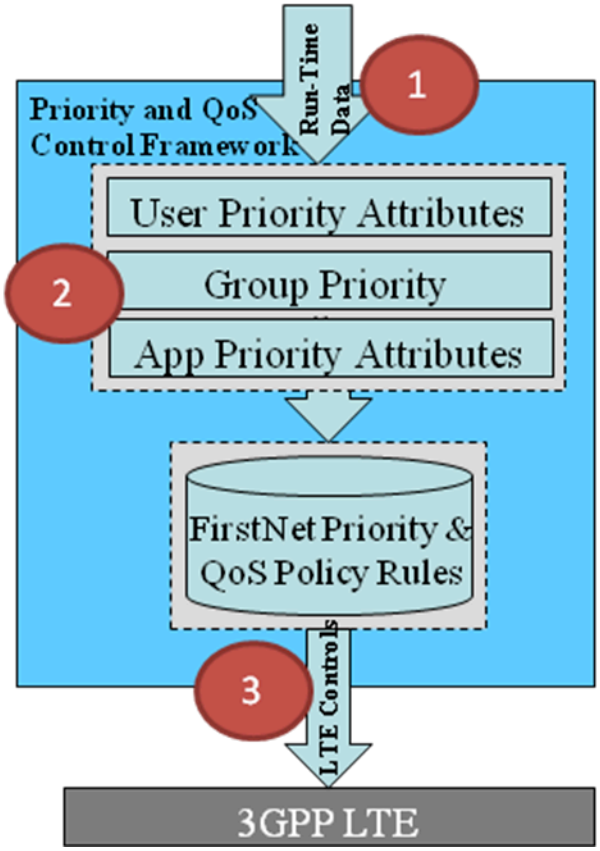


FIGURE 10. RESPONDER EMERGENCY EXAMPLE

1. The NPSBN PQoS solution is notified in real time of a priority attribute value change and initiates a policy check
2. Priority Attribute Values
   - U1 – Type of user = "Primary User"
   - U2 – Type of Application shall be in list of user's User Entity predefined applications for responder emergency
   - U6 – Responder Emergency = "Enabled"
   - Other priority attributes – Value has no impact on result
3. Resulting LTE PQoS Attributes that are provided to LTE system by the NPSBN PQoS Solution
   - Access priority
     - No Change, defaults static value is still applied
   - Admission Priority
     - ARP=1 (Highest)

- Preemption Capability: True (Emergency applications can get resources from pre-empting other applications)
- Preemption Vulnerability: False (These applications cannot be pre-empted)

– Scheduling Priority

- QCI = appropriate value based on "Type of Application" attribute value,
  for example "65 = Mission Critical user plane Push To Talk voice" for PTT application and "70 = Mission Critical Data" for health monitoring application.

5.12.2 Push-to-Talk Call

Use case: A multi-vehicle car crash during a snowstorm has involved more than 40 vehicles. An EMS technician on-site, attempts to initiate a PTT voice session with his home hospital.

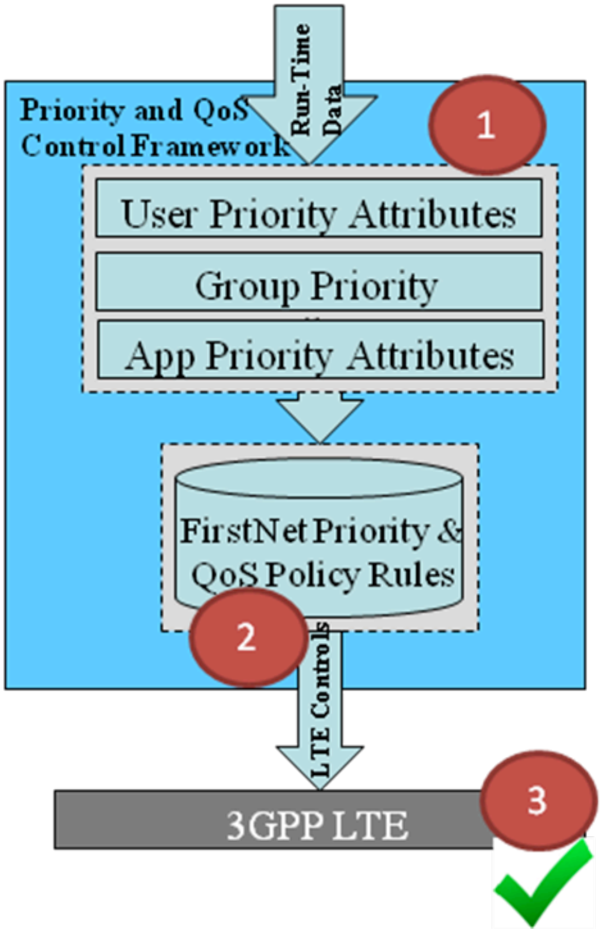


FIGURE 11. PUSH-TO-TALK CALL EXAMPLE

1. EMS technician attempts to start a new PTT session on his device

– U1 – Type of user = "Primary User"

– U2 – Type of Application = "Mission Critical Voice "

- U3 – Default Role = “Technician”
- U4 - User Location = “In-Jurisdiction”
- U5 - Operational Status = “On-Duty”
- U6 - Responder Emergency = “Disabled”
- U7 - Immediate Peril = “Disabled”
- U8 - Incident Severity = “None”
- U9 - Incident Role = “None”

2. Resulting LTE Priority and QoS Attributes that are provided to LTE system
    - Access priority
        - No Change, defaults static value is still applied
    - Admission Priority
        - ARP=6
        - Preemption Capability: true (this application can pre-empt other applications to get resources)
        - Preemption Vulnerability: false (this application cannot be pre-empted by another application)
    - Scheduling Priority
        - QCI = 65 (“Mission Critical user plane Push To Talk voice ”)
3. The NPSBN system is congested and recognizes that EMS technician has higher priority. Admission control process allows resources to be allocated for the PTT session. The call goes through.

6 System Administration

6.1 Context and Overview

There are a number of system administration tasks needed for the configuration and operations of PQoS. This section describes the context for these tasks. The section is focused only on PQoS and does not cover administration of other system attributes.

On a very general level, system administration can be seen as a task performed by an actor (i.e., administrator) changing or viewing an attribute of a specific system entity or a group of system entities. An example of an attribute in the PQoS context may be the default role of a user or the relative priority of an application.

This section describes in further detail who these actors are and a base data model for the PQoS related data attributes. Requirements in subsequent sections are formulated using this terminology. The requirements are divided into four main areas:

1. Administration of attributes associated with the overall PQoS system or PQoS system entities common to multiple users (e.g., an application or a PSE), often part of a provisioning process

2. Administration of attributes associated with an individual user, including day-to-day (aka., static) attributes, often part of a provisioning process

3. Administration of attributes associated with dynamic conditions, often part of an incident response process

4. Administration of attributes associated with the usage of the PQoS system, including charging records

The PQoS system administration functions may be performed by many different types of individuals. For the purposes of this document they can fall into one of the following administrator roles:

1. Public Safety Entity (PSE) Administrator

   The PSE administrator is responsible for administration of PSE-related system entities, e.g., applications, PSE user groups, PSE users, and PSE devices. The PSE administrator manages all static aspects of the PQoS system on behalf of the PSE. It is envisioned the PSE administrator leverages dedicated system administration tools to perform the PQoS administrative functions.

2. Public Safety Entity(PSE) Dispatcher

   The PSE dispatcher is responsible for assigning NPSBN users to incidents. As a part of this assignment certain PQoS attributes may be set for the incident as well as user groups and users assigned to the incident on a dynamic basis for the duration of the incident. The PSE dispatcher role is not expected to include system administration functions.

3. NPSBN PQoS Administrator

   The NPSBN administrator is responsible for the administration of NPSBN. This role could be subdivided into further specialist roles which are beyond the scope of this document. NPSBN-scoped PQoS attributes are those which are common across PSEs. These attributes provide a structured framework for the relative priority values which can be asserted into the NPSBN.

4. Commercial Mobile Network Operator (MNO) Administrator

   The MNO administrator is responsible for administration of commercial users accessing NPSBN and for commercial networks accessed by an NPSBN user.

There are many components of the PQoS system which are identified below:

1. User
   a. Public safety user also called NPSBN–user. This is often a human user subject to ICAM processes but could also encompass machine type users (e.g., a sensor)
2. Subscription
   a. FirstNet public safety subscription
   b. Commercial mobile network operator (MNO) provider (CLA partner) subscription (aka commercial user)
3. UICC (Subscriber Identity Module, e.g., SIM Card)
   a. Portable
   b. Embedded
   c. Software defined (e.g., eSIM)
4. Device (UE)
   a. FirstNet device (includes handheld and vehicle modem form factors)
   b. Commercial mobile network operator (MNO) provider device
   c. Public safety entity device - "BYOD"
5. Application
   a. Client on device
   b. Server in NPSBN or PSE network
6. PQoS
   a. PQoS configuration data
   b. PQoS processing function
7. User Groups, e.g., talk groups
   a. PSE static groups
   b. Incident dynamic groups
8. Public Safety Entity (PSE)
9. Nationwide Public Safety Broadband Network (NPSBN)
10. Commercial Public Mobile Network

PQoS attributes associated with these system entities are described in section 5.

It is recognized that PQoS administration may be an integral part of other administration activities and not necessarily a separate activity. As an example, provisioning a user's default PQoS attributes may be part of the overall user provisioning process. Such process linkages are however outside the scope of this document and not further defined.

The system administration may be performed by several individuals where each individual administrator has a specific administrative authority. The administration of the administrative users including their administrative authority are considered to be outside the scope of this document.

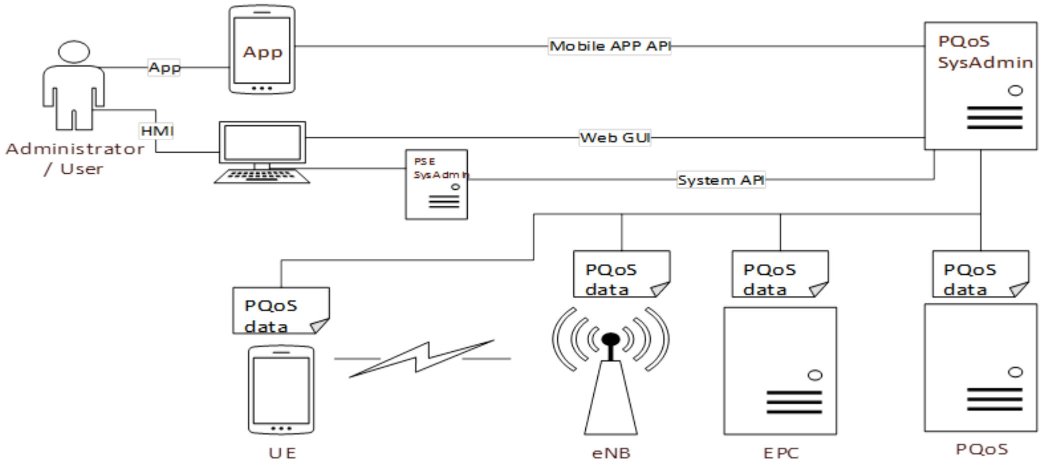


FIGURE 12. PRIORITY AND QOS SYSTEM ADMINISTRATION

6.2 User's PQoS Profile Configuration

"User profiles will be used to configure devices and will include a number of PQoS attributes and settings. In addition to defining default priority values, the profile will also provide instructions to the device on how certain PQoS features will behave. This includes the programming for Responder Emergency activation."

Law enforcement agencies may configure their Responder Emergency application to trigger a different set of applications than a fire department or EMS agency.

It is anticipated that manual intervention is the last resort, based on the risk of creating unintended disruption to the network. Following are assumptions related to manually configuring the PQoS profile for users:

- A sufficient number of COML personnel will be completely trained to make real time adjustments.
- Any role or involvement of the FirstNet Network Operations Center (NOC) will be defined.
- A COML at the scene of a major incident (e.g., fire) will be aware that another agency is also managing a high-risk incident which could be compromised by adjustments to the users or the network.
- Policies will be established to govern changes associated with a user's profile and a group's profile.
- Policies will be established to govern priority assignments associated with commercial users treated as visitors (i.e., roamers). Note that PSE administrators will not have access to commercial subscribers profile and data therefore cannot modify such data.
- With roles defined for PSE stakeholders, a priority hierarchy model will be established..

It is assumed that FirstNet will determine the best technical solution. All requirements below could apply to user data in general and/or to a set of users' profiles. No distinction is made.

TABLE 33. USER PROFILE CONFIGURATION REQUIREMENTS

#	Requirement
99	A visual interface (e.g., GUI-friendly portal) SHALL be provided to enable management of subscribers (and groups) profiles by authorized administrators.
100	Authorized administrators SHALL be assigned a well defined jurisdiction and/or user groups for PQoS management.
101	Authorized administrators SHOULD be capable of managing Users (and user group) profiles via a portable device and/or a fixed console
102	Authorized administrators SHALL be provided with the capability to manage a agency account(s), user profiles, and subscription data under that (those) account(s).
103	Authorized administrators SHALL be provided with the capability to assign a device or devices to a single user, and to assign multiple users to a single device (e.g., vehicle modem/router device).
104	Authorized administrators SHALL be provided with the capability to provision and alter a user's Type and/or Roles.
105	Authorized administrators SHALL be provided with the capability to enable/disable roaming service on a per subscription basis.
106	Authorized administrators SHALL be provided with the capability to create/view/configure/modify/delete user profiles and subscription profiles.
107	Authorized administrators SHALL be provided with the capability to view usage data per user.
108	Authorized administrators SHALL be provided with the capability to view/modify preemptive rights of a user.
109	Authorized administrators SHALL be provided with the capability to view/modify preemption vulnerability of a user.
110	Authorized administrators SHALL be provided with the capability to view/modify the priority level of a user.
111	Authorized administrators SHALL be provided with the capability to view/modify Access Point Name (APNs) assigned to a subscription.
112	Authorized administrators SHALL be provided with the capability to establish bandwidth limits for a user. *Note 1: One possible implementation of this requirement is to establish uplink and downlink guaranteed bit rate (GBR) and maximum bit rate (MBR) limits; however, other implementations are possible. This capability can, for example, be used to establish a maximum amount of bandwidth a user can utilize for general Internet traffic, or establish a range of bandwidth that*

	can be used for a video application. *Note 2: It is recognized that configuration of bandwidth requires highly specialized training and expertise. Bandwidth for applications must be appropriately tuned in order to provide the correct user experience.*
113	Authorized administrators SHALL be provided with the capability to set a user's default PQoS attributes.
114	Authorized administrators SHALL be provided with the capability to enable/disable specific applications associated with a user.
115	Authorized administrators SHALL be provided with the capability to override inconsistent modifications to a user profile.
116	Authorized administrators SHALL be provided with the capability to reset user profiles to default settings.
117	Arrangements SHALL be made with FirstNet to adapt policy enforcement rules based on an agency's needs.
118	An authorized PSE administrator SHALL be able to configure which users can initiate and clear the emergency condition. This means, for example, the administrator can elect the responder, the dispatcher, or both to clear the emergency condition.
119	An authorized PSE administrator SHALL be able to configure which users can clear the Immediate Peril condition. This means, for example, the administrator can elect the responder, the dispatcher, or both to clear the Immediate Peril condition.
120	It SHALL be possible for an authorized NPSBN administrator (NPSBN and PSE) to configure which applications can utilize resources previously assigned to other applications.
121	Authorized PSE administrators SHALL be able to view a QoS configuration history for users under their authority.

During the creation of this section, the Working Group noted a potential scenario requiring further investigation. Should the NPSBN support commercial users "roaming in" to band class 14 who are home to other commercial systems, can those users flood the NPSBN with 9-1-1 calls? What impact will this have on the accessing the NPSBN (i.e. the RACH) and on general resource utilization? This issue requires further study.

6.3 User Provisioning

Access to the NPSBN will require users to be set up by an authorized NPSBN administrator. Along with the new employee set up process for CJIS, email, CAD, etc., users will need to be entered into the NSPSBN user database and have their authorizations and PQoS settings established. For instance, a new patrol officer may only need authorization to access 15 applications, default PQoS settings, and fundamental CAD access with no CJIS and limited NPSBN capability to begin with. In addition to new set ups, users getting promotions, gaining new skills and certifications, or new assignments may need alterations in their NPSBN settings.

The initial set up will also establish the users PQoS settings either directly or through the application they are assigned. To facilitate efficient and accurate configuration, the use of templates by user type or category is required of the system. The user category names should be configurable so that they can match the naming conventions within the organization. If an assigned template is updated with a new setting or application then all users who were established under that template should have their settings, devices, and applications updated automatically. Considerations need to be made to ensure there are no negative impacts to the operations of the user during the update.

The PQoS settings used across the entire organization should be optimized for maximum usage of the available spectrum in the commonly used coverage area. This would include factoring in the level of usage from other organizations in the area. FirstNet, in conjunction with public safety representatives, should establish best practices and guidelines for organizations to use when setting up their templates.

A user's net PQoS is a blend of their user priority (e.g., user priority attributes, such as role) and the priorities associated with the applications they use. For instance, a secondary user may utilize mission critical push-to-talk and inherit much higher PQoS settings as a result. This increase only applies to the specific application the user is using and will not carry over to their PQoS settings for other devices or applications.

TABLE 34. PRIORITY AND QOS USER PROVISIONING REQUIREMENTS

#	Requirement
122	When assigning default PQoS to an NPSBN user, the authorized administrator (NPSBN or PSE) SHALL have the ability to choose from a list of standardized 'templates.'
123	It shall be possible for an authorized administrator to define templates (groupings) for combinations of packet loss and packet latency rates. *Note: Packet loss and latency are aspects of Scheduling Priority (section 5.2.3). This requirement is attempting to simplify the user provisioning process by suggesting these complex parameters be grouped into provisioning templates. This means, for example, a user can be provisioned for "High Quality Video" as a template name and that would equate to a specific packet loss and latency for the user's associated video applications.*

6.4 Administration Operations

This section contains requirements associated with administrative operations which are associated with dynamic change & reassignment of PQoS attributes. These attributes may be associated with the NPSBN and/or its users.

TABLE 35. DYNAMIC ADMINISTRATION OPERATIONS REQUIREMENTS

#	Requirement
124	Each PSE administrator or authorized PSE user (e.g., the dispatcher) SHALL have the ability to change the user's PQoS priority attributes (Responder Emergency state, Incident Status, etc.) based on the incident and locally controlled needs.
125	Each PSE administrator or authorized PSE user (e.g., the dispatcher) SHOULD have the ability to reset a user's priority attributes to their pre-incident setting in a one-step action.
126	It SHALL be possible for an authorized administrator (NPSBN or PSE) to alter, in run-time (i.e., while the NPSBN is operating), the template assigned to an NPSBN user or group of NPSBN users.
127	It SHALL be possible for an authorized NPSBN Administrator (NPSBN and PSE) to configure which applications can utilize resources previously assigned to other applications.
128	Authorized PSE administrators SHALL be able to view a QoS configuration history for users under their authority.
129	PSE administrators SHALL be able to view the real-time dynamic priority condition of all users under their authority.
130	PSE administrators SHALL be able to retrieve information that allows for "post-mortem" evaluation of the effectiveness of QoS configurations in providing for effective incident communications.
131	PSE administrators SHALL be able to modify the QoS role of users within their scope.

6.5 Charging and Usage Records

The network should have the capability to generate accurate user/service-level charging information in real time and report this information to upstream billing systems. 3GPP [TS32.240, TS32.251] has defined a standardized architecture for charging for packet-switched domains. It defines the structure and content of charging records to be generated by the network elements as well as the interfaces and protocol for transfer of these records to upstream charging nodes. The charging mechanisms are defined as:

Offline charging is where charging information for network resource usage is reported by the network to the billing system after resource usage has occurred. This mechanism is used for post-paid services and for billing reconciliation.

Online charging is where authorization for the network resource usage must be obtained by the network from the Online Charging System (OCS) prior to the actual usage. This mechanism is used for pre-paid services or on-demand type of services

Law enforcement agencies may decide to use different type of billing mechanisms based on their user needs. For example, a first responder user may have post-paid services while a non-first responder/secondary user may have on-demand type services based on usage. The charging systems described above should be offered as it provides flexible billing options for FirstNet and secondary users on the NPSBN network. These charging systems provide the mechanisms to generate additional revenue.

TABLE 36. CHARGING AND USAGE RECORDS REQUIREMENTS

#	Requirement
132	The NPSBN SHALL provide detailed usage and/or billing records to individual agencies.
133	The NPSBN core network SHALL have the ability to set the criteria and granularity (information) for PQoS information associated with the Call Detail Records (CDRs) that are generated (i.e., volume based, etc.).
134	The NPSBN SHALL provide additional details of user identifying usage of dynamic PQoS controls. *The intent is for agencies to be able to identify usage patterns of dynamic PQoS usage by specific NPSBN-users.*
135	The NPSBN network SHALL have the ability to generate and report Key Performance Indicators (KPIs) specific to QoS type of services for each user. I.e., QoS usage, preemption occurrence, etc. on a weekly/monthly basis.
136	The NPSBN network SHALL provide different types of charging policies (i.e., Post-Paid and Pre-Paid)

Appendix A: Definitions

3GPP	3rd Generation Partnership Project
APN	Access Point Name. The name of a gateway between a GPRS, 3G, or 4G mobile network and another computer network, frequently the public Internet. A mobile device making a data connection must be configured with an APN to present to the carrier.
ARP	Allocation and Retention Priority. The LTE admission priority parameter that determines the allocation and retention priority of an LTE bearer. See 3GPP TS 23.401.
Authorized Administrator	NPSBN or PSE Administrator
BYOD	Bring Your Own Device
CDR	Call Detail Record
CII	Critical Infrastructure Industry. State, local government, and non-government entities, including utilities, railroads, metropolitan transit systems, pipelines, private ambulances, volunteer fire departments, and not-for-profit organizations that offer emergency road services, providing private internal radio services, provided these private internal radio services are used to protect safety of life, health, or property; and are not made commercially available to the public.[8]
CLA	Covered Lease Agreement
COML	Communications Unit Leader
COP	Common Operational Picture
DB	Database
DS	Deployable System
eNB	Evolved Node-B. This is the LTE base station.
GETS	Government Emergency Telecommunications Service. GETS is a calling card program that provides priority access and prioritized processing for voice calls in the local and long distance segments of landline networks, greatly increasing the probability of call completion. GETS is intended to be used in an emergency or crisis situation when the landline network is congested and the probability of completing a normal call is reduced.
GBR	Guaranteed Bit-Rate

[8] FCC Rules, Title 47 CFR, section 90.7

IC Incident Commander

ICAM Identity, Credential, and Access Management. The process of establishing a user's identity using their credentials (e.g., password), which is then used in determining the user's authorization to perform electronic tasks associated with the NPSBN.

ICS Incident Command System as defined by NIMS

IP Immediate Peril

LMR Land Mobile Radio

MBMS Multimedia Broadcast Multicast Service

MVPN Mobile Virtual Private Network

NGN Priority Service Next Generation Network Priority Service. The NGN Priority Services Program is transitioning legacy priority voice capabilities PTS (Priority Telecommunications Services) to NGN packet-based services in the commercial service providers' networks. Legacy PTS includes the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS). NGN-Priority Service, when available, will provide per call or per-session priority for voice, data, and video communications originating in capable commercial networks.

NIMS National Incident Management System

NPSBN Nationwide Public Safety Broadband Network

NPSBN Administrator An NPSBN (e.g., FirstNet) employee acting on behalf of a User Entity to provision users, perform system planning, and perform operations and maintenance.

NPSBN PQoS Policy Preconfigured rules indicating the PQoS experience a user or group should receive from the NPSBN. NPSBN PQoS policy associates a change in a user or group's priority attributes with specific changes to LTE technology.

PQoS Priority and Quality of Service

Priority Determines the probability of obtaining and retaining resources on the NPSBN, including, but not limited to:

- the process of determining priority for a user, determining his/her associated devices and for each device determining when to access (attach to) the NPSBN
- the process of determining priority for a user, determining his/her associated devices and for each device determining if a new resource can be obtained from (i.e., be admitted to) the NPSBN
- the process of determining how user traffic is scheduled for delivery over-the-air

Priority Attribute A parameter which represents a characteristic of PQoS behavior. The aggregate of a user or group's priority attributes may be mapped to specific PQoS controls by NPSBN PQoS policy.

PTT Push to Talk

Public Safety Entity (PSE) A User Entity focused on public safety functions (e.g., police, fire, EMS agency).

Public Safety Enterprise Network (PSEN) A secure network domain associated with a PSE.

PSE Administrator A PSE employee acting on behalf of a User Entity to provision users and applications, and perform operations and maintenance.

QoS Quality of Service. Focuses on the quality of experience attributes (latency, packet loss, etc.) supplied by the broadband network to an application or device.

RACH Random Access Channel

RE Responder Emergency

RMS Records Management System

SCBA Self-Contained Breathing Apparatus

Secondary User NPSBN users, excluding Primary Users, who are authorized to utilize the NPSBN and its licensed spectrum.

Session Coordinated Priority and QoS involving two or more communication entities.

SHALL The word "SHALL" (capitalized) is used herein to identify those items that the Working Group considered critical to the success of the NPSBN. In the opinion of the Working Group, the network is unlikely to fulfill its mission and promise if these factors are not considered.

SHOULD The word "SHOULD" (capitalized) is used herein to identify those items that the Working Group considered important to the success of the NPSBN. In the opinion of the Working Group, the network would benefit from including items so indicated.

Subscription The collection of user or device data stored in the infrastructure which is used to

- authenticate a user or device
- determine which applications the user or device can use
- determine what policies and capabilities apply to the user or device

A subscription is typically created for a user when she/he initiates service with the NPSBN or other commercial carrier.

User Entity(ies) Agencies and organizations (e.g., local, state, tribal, and federal) authorized to use the NPSBN as end users.

User Entity Administrator — A User Entity (e.g., local agency) employee or individual empowered by User Entity governance to perform priority and QoS provisioning and configuration functions for the associated User Entity.

UE — User Equipment (responder device)

USIM — Universal Subscriber Identity Module

VPN — Virtual Private Network

WPS — Wireless Priority Service. An add-on feature subscribed to on a per-cell phone basis, which provides priority access and prioritized processing for voice calls in all nationwide and several regional commercial cellular networks, greatly increasing the probability of call completion. WPS is intended to be used in an emergency or crisis situation when utilizing commercial cellular networks that are congested and the probability of completing a commercial cellular call is reduced.

APPENDIX B: LTE TECHNOLOGY OVERVIEW

This appendix is for informational purposes and does not include requirements or recommendations.

This section provides an LTE overview and includes the following topics:

1. LTE Basics
2. Control Access to Air Interface
    - Access Class barring
    - Establishment cause
3. Control Use of Resources
    - ARP
    - QCI
    - Policy rules

LTE BASICS - NETWORK ARCHITECTURE

The key elements making up an LTE network are shown if the figure below.

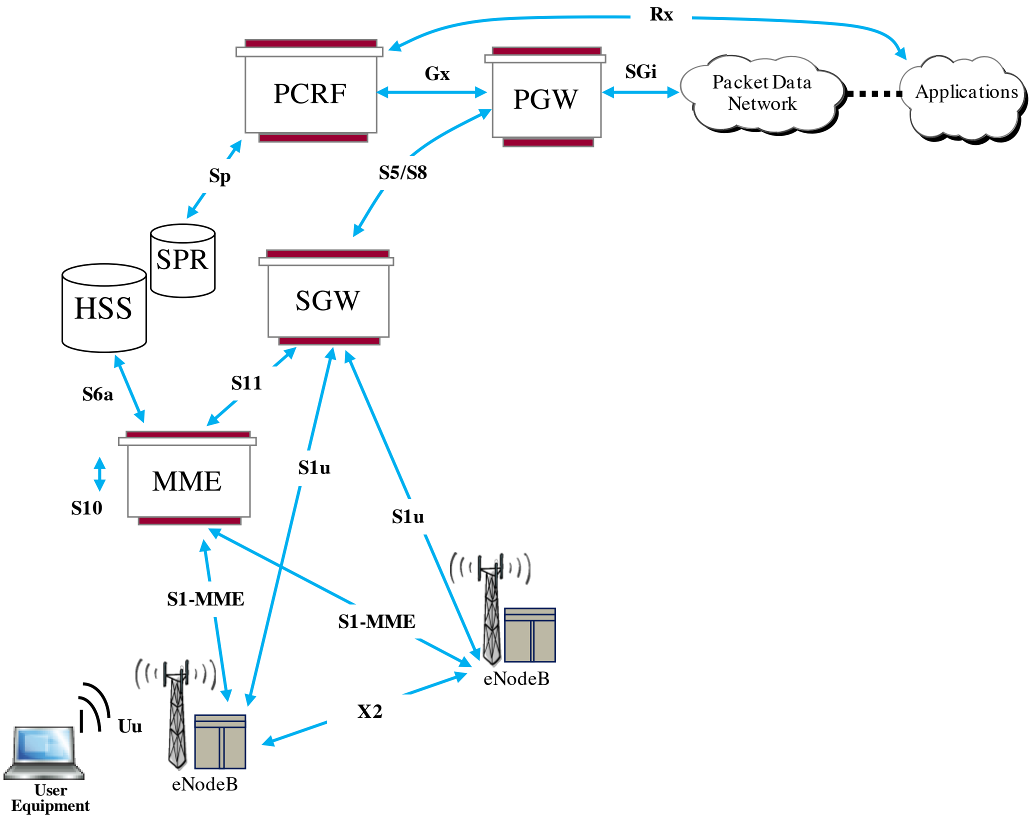


FIGURE 13. LTE NETWORK ARCHITECTURE

The eNodeB is the LTE element that supports the radio interface with user equipment (UE)/devices. It provides the following high level functions:

- Radio admission control
- Scheduling of UpLink (UL) and DownLink (DL) data transmissions
- Scheduling and transmission of paging information used to alert idle UEs/devices that information is available for them, and system broadcast information
- The eNodeB also provides IP header compression to optimize capacity

The eNodeB interfaces with the Mobility Management Entity (MME) which interfaces with the Home Subscriber System (HSS) to obtain user device authentication information and user subscription information, and authenticates user devices. The HSS is also used to maintain the subscriber tracking area and identity of the MME serving the subscriber.

Once a user is successfully authenticated one of the roles of the MME is to manage the bearer connections associated with the device. As part of this the MME selects the Serving GateWay (SGW) and the Packet Data Network GateWay (PDN-GW or PGW).

The SGW provides packet routing and forwarding for data coming from and going to the UE/device. It is also the local mobility anchor point for inter-eNB handovers, performed when a UE/device moves from one eNodeB to another. Another function of the SGW is to notify the MME that a data packet is received for an idle UE/device. When this happens the SGW buffers the packet while the MME pages the UE to make it active again so the data can be sent to the UE.

The PGW provides the interface to the packet data network (PDN), connecting the LTE system to the rest of the IP network (e.g., the Internet, a PSE network) with the various applications. It allocates the IP address(es) for the UE which are used with the rest of the network, and is the anchor point for the UE towards the rest of the network, allowing a UE to move around while maintaining the same IP address towards the rest of the network. The PGW also provides per-user packet filtering and policy enforcement.

The Policy and Charging Rules Function (PCRF) is the entity in the network that authorizes QoS resources for each connection created in the LTE network based on a variety of information, such as a user's role and type of data to be transmitted (e.g., voice versus Internet traffic). This allows making dynamic policy decisions on service data flow treatments in the PCEF (PGW). A service data flow represents one or more bearers with the same QoS characteristics including QCI and ARP. It can also provide flow-based charging functions. The PCRF obtains subscriber specific policy information from the Subscriber Policy Repository (SPR) database (e.g., role of the subscriber). The SPR database can be either on the same database platform as the HSS or on a different one.

LTE CALL SETUP

The figure below shows a high-level call flow when a UE connects to the LTE network, e.g., because it is powered up.

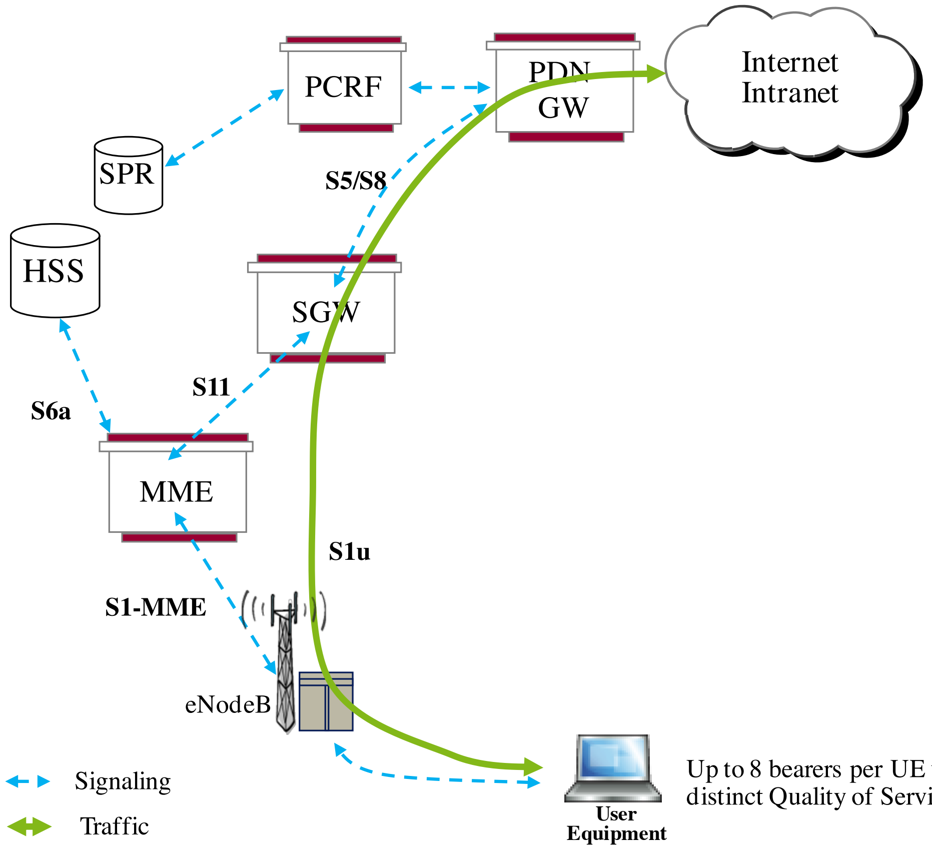


FIGURE 14. LTE CALL SETUP

It consists of the following high-level steps:

1. UE sends an attach request to the eNB using its International Mobile Subscriber Identity (IMSI), which is a globally unique identity.

2. eNB send the request to the appropriate MME including the IMSI.

3. MME extracts user information from the HSS such as authentication information using the Public Land Mobile Network (PLMN) identity which is part of the IMSI. Each service provider has a globally unique PLMN for its network, which allows the network to find the HSS for that specific service provider with the subscriber information.

4. MME authenticates the UE with the information obtained from the HSS.

5. Once successfully authenticated the MME sends a bearer setup request to SGW.

6. SGW forwards the request to the PGW (thru S8 if roaming).

7. The PGW in turn sends a request to the PCRF which determines QoS and Traffic policy for the new bearer.

8. If successful, MME accepts attachment of UE.

9. Always-on IP setup uses P-GW as anchor.

10. eNB sets up a radio bearer for UE.

11. Communications starts.

LTE ENODEB BASICS

As shown in the figure below an eNodeB typically consists of three sectors, each covering one third of the area surrounding the eNodeB site, and a given UE is typically served by one of the three sectors.

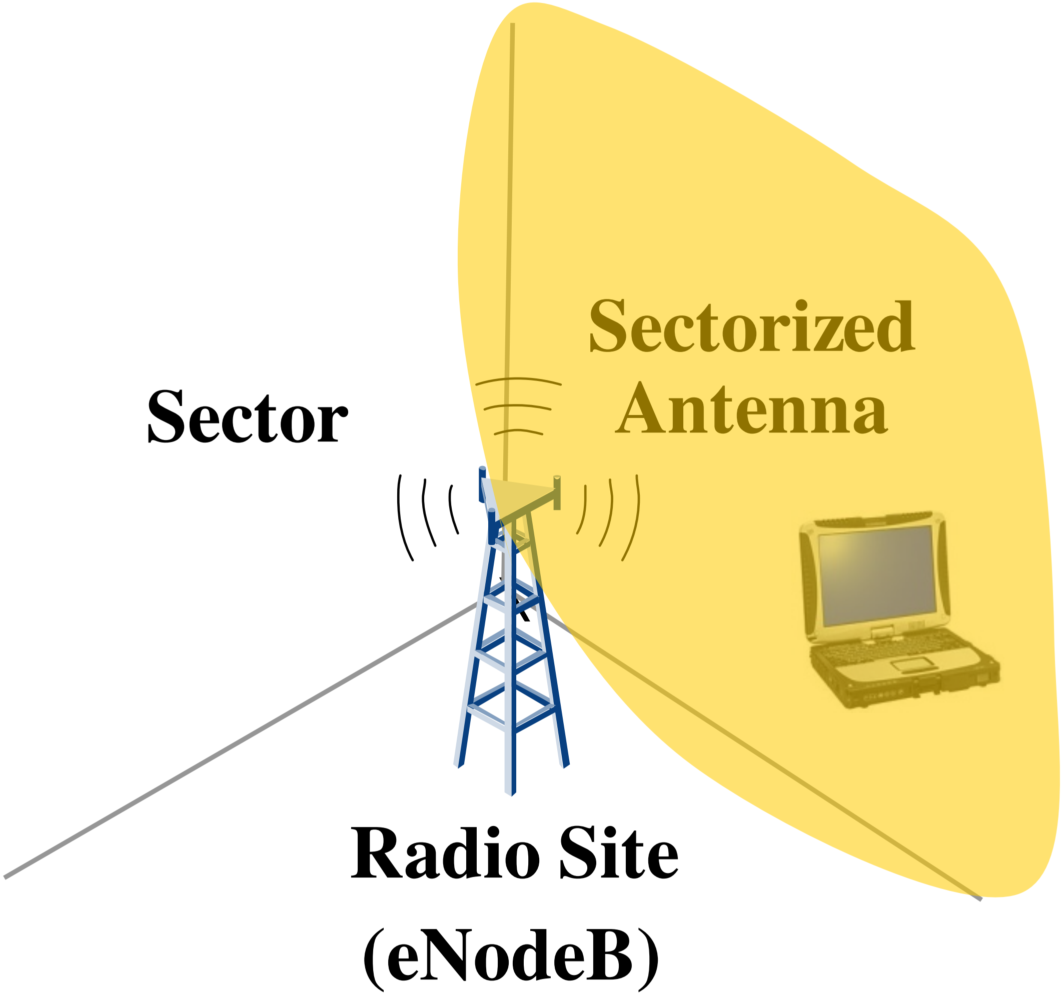


FIGURE 15. LTE ENODEB BASICS

One key differentiator is that in LTE each sector uses the same frequency band (also called a frequency re-use of 1) as shown in the figure below, whereas in examples LMR and 1G/2G wireless adjacent sites use different frequencies.

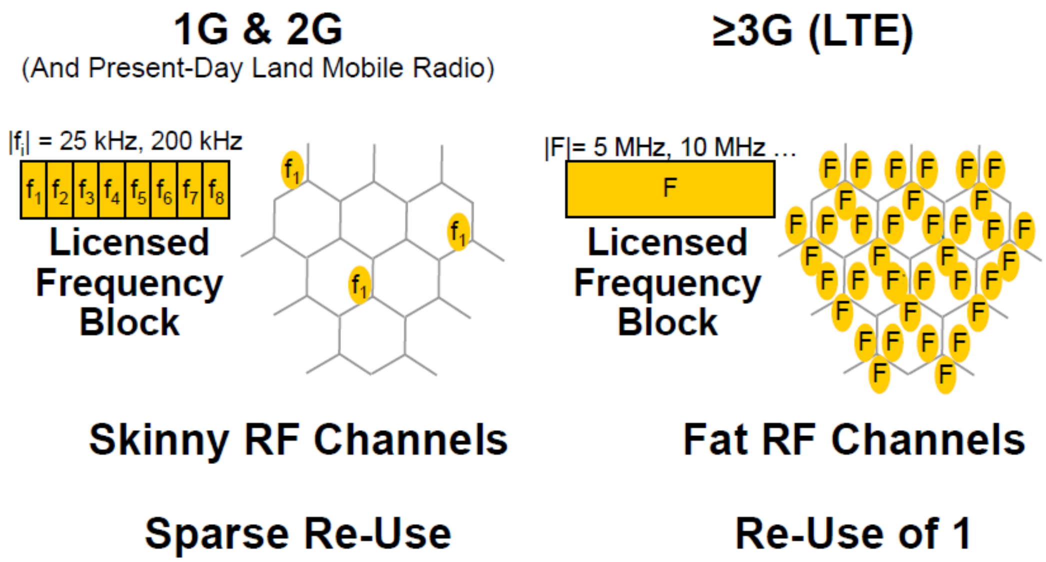


FIGURE 16. LTE FREQUENCY RE-USE

This leads to much greater capacity for LTE since all available spectrum can be used in every sector/site, but does require interference mitigation techniques providing for coordination at the border of cells for both uplink and downlink transmission. This coordination is established through signaling exchange between adjacent cells using the X2 interface. Various capabilities to mitigate the interference are introduced in different LTE releases, most recently the enhanced Inter Cell Interference Coordination (eICIC), thus maximizing the capacity provided by a cell. The figure below shows the interference.

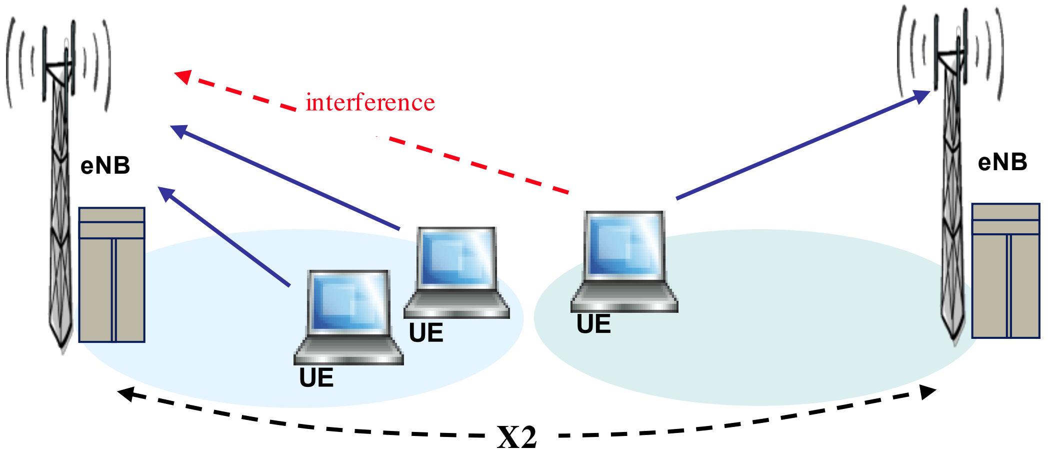


FIGURE 17. MINIMIZING INTERFERENCE

The amount of data a user can send and receive depends on various parameters including the amount of available spectrum (10 MHz downlink and 10 MHz uplink for public safety band 14), the number of antennas (typically two send and two receive antennas, called 2x2 MIMO), the number of users and how they are distributed over the cell sector, and the distance from the device to the cell site. The figure below shows the peak and average rates that can be achieved in B14 using 2x2 MIMO.

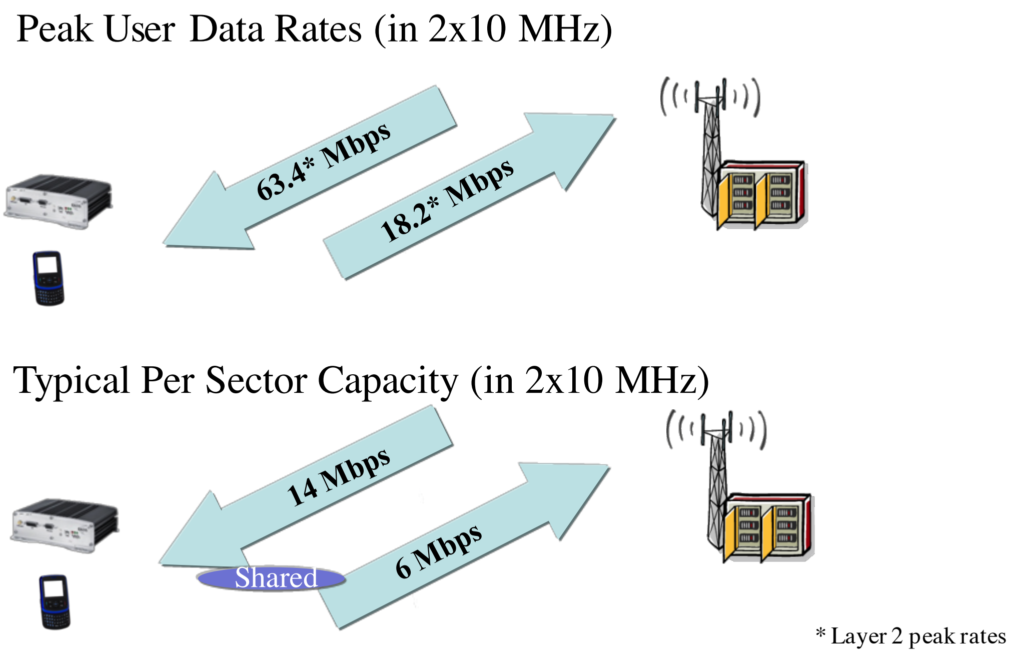

Peak User Data Rates (in 2x10 MHz)
63.4* Mbps
18.2* Mbps
Typical Per Sector Capacity (in 2x10 MHz)
14 Mbps
6 Mbps
Shared
* Layer 2 peak rates

FIGURE 18. PEAL AND TYPICAL UPLINK AND DOWNLINK DATA RATES

As mentioned, the other parameter that affects the achieved data rates is the distance from the device to the cell site. Below the figure demonstrates this.

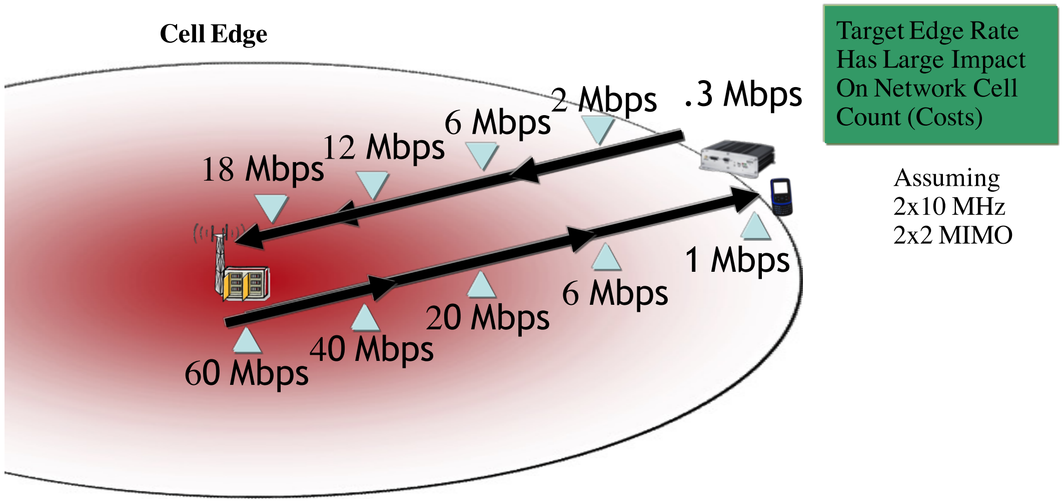


FIGURE 19. PEAK USER DATA RATES AND DISTANCE FROM CELL

In this specific example it shows a rate of 1 Mbps down and 0.3 Mbps up at the edge of the cell (beyond which the device would be handed off to an adjacent cell). As cells are spaced further apart this rate decreases. As a consequence, the number of cells highly depends on the desired cell edge rate. The FCC specified cell edge rates of 768 Kbps downlink and 256 Kbps uplink for the public safety network. Increasing the cell edge rates would increase the number of cell sites to cover an area, and decreasing the cell edge rate would reduce the number of sites required.

CONTROL ACCESS TO AIR INTERFACE

Emergency events in the NPSBN network could cause network congestion; in this case there may be a need to restrict primary and secondary users from accessing the network to prevent overload conditions. The network should have the ability to prevent users from making access attempts or responding to pages in specified areas of a network. The ability to prevent users from overloading the access channel during these critical conditions is vital. Users that do not need priority access can be restricted based on Access Class which corresponds to the permitted classes as signaled over the air interface.

Any number of these classes as defined by 3GPP can be barred at any one time.

- Mechanism to limit regular users from accessing a cell
- Only applies to mobile originations
- Typical use:
    - Reduce access overload in time of emergency or congestion
    - Reserve cells for operator activities – maintenance, growth, etc.
    - 3GPP R11 introduces Extended Access Barring (EAB) in LTE to manage Machine Type Communications (MTC)
- Low-priority access UEs send “delay-tolerant” indication
- RAN sends “Extended wait time” (up to 30 minutes) to low priority UEs

The enodeB policies the access control based on the following:

- Access control using access classes:
    - Access class stored in USIM of device
        - Classes 0-9 randomly assigned to commercial users
        - Class 10 -> E911 calls
        - Classes 11 & 15 are reserved for network administrative devices
        - Remaining classes for Public Safety & NGN-Priority Service users
            - Class 12 – Security Services (police, …)

- Class 13 – Public Utilities (water, gas, …)
- Class 14 – Emergency Services (fire, EMT, ..)

eNodeB controls user access through broadcast of access class barring parameters in SIB2 and UE perform actions according to Access Class in USIM.

SIB2 (System Information Block Type2) parameters for access control:

- For regular users with AC 0 – 9, their access is controlled by ac-BarringFactor and ac-BarringTime.
    - "Rand" generated by the UE has to pass the "persistent" test in order for the UE to access. By setting ac-BarringFactor to a lower value, the access from regular user is restricted (UE must generate a "rand" that is lower than the threshold in order to access) while priority users with AC 11 – 15 can access without any restriction.
- For users initiating emergency calls (AC 10) their access is controlled by ac-BarringForEmergency – boolean value: barring or not.
- For UEs with AC 11- 15, their access is controlled by ac-BarringForSpecialAC - boolean value: barring or not. The standard defined these AC as follows (22.011, section 4.2):
    - Class 15 - PLMN Staff;
    - Class 14 - Emergency Services;
    - Class 13 - Public Utilities (e.g., water/gas suppliers);
    - Class 12 - Security Services;

After the initial information from the enodeB described above, the user device sends a connection request to the enodeB.

- The "RRCConnectionRequest" from an UE contains the EstablishmentCause, which when set to "highPriorityAccess" is a way for the eNB to prioritize those requests
    - The Establishment Cause marked as "highPriorityAccess" indicates that the access request is originated from a UE operating in AC 11-15 Class 11 - For PLMN Use
    - This prevents lower priority users from utilizing the limited radio resources.

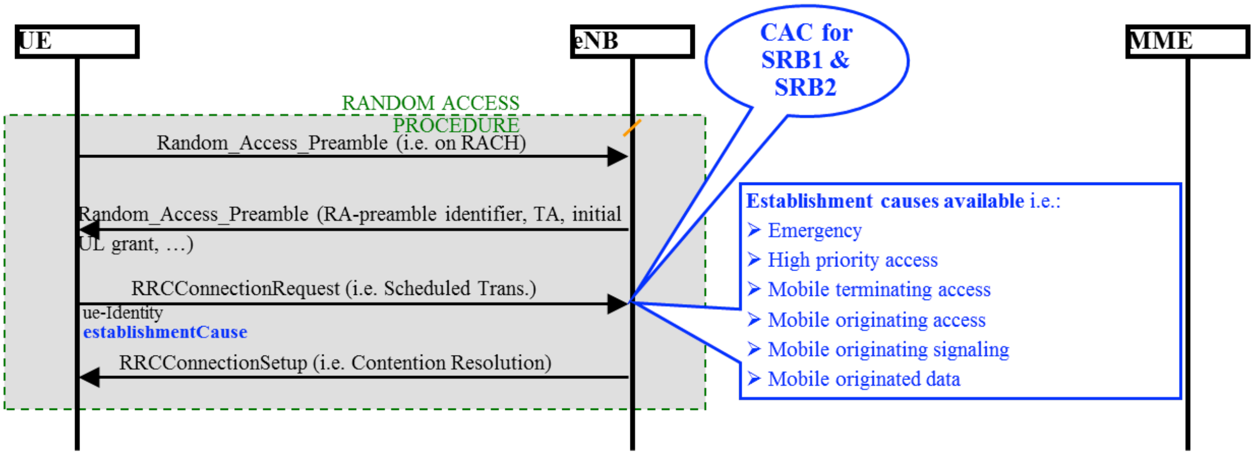

UE
eNB
MME
CAC for SRB1 & SRB2
RANDOM ACCESS PROCEDURE
Random_Access_Preamble (i.e. on RACH)
Random_Access_Preamble (RA-preamble identifier, TA, initial UL grant, …)
RRCConnectionRequest (i.e. Scheduled Trans.)
ue-Identity
establishmentCause
RRCConnectionSetup (i.e. Contention Resolution)
Establishment causes available i.e.:
➢ Emergency
➢ High priority access
➢ Mobile terminating access
➢ Mobile originating access
➢ Mobile originating signaling
➢ Mobile originated data

FIGURE 20. ACCESS REQUEST FROM UE

CONTROL OF EVOLVED PACKET SYSTEM QOS AND PRIORITY RESOURCES

- EPS bearers provide the UE access to PDN services and applications.
  - Default Bearer is established during attachment, & maintained throughout the lifetime of the connection (always-on IP connectivity).
  - This is no guarantee for service access; it merely is reservation of resources before packet flows are admitted in the system.
  - Additional Dedicated Bearers can be established, dynamically, as a result of service requests or access to services.

The figure below shows a general description of the bearers that are established.

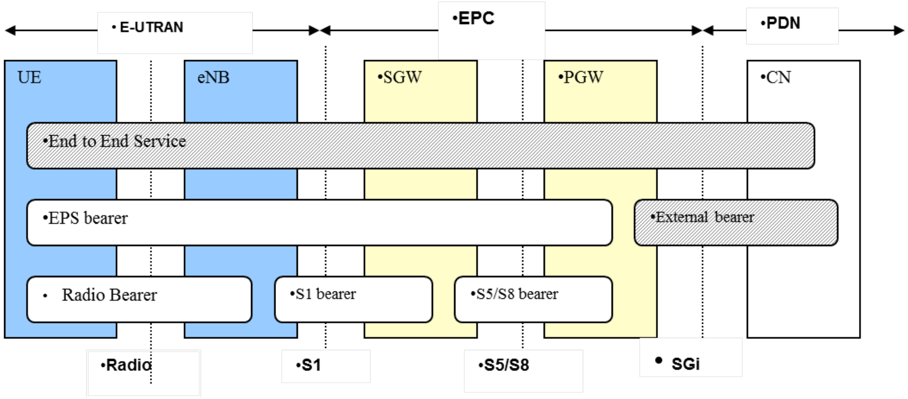


FIGURE 21. LTE BEARERS

EPS BEARER MANAGEMENT

The two types of bearers supported by LTE are shown below:

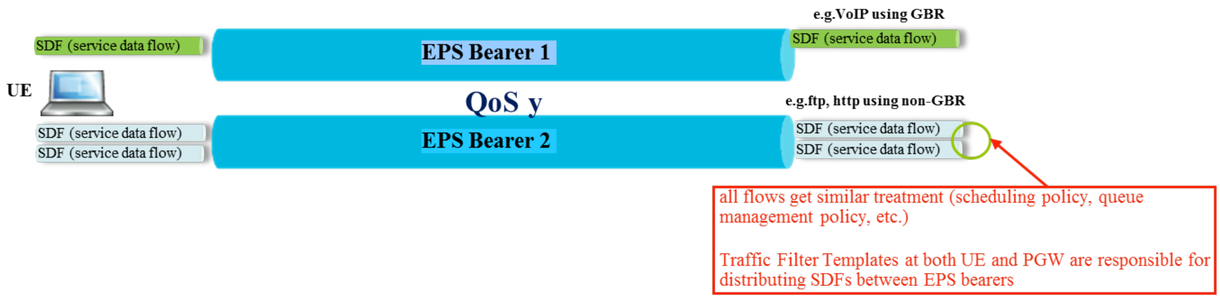
Guaranteed Bit Rate (GBR)

    - Specified Guaranteed Bit Rate (GBR) and Maximum Bit Rate (MBR)
    - Has associated ARP and QCI
    - Service will not experience congestion-related packet loss (provided that the user traffic is compliant to the agreed GBR QoS parameters)
    - Established on demand because it allocates transmission resources by reserving them during the admission control function
    - Precedence of service blocking over service dropping in congestion situation
    - Inactivity timers are used to control air interface and S1 interface to free up resources

- Non-Guaranteed Bit Rate (Non-GBR)
    - May have a Maximum Bit Rate (MBR)
    - Has associated ARP and QCI
    - Service must be prepared to experience congestion-related packet loss
    - Can remain established for long periods of time because it does not reserve transmission resources
    - Precedence of service dropping over service blocking in congestion situation
    - Stay up (no reserved resources)

These bearers can be manipulated with parameters to provide QoS and priority on a per bearer (or bearer aggregate) basis

- QoS Class Identifier (QCI)
    - To control packet forwarding treatment (e.g., scheduling weights, queue management thresholds, link layer protocol configuration, etc.), and typically pre-configured by the operator
- Allocation and Retention Priority (ARP)
    - The primary purpose or ARP is to decide if a bearer establishment/modification request can be accepted or rejected in case of resource limitation.
- Guaranteed Bit Rate and Maximum Bit Rate – Per GBR bearer
- Aggregate Maximum Bit Rate (AMBR) – Sums all non-GBR bearers per terminal/Access Point Name (APN)



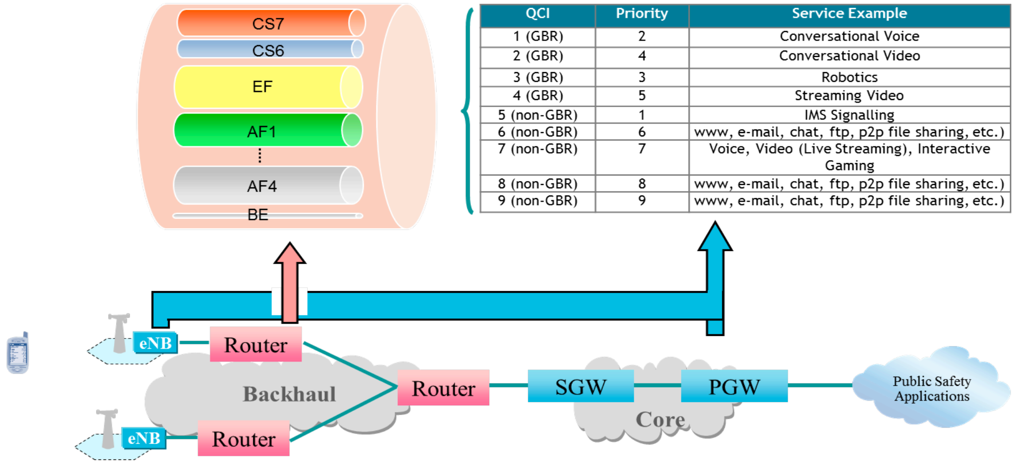
all flows get similar treatment (scheduling policy, queue management policy, etc.)

Traffic Filter Templates at both UE and PGW are responsible for distributing SDFs between EPS bearers

FIGURE 22. QUALITY OF SERVICE

LTE QOS CLASSES

The figure below shows the different types of LTE QoS classes as recommended by 3GPP:



QCI	Priority	Service Example
1 (GBR)	2	Conversational Voice
2 (GBR)	4	Conversational Video
3 (GBR)	3	Robotics
4 (GBR)	5	Streaming Video
5 (non-GBR)	1	IMS Signalling
6 (non-GBR)	6	www, e-mail, chat, ftp, p2p file sharing, etc.)
7 (non-GBR)	7	Voice, Video (Live Streaming), Interactive Gaming
8 (non-GBR)	8	www, e-mail, chat, ftp, p2p file sharing, etc.)
9 (non-GBR)	9	www, e-mail, chat, ftp, p2p file sharing, etc.)

FIGURE 23. LTE QOS CLASSES

ADMISSION CONTROL-ALLOCATION RETENTION PRIORITY (ARP)

- ARP is stored in the Subscriber profile (HSS) on a per APN basis (at least one APN must be defined per subscriber) and consists of:
    - Priority level: 1 – 15, with 1-8 intended for prioritized treatment within operator domain (per 3GPP 29.212, Section 5.3.45)
    - Preemption capability flag: can pre-empt other users
    - Preemption vulnerability flag: can be pre-empted by other users
- PCRF can modify ARP and QCI based on user role, application, etc. when the bearer is setup
- At every Radio Bearer (RB) setup request (including HO and RRC connection re-establishment), the eNodeB Radio Admission Control (RAC) entity checks the current eNodeB's ability to accept the request, considering factors such as:

- Maximum number of UEs and RBs,
- Number of RBs on GBR

APPENDIX C: LTE QOS CLASS IDENTIFIERS

This appendix is for informational purposes and does not include requirements or recommendations.

The 3GPP standards have defined “QoS Class Identifiers” (QCI) which are essentially indexes into Table 37. A QCI can be thought of as a number that is associated with a tolerance for over-the-air packet loss, latency, and whether or not a guaranteed bit-rate is made available.

Once the LTE technology has admitted or allowed a new resource (bearer) to commence, each bearer is then associated with a QCI. For example, a push-to-talk application might have 1 bearer for signaling and 1 bearer for voice and floor control. Each of the bearers would have a different QCI.

Table 37 lists the standardized QCI values, including QCI values added specifically for push-to-talk in 3GPP release 13. LTE vendors have varying degrees of support for these standard QCIs.

TABLE 37. STANDARDIZED 3GPP QCI CHARACTERISTICS

QCI	Resource Type	Priority Level	Packet Delay Budget	Packet Error Loss Rate (NOTE 2)	Example Services
1 (NOTE 3)	GBR	2	100 ms (NOTE 1, NOTE 11)	10^{-2}	Conversational Voice
2 (NOTE 3)		4	150 ms (NOTE 1, NOTE 11)	10^{-3}	Conversational Video (Live Streaming)
3 (NOTE 3)		3	50 ms (NOTE 1, NOTE 11)	10^{-3}	Real Time Gaming
4 (NOTE 3)		5	300 ms (NOTE 1, NOTE 11)	10^{-6}	Non-Conversational Video (Buffered Streaming)
65 (NOTE 3, NOTE 9)		0.7	75 ms (NOTE 7, NOTE 8)	10^{-2}	Mission critical user plane Push To Talk voice (e.g., MCPTT)
66 (NOTE 3)		2	100 ms (NOTE 1, NOTE 10)	10^{-2}	Non mission critical user plane Push To Talk voice
5 (NOTE 3)	Non-GBR	1	100 ms (NOTE 1, NOTE 10)	10^{-6}	IMS Signalling
6 (NOTE 4)		6	300 ms (NOTE 1, NOTE 10)	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7 (NOTE 3)		7	100 ms (NOTE 1, NOTE 10)	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8 (NOTE 5)		8	300 ms (NOTE 1)	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9 (NOTE 6)		9			
69 (NOTE 3, NOTE 9)		0.5	60 ms (NOTE 7, NOTE 8)	10^{-6}	Mission critical delay sensitive signalling (e.g., MC-PTT signalling)
70 (NOTE 4)		5.5	200 ms (NOTE 7, NOTE 10)	10^{-6}	Mission critical data (e.g. example services are the same as QCI 6/8/9)

APPENDIX C: RATE LIMITING AND BANDWIDTH MANAGEMENT DETAILS

This appendix is for informational purposes and does not include requirements or recommendations.

Rate limiting and bandwidth management enables the authorized User Entity administrator to control the utilization of NPSBN over the air bandwidth resources. There are a number of standard LTE features that can be used to control the amount of bandwidth utilized by NPSBN devices.

Rate limiting is implemented using controls for non-GBR [guaranteed bit rate] bearers. For example, the amount of bandwidth a responder utilizes while accessing the Internet can be limited. These controls consist of setting an aggregate maximum bit rate (AMBR) for a device related to a specific LTE Access Point (APN). For LTE networks, this parameter is the Access Point Name Aggregate Maximum Bit Rate (APN-AMBR). This rate limiting control enforces a maximum aggregate bit rate across all of the device bearers for one APN (i.e., all non-GBR bandwidth used for a particular IP network). Once the APN-AMBR value is exceeded, data will no longer be transported by the NPSBN until the data rate falls under the APN-AMBR value. Another rate limiting control for non-GBR bearers is the per device aggregate maximum bit rate (UE-AMBR). This rate liming control is enforced across all non-GBR LTE bearers that are associated with a device, independent of the bearer's termination point (APN). The LTE network will allow rates up to the value of the UE-AMBR for a device, and once above this value, data rates will be throttled. Once the device's aggregate bit rate falls below the UE-AMBR value, the system will no longer throttle data.

There are bandwidth management controls that enable the NPSBN to allocate specified amounts of bandwidth to LTE dedicated GBR bearers. GBR bearers are often used, for example, by streaming real-time audio and video applications. The bandwidth management controls for GBR bearers consist of a guaranteed bit rate (GBR) as well as a maximum bit rate (MBR) for each LTE bearer. The guaranteed bit rate value is the minimum bandwidth provided by NPSBN should the bearer be admitted to the LTE system. The admission process allocates enough bandwidth to assure delivery of data up to the value of the GBR. This bandwidth is available to the device independent of the NPSBN congestion levels. The maximum bit rate (MBR) is the absolute maximum amount of bandwidth an LTE GBR bearer can utilize once it has been admitted. The MBR allows for additional bandwidth utilization above the GBR value assuming there are resources available in the NPSBN. Once the MBR bandwidth is exceeded, the NPSBN will throttle the excessive bandwidth usage. The GBR and MBR limits essentially create a minimum and maximum amount of bandwidth that can be used for a given GBR bearer. These GBR controls are only applicable to GBR bearers.

The combination of the controls described provides flexibility in allocation of bandwidth in the NPSBN. These controls can be set by the authorized User Entity administrator to meet the required needs of the responders who are utilizing bandwidth on the NPSBN.

APPENDIX D: TRANSPORT PRIORITY DETAILS

This appendix is for informational purposes and does not include requirements or recommendations.

The LTE characteristic that is utilized to determine LTE EPS transport priority is the LTE assigned QCI for the LTE bearer (see Appendix 0). The LTE QCI for the EPS bearer is chosen from the standards defined set of QCIs (3GPP TS 23.203). One means to specify transport architecture is to utilize the QCI and map the QCI to the EPS tunnel header Diffserv CodePoint (DSCP) in a manner such that the transport treatment at the DSCP layer is consistent with the priority of the LTE QCI. The mapping of the QCI to the DSCP is not specified in 3GPP standards, thus is operator configurable.

The use of DSCP is a means of prioritizing transport, mapping of the LTE QCI to the appropriate class and per hop behavior specified by the IETF. The following are recommendations that could be implemented to differentiate the EPC-based bearers to provide end-to-end QoS based transport.

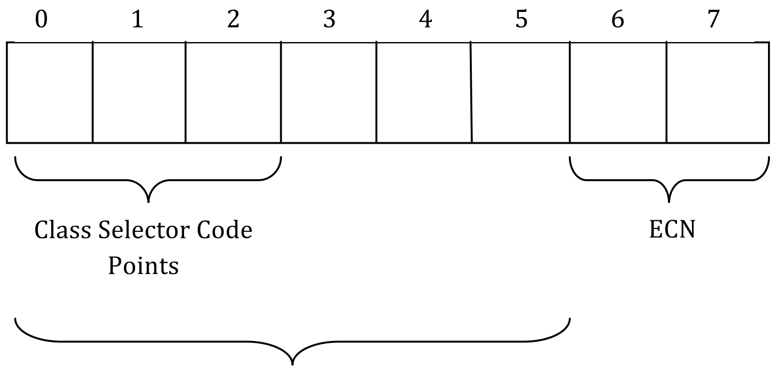
The Expedited Forwarding DSCP class provides transport prioritization that optimizes for low delay, loss, and jitter. Voice services have requirements that are within these categories, thus it is recommended that the voice based QCI 1, as well as QCI 7 would be mapped to the EF DSCP class. The signaling QCI (QCI 5) could also be mapped to the EF DSCP class due to the importance of the signaling traffic carried over QCI 5 bearers.

The Assured Forwarding classes offer a range of performance attributes. Each AF class has 3 levels of packet drop precedence. The higher priority AF classes SHOULD be utilized for QCI transport associated with video and related services. This would map a high priority AF class (i.e., AF Class 4) to QCI 2 and QCI 3. For non-GBR video services, a lower AF class (i.e., AF Class 2) could be mapped to QCI 6. QCI 4 could be mapped to an intermediate AF Class (i.e., AF Class 3) due to the low packet loss rate.

The Best Effort DSCP class provides packet delivery that is provided by the network nodes after the other DSCP classes (i.e. EF, AF) have been satisfied. Thus, it would be consistent to map the BE DSCP class with best effort QCI(s). Based on the 3GPP definitions, QCI 8 and QCI 9 would be mapped to the BE DSCP class.

IETF DSCP Info

The DSCP is provisioned as part of the ToS IP header. The six most significant bits of the Type of Service (ToS) IP header byte are defined as the DSCP. These six DSCP bits are mapped to the per hop behavior (PHB) classes or categories. PHB describes what a Diffserv class should experience in terms of loss, delay, and jitter. A PHB determines how bandwidth is allocated, how traffic is restricted, and how packets are dropped during congestion.



DSCP (RFC 2474)

The three most significant bits of the DSCP are used as class selector bits (CS), these bits are used to maintain backward compatibility with network devices that use the ToS Precedence field, and as such DiffServ defines the Class Selector. The Class Selector codepoints are of the form 'xxx000.' The first three bits are the IP precedence bits. Each IP precedence value can be mapped into a DSCP class.

Class Selector Name	DSCP Value	IP Precedence	DSCP Class
CS7	56 [111000]	7	---
CS6	48 [110000]	6	---
CS5	40 [101000]	5	Expedited Forwarding
CS4	32 [100000]	4	Assured Forwarding 4
CS3	24 [011000]	3	Assured Forwarding 3
CS2	16 [010000]	2	Assured Forwarding 2
CS1	8 [001000]	1	Assured Forwarding 1
CS0	0 [000000]	0	Best Effort

Three PHBs are defined in DS based on the forwarding behavior required:

- Expedited Forwarding (EF) PHB—Class selector bits set to 101, optimal for low-loss, low-latency traffic
- Assured Forwarding (AF) PHB—Class selector bits set to 001, 010, 011, or 100, gives assurance of delivery under prescribed conditions
- Best-effort class—Class selector bits set to 000, typically best-effort traffic

The IETF defines Expedited Forwarding (EF) behavior as having characteristics of low delay, low loss, and low jitter. These characteristics are suitable for voice, video, and other real-time services.

The IETF defines the Assured Forwarding (AF) behaviors to provide assurance of delivery as long as the traffic does not exceed some subscribed rate. The Assured Forwarding standard specifies four guaranteed bandwidth classes and describes the treatment each should receive. It also specifies drop preference levels, resulting in a total of 12 possible AF classes. Traffic that exceeds the subscription rate faces a higher probability of being dropped if congestion occurs. The AF behavior group defines four separate AF classes (see table below). Within each class, packets are given a drop precedence (high, medium, or low). The combination of classes and drop precedence results in twelve separate DSCP encodings. Should congestion occur between classes, the traffic in the higher class is given priority. If congestion occurs within a class, the packets with the higher drop precedence are discarded first.

Drop Precedence	Class AF1	Class AF2	Class AF3	Class AF4
Low Drop	AF11 (DSCP 10)	AF21 (DSCP 18)	AF31 (DSCP 26)	AF41 (DSCP 34)
Medium Drop	AF12 (DSCP 12)	AF22 (DSCP 20)	AF32 (DSCP 28)	AF42 (DSCP 36)
High Drop	AF13 (DSCP 14)	AF23 (DSCP 22)	AF33 (DSCP 30)	AF43 (DSCP 38)

The default PHB is used for traffic that does not meet the requirements of any of the other defined classes. The default PHB has best effort forwarding characteristics.

Differentiated Services is described and defined in the following RFCs:

- RFC 2474, Definition of the Differentiated Service Field (DS Field)
- RFC 2475, An Architecture for Differentiated Service
- RFC 2597, Assured Forwarding PHB Group
- RFC 2598, An Expedited Forwarding PHB
- RFC3168, The Addition of Explicit Congestion Notification (ECN) to IP

APPENDIX E: TASK GROUP AND WORKING GROUP PARTICIPANTS

2011-2012 Task Group Participants:

Users:

Edgardo Barreto, Dr. Michael Britt, State of AZ; Todd Crosby, Dave Buchanan, NPSTC; Cynthia Cole, State of TX; M. Jay Farr, Arlington PD; Jeff Farris, Honolulu FD; Warren Izumigawa, Patrick Kenealy, State of MI; Frank Kiernan, Joe Kuran, Wayne Masuda, Pam Montanari, Pinellas County, FL; Bill Schrier, Tom Sorley, NPSTC; Alvin Sunahara, Robert Wilson, Wyoming DOT and Patrol

Government/Standards:

Darcy Anton, Michael Barone, Jeff Bratcher, PSCR; Yoon Chang, Sandy Dawkins, NPSTC; Rick Galway, NPSTC; Behzad Ghaffari, Gina Harrison, Barry Luke,NPSTC; Ralph Parker, Next Generation Communication Services; Bob Pavlak, John Powell, NPSTC; Rasoul Safavian, Andrew Thiessen, PSCR; Marilyn Ward; NPSTC

Industry:

Wim Brouwer, Brian Daly, Martin Dolly, Chris Fischer, James Garrahan, Tom Hengeveld, Harris; Gordon Hsu, Reid Johnson, Guy Jouannelle, Ajit Kahaduwe, NSN; Brian Kassa, Frank Korinek, Jim Marocchi, MSI; Roy McClellan, Trent Miller, Motorola Solutions; Peter Musgrove, Val Oprescu, MSI; Don Newberg, Doug Onhaizer, Dewayne Sennett, DJ Shyy, Keith Stanley, Lincoln Unruh, Curt Wong, NSN

2014-2015 Working Group Participants:

Users:

Karen Allen, Dr. Michael Britt, State of AZ; Dave Buchanan, NPSTC; Cynthia Cole, State of Texas; Kimberlei Coleman, Todd Crosby, Jay English, Barry Fraser, Chris Kindelspire, John Lenihan, NPSTC; Guy Mallery, Brian Moore, Charles Musgrove, Bill Petrea, William Springer, Alvin Sunahara, Greg Sundie, Terek Taillon

Government/Standards:

Gina Harrison, Ryan Hedgpeth, Barry Luke, NPSTC; Gabriel Martinez, Ralph Parker, Next Generation Communication Services; John Powell, NPSTC; Carollyn Taylor, Marilyn Ward; NPSTC

Education/Industry:

Dominick Arcuri, Natalie Baker, Rajesh Benjamin, Wim Brouwer, ALU; Martin Dolly, Bharat Doshi, Tewfik Doumi, Jim Eastwood, David Eierman, Motorola Solutions; Reid Johnson,Harris; Shawn Lefebre, Trent Miller, Peter Monnes, Prithu Prakash, Mark Raczynski, Patrik Ringqvist, Gino Scribano, DeWayne Sennett, Dean Skidmore