TIA COMMITTEE TR-8
Broadband Data (TR-8.8)

TITLE: TIA-4973.211

Requirements for the Mission Critical Priority and QoS Control Service

---

CONTRIBUTION SOURCE: Respectfully submitted by Trent Miller
Motorola Solutions

DATE: May 13, 2014
PRINT DATE: 13 May 2014:11:25

ABSTRACT: This document provides requirements for a service to manage priority and quality of service for users sharing a broadband transport network.

RECOMMENDATION: This document is sent out for review by the committee members for consideration as part of a proposed series of standards.

COPYRIGHT STATEMENT

TIA DRAFT PROPOSAL

Requirements for the Mission Critical Priority and QoS Control Service

TR-8.8 Broadband Data

TIA-4973.211

Document Number: 8.8_12-004765
Rev 0.80
May 13, 2014

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Foreword

(This foreword is not part of this standard.)

This document is being promulgated and will be maintained by the TR-8.8 Private Radio Technical Standards committee, responsible subcommittees, and working groups under the sponsorship of the Telecommunications Industry Association.

It describes requirements for a mission critical Priority and QoS Control Service specifically intended to operate over LTE and other broadband networks.

Patent Identification

The reader's attention is called to the possibility that compliance with this document may require the use of one or more inventions covered by patent rights. By publication of this document no position is taken with respect to the validity of those claims or any patent rights in connection therewith. The patent holders so far identified have, we believe, filed statements of willingness to grant licenses under those rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such licenses.

The following patent holders and patents have been identified in accordance with the TIA intellectual property rights policy:

No patents have been identified.

TIA shall not be responsible for identifying patents for which licenses may be required by this document or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Trademark Identification

The following trademarks are referenced in this specification:

3GPP® and LTE® are registered trademarks of the European Telecommunications Standards Institute (ETSI).

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

DOCUMENT REVISION HISTORY

Table 1: Document Revision History

Version	Date	Description
0.1	1/22/2013	Initial contribution from MSI
0.2	1/23/2013	Initial version for TR8.8 review.
0.3	6/9/2013	Added introduction from Harris (Hengeveld) and Alcatel Lucent (Dolan). Resolved issues from TR88-13-024.
0.4	3/3/2014	Updates from TR8.8 review (comment matrix TR88-13-111-R12).
0.5	4/14/2014	Updates from TR8.8 review of TR88-14-011-R1.
0.6	4/16/2014	Continued updates from TR8.8 review of TR88-14-011-R1.
0.7	5/2/2014	Updates from TR8.8 review (comment matrix TR88-14-022-R4).
0.8	5/13/2014	Editorial cleanup.

1 Introduction

This specification identifies requirements for a Priority and QoS Control Service (PQCS) intended to operate over wireless broadband networks, including, particularly, the National Public Safety Broadband Network.

This specification comprises a portion of the requirements of the TIA-PN-4973 suite of standards. This specification identifies requirements for a PQCS over Broadband Networks in the context of the Broadband Data Protocol Standards Overview [5], and this section provides an introduction, including the scope of the specification, abbreviations and references. To facilitate the analysis and understanding of the requirements, a set of informative models of the standardized services is presented in Section 2. Section 3 enumerates the normative requirements that are the basis of the standards to be developed.

1.1 Scope (Informative)

Priority and QoS refers to the access and control of system resources; especially with respect to a wireless broadband network. While the lion's share of attention is paid in this specification to wireless broadband network resources, this specification is not limited thereto. Transport network, backhaul, and interconnected systems are all considered.

The public safety broadband network is a challenging environment. Various types of users (e.g., first responders, second responders, etc.) with various disciplines (police, fire, EMS , etc.) and all types of applications (voice, video, data) all share the same resources. This creates an unprecedented environment for the management of resources for a public safety system. Conventional LMR systems have dedicated resources for Push-to-Talk, and there is traditionally only limited sharing of a system between disciplines. Trunked LMR systems improve sharing between disciplines, but still don't have to share resources like LTE all-IP users.

Priority, as used herein, refers to the ability for a given user to access and obtain resources from the broadband network. Once a user has been granted resources by the system, quality of service (QoS) refers to the specific attributes (e.g., latency, packet loss rate) that govern the experience of content exchange with the user. Users of the public safety broadband network need a consistent and deterministic service for real-time management of priority and QoS.

Commercial cellular network operators typically offer elevated priority to premium customers on a statically assigned basis (i.e., the customer's priority only changes with changes in their subscription level). While this is sufficient for commercial use, public safety users require priority services that are *situational.* The sheriff at a traffic stop does not require the same priority on the broadband network as a patrolman exchanging gunfire at a bank robbery. Pre-emption of lower-priority resources is essential in order to provide resources to the highest priority incidents.

Mission critical communications require immediate access to resources. Many factors can impact the resources available to a given traffic flow: number of users, number of incidents, distance to cell antenna, interference, etc. Further, many factors can contribute to wireless congestion at a cell. For this reason, Priority and QoS capabilities for public safety need to consider the dynamic situational aspects of responders. It is insufficient to statically assign a priority to a given responder that will be sufficient for all situations.

Another important aspect of priority and QoS is that it is based on the user and not a given device. In the commercial cellular world, users obtain a personal device and that device and its telephone number are assumed to be associated with a user. In the public safety world, devices are re-used across shifts (e.g., tablets, radios, fire trucks, etc.). It is not realistic to assume that all public safety broadband devices are personally issued. For example, an incident commander can pick up a shared laptop belonging to her agency and sign-in, or can be assigned to a vehicle having a fixed-mount laptop in the vehicle. Therefore, public safety priority and QoS needs to be derived for a user also taking into account the application(s) that he/she is currently invoking, and applied to the devices currently being used by the user. The type of user is one of many factors affecting a Subscriber's overall priority and QoS state. See sections 3.1.3 and 3.1.4 for more information.

Responders are trained today with procedures that have taken decades to perfect. Any service provided to responders has to complement their existing workflow. This service attempts to avoid distracting a user from the mission by requiring him/her to enter a broadband maintenance terminal or to become aware of the broadband network's detailed prioritization parameters. In this specification, prioritization is integrated into usage patterns familiar to the user (e.g., the emergency button).

Applications can be deployed by various domains utilizing the network. For example, telephony might be deployed nationally and push-to-talk might be deployed regionally by a state (e.g., in a separate APN). The priority and QoS capabilities described herein are intended to consistently govern resources for all applications, regardless of the entity (national, regional, local) that is operating the application.

This specification defines a Priority and QoS Control Service (PQCS) to address these complex and varied needs. The PQCS:

- Allows Subscribers, other users, and other services to control and coordinate dynamic priority changes;
- Translates a coherent model of PS state (responder emergency, etc.) to service effecting controls in a Subscriber's transport network;
- Is consistent with the principles expressed by the NPSTC Local Control Task Group [4] the Priority and QoS Task Group [3] and the Broadband Data Protocol Standards Overview [5]; and,
- Supports "all IP" broadband networks (e.g., LTE). The PQCS does not support circuit-switched networks.

1.2 Scope (Normative)

This document pertains to the control of Priority and Quality of Service (QoS) for communications on a wireless broadband network using Internet Protocols (IP). This document describes requirements for a mission critical Priority and QoS Control Service for a wireless broadband network. The network and its resources are assumed to be shared by different classes of users, and different types of applications. Prioritization is the ability to determine which resource requests should be granted and which granted resources should be discontinued or pre-empted. This document includes requirements to determine a user's default priority on the

broadband network, and also provides requirements for dynamic prioritization changes to meet situational needs. Quality of Service is the ability to ensure that IP packet flows associated with different applications satisfy performance objectives needed for the applications to operate. The requirements contained herein allow an operator to define consistent and deterministic policies to moderate usage of the shared wireless broadband network. Requirements are further provided for end-users and applications to dynamically influence policy selection.

1.3 Abbreviations

1

1.4 Definitions

Access Class Barring: A 3GPP LTE method to prevent overloading of radio resources (e.g., the random access channel) by slowing or preventing communication with the LTE system by certain classes of device (Managed UT). 33

Access Priority: A form of Subscriber priority that governs a Managed UT's ability to initiate communications with the WTN. 12

Admission Priority: A form of priority that governs whether a request for resources from an Application Service, Application Client, or Subscriber will be granted by the WTN..... 13

Agency O&M User: A specialized Subscriber that can provision & monitor Subscribers, and configure the PQCS for the user's associated Agency. 16

Agency: An agency is an enterprise to which one or more Subscribers who generally perform the same function are associated. Public Safety agencies can be of federal, state, county, city, local, borough, and tribal scope. Agencies need not be associated with first responder functions. Examples include: state police, county fire, city emergency medical services, city streets and sanitation. 2

Application Client: Applications (Apps) or other mobile system entities that are authorized to affect or monitor the priority state of one or more Subscribers. Usually, the Application Client operates on a Managed UT. In some cases (e.g., Immediate Peril), a Subscriber will choose an Application Client on their Managed UT to receive dynamic PQCS treatment. 12

Application Service: Applications or other fixed network system entities that are authorized to affect or monitor the priority state of one or more Subscribers. In a traditional client-server model (e.g., MC-PTT TA \l "MC-PTT: Mission Critical Push-to-Talk" \s "MC-PTT" \c 8), back-end managed server equipment would host the MC-PTT TA \l "PTT: Push-to-Talk" \s "PTT" \c 8 Application Service and the Managed UT would operate an Application Client (e.g., MC-PTT client). 12

Authorized Administrator: Either an Agency O&M User or an Operator O&M User or both. ... 16

Default Priority: A collection of attributes tracked for each Subscriber by the PQCS that are used in the determination of a Subscriber's priority when no Dynamic Priority capabilities have been activated. 13

Dynamic Admission Priority Control: The usage of Responder Emergency, Immediate Peril, or Incident Severity by a Subscriber or Supervisory Subscriber to influence the priority and QoS selected by the PQCS. 30

Dynamic Priority: A collection of attributes tracked for each Subscriber by the PQCS that identify special, potentially life-threatening conditions, that are used in the determination of a Subscriber's priority. Typically, activation of Dynamic Priority attributes result in heightened priority for a Subscriber. 14

Immediate Peril: A Dynamic Priority attribute that indicates an imminent and ongoing threat to life or property. An Immediate Peril condition may be declared by a Subscriber for herself/himself or by an authorized Subscriber on behalf of another Subscriber. For more information, see section 2.2. 14

1.5 References

The following documents contain provisions that, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this document are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. The American National Standards Institute (ANSI), TIA, 3GPP, Wi-Fi Alliance, and other organizations maintain registers of currently valid standards published by them.

References marked as "(INFORMATIVE)" are for informational purposes only and do not constitute normative provisions of this document.

[1] Public Law 112-96: The Middle Class Tax Relief Act of 2012. s.l. : US GPO, 2012. (INFORMATIVE).

[2] TIA-102 Documentation Suite Overview. TIA. June 2012. (INFORMATIVE). TSB-102-B.

[3] Priority and QoS in the Nationwide Broadband Network. National Public Safety Telecommunications Council. Rev 1.0, s.l. : National Public Safety Telecommunications Council, April 2012. (INFORMATIVE).

[4] Local Control in the Nationwide Public Safety Broadband Network. National Public Safety Telecommunications Council. Rev F, s.l. : National Public Safety Telecommunications Council, March 2012. (INFORMATIVE).

[5] Broadband Data Protocol Standards Overview. TIA. May 2013. (INFORMATIVE). TSB 4973.000.

[6] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture. s.l. : 3GPP, 2014. 3GPP TS 23.203. (NORMATIVE).

[7] Requirements for Mission Critical PTT and Related Supplementary Services. s.l. : TIA, 2014. TIA-4973.201. (INFORMATIVE).

[8] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service accessibility. s.l. : 3GPP, 2014. 3GPP TS 22.011. (NORMATIVE).

1.6 Nomenclature

Herein, the words "SHALL", and "REQUIRED", in capital letters, identify items that are absolute requirements of this specification. The phrase "SHALL NOT" in capital letters, identifies items that are prohibited by the specification.

The words "SHOULD" and "RECOMMENDED" identify items for which there may be valid reasons in particular circumstances to ignore the item, but for which due considerations of the full implications of so doing should be considered before choosing a different course. Likewise the phrase "SHOULD NOT" identifies items for which circumstances may exists in which the item can be reasonably ignored.

The words "MAY" or "OPTIONAL" in capital letters, identify items that are truly options. One vendor may choose to include the item while another may omit the item, without impact on the core interoperability of the protocol.

Lower case instances of the above defined "specification words" have their common meaning in Standard English, and related statements should not be taken as normative.

In the specification, the phrase "by some means" means that the method by which the indicated action is effected is outside of the scope of this specification. It may be established by some other standard, or be left to the developer.

2 Priority and QoS Service Requirements Model (Informative)

2.1 System Model

Figure 1 illustrates the system model for the Priority and QoS Control Service (PQCS). In the figure, transport reference points are illustrated with dashed lines, while application level reference points are illustrated with solid lines.

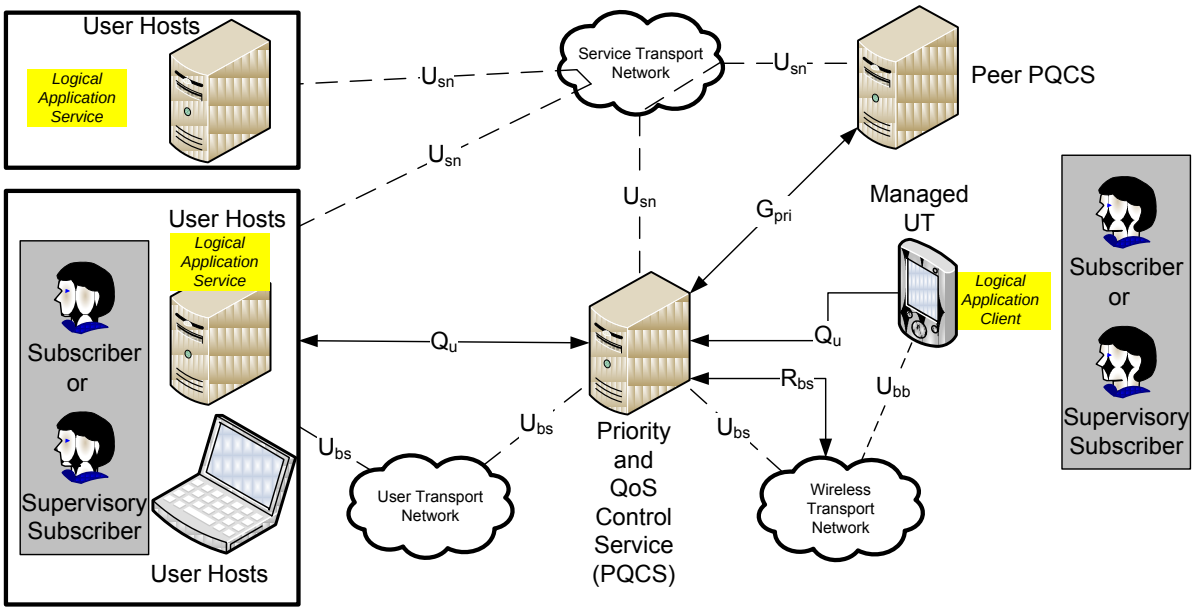

Figure 1: Priority and QoS Control Service System Model

Logically, the PQCS functions as a single service for the entire WTN. Physically, the PQCS may have many peers that each support different geographical segments of the WTN or different Subscriber populations. User Hosts represent computer equipment that contains Application Services providing Subscribers with access to the PQCS. Similarly, the Managed UT represents a user terminal that contains Application Clients providing Subscribers with access to the PQCS.

Transport networks carry the IP traffic associated with the PQCS. For the purposes of this specification, Transport Networks are further subdivided into the following classes:

- Wireless Transport Networks (WTNs) – Transport Networks which carry the Application Client traffic of a Managed UT and which support dynamic priority effecting capabilities that can be managed by the PQCS.
- Service Transport Network (STNs) – Transport networks associated with the interconnection of Peer PQCS instances, and the interconnection of Application Services resident in the same network domain.
- User Transport Network (UTNs) – Transport networks that carry the traffic associated with Subscribers and Application Services that wish to affect or monitor Subscriber

priority. Subscribers and Application Services can employ a Wireless Transport Network or a Service Transport Network as a User Transport Network.

The U_{sn}, U_{bs}, and U_{bb} reference points illustrated in Figure 1 are as described in [5]. The R_{bs} reference point is also described in [5], representing the services provided by a transport network that are available to external (e.g., transport network) services. The Q_u reference point represents functionality provided to a Subscriber, Application Service, or Application Client by the PQCS. Q_u corresponds to distinct capabilities provided at the E_n reference point of [5]. Finally, the G_{pri} reference point corresponds to the priority and QoS capabilities provided at the G reference point of [5]. Q_u and G_{pri} are described in more detail in section 2.3.1.

2.2 Priority Model

In 2012, the National Public Safety Telecommunications Council (NPSTC) formed a number of task groups, including a Priority and QoS task group [3] for broadband. This group was comprised of responders, government representatives, and industry participants, and the task group identified several priority and QoS concepts, as utilized in this section.

Figure 2 shows the sequential steps a Subscriber's Managed UT undergoes in order to obtain resources from a WTN. It is worth noting that the steps illustrated in the following figure represent the ideal case for a WTN. Not all types of WTN (e.g., Wi-Fi) support each of the following steps.

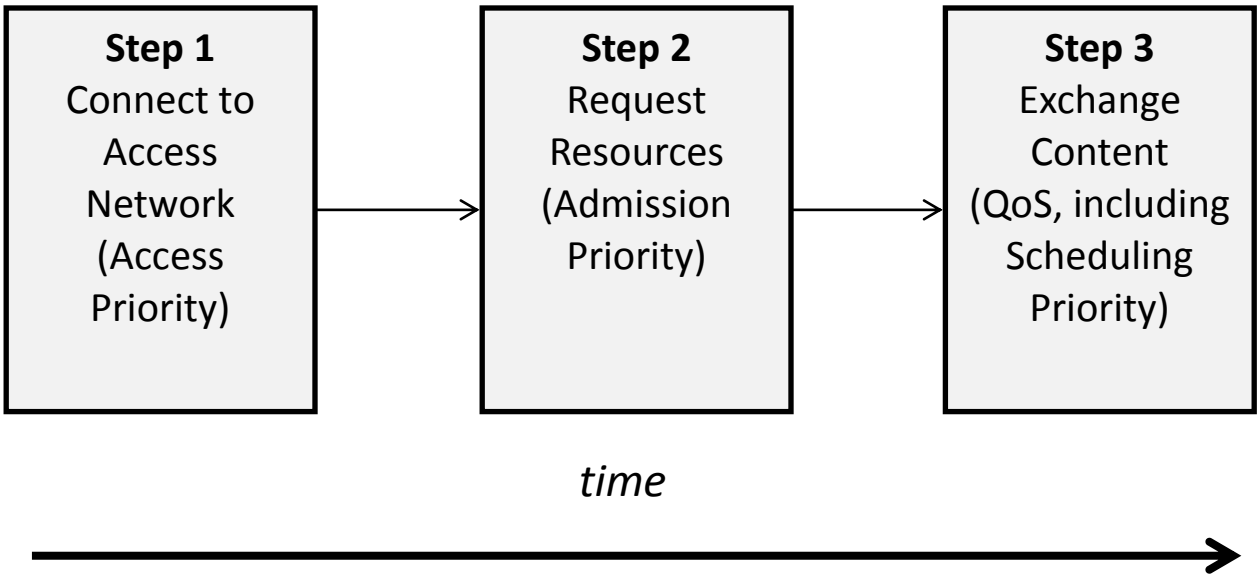

Figure 2: Priority and QoS Steps

- **Step 1** – When a Subscriber's Managed UT has suitable priority, it is authorized to communicate with the WTN. Access Priority is a means to mitigate "access storms" seen by wireless transport networks when a large number of UTs attempt to access a single cell in a short period of time. Access Priority is a method for access network

administrators to give system access to those devices that most need to interact with the WTN. Lower priority devices are required to wait before accessing the system. Access Priority requirements are defined in section 3.1.2.

- **Step 2** – When devices or the WTN determine that resources are required to exchange content, a request for resources is initiated. Resources can be point-to-point (unicast) or point-to-multipoint (broadcast and multicast). There is a need to fairly and consistently moderate all resource requests from all WTN users. PQCS Admission Priority is derived for a Subscriber based on the Subscriber's default and dynamic attributes. Admission Priority requirements are defined in sections 3.1.3 and 3.1.4.
- **Step 3** – Once a resource request has been granted by the WTN, content is scheduled for delivery over various links, including wireless links. Scheduling Priority requirements are defined in section 3.1.5.

For the purposes of this specification, each Subscriber is modeled as illustrated in Figure 3[1].

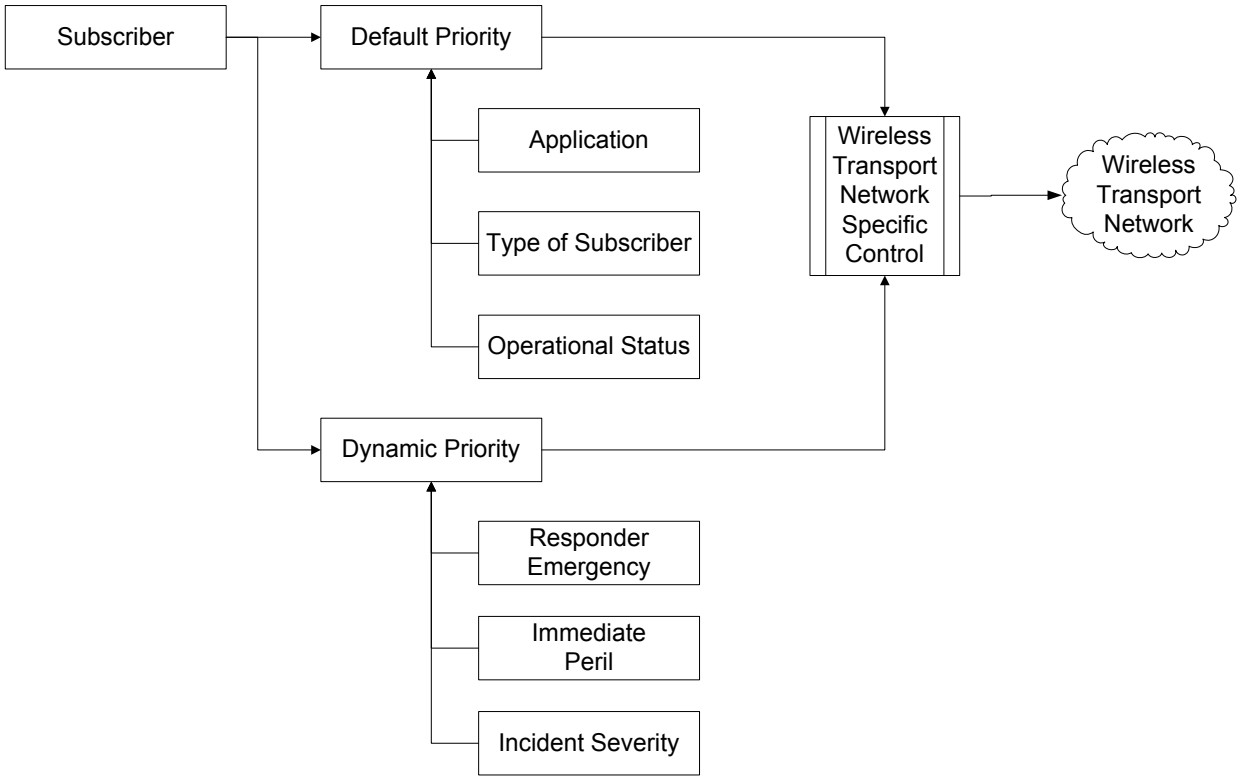

Figure 3: Priority Model

- **Default Priority** – the PQCS examines several attributes about a Subscriber and derives their normal day-to-day priority on the system. The goal of Default Priority is to capture

[1] This model draws heavily on the work published by the National Public Safety Telecommunications Council in [3].

default priority attributes as determined by existing steps and activities which are already part of public safety workflows. In other words, the default priority in the PQCS seeks to avoid adding new and/or disruptive steps for priority and QoS. Those attributes are:

- The **application** being used by the Subscriber (e.g., MC-PTT). Resources for applications on the WTN are categorized and given a relative priority to other applications. A Subscriber that is using multiple applications may have a different default priority per application.
- The **Type of Subscriber** considers characterization of the user using attributes that change infrequently:
  - the Subscriber's *class* (e.g., primary user/first responder, secondary user, etc.) on the WTN. Generally, primary users (e.g., first responders) are anticipated to be assigned a higher priority than secondary users; and
  - the Subscriber's *organizational role* (e.g., the chief of police). This essentially represents the subscriber's relative priority within their class and agency.
- The Subscriber's **Operational Status** considers what the responder is doing at the moment priority is evaluated. The operational status reflects two things:
  - whether the Subscriber is *on or off duty*; and
  - whether the Subscriber is operating *in or out her/his Jurisdictional Area*. The jurisdictional status is intended to prevent the unintentional consumption of resources by a responder entering your jurisdictional area. For example, a public safety user who is on patrol in her/his jurisdictional area can have a different Operational Status, and hence priority, than one who is traveling to court, out of jurisdiction.

It is envisioned that the consideration of these attributes will fairly and consistently address the majority of mission critical incidents. However, there are special situations that arise (e.g., a threat to a responder's life) which require an ability to override a user's default priority.

- **Dynamic Priority** – a human (e.g., responder, dispatcher, etc.) who has explicitly chosen to provide an indication to the PQCS that a special condition has occurred or is about to occur, requiring modified priority on the WTN. Dynamic Priority is typically used for serious incidents or threats to human life, requiring guaranteed and immediate resources. A Subscriber's dynamic priority is derived from a combination of three attributes:
  - **Responder Emergency** – A Subscriber has a "Responder Emergency" when the Subscriber or Supervisory Subscriber has declared personal danger to the Subscriber's life and limb. Responder Emergency corresponds to the emergency state of traditional public safety LMR systems. Responder Emergency is a binary attribute.
  - **Immediate Peril** –"Immediate Peril" identifies a condition in which a Subscriber is responding to an imminent and ongoing threat to life or property. Like Responder Emergency, Immediate Peril is a binary attribute.
  - **Incident Severity** – "Incident Severity" is a multi-valued attribute that considers the type of incident the responder is serving and the responder's assigned role within the

incident. The Incident Command System (ICS) defines three relative priorities of incidents:

1. Life Safety
2. Incident Stabilization
3. Preservation of Property/Environment

In the ICS framework, responders are assigned a specific task/role, which can be used to help prioritize resources with the PQCS. This incident role exists while the responder is supporting an ICS incident. This incident role is different than the Responder's long-lived organizational role.

The Subscriber attributes in Figure 3 do not apply universally to each of the priority steps from Figure 2. For example, step 1 governs whether a Managed UT should even be able to connect and register with the WTN, and thus the specific application that the Subscriber wishes to use is immaterial for the initial connection. Table 2 identifies which Subscriber attributes are utilized in priority determination of each priority step.

Table 2: PQCS Subscriber Attributes for Each Priority Step

PQCS Subscriber Attribute	Applies to Access Priority (Step 1)?	Applies to Admission Priority (Step 2)?	Applies to Scheduling Priority (Step 3)[2]?
Default Priority			
Application	No	Yes	Yes
Type of Subscriber	Yes	Yes	Yes
Operational Status	No	Yes	Yes
Dynamic Priority			
Responder Emergency	Yes	Yes	Yes
Immediate Peril	Yes	Yes	Yes
Incident Severity	Yes	Yes	Yes

[2] Changes to scheduling priority for WTN resources may result in a service interruption (i.e., in some cases the WTN resource must be discontinued and restarted to implement the scheduling priority change).

2.3 Context Diagrams

2.3.1 Service Context

Figure 4 illustrates the reference points that comprise the context of the PQCS. These are described in the following subsections. This specification uses the term "authorized administrator" to refer to either an "Agency O&M User" or an "Operator O&M User" or both.

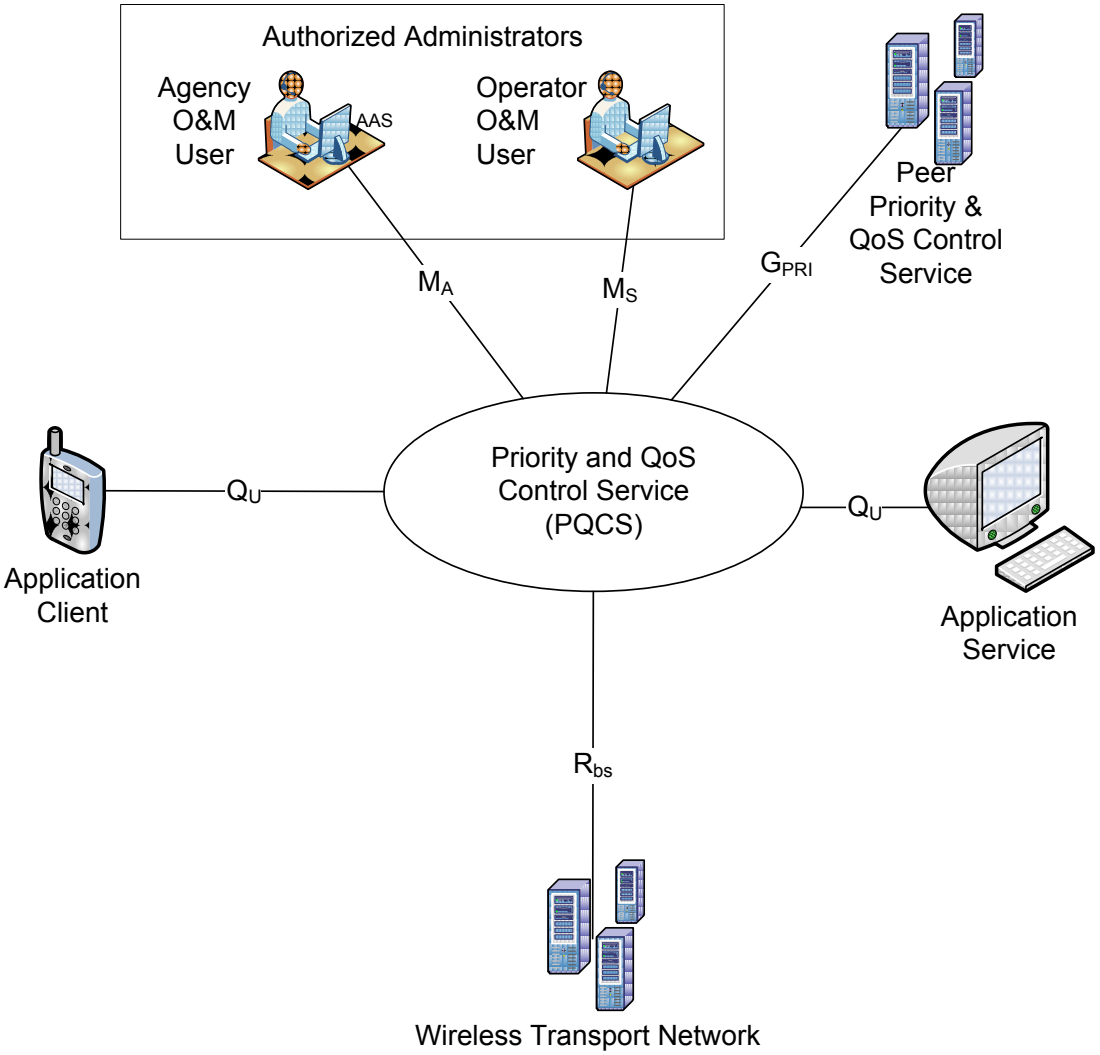

Figure 4: Service Context

2.3.1.1 Q_u Reference Point

The Q_u reference point identifies functions and interfaces operating between Applications (Client and Services) and the PQCS. These include, for example:

- Registration and association of a Subscriber to one or more Managed UTs;
- Authentication and authorization of Subscribers seeking access to view and affect their own priority and QoS attributes;
- Authentication and authorization of Supervisory Subscribers seeking access to view and affect priority and QoS attributes of another Subscriber;
- Reporting of a Subscriber's location
- Forming and managing PQCS groups of Subscribers;
- Session resource control for Application Clients and Application Services;
- Notification of changes to a Subscriber regarding changes to their own Subscriber attributes; and,
- Notification of changes to a Supervisory Subscriber regarding the changes to another Subscriber's attributes.

2.3.1.2 G_{pri} Reference Point

The G_{PRI} reference point identifies the functions and interfaces between peer PQCS instances, which are defined by this specification. The G_{PRI} reference point is used to locate the PQCS instance serving a particular Subscriber for the Subscriber's serving WTN.

2.3.1.3 M_A Reference Point

As defined in this series of standards, M_A is specifically an interface between the service (PQCS) and an Agency Administration Server (AAS). The AAS is outside the scope of this specification and is assumed to provide suitable interfaces and business logic in support of its Agency O&M Users. M_A is assumed to utilize an IP network interface designed for extensibility to accommodate differences in manufacturer features and implementations, while still providing all required functionality per this specification. Functions of the M_A reference point include, for example:

- Configuration of the agency's jurisdictional boundaries;
- Configuration of applications (name, transport information, pre-emption settings, group capabilities, etc.);
- Configuration of applications that should receive elevated priority during a Responder Emergency; and,
- Provisioning of Subscribers and Supervisory Subscribers

- Fault detection and maintenance of Managed UTs, Application Clients, Application Services, the PQCS, and the WTN[3]

2.3.1.4 M_S Reference Point

Some Subscribers are assumed to be managed by the WTN operator. The M_S reference point identifies the functions and interfaces between equipment serving an Operator O&M User and the PQCS. These include, for example:

- Configuration of the agency's jurisdictional boundaries;
- Configuration of applications (name, transport information, pre-emption settings, group capabilities, etc.);
- Configuration of applications that should receive elevated priority during a Responder Emergency;
- Provisioning of Agency O&M Users; and,
- Provisioning of Subscribers and Supervisory Subscribers
- Fault detection and maintenance of Managed UTs, Application Clients, Application Services, the PQCS, and the WTN[3]

2.3.1.5 R_{bs} Reference Point

The R_{bs} reference point represents services provided by the Wireless Transport Network to the PQCS in order to effect priority and QoS changes for a Subscriber's associated Managed UT(s). While this reference point corresponds to functions and protocols provided by the WTN, it is within the scope of this specification to define capabilities that would influence the way in which the PQCS uses this reference point.

2.3.2 Application Client Context

Figure 5 illustrates the reference points that comprise the context of the Application Client used for Subscriber priority control. The Q_u reference point is described in section 2.3.1.1 and the U_{bb} reference point is described in section 2.1 and [5]. The A_u reference point is described in the following section.

[3] Management of the WTN, Application Clients, and Application Services (other than the PQCS itself) is out of scope of this specification.

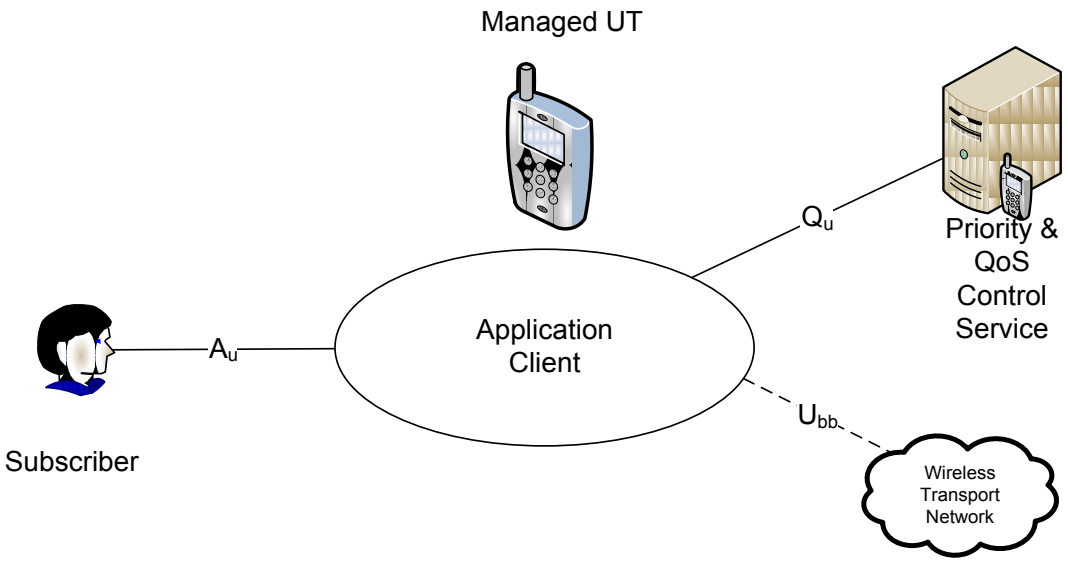

Figure 5: Application Client Context

2.3.2.1 A_u Reference Point

The A_u reference point represents the man-machine interface between an Application Client and Subscriber. The A_u reference point is outside of the scope of this series of specifications.

3 Broadband Transport Service Requirements (Normative)

3.1 Priority and QoS Control Service Requirements

3.1.1 General Priority and QoS Control Service Requirements

The following requirements concern the Priority and QoS Control Service, including capabilities for the Wireless Transport Network. WTN-specific requirements for this section can be found in section 3.1.15.

1) It SHALL be possible for the PQCS to track Subscriber priority and QoS attributes at run-time.

2) Using the PQCS, it SHALL be possible to associate one or more Managed UTs with a Subscriber.

3) Using the PQCS, it SHALL be possible to associate one or more Subscribers with a Managed UT.

   Note: The intent of this requirement is to support cases of multiple Subscribers sharing a Managed UT, such as a vehicular modem.

4) Within the confines of a Wireless Transport Network, the PQCS SHALL apply a consistent set of deterministic priority and QoS rules and policies to all Subscribers of the particular Wireless Transport Network and to roaming users of other networks utilizing the Wireless Transport Network.

5) It SHALL be possible for the PQCS to apply priority and QoS for a Subscriber in all parts of the WTN's coverage.

6) The PQCS SHALL provide a point of contact through which an authorized Supervisory Subscriber can dynamically affect and monitor the priority and QoS of himself/herself and other Subscribers.

7) The PQCS SHALL provide a point of contact through which an authorized Subscriber can dynamically affect and monitor his/her own priority and QoS.

8) The PQCS SHALL provide a point of contact through which authorized Application Clients and Application Services can dynamically affect and monitor the priority and QoS parameters of Subscribers and roamers to the WTN.

9) The PQCS SHALL be able to affect the priority and QoS of Subscribers who are operating in another administrative area of the WTN.

   Note: The intent of this requirement is to indicate that the PQCS can operate ubiquitously across the WTN, regardless if the network is comprised of one or more administrative areas.

10) The PQCS SHALL provide a similar priority and QoS experience for a Subscriber regardless of the Wireless Transport Network being used by the Subscriber's

Managed UT, subject to the capabilities of each WTN and subject to the limits of available WTN resources.

11) It SHALL be possible to scale the capacity of PQCS on a single WTN by supporting multiple physical PQCS instances.

12) It SHALL be possible to associate a Subscriber's attributes and state with one PQCS instance for a WTN.

13) It SHALL be possible for an application to further refine the priority and QoS selection made by the PQCS for a Subscriber's traffic (U_{bs} & U_{bb}).

Note: The intent of this requirement is to provide certain authorized applications (e.g., MC-PTT) with the ability to further refine the priority and QoS of flows pertaining to application control and media traffic (e.g., a scan call is traditionally of lower priority than a group call to which the responder is a member). The PQCS doesn't have visibility to application constructs like calls and sessions and thus has to be told if flow differentiation is required.

14) It SHALL be possible for the PQCS to simultaneously support multiple WTNs.

3.1.2 Access Priority Requirements

In order to prevent overload of the wireless random access channel (i.e., to prevent "access storms"), a Subscriber's access to the wireless transport network needs to be prioritized. In this context, Access Priority refers to the relative priority a Subscriber's Managed UT has in accessing the WTN's random access channel, relative to other Managed UTs. WTN-specific requirements for this section can be found in section 3.1.15.

1) It SHALL be possible for the PQCS to assign an Access Priority to a Subscriber's Managed UT(s) based on the Type of Subscriber associated with the device and whether or not any Dynamic Priority capabilities have been activated.

2) In times of WTN initial access contention, it SHALL be possible for the PQCS to configure the WTN to prioritize which Managed UTs can access the WTN, based on the Subscriber's Access Priority.

3) It SHALL be possible for the PQCS to automatically enable and disable Access Priority control based on WTN loading and Dynamic Priority conditions.

4) It SHALL be possible for an authorized administrator to manually enable and disable Access Priority control.

5) It SHALL be possible for the PQCS to modify WTN Access Priority parameters within authorized ranges based on the Subscriber's Access Priority, e.g., to improve the probability of obtaining radio access to the network.

3.1.3 Default Admission Priority Requirements

Admission Priority concerns whether or not a Subscriber's request for resources can be granted. Default Admission Priority is the priority assigned to a Subscriber on a day-to-day basis and is

intended to suffice for the vast majority of normal activities. A properly configured PQCS computes a Subscriber's Default Admission Priority without human intervention.

1) It SHALL be possible for an authorized administrator to configure an application with the PQCS and categorize IP flows associated with the application according to the following relative priorities:
   a) Mission-Critical Voice (MC-PTT, MC-Telephony)
   b) Mission Critical Data Applications (e.g., CAD, DB queries/RMS, location services, dispatch data, Subscriber health/telemetry)
   c) Low Priority Voice (e.g., cellular telephony or back-up PTT applications)
   d) Video or Multimedia (e.g., streaming video, progressive video, etc.)
   e) Routine text messaging, multimedia messaging, file transfers, device management, web browsing
2) It SHALL be possible for the PQCS to identify the application being used by a Subscriber and assign the application's IP flows a relative priority.
3) It SHALL be possible for an authorized administrator to configure the geographical jurisdictional boundary of an agency with the PQCS.

   Note: this requirement is not attempting to be prescriptive so as to choose a method to identify said boundaries. Numerous methods exist, such as cell identifiers, geo-coordinates, etc.

4) Minimally, the PQCS SHALL support the following operational status for each Subscriber:
   a) Unknown/Not-Registered with Network
   b) Off Duty
   c) On Duty, In Home Jurisdictional Area
   d) On Duty, Out of Home Jurisdictional Area
5) The PQCS SHALL support modification of a Subscriber's operational status by an Application Client or Application Service.

   Note: Some Application Services, for example Computer Aided Dispatch, oversee many Subscribers, and thus need an ability to modify the operational status of many users within the authority of the dispatcher.

6) It SHALL be possible for the PQCS to determine a Default Admission Priority for a Subscriber, using the Subscriber's selected application, the type of Subscriber (e.g., primary user, secondary user, etc.), and the Subscriber's operational status.
7) Subscribers SHALL NOT be required to interact with the PQCS's parameters in order to receive default admission priority.

   Note: The intent is to avoid distracting a responder with the need to program the PQCS or WTN to perform their normal day-to-day mission. The intent of this requirement is to say that computation of a Subscriber's default admission

priority does not require the Subscriber to interact with PQCS or WTN parameters. Instead, entities already part of the responder's workflow (e.g., CAD) will interact on behalf of the Subscriber with the PQCS.

8) Application Clients SHALL be notified of changes to Default Admission Priority information for the Subscriber.

3.1.4 Dynamic Admission Priority Requirements

When special incident or life-threatening conditions arise, the Default Priority methods outlined in section 3.1.3 can be insufficient to meet the needs of Subscribers. For this reason, Dynamic Admission Priority is provided to Subscribers as a means to allow them to receive service in accordance with the severity of their situation.

1) Initiation of Dynamic Admission Priority capabilities (sections 3.1.4.1 - 3.1.4.3) SHALL cause the PQCS to temporarily override the Default Priority assigned to the Subscriber.

2) The PQCS SHALL determine the Dynamic Priority of a Subscriber as a function of that Subscriber's Responder Emergency, Immediate Peril and Incident Severity attributes.

3) The PQCS SHALL modify WTN-specific controls to effect changes to the priority of a Subscriber in response to changes in Dynamic Priority.

4) The PQCS SHALL provide an interface to authorized Application Clients and Application Services to influence Dynamic Admission Priority for a Subscriber.

5) The PQCS SHALL provide an interface to each suitably authorized operating agency (e.g., national, state, local, tribal, federal) for the purposes of managing the Dynamic Admission Priority capabilities described herein.

6) Application Clients SHALL be notified of changes to Dynamic Admission Priority information for the Subscriber.

3.1.4.1 Responder Emergency

Responder Emergency allows a Subscriber or Supervisory Subscriber to indicate to the PQCS that they or one of their related Subscribers are involved in a life-threatening condition (e.g., "I'm being attacked.").

1) It SHALL be possible for an Agency O&M User to configure with the PQCS which applications can receive emergency priority when the 'Responder Emergency' capability is activated.

2) Applications that have been designated to receive emergency priority when the 'Responder Emergency' capability is activated SHALL receive elevated priority on the system.

Note: In some cases, the highest admission priority is given to the WTN administrative staff in order to 'fix' issues with a WTN cell. Responders participating in the NPSTC Priority and QoS Task Group [3] *requested that Responder Emergency be the highest Admission Priority available on the system. This is ultimately a policy decision for the operators of the WTN.*

3) When a Subscriber has successfully signed in to the PQCS, it SHALL be possible for the Subscriber to initiate the 'Responder Emergency' capability for herself/himself.

4) When a Supervisory Subscriber has successfully signed in to the PQCS, it SHALL be possible for the Supervisory Subscriber (e.g., dispatcher) to initiate the 'Responder Emergency' capability on behalf of another Subscriber.

5) It SHALL be possible for a Subscriber to clear the 'Responder Emergency' condition with the PQCS for herself/himself.

6) It SHALL be possible for a Supervisory Subscriber (e.g., dispatcher) to clear the 'Responder Emergency' condition with the PQCS for another Subscriber.

7) When initiated, the 'Responder Emergency' capability SHOULD provide a clear indication on the Subscriber's Managed UT that the service was successfully activated by the PQCS.

8) An Agency O&M User SHALL be able to configure what notifications are received by the agency when the 'Responder Emergency' capability is activated by one of the agency's Subscribers. Notifications SHOULD include, but are not limited to:

   a) Operations terminal alarm (visual, audio, etc.)

   b) Application Programming Interface (API) operations

   c) Usage Records

3.1.4.2 Immediate Peril

Immediate Peril allows a Subscriber or Supervisory Subscriber to indicate to the PQCS that a situation, if unchecked, will quickly become a life-threatening condition (e.g., a tanker truck about to explode).

1) When a Subscriber has successfully signed in to the PQCS, it SHALL be possible for the Subscriber to initiate the 'Immediate Peril' capability for herself/himself.

2) When a Supervisory Subscriber has successfully signed in to the PQCS, it SHALL be possible for the Supervisory Subscriber (e.g., dispatcher) to initiate the 'Immediate Peril' capability with the PQCS on behalf of another Subscriber.

3) A Subscriber initiating the 'Immediate Peril' capability SHALL be able to choose one or more Application Services to receive elevated priority.

4) An authorized administrator SHOULD have the ability to associate a time-out with the 'Immediate Peril' capability. Upon expiration of this time-out, the 'Immediate Peril' capability SHOULD be deactivated for the Subscriber.

5) It SHALL be possible for a Subscriber to clear the 'Immediate Peril' condition with the PQCS for herself/himself.

6) It SHALL be possible for a Supervisory Subscriber (e.g., dispatcher) to clear the 'Immediate Peril' condition for another Subscriber.

7) When initiated, the 'Immediate Peril' capability SHOULD provide a clear indication to the Subscriber that the service is active.

8) An Agency O&M User SHALL be able to configure what notifications are received by the agency when the 'Immediate Peril' capability is activated by one of the agency's Subscribers. Notifications SHOULD include, but are not limited to:

   a) Operations terminal alarm (visual, audio, etc.)

   b) Application Programming Interface (API) operations

   c) Usage Records

3.1.4.3 Incident Priority

A relationship between the incident, a Subscriber's Access Priority (section 3.1.2), and a Subscriber's Admission Priority (sections 3.1.3 and 3.1.4) needs to be established. For example, a hostage barricade is more severe than a traffic stop for police.

1) It SHALL be possible for an authorized Application Service (e.g., CAD) to provide the PQCS with the Subscriber's assigned incident type and role within the incident.

2) It SHALL be possible for the PQCS to modify the Subscriber's Dynamic Admission Priority based on the Subscriber's assigned incident type and role within the incident.

3) It SHALL be possible for an authorized Application Service (e.g., CAD) to inform the PQCS that the Subscriber's incident information has changed.

4) It SHALL be possible for an authorized Application Service (e.g., CAD) to inform the PQCS a given Subscriber is no longer associated with an incident.

3.1.5 Scheduling Priority Requirements

After a Subscriber's session has been admitted to the WTN, quality of service focuses on the experience the user (and the user's applications) receives. For example, a sub-optimal quality of service can result in a choppy or pixilated video experience. Quality of Service priority typically influences scheduling of packet delivery for the U_{bb} interface (section 2.1). WTN-specific requirements for this section can be found in section 3.1.15

3.1.6 Pre-emption Requirements

Pre-emption refers to the WTN's ability to immediately provide system resources to a higher priority Managed UT (immediately removing the resource from a lower priority Managed UT) in cases where there is resource contention and queuing of the higher priority Managed UT's service request is unacceptable. Pre-emption is a critically essential capability for public safety and is necessary to support the Dynamic Priority requirements outlined in section 3.1.4. WTN-specific requirements for this section can be found in section 3.1.15.

1) It SHALL be possible for an authorized administrator to configure with the PQCS which IP traffic flows associated with applications can utilize resources of another application that has been pre-empted.

2) It SHALL be possible for an authorized administrator to configure with the PQCS whether or not IP traffic flows associated with a given application can be pre-empted.

3) In the event IP traffic flows associated with a Subscriber's application are pre-empted and can no longer function, a suitable notification SHOULD be provided by the PQCS to the Subscriber indicating the reason for the pre-emption.

4) Whether operating with Default or Dynamic Priority, it SHALL be possible for an authorized administrator to configure with the PQCS that certain application flows are non-pre-emptable.

   Note: For certain applications (e.g., MC-PTT) and certain dynamic PQCS capabilities (e.g., Responder Emergency and Immediate Peril), it may be desirable to configure user traffic as non-pre-emptable in order to provide controlled usage of the WTN under the most congested conditions.

5) It SHALL be possible for an application at run-time to designate to the PQCS that certain application flows associated with the application are pre-emptable, even if previously configured as non-pre-emptable.

   Note: Applications are, by default, associated with an indication as to whether or not their Subscriber traffic should be pre-empted. Because the PQCS is not aware of individual calls or sessions in an application, a means is necessary for the application to be able to indicate to the PQCS that certain flows, calls, or sessions may be pre-empted (e.g., MC-PTT scan calls). The intent is to be able to permit pre-emption in certain cases when the application's traffic is defaulted to non-pre-emptable. The reverse is not true: applications that are, by default, pre-emptable cannot ask to be non-pre-emptable.

3.1.7 Bandwidth Management Requirements

Bandwidth management refers to the control of the rate at which IP traffic is transferred between Managed UTs and Application Services. WTN-specific requirements for this section can be found in section 3.1.15

3.1.8 Group Admission Priority Requirements

Certain applications, such as MC-PTT, naturally involve many Subscribers. In LMR systems, priority is frequently associated with the talk group being used. When group applications are utilized, prioritization needs to account for the nature of the group, rather than the individual's specific prioritization attributes. Subscribers utilizing a group application may need to receive consistent priority and QoS for the given group application. This LMR behavior can be replicated by the PQCS using the wireless transport network.

The PQCS supports group applications over broadband networks in one of two ways:

- **unicast resources** – these are uplink and downlink resources to/from the Application Service from/to a Managed UT. PQCS 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** – some WTNs, such as 3GPP LTE, provide a downlink point-to-multipoint capability (i.e. single resource to distribute simultaneously to multiple receiving Managed UTs). Unicast uplink (Managed UT to infrastructure) resources are still required for each Managed UT. PQCS 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.

A group application can use a hybrid of broadband unicast and broadcast resources.

The important aspect to note is that when a Subscriber utilizes a group application, priority and QoS will be associated with the group application's session and not the individual Subscriber.

1) It SHALL be possible for an authorized administrator to configure with the PQCS an application as a group application.

2) It SHALL be possible for an authorized administrator to configure certain groups associated with a group application to have the priority and QoS of the group's resources aligned.

3) It SHALL be possible for the PQCS to support groups constructed exclusively of unicast resources.

4) It SHALL be possible for the PQCS to support groups constructed exclusively of broadcast resources

5) It SHALL be possible for the PQCS to support groups constructed with a mixture of unicast and broadcast resources.

6) It SHALL be possible for a group application to designate with the PQCS that a Subscriber is participating in a specific group (e.g., push-to-talk talkgroup 4).

7) It SHALL be possible for an application to indicate to the PQCS that the priority and QoS of resources associated with a Subscriber group should be aligned.

Note: The intent of this requirement is to support a consistent priority and QoS experience for calls with multiple, independently prioritized call legs (e.g., a group

constructed of multiple unicast resources). Failure to align priority and QoS attributes may lessen the probability of completing calls with the desired participants. This requirement is also valid for the mix of point-to-point and point-to-multipoint resources for a single call.

8) It SHALL be possible for the PQCS to apply the same Default Admission Priority (section 3.1.3) to selected flows belonging to a group in a group application.

9) It SHALL be possible for a group application to designate to the PQCS that certain group application flows are of higher priority than other flows. For example, a push-to-talk application should be able to identify which talk-group flows are more important than others.

10) It SHALL be possible for an authorized Subscriber participating in a group to utilize the Dynamic Admission Priority capabilities outlined in section 3.1.4.

11) When a Subscriber or Supervisory Subscriber initiates a Dynamic Admission Priority capability (section 3.1.4) and the service indicates priority for the group application, all members of the Subscriber's associated group session SHALL receive the same dynamic admission priority for resources associated with that group.

3.1.9 Transport Network Requirements

While it is important to provide focus for QoS on the WTN, the overall experience of the Subscriber can be hampered if QoS in all transport networks is not aligned. Transport network facilities, such backhaul, IP and MPLS networks need to be coordinated with the QoS capabilities provided by the WTN. We focus on the WTN's QoS (Scheduling Priority) rather than Admission Priority, because the WTN's Scheduling Priority governs the quality of experience in exchanging user content after the Subscriber's session has been admitted.

1) It SHALL be possible to coordinate transport priority (e.g., backhaul and IP network) for an application's flows with the application's determined WTN Scheduling Priority (section 3.1.5).

3.1.10 End-to-End Requirements

Responders and National Security personnel often need to communicate across systems. For example, responders often need to communicate with utility users using a commercial system. Incidents traditionally impact loading on multiple systems in a geographic area, therefore it is important to be able to convey priority between systems so that each 'leg' of a session (e.g., call) can be given priority treatment.

1) When Subscribers operating on the WTN attempt to communicate with users operating on other networks, the PQCS SHOULD 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.

Note: In many cases, end-to-end calls can only be partially controlled by the Wireless Transport Network. In such cases, the PQCS needs to be able to convey a priority indication to the system serving the terminating party. For example, responders need to call witnesses or other users served by commercial systems.

2) When a Subscriber receives an incoming session request from a non-public safety system (e.g., peer IP-based systems such as the Internet and some commercial networks), it SHOULD be possible for the originating system to convey end to end priority needs to the PQCS in order to increase the probability of completing communications during periods of network congestion or impairment.

3.1.11 Provisioning Requirements

Provisioning refers to an authorized administrator's ability to add, change, delete, and view information pertaining to Subscribers of the PQCS.

1) It SHALL be possible for an authorized administrator to provision with the PQCS Default Priority and QoS parameters (section 3.1.3) for Subscribers under their authority.

Note: This requirement and others in this section are intended to support multiple operational models: (1) Subscribers provisioned by an Agency O&M User and (2) Subscribers provisioned by an Operator O&M User.

2) It SHALL be possible for an authorized administrator to identify and provision the Subscriber's class (e.g., primary user, secondary user, etc.) and the Subscribers's organizational role (e.g., chief, sergeant, etc.) in the PQCS.

3) It SHALL be possible for an authorized administrator to provision with the PQCS the Bandwidth Management capabilities defined in section 3.1.15.1.5.

4) The PQCS SHOULD provide provisioning templates (e.g., primary user, secondary user, etc.) to minimize the authorized administrator's provisioning burden.

5) It SHALL be possible for an authorized administrator to view the current priority and QoS attributes of Subscribers under their authority.

6) It SHALL be possible for an authorized administrator to view historical changes to a Subscriber's priority and QoS attributes for Subscribers under their authority.

7) It SHALL be possible for an authorized administrator at run-time to modify a Subscriber's Dynamic Priority attributes (section 3.1.4) for Subscribers under their authority. This includes, but is not limited to:

   a) Activate/de-activate Responder Emergency

   b) Activate/de-activate Immediate Peril

   c) Add and remove Subscribers from incidents and change incident type and role

8) It SHALL be possible for an authorized administrator to provision the action that needs to occur when a Subscriber activates and clears a Dynamic Priority capability. Such actions SHOULD include, but not be limited to:

   a) Configure a maintenance terminal alert

   b) Configure an alert for certain types of Subscribers (e.g., shift supervisors, dispatcher)

   c) Configure an alert for certain applications (e.g., dispatch application)

9) It SHALL be possible for an authorized administrator to provision the quality of service attributes utilized by a Subscriber.

   Note: This requirement is not intended to provide real-time changes to a Subscriber's in-progress sessions. Instead, the focus is to allow the authorized administrator the ability to pre-configure the WTN with a Subscriber's QoS attributes.

10) It SHALL be possible for an authorized Application Client or Application Service to query the default and dynamic attribute information of one or more Subscribers.

11) It SHALL be possible for an authorized Subscriber to query the PQCS's view of her/his current default and dynamic attributes.

12) It SHALL be possible for an authorized Application Client or Application Service to subscribe to the changes in default and dynamic attributes of one or more Subscribers.

13) The PQCS SHALL provide to authorized administrators the ability to view the current state of WTN parameters that can be modified by the PQCS.

14) The PQCS SHALL provide to authorized administrators the ability to modify WTN parameters pertaining to priority and QoS.

3.1.12 Usage Record Requirements

Usage records are traditionally charging-related data records. A simple minutes-of-use model is likely insufficient for the PQCS because the quality of experience for the Subscriber can vary widely, depending on the priority and QoS the Subscriber has utilized.

1) Usage records SHOULD be created by the PQCS and delivered to the Subscriber's agency each time a Subscriber utilizes an Application Service with Default Admission Priority (section 3.1.3).

2) Usage records SHOULD be created by the PQCS and delivered to the Subscriber's agency each time a Subscriber utilizes a Dynamic Admission Priority Control outlined in section 3.1.4.

3) PQCS usage records SHOULD minimally include:

   a) the date/time, and duration of usage

b) the application being used

c) the Subscriber's current Access Priority, Admission Priority, and Scheduling Priority for the application being used.

d) the Dynamic Admission Priority Control, if any, being used

e) the Subscriber initiating the Dynamic Admission Priority Control, if any

f) details of the party(ies) involved in the session, if applicable

g) group membership, if using a group application

3.1.13 Service Discovery Requirements

Service discovery refers to an entity's ability to (re-)establish communications with the PQCS.

1) It SHALL be possible for a Subscriber using an Application Service to discover and initiate communications with the PQCS using the Q_u reference point.

2) It SHALL be possible for a Subscriber using an Application Client to discover and initiate communications with the PQCS using the Q_u reference point.

3) The PQCS SHALL prevent a Managed UT from communicating with more than one instance of the PQCS.

4) The PQCS SHALL prevent a User Host from communicating with more than one instance of the PQCS.

5) It SHALL be possible for authorized administrators, using O&M equipment on the M_A and M_S reference points, to securely establish communications with the PQCS.

6) Using configured information, it SHALL be possible for one PQCS instance to establish communications using the G_{pri} reference point with one or more peer PQCS instances for the same WTN.

7) It SHALL be possible for a PQCS instance to discover which PQCS instance is serving a Subscriber.

8) It SHALL be possible for the PQCS to initiate communications with the WTN, using the R_{bs} reference point.

3.1.14 Security Requirements

The following security requirements are applicable to all aspects of the PQCS.

1) The PQCS SHALL employ compliant open standards for encryption and authentication.

2) The PQCS SHALL support security of the Q_u, M_A, M_S, R_{bs}, and G_{pri} reference points, as follows:

a) Security of the reference points SHALL allow for seamless evolution of all security algorithms and methods.
b) The PQCS SHALL provide for optional encryption of all service related traffic.
c) The PQCS SHALL support strong authentication of Subscribers and authorized administrators before service access is granted.
d) The PQCS SHALL support a means by which an application may require strong authentication of the service.
e) The PQCS SHALL support strong mutual authentication of peer PQCS instances on the G_{pri} interface.

3) The PQCS SHALL support confidentiality and integrity for Privileged Information.

a) Privileged Information SHALL be encrypted over publicly available interfaces.

b) Encryption of privileged information SHALL include provisions for seamless evolution of cryptographic methods and algorithms.

4) The PQCS SHALL provide security mechanisms for sensitive Subscriber controls.

a) The PQCS SHALL support End-to-End Message Integrity[4] checking for sensitive Subscriber controls.

b) The PQCS SHALL support End-to-End source authentication for sensitive Subscriber controls.

c) Sensitive Subscriber controls SHALL be construed to be sensitive Subscriber information.

5) The PQCS SHALL provide an ability to authorize a Supervisory Subscriber or Subscriber to perform some to all capabilities on the Q_u reference point.

6) The PQCS SHALL provide an ability for an Operator O&M User to authorize an Agency O&M User to perform some to all capabilities on the M_A reference point.

3.1.15 Wireless Transport Network Specific Requirements

This section defines requirements for specific realizations of the Wireless Transport Network. The PQCS supports multiple WTNs simultaneously.

3.1.15.1 Requirements for 3GPP LTE as the Wireless Transport Network

This section defines specific requirements for the case when 3GPP LTE is realized as the WTN. Requirements in this section are based on 3GPP TS 23.203 [6].

[4] In this specification, End-to-end message integrity is defined to be a crypto-graphic message integrity mechanism in which information is "signed" within an originating Application Client or Application Service, and the signature is verified at the PQCS.

3.1.15.1.1 General Requirements for 3GPP LTE

These requirements are related to the general requirements in section 3.1.1.

1) The PQCS SHALL control priority and QoS applicable to a Subscriber's initial access to the WTN (i.e., Access Priority).

2) The PQCS SHALL control priority and QoS applicable to a Subscriber initiating an application on the WTN (i.e., Admission Priority).

3) The PQCS SHALL control priority and QoS policy applicable to a Subscriber's Managed UT sending or receiving IP traffic (i.e., Scheduling Priority).

4) It SHALL be possible for the PQCS to derive and apply a Managed UT's bearer characteristics from Subscriber priority and QoS attributes.

5) It SHALL be possible for the PQCS to consistently apply priority and QoS to IP traffic flows supporting any of the Subscriber's applications, regardless of the entity operating the application (e.g., nationally-deployed, regionally-deployed, agency-deployed, etc.) and regardless of where the application is deployed (e.g., regardless of the IP network/APN that contains the application).

3.1.15.1.2 Access Priority for 3GPP LTE

These requirements are related to the Access Priority requirements in section 3.1.2 and are based on 3GPP's Access Class Barring [8] capability.

1) Public Safety emergency calls SHALL be given preferential access to the WTN's random access channel. For more information, see section 3.1.4.1.

   Note: Public Safety emergency calls are intended to be, for example, services utilized by a first responder after the responder activates his/her emergency button. This is not to be confused with a commercial-like 911 call.

2) It SHALL be possible for the PQCS to alter a Managed UT's assigned access class(es) at run-time.

3) It SHALL be possible for the PQCS to enable and disable access class barring for all access classes at run-time for a given WTN cell based on WTN loading and Dynamic Priority conditions.

4) It SHALL be possible for the PQCS to alter access class 0-9 barring parameters for a WTN cell at run-time.

3.1.15.1.3 Scheduling Priority for 3GPP LTE

For LTE, [6] defines the Policy and Charging Control Architecture. Within this specification, Quality of Service attributes are bundled and associated with a QoS Class Identifier (QCIs)):

- GBR/Non-GBR – defines whether or not the bandwidth assignment to the associated bearer is enforced

- Scheduling Priority – for all packets (GBR and Non-GBR) defines the relative importance of the packet for transmission over-the-air.
- Packet Loss Rate – for the associated bearer, this is the maximum tolerable packet loss rate with or without the presence of congestion.
- Packet Delay Budget – for the associated bearer, this is the maximum tolerable transmission delay for a packet.

[6] identifies recommended values for these parameters and associates these values to standard QCI values. The NPSTC Priority and QoS Task Group [3] reviewed these parameters and found them to be generally suitable for Public Safety applications.
When a new application is being added to the system and requires services from the PQCS, it is anticipated that an authorized administrator will configure with the PQCS QoS attribute needs for each application flow. When QoS attributes are configured for a particular application, this information usually does not change unless the QoS characteristics of application flows fundamentally change (e.g., a change in codec after a software upgrade). When the PQCS receives a request for resources, it will select an appropriate QoS profile and communicate with LTE to select the correct QCI for an Application flow.

This section specifies requirements for the relationship of the PQCS QoS to LTE QoS. These requirements are related to the Scheduling Priority requirements in section 3.1.5.

1) It SHALL be possible for the PQCS to specify quality of service attributes (packet latency, packet loss, and scheduling priority) for an application's associated flows and configure the WTN to support these QoS attributes.

2) It SHALL be possible for the PQCS to alter the Subscriber's associated quality of service attributes with the WTN while application(s) are currently being used.

3.1.15.1.4 Pre-emption for 3GPP LTE

These requirements are related to the pre-emption requirements in section 3.1.6.

1) The PQCS SHALL identify to the WTN which Managed UT flows are pre-emptable.

2) It SHALL be possible, based on Subscriber A's allocation and retention priority (ARP) to quickly remove resources assigned to one or more alternate Subscribers in order to provide resources to Subscriber A.

Note 1: The ARP pre-emption vulnerability flag for bearers associated with alternate Subscribers needs to be set to 'true'.

Note 2: The ARP pre-emption capability flag for bearers associated with Subscriber A needs to be set to 'true'.

3.1.15.1.5 Bandwidth Management for 3GPP LTE

These requirements are related to the Bandwidth Management requirements in section 3.1.7.

1) It SHALL be possible for an authorized administrator to configure the maximum amount of bandwidth allowable for non-GBR IP traffic flows associated with a given agency (all Subscribers).

2) It SHALL be possible for an authorized administrator to configure the minimum and maximum bandwidth allowed for IP traffic flows associated with a given Application Service.

3) It SHALL be possible for an authorized administrator to configure the maximum amount of bandwidth allowed per Subscriber for IP traffic flows associated with Internet traffic.