ATIS-0700044

ATIS Standard on -

Study of Emergency Services and National Security Emergency Preparedness Next Generation Network Priority Service (NS/EP NGN-PS) Coexistence on LTE Access Networks

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0700044

ATIS Standard on

Study of Emergency Services and National Security Emergency Preparedness Next Generation Network Priority Service (NS/EP NGN-PS) Coexistence on LTE Access Networks

Alliance for Telecommunications Industry Solutions

Approved June 26, 2019

Abstract

This technical report is a study of contention issues between different access classes such as Emergency Services and National Security / Emergency Preparedness Next Generation Priority Services (NS/EP NGN-PS) communications on Long-Term Evolution (LTE) Access during network degradation conditions (e.g., network congestion during certain disaster events).

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. This ATIS Standard was developed jointly between ESIF, PTSC, and WTSC.

The Emergency Services Interconnection Forum (ESIF) provides a forum to facilitate the identification and resolution of technical and/or operational issues related to the interconnection of wireline, wireless, cable, satellites, Internet and emergency services networks.

PTSC develops standards related to services, architectures, signaling, network interfaces, next generation carrier interconnect, cybersecurity, lawful intercept, and government emergency telecommunications service within next generation networks. As networks transition to all-IP, PTSC will evaluate the impact of this transition and develop solutions and recommendations where necessary to facilitate and reflect this evolution.

The Wireless Technologies and Systems Committee (WTSC) develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional, and international standards bodies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, WTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of initiation or issuance of the letter ballot for this document, the committees responsible for its development, had the following leadership:

R. Marshall, ESIF Chair (Comtech)
J. Green, ESIF First Vice Chair (Sprint)
R. Muscat, ESIF Second Vice Chair (Bexar Metro 911)

M. Dolly, PTSC Chair (AT&T)
V. Shaikh, PTSC Vice Chair (Perspecta Labs)

D. Zelmer, WTSC Chair (AT&T)
M. Younge, WTSC Vice Chair (T-Mobile)
F. Khatibi, WTSC RAN and NSEP Chair (Qualcomm)

G. Pollini, Technical Editor (Perspecta Labs)
R. Singh, Technical Editor (Perspecta Labs)

The WTSC NSEP Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

ATIS Standard on –

Study of Emergency Services and National Security Emergency Preparedness Next Generation Network Priority Service (NS/EP NGN-PS) Coexistence on LTE Access Networks

1 Scope, Purpose, & Application

Emergency Services and National Security/Emergency Preparedness (NS/EP) Next Generation Network Priority Services (NGN-PS) will have to coexist in commercial Long-Term Evolution (LTE) network service deployments. Both are expected to be served along with commercial priority services, and non-priority commercial services under network degradation conditions (e.g., congestion and overload conditions). There are 3GPP defined mechanisms for admission and congestion controls such as the Access Class Barring (ACB) mechanism, and scheduler imposed restrictions on throughput; however, it is not clear how and when these capabilities may be invoked in an optimal manner. For example, it might be possible for a flood of Emergency Services sessions and normal sessions (e.g., voice, video and messaging sessions), initiated as a result of a disaster or emergency event, to monopolize LTE access resources.

This technical report provides a study analyzing contention issues between different services such as Emergency Services and NS/EP NGN-PS communications during network degradation conditions (e.g., network congestion during certain disaster events). The analysis involves:

- Identifying and analyzing network admission and congestion control capabilities and mechanisms defined in 3GPP LTE specifications to determine adequacy and identify gaps in addressing the problem,
- Investigating operational (i.e., network element and resource management) means,
- Consideration of regulatory rules/policy implications, and
- Providing guidance on how 3GPP-defined mechanisms can be used.

The analysis in this report examines all of the network admission and congestion control capabilities and mechanisms defined in 3GPP specifications through Release 14 inclusive independent of whether they are implemented and supported in service provider networks. However, it is possible that not all of the network admission and congestion control capabilities and mechanisms defined in 3GPP specifications are implemented and supported in a given service provider network. Furthermore, the analysis in this report does not imply that all the network admission and congestion control capabilities and mechanisms defined in 3GPP specifications should be supported by service provider networks. The analysis in this report is intended to be a complete analysis of the network admission and congestion control capabilities and mechanisms defined in 3GPP specifications through Release 14 inclusive.

Although NS/EP NGN-PS and Emergency Services will have to coexist with other priority services, the report focuses only on contention between NS/EP NGN-PS and Emergency Services. Contention with other priority services (e.g., Public Safety) including commercial priority services offered by service providers [e.g., Mission Critical Push to Talk (MCPTT) for utility and transportation organizations] is not included in the scope of this report.

This analysis report is applicable to North American public LTE networks consisting of the radio access network (RAN) and the Evolved Packet Core (EPC).

2 References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and

parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] FCC 47 CFR § 64 Appendix B, *FCC Title 47 Telecommunication Appendix B to Part 64; Appendix B to Part 64—Priority Access Service (PAS) for National Security and Emergency Preparedness (NSEP)*.[1]

[Ref 2] ATIS-1000057, *Service Requirements for Emergency Telecommunications Service (ETS) in Next Generation Network.*[2]

[Ref 3] ATIS-1000065*, Emergency Telecommunications Service (ETS) Evolved Packet Core (EPC) Network Element Requirements.*[2]

[Ref 4] 3GPP TS 22.011, *Service accessibility*.[3]

[Ref 5] 3GPP TS 22.153, *Multimedia Priority Service*.[3]

[Ref 6] 3GPP TS 36.331, *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification*.[3]

[Ref 7] 3GPP TS 23.401, *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.*[3]

[Ref 8] 3GPP TS 24.301, *Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3.*[3]

[Ref 9] 3GPP TS 31.102, *Characteristics of the Universal Subscriber Identity Module (USIM) application.*[3]

[Ref 10] 3GPP TS 24.173*, IMS Multimedia telephony communication service and supplementary services; Stage 3.*[3]

[Ref 11] 3GPP TS 27.007*, AT command set for User Equipment (UE).*[3]

[Ref 12] 3GPP TS 24.105, *Application specific Congestion control for Data Communication (ACDC) Management Object (MO)*.[3]

[Ref 13] 3GPP TS 36.304, *Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode*.[3]

[Ref 14] 3GPP TS 24.368, *Non-Access Stratum (NAS) configuration Management Object (MO)*.[3]

[Ref 15] 3GPP TS 24.011, *Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface*.[3]

[Ref 16] 3GPP TS 24.341, *Support of SMS over IP networks; Stage 3.*[3]

[Ref 17] 3GPP TS 36.413, *Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)*.[3]

[Ref 18] 3GPP TS 29.274, *3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3.*[3]

[Ref 19] 3GPP TS 29.272, *Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol*.[3]

[Ref 20] 3GPP TS 24.008, *Mobile radio interface Layer 3 specification; Core network protocols; Stage 3*.[3]

[Ref 21] ATIS-1000079, *National Security Emergency Preparedness Next Generation Network Priority Service (NS/EP NGN-PS): Transport Level Packet Marking and Packet Scheduling*.[2]

[Ref 22] 3GPP TS 23.203, *Policy and charging control architecture*.[3]

---

[1] This document is available from the Federal Communications Commission (FCC) < http://www.fcc.gov/ >.

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) < https://www.atis.org/ >.

[3] This document is available from the 3rd Generation Partnership Project (3GPP) < http://www.3gpp.org/ >.

[Ref 23] Communications Security, Reliability and Interoperability V (CSRIC V) Working Group 8, *Priority Services Report*.[4]

[Ref 24] Ben-Gurion University of the Negev Cyber-Security Research Center, *9-1-1 DDoS: Threat, Analysis and Mitigation* by Mordechai, Yisoel Mirsky and Yuval Elovici.[5]

[Ref 25] FCC 47 CFR § 20.18, FCC Title 47 Telecommunication Part 20 Commercial Mobile Service § 20.18, *911 Service*.[1]

[Ref 26] GSMA SG.24, *Anti-Theft Device Feature Requirements v3.0*.[6]

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

3.1 Definitions

Emergency Services: Are services such as 9-1-1 and Enhanced 9-1-1 (E9-1-1) used in North America.

NOTE: In 3GPP specifications the term “Emergency” is used which is applicable to “9-1-1” and “E9-1-1” in the US.

NS/EP NGN Priority Services (NS/EP NGN-PS) (ATIS-1000057 [Ref 2]): are the evolution of legacy Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) to achieve continuity in the packet-switched NGN, and to leverage the NGN to offer new features and priority multimedia services.

3.2 Acronyms & Abbreviations

3GPP	3rd Generation Partnership Project
AB	Access Barring
AC	Access Class
ACB	Access Class Barring
ACDC	Application specific Congestion control for Data Communication
APN	Access Point Name
ARP	Allocation and Retention Priority
AT	ATtention
ATIS	Alliance for Telecommunications Industry Solutions
AVP	Attribute Value Pair
CFR	Code of Federal Regulations
CIoT	Cellular Internet of Things
CS	Circuit Switched
CSFB	Circuit Switched Fallback
CSRIC	Communications Security, Reliability and Interoperability Council
DDoS	Distributed Denial of Service
DSCP	DiffServ Code Point

[4] This document is available from the FCC at < https://www.fcc.gov/files/csric5-wg8-finalreport031517pdf >.

[5] This document is available from Cornell University < https://arxiv.org/abs/1609.02353 >.

[6] This document is available from the Groupe Spéciale Mobile Association (GSMA) < https://www.gsma.com/ >.

E9-1-1	Enhanced 9-1-1
EAB	Extended Access Barring
EMM	Evolved Packet System Mobility Management
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESM	Evolved Packet System Session Management
ETS	Emergency Telecommunications Service
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FCC	Federal Communications Commission
GERAN	GSM Enhanced Radio Access Network
GETS	Government Emergency Telecommunications Service
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GSMA	GSM Association
GTP-C	General Packet Radio Service Tunneling Protocol for the Control Plane
HPA	High Priority Access
HPLMN	Home Public Land Mobile Network
IE	Information Element
IMEI	International Mobile Equipment Identity
IMS	Internet Protocol Multimedia Sub-system
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LTE	Long-Term Evolution
MAC	Medium Access Control
MCPTT	Mission Critical Push to Talk
ME	Mobile Equipment
MME	Mobility Management Entity
MMTEL	MultiMedia TELephony
MO	Mobile Originated
MPS	Multimedia Priority Service
MT	Mobile Terminated
MTC	Machine Type Communications
NAS	Non-Access-Stratum
NB-IoT	NarrowBand Internet of Things
NB-S1	NarrowBand S1
NGN	Next Generation Network
NGN-PS	Next Generation Network Priority Service
NS/EP	National Security / Emergency Preparedness
OS	Operating System
PAS	Priority Access Service
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCI	Preemption Capability Indicator
PCRF	Policy and Charging Rules Function
PDB	Packet Delay Budget

PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDN-GW	Packet Data Network Gateway
PHY	Physical Layer
PLMN	Public Land Mobile Network
PSAP	Public Safety Answering Point
PVI	Preemption Vulnerability Indicator
QCI	Quality of Service Class Identifier
RAN	Radio Access Network
RLC	Radio Link Control
RRC	Radio Resource Control
SCM	Smart Congestion Management
SDF	Service Data Flow
S-GW	Serving Gateway
S1-AP	S1 Application Protocol
SIB2	System Information Block Type 2
SIB14	System Information Block Type 14
SIB14-NB	System Information Block Type 14 - NarrowBand
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SMSovIP	SMS over IP
SSAC	Service Specific Access Control
TAU	Tracking Area Update
TS	Technical Specification
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
ViLTE	Video over LTE
VoLTE	Voice over LTE
WB-IoT	WideBand Internet of Things
WG	Working Group
WPS	Wireless Priority Service

4 Analysis

4.1 Overview

4.1.1 Problem Description

There are 3GPP defined mechanisms for admission and congestion controls such as the Access Class Barring (ACB) mechanism, and scheduler imposed restrictions on throughput; however, experience with 4G (LTE) indicates that it might be possible for a flood of Emergency Services sessions and normal sessions (e.g., voice, video and messaging sessions), initiated as a result of a disaster or emergency event, to monopolize LTE access resources and impact NS/EP NGN-PS. In general, NS/EP NGN-PS could be impacted as a result of (a) traffic contention with Emergency traffic, and (b) security issues related to Emergency Services.

Implementing effective controls of Emergency (i.e., citizen-to authority) traffic is problematic because of limitations associated with regulatory rules, liability risks, and the fact that the 3GPP specified Access Class Barring (ACB) mechanism only provides operators with on/off control of Emergency traffic. For example, invoking ACB for Access Class 10 blocks all emergency calls except those from UEs configured to be a member of special access classes and for which exemptions are provided in system broadcast. This problem is recognized in the Communications Security, Reliability and Interoperability V [Communications Security, Reliability and Interoperability Council (CSRIC) V] Working Group (WG) 8, *Priority Services Report* [Ref 23]. Section 6 of the CSRIC V report [Ref 23] indicates that current standardized means of 911 access control are extremely coarse, only providing carriers with on/off control of 911 calls at any time. In a crisis situation, a massive number of 911 calls would likely overwhelm the resources of associated Public Safety Answering Points (PSAPs), which means many of these calls are likely to be unsuccessful. Operators have indicated a reluctance to make use of the barring feature for fear of being responsible for blocking critical 911 calls. Lack of freedom to invoke ACB for Emergency Services means that it is possible for regular services and Emergency traffic to monopolize network resources and impact the availability of NS/EP NGN-PS during certain disaster events (see Traffic Contention Example below).

The Emergency Attach procedure defined by 3GPP provides for Emergency service under conditions where normal service is disallowed, such as network-imposed constraints, lack of a subscription, inability to be authenticated by the network, or calling from a User Equipment (UE) without a Universal Subscriber Identity Module (USIM). This allows Emergency Services from unauthenticated UEs. The ability to make emergency calls from unauthenticated UEs poses security vulnerabilities that could be exploited. For example, it could be exploited by threat agents to execute attacks on the Emergency system by flooding a targeted cell site with Emergency sessions which in turn could result in a Distributed Denial of Service (DDoS) attack on NS/EP NGN-PS (see Security example below).

The research paper from Ben-Gurion University of the Negev Cyber-Security Research Center, *9-1-1 DDoS: Threat, Analysis and Mitigation* by Mordechai, Yisoel Mirsky and Yuval Elovici [Ref 24] discusses DDoS threats on the USA current 911 infrastructure. The researchers show how attackers can exploit the cellular network protocols to launch an anonymized DDoS attack on 911. Federal Communications Commission (FCC) Title 47 Telecommunication Part 20 Commercial Mobile Services § 20.18, *911 Service* [Ref 25], requires CMRS providers to transmit all wireless 911 calls without respect to their call validation process. The researchers indicate that a rootkit can be placed within the baseband firmware of a mobile phone to mask and randomize the cellular identifiers [e.g., International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI)] of the mobile phone. Such anonymized phones can issue repeated emergency calls that cannot be blocked by the network or the emergency call centers. The researchers simulate and analyze anonymous attacks on a model of the current 911 infrastructure to measure the severity of their impact. The research found that with less than 6K bots (from hardware that can be acquired easily), attackers can block Emergency Services in an entire state for days.

The following are two example scenarios where Emergency Services sessions and normal sessions (e.g., voice, video and messaging sessions) could monopolize LTE access resources and impact NS/EP NGN-PS communication sessions:

Example	Description	NS/EP NGN-PS Considerations
Traffic Contention Example	In this scenario, there is an emergency incident (e.g., terrorist attack, earthquake) resulting in a flood of communication sessions to the serving local LTE network system: • Flood of Emergency sessions (9-1-1 calls). • Increased normal calls (e.g., calls to family and friends). • Increased data sessions (e.g., email or web searches to news and local government sites).	It is assumed that there is some time lag from when the incident occurred to the time when NS/EP NGN-PS Service Users became aware of the incident and need to make NS/EP NGN-PS communications (i.e., both originating and terminating sessions) to the local serving LTE network. By this time, it is possible that all available resources [i.e., local Radio Access Network (RAN) and eNode resources] are tied up or utilized in supporting established sessions. Specifically, NS/EP NGN-PS session would only succeed if there is still some remaining available resource (i.e., there is still spare capacity) or resource were to become available as a result of established sessions becoming released.
Security Example	In this scenario, it is assumed the objective of threat agents are to (a) execute a flooding attack on the Emergency system or (b) execute a denial	It is assumed that enough time has elapsed allowing the flood of Emergency sessions to utilize all available RAN resources of the

	of service attack on NS/EP NGN-PS using Emergency Services on a targeted cell site. In both cases, the objective of the cybersecurity attack is to flood the targeted cell site with Emergency sessions.	targeted eNodeB. Specifically, NS/EP NGN-PS session would only succeed if the attacker was unable to utilize all available resource (i.e., there is still spare capacity) or resource were to become available as a result of established sessions being released (e.g., hang-up at the Emergency Center/PSAP).

4.1.2 Regulatory Policy Considerations

This clause discusses consideration of applicable regulatory rules/policy.

4.1.2.1 NS/EP

FCC 47 Code of Federal Regulations (CFR) § 64 Appendix B, *FCC Title 47 Telecommunication Appendix B to Part 64; Appendix B to Part 64—Priority Access Service (PAS) for National Security and Emergency Preparedness (NSEP)* [Ref 1] provides the FCC rules for the assignment and approval of priorities for access to commercial mobile radio service (CMRS) networks. It includes the Commission's Order to CMRS providers and users to comply with policies and procedures establishing Priority Access Service (PAS).

Per FCC 47 CFR § 64 Appendix B, [Ref 1] PAS provides the means for NSEP telecommunications users to obtain priority access to available radio channels when necessary to initiate emergency calls. The NSEP priority service does not preempt calls in progress. It is used during situations when CMRS network congestion is blocking call attempts. PAS is to be available to authorized NSEP users at all times in equipped CMRS markets where the service provider has voluntarily decided to provide such service. Authorized users would activate the feature on a per call basis by dialing a feature code such as *XX. PAS priorities “1” through “5” are reserved for qualified and authorized NSEP users, and those users are provided access to CMRS channels before any other CMRS callers.

FCC 47 CFR § 64 Appendix B, [Ref 1] provides the rules for PAS priority levels and the qualifying criteria to be used as a basis for assignments. There are five levels of NSEP priorities, priority “1” being the highest. The five priority levels are:

1. Executive Leadership and Policy Makers,
2. Disaster Response/Military Command and Control,
3. Public Health, Safety and Law Enforcement Command,
4. Public Services/Utilities and Public Welfare, and
5. Disaster Recovery.

4.1.2.2 Emergency Services

FCC 47 CFR § 20.18 [Ref 25] provides FCC rules for 911 Service. It indicates that CMRS providers subject to FCC 47 CFR § 20.18 must transmit all wireless 911 calls without respect to their call validation process to a Public Safety Answering Point, or, where no Public Safety Answering Point has been designated, to a designated statewide default answering point or appropriate local emergency authority pursuant to §64.3001 of this chapter, provided that “all wireless 911 calls” is defined as “any call initiated by a wireless user dialing 911 on a phone using a compliant radio frequency protocol of the serving carrier.”

In addition to FCC 47 CFR § 20.18 [Ref 25], there are state specific rules and regulations for 911 Service.

4.1.3 Implementation & Operational Considerations

This clause discusses implementation and network operational (i.e., network element and resource management) aspects.

4.1.3.1 NS/EP NGN-PS

Standards and service requirements specifications for NS/EP NGN-PS make the assumption that NS/EP NGN-PS traffic volume should not prevent public access. Specifically, Subclause 5.1 of 3GPP Technical Specification (TS) 22.153, *Multimedia Priority Service* [Ref 5] has the following statement:

> "Subject to regional/national regulatory policy, a PLMN should have the capability to retain public access as a fundamental function. Therefore, MPS[7] traffic volumes should be limited (e.g., not to exceed a regional/national specified percentage of any concentrated network resource, such as eNodeB capacity), so as not to compromise this function."

4.1.3.2 Emergency Services

There is no corresponding guidance in standards specifications about limiting Emergency traffic volume as described in Clause 4.1.3.1 for NS/EP NGN-PS.

4.1.3.3 Relative Treatment of NS/EP NGN-PS and Emergency Traffic

3GPP specifications leave relative treatment of the traffic associated with priority services (e.g., Emergency Services, MPS, MCS) up to regional/national regulatory rules and operatory policy.

During conditions when limited network resources are available and all communications cannot be supported, actions by operators to manage different congestion scenarios are guided by the applicable regulatory rules. However, regulatory rules do not provide clear guidance on how operators are to handle relative treatment between the traffic associated with priority services (e.g., Emergency Services, MPS, MCS and commercial priority services) under conditions where all traffic cannot be supported (i.e., due to network resource limitations). This issue is highlighted by the following recommendation documented in CSRIC V WG 8 report [Ref 23]:

> "Policy-makers should reaffirm existing guidance with respect to user classifications (e.g., FCC R&O 00-242), and clear guidelines should be given as to priority assigned to different roles in the face of limited capacity and events that invoke a high density of priority users. Similarly, policy-makers should provide clarification going forward related to pre-emption of communications for non-priority and lower-priority users (on a per application basis), in a congested environment. Relative priority classification of 911 and priority services communications in light of technical capabilities (i.e., LTE) should continue to be assessed."

4.1.4 General Considerations

Tools such as ACB, Extended Access Barring (EAB) and AB are defined by 3GPP to control Emergency Services and NS/EP NGN-PS network access. However, the 3GPP specifications only define the tool (e.g., ACB, EAB, or AB). The 3GPP specifications do not provide any guidance on how these tools should be implemented by equipment vendors and used by operators. For example, ACB is the key mechanism used in LTE to control RAN congestion/overload. However, 3GPP specifications defining the ACB mechanism and the associated procedures do not provide any guidance for equipment vendors or criteria for activation (e.g., automatically based on specific configured criteria or manually based upon observed congestion/overload).

Since 3GPP specifications are subject to interpretation, it means that there would be differences on how these tools are implemented by equipment vendors and used by network operators to combat various congestion/traffic scenarios in the multiple service provider national network environment. Each network operator is expected to deploy and use the tools provided by their equipment vendors to meet their network specific objectives and policies.

Clause 4.2 identifies and analyzes the network admission and congestion control capabilities and mechanisms defined in 3GPP LTE specifications.

[7] Multimedia Priority Service (MPS) is the term used in 3GPP specifications for NS/EP NGN-PS.

4.2 3GPP Defined LTE Access & Congestion Control Mechanisms

This clause identifies and analyzes network admission and congestion control capabilities and mechanisms defined in 3GPP LTE specifications to determine applicability, adequacy, and gaps in addressing the problem described in Clause 4.1.1.

4.2.1 General

Some of the 3GPP defined network functions and procedures used by both Emergency Services and NS/EP NGN-PS to obtain priority treatment are the same. However, Emergency Services differ from NS/EP NGN-PS in two fundamental ways, based on the following 3GPP functions defined for the support of Emergency Services:

1. Emergency Bearer Services, and
2. Emergency Attach.

The concept of Emergency Bearer Services provides the means for certain priority treatments to Emergency Services. Emergency Bearer Services can apply in normal mode and for emergency attached UEs. In normal mode, the UE attaches to the network and does not establish Emergency Bearer Services until an emergency call is initiated. On the other hand, Emergency Attach applies only after an emergency call is initiated and only when normal service is not available.

The concept of an Emergency Attach provides for Emergency Services under conditions where normal service is disallowed, such as network-imposed constraints, lack of a subscription, inability to be authenticated by the network, or calling from a UE without an USIM. The term “Emergency attached UE” is defined in Subclause 3.1 of 3GPP TS 23.401, *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access* [Ref 7] as a UE which only has bearers related to Emergency Services. It is equivalent to the Stage 3 terminology “attached for emergency bearer services” used in 3GPP TS 24.301, *Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3* [Ref 8].

Except for these two functional capabilities (i.e., Emergency Bearer Services and Emergency Attach), the functional capabilities and procedures used to support and control Emergency Services and NS/EP NGN-PS are the same.

Access to the LTE system for an emergency call is identified within the UE via digit analysis. Certain sequences of dialed digits are internationally standardized. To accommodate other locally used patterns, the network signals the list of phone numbers to be considered as emergency calls. If a user places an emergency call using a number that is neither standardized, nor downloaded from the network, the UE cannot recognize the call as an emergency call, and the initial phases of the emergency call cannot be given priority. This includes the access control mechanisms. Upon recognition by the UE that the user has dialed an emergency call, the UE may signal the network using either a tel URI or an emergency URI configured in the UE.

Access to the LTE system for an NS/EP call is based on membership in the access class allocated by the Service Provider for NS/EP use. There is no functionality specified in the UE for digit analysis in support of NS/EP calling. Instead, NS/EP priority is provided during access in advance of the network receiving, analyzing, authenticating and authorizing the dialed digits. This is called “Advance Priority” in ATIS-1000065*, Emergency Telecommunications Service (ETS) Evolved Packet Core (EPC) Network Element Requirements* [Ref 3].

A unique access class assignment for exclusive use for Multimedia Priority Service (MPS) is required since Release 10 as per Subclause 4.4a of 3GPP TS 22.011, *Service accessibility* [Ref 4]. Specifically, Subclause 4.4a of 3GPP TS 22.011 [Ref 4] indicates that MPS (as defined in 3GPP TS 22.153 [Ref 5]) shall be assigned its own unique access class value (i.e., one of the special access classes 11 to 15). The assigned access class value for MPS is based on regional/national regulatory requirements and operator policy. NS/EP NGN-PS builds on this requirement and allocated Access Class (AC) 14 for exclusive use for NS/EP NGN-PS as per ATIS-1000065 [Ref 3].

The following subclauses discuss the functional capabilities and procedures used to control Emergency Services and NS/EP NGN-PS access to network resources.

4.2.2 Access Controls

Access control mechanisms can be characterized as UE-based or eNodeB-based.

UE-based mechanisms are applied in the UE prior to any access to the network. Inputs to these mechanisms include the purpose of accessing the network [as determined by the Non-Access-Stratum (NAS) and Radio Resource Control (RRC) layers in the UE], USIM configurations associated with the user subscription, and system broadcast information provided by the RAN.

eNodeB-based mechanisms are applied in the eNodeB and are triggered by the initial RRC Layer message received by the UE. As such all applicable UE-based mechanisms need to permit the access prior to the application of any eNodeB-based mechanisms.

Except if noted as being “eNodeB-based” in the subclause title, all of the remaining subclauses discuss UE-based mechanisms.

4.2.2.1 Access Class Barring (ACB) and High Priority Access (HPA)

Allocation of Access Classes and Access Class Barring are specified in Clause 4 of 3GPP TS 22.011 [Ref 4].

All UEs are members of one out of ten randomly allocated mobile populations, defined in 3GPP TS 22.011 [Ref 4] as Access Classes 0 to 9. The population number is statically provisioned in the Subscriber Identity Module (SIM)/USIM on the UE. In addition, UEs may be members of one or more out of 5 special classes (Access Classes 11 to 15), also held in the SIM/USIM. Access Class information is encoded on the USIM within the EF_{ACC} parameter as per Subclause 4.2.15 of 3GPP TS 31.102 [Ref 9].

In Legacy (pre-Release 8) systems [e.g., Global System for Mobile communications (GSM), Universal Mobile Telecommunications System (UMTS)], barring of a specific access class in the range 0 through 9 was accomplished by explicit signaling from the network. In these legacy implementations, an access class was either unrestricted or completely barred from accessing the network.

In E-UTRA (introduced in Release 8), the specific access class value in the range 0 through 9 assigned to the USIM has no impact on ACB operation. (It does impact EAB operation, as described in Clause 4.2.2.4, and AB for NB-IoT, as described in Clause 4.2.2.7.) It is not possible to selectively bar or allow a particular access class in the range 0 through 9. Instead a probabilistic mechanism was adopted in which access from the UE (without consideration of the access class membership in 0 through 9) is barred with a probability that is signaled over the air interface, where several different thresholds are signaled by the eNodeB, and the one which applies depends only upon the purpose of the access (not on the access class). The duration of barring is also probabilistically determined.

In E-UTRA, access class 10 is reserved for Emergency Services, but it has not been used for any procedure up through Release 14 inclusive. It is not possible to configure membership in access class 10. Within the USIM parameter EFACC, of size 2 bytes, bit 3 of byte 1 (AC 10) is always set to “0” as it is a special indicator, historically used for emergency calls, but having no specified use in LTE. See Subclause 4.2.15 of 3GPP TS 31.102 [Ref 9].

In E-UTRA, access classes 11 through 15, denoted the special access classes, can be individually marked as being exempt from barring (for a particular purpose of access).

A UE establishing an RRC Connection for a mobile terminating call is not barred access to the cell by Access Class Barring (ACB), unless timer T302 is running. For RRC Connection establishment for other accesses, the UE performs the Access Barring Check specified in Subclause 5.3.3.11 of 3GPP TS 36.331, *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification* [Ref 6] which includes the procedures for the eNodeB to selectively exempt a particular AC from ACB. Procedures for ACB can be found in Subclauses 5.3.3.2 and 6.2.2 of 3GPP TS 36.331 [Ref 6].

NS/EP

Due to the assignment of a specific access class for MPS, the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) can be configured to give preferential access to NS/EP NGN-PS subscribed UEs by setting the corresponding bit of the MPS access class (AC14) to zero in the ac-BarringForSpecialAC in System Information Block Type 2 (SIB2), while barring non-NS/EP NGN-PS subscribed UEs. ACB is a critical component in the suite of capabilities needed to provide priority to NS/EP NGN-PS.

Emergency Services

ACB for emergency calls is specified in Subclause 4.4 of 3GPP TS 22.011 [Ref 4]. ACB for Emergency Services works completely differently than normal ACB. There is no way to bar a fraction of emergency calls, i.e., all are allowed, or all are barred.

Specifically, Subclause 4.4 of 3GPP TS 22.011 [Ref 4] indicates that an additional control bit known as "Access Class 10" within Stage 1 specifications is also signaled over the air interface to the UE. This indicates whether or not network access for emergency calls is allowed for UEs with access classes 0 to 9 or without an IMSI. In Stage 3 specifications, this information is signaled within SIB2 using the ac-BarringForEmergency Information Element (IE) as per Subclause 6.3.1 of 3GPP TS 36.331 [Ref 6]. Within SIB2 if ac-BarringForEmergency is set to true, all emergency calls are barred. This parameter is included in a common and a per-Public Land Mobile Network (PLMN) part of the message.

Emergency Services from an NS/EP subscribed UE

For UEs with valid AC11-15, emergency calls are allowed even when ac-BarringForEmergency is set to true. emergency calls from other UEs are barred.

For UEs with AC11-15, emergency calls are not allowed if both ac-BarringForEmergency is set to true and the relevant access class (11-15) are barred.

Relative Priority of NS/EP and Emergency Services

Annex D of 3GPP TS 24.301 [Ref 8] specified that for all NAS procedures related to an emergency call, the “emergency” value of the Establishment Cause is selected by NAS layer and signaled to the RRC layer within the UE (see Subclause 5.3.3.2 of 3GPP TS 36.331 [Ref 6]), and subsequently transmitted over the Uu Interface to the eNodeB.

If the UE is a member of a “valid” (defined in Note 1 of Table D.1.1 of Annex D.1 of 3GPP TS 24.301 [Ref 8]) access class in the range AC 11 through 15, (for AC 12, 13, and 14, “valid” requires the UE to be in its home country; and for AC 11 and 15, “valid” requires the UE to be in its home network) the “emergency” value is overwritten by the “highPriorityAccess” value. Such an action implies that “highPriorityAccess” is a higher priority setting than emergency, although there is no specific statement on the relative priority ranking of “emergency” and “highPriorityAccess” in the 3GPP specifications.

4.2.2.2 Service Specific Access Control (SSAC)

This clause presents Service Specific Access Control (SSAC), introduced in Release 9. SSAC provides a means to manage system overload by restricting access from Voice over LTE (VoLTE) and Video over LTE (ViLTE) applications, while still providing configurable exemptions for the special access classes.

SSAC operation is based on the same probabilistic mechanisms used for ACB as described previously in Clause 4.2.2.1. New parameters were introduced in SIB2 to facilitate SSAC operation. See Subclause 6.3.1 of 3GPP TS 36.331 [Ref 6]).

SSAC is implemented at the MultiMedia TELephony (MMTEL) layer, the application layer for Internet Protocol (IP) Multimedia Sub-system (IMS)-based voice and video and specified in Annex J.2.1.1 of 3GPP TS 24.173, *IMS Multimedia telephony communication service and supplementary services; Stage 3* [Ref 10]. It is the top of a user plane stack, including the IMS, Session Initiation Protocol (SIP), transport (e.g., TCP), IP, and then the common lower layers: Packet Data Convergence Protocol (PDCP), Radio Link Control (RLC), Medium Access Control (MAC), and Physical Layer (PHY). Due to the decision to implement SSAC at the MMTEL layer, two aspects were a particular concern in the design of the SSAC procedures:

- The MMTEL layer is not aware of SIB2 information available only within the RRC Layer; and
- The MMTEL layer cannot access the USIM, and therefore cannot determine access class membership from the USIM.

The agreed SSAC solution which addressed the above two problems was as follows:

- The MMTEL layer will request the relevant SIB2 information from the RRC Layer, and the RRC Layer will provide this in a response. To allow these layers to be implemented independently, a standardized means of exchange using the ATtention (AT) command set was agreed. See Subclause 7.37 of 3GPP TS 27.007 [Ref 11].
- The RRC layer will be responsible for implementing any exemptions required for the special access classes by altering the received SIB2 information prior to passing it in local variables to the MMTEL Layer. See Subclause 5.3.3.10 of 3GPP TS 36.331 [Ref 6].

NS/EP

As per Subclause 5.3.3.10 of 3GPP TS 36.331 [Ref 6], by virtue of being assigned to a valid access class in the range 11-15, the system can configure the UE to be exempt from SSAC. This is accomplished via information broadcast in SIB2 in the ssac-BarringForMMTEL-Voice-r9 (for voice exemption) and the ssac-BarringForMMTEL-Video-r9 (for video exemption) as defined in Subclause 6.3.1 of 3GPP TS 36.331 [Ref 6].

Emergency Services

As per Annex J.2.1.1 of 3GPP TS 24.173 [Ref 10], an emergency call is exempt from SSAC.

Emergency Services from an NS/EP subscribed UE

The SSAC exemption for emergency MMTEL voice and video calls does not depend on access class membership.

Relative Priority of NS/EP and Emergency Services

Emergency calls are always exempt from SSAC, while NS/EP can be configured to be exempt through configuration parameters signaled over the air interface by the eNodeB via SIB2 as detailed in the NS/EP discussion above.

4.2.2.3 Access Control for CSFB

This clause presents ACB for Circuit Switched Fallback (CSFB), a Release 10 enhancement to the ACB procedure described previously in Clause 4.2.2.1.

The Release 9 E-UTRAN provided the means to control access for voice service implemented via VoLTE using SSAC as described in Clause 4.2.2.2 but did not provide a means to control access for voice service delivered via CS fallback. ACB for Circuit Switched Fallback closed this gap in Release 10.

Unlike IMS services in which the call establishment signaling is communicated via the user plane and transparent to all FEs within the EPS (except the UE but the protocols are isolated), a Circuit Switched (CS) fallback call establishment via Universal Terrestrial Radio Access Network (UTRAN)/GSM Enhanced Radio Access Network (GERAN) is accomplished via the control plane, and is visible to the Mobility Management Entity (MME), eNodeB, and UE (both NAS and RRC). This allowed the new capability to be entwined in a careful manner with existing ACB functionality and provided a key advantage for voice via CSFB over voice via VoLTE. VoLTE was subject to two levels of access control, one at the MMTEL Layer due to SSAC, and the second at the NAS/RRC layers due to ACB. In contrast, CSFB only had to pass a single access control hurdle (at the NAS/RRC layer), which for certain configurations of access control provided priority for CSFB over VoLTE.

Three technical challenges drove the details of the solution:

- Not all UEs will support CSFB;
- Not all networks supporting CSFB will elect to use Release 10 ACB for CSFB capabilities, and may instead broadcast only pre-Release 10 ACB configurations; and
- Only the RRC layer (not the NAS) is aware of the broadcast (or absence) of the ACB for CSFB parameters.

The agreed ACB for CSFB solution which addressed the above challenges included the following aspects:

- The NAS determines the Call Type and Establishment Cause as per Annex D of 3GPP TS 24.301 [Ref 8]. For a UE supporting CSFB, the Call Type includes the CSFB specific value, the “mobile originated CS fallback” value, rather than the “mobile originated calls” value.
- The RRC must address all three technical challenges for the provided Call Type and select the applicable set of barring parameters to apply.
  a) For a “mobile originated CS fallback” Call Type, if the CSFB-specific parameters are included in SIB2, use those values. If barring is determined to be in effect, it impacts only future “mobile originated CS fallback” calls and does not impact any calls categorized with the “mobile originated calls” value.
  b) For a “mobile originated CS fallback” Call Type, if the CSFB-specific parameters are NOT included in SIB2, use the parameters associated with the “mobile originated calls” value. If barring is determined to be in effect, it impacts both future “mobile originated CS fallback” calls, and calls categorized with the “mobile originated calls” value.
  c) For a “mobile originated calls” Call Type, use the parameters associated with the “mobile originated calls” value. If barring is determined to be in effect, it impacts future calls categorized with the “mobile originated calls” value. In addition, if the CSFB-specific parameters are not included in SIB2, and the UE supports CSFB, barring of future “mobile originated CS fallback” calls is in effect.

Figure 4.1 depicts the applicability of the above three cases as a function of network and UE capabilities. The columns represent the cases where the system does broadcast CSFB-specific parameters in SIB2 (labeled yes) and the case where it does not (labeled no). The rows represent the case where a UE supports the CSFB-specific indicators (labeled yes) in which it can read the CSFB-specific parameters from SIB2 and can internally support the CSFB-specific Call Type indication between the NAS and RRC layers; and the case where the indicators are not supported (labeled no).

UE can interpret CSFB-specific indicators in SIB2 and supports CSFB-specific Call Type	SIB2 includes CSFB-specific barring parameters: Yes	SIB2 includes CSFB-specific barring parameters: No
Yes	If Call Type = “mobile originated CSFB” then **case A** applies. If Call Type = ”mobile originated calls” then **case C** applies	If Call Type = “mobile originated CSFB” then **case B** applies. If Call Type = ”mobile originated calls” then **case C** applies
No	If Call Type = ”mobile originated calls” then **case C** applies	

Figure 4.1 - Cases for selection of barring parameters according to whether SIB2 includes the CSFB-specific parameters, and whether the UE can interpret the parameters and internally support the CSFB-specific Call Type associated with these parameters.

NS/EP

As per Subclause 5.3.3.2 of 3GPP TS 36.331 [Ref 6], by virtue of being assigned to a valid access class in the range 11-15, the system can configure the UE to be exempt from ACB for CSFB.

This is accomplished via information broadcast in SIB2 in the ac-BarringForCSFB-r10 as defined in Subclause 6.3.1 of 3GPP TS 36.331 [Ref 6]. If this IE is not broadcast, NS/EP exemptions are provided by appropriate configurations in ac-BarringForMO-Data.

Beginning in Release 12, per-PLMN values of these IEs may be broadcast in a per-PLMN as well as a common portion of the SIB2.

Emergency Services

As per Subclause 5.3.3.2 of 3GPP TS 36.331 [Ref 6], an emergency call is exempt from ACB for CSFB.

Emergency Services from an NS/EP subscribed UE

Emergency calls are not impacted by NS/EP configurations of ACB for CSFB.

Relative Priority of NS/EP and Emergency Services

Emergency calls are always exempt from ACB for CSFB, while NS/EP can be configured to be exempt through configuration parameters signaled over the air interface by the eNodeB via SIB2 as detailed in the NS/EP discussion above.

4.2.2.4 Extended Access Barring (EAB)

This clause presents EAB, introduced in Release 11. EAB provides a means to manage system overload by restricting access from UEs which, by virtue of USIM configuration, are associated with particular access classes. Unlike ACB, SSAC, and ACB for CSFB, each of which depends upon the access class as well as the requested procedure, EAB was envisioned as a pure access class driven mechanism.

EAB was intended as a tool to manage access from Machine Type Communications (MTC) devices so the following simplifications were introduced:

- No dependence on the procedure for which the network access is required; and
- A return to the pre-Release 8 legacy bar/no-bar indication associated with the UMTS system.

The first simplification proved unviable and needed to be modified. There was a need for exemptions for page response, emergency calls, and for access from devices configured to be members of the special access classes. The agreed approach required changes only to the NAS logic to determine if EAB applies, so procedural independence was still achieved from the perspective of the RRC layer.

The evolution of EAB was done in parallel with the notion of a “NAS signalling low priority” indicator and the two features are conceptually linked. At one point in time, EAB was associated exclusively with RRC operation in the 3GPP RAN2 WG, and Low Priority Indication was associated with NAS operation in the 3GPP CT1 WG. In the agreed solution it is the responsibility of the NAS to indicate to the RRC that EAB applies or not, thus the NAS has common knowledge of the use of both of the mechanisms, while the RRC is only aware of EAB operation.

As per Annex D.1 of 3GPP TS 24.301 [Ref 8], EAB does not apply for the following cases:

- The UE is a member of a valid access class in the range 11 through 15 inclusive,
- The UE is answering to paging,
- The UE is placing an emergency call, or
- An application which is allowed to override EAB is started, or a Packet Data Network (PDN) connection supporting that application is already established.

The agreed solution included the following key aspects:

- The NAS is aware or, or can obtain EAB configuration information from the Mobile Equipment (ME) as per Clause 5 of 3GPP TS 24.368, *Non-Access Stratum (NAS) configuration Management Object (MO)* [Ref 14], or the USIM as per Subclause 4.2.94 of 3GPP TS 31.102 [Ref 9], and is aware of or can obtain access class membership from the USIM, as described in Subclause 4.2.15 of 3GPP TS 31.102 [Ref 9]. This provides the information needed by the NAS to determine if EAB applies or not based on UE configuration, and whether a special access class exemption applies or not.

- At the time that the NAS requests the RRC to establish an RRC Connection, an indication that EAB applies is provided to the RRC.
- The RRC layer is responsible for checking if the UE is allowed to access the system based on configuration information provided in system broadcast [System Information Block Type 14 (SIB14)] according to the procedure in Subclause 5.3.3 and Subclause 5.3.3.12 of 3GPP TS 36.331 [Ref 6]. One notable aspect is regarding the handling of common vs. PLMN-specific procedures. In all access control procedures PLMN-specific parameters take precedence over common parameters. The opposite is true for EAB, that is, if common parameters are present, the PLMN-specific broadcasts are ignored.
- The network can condition EAB functionality depending upon the PLMN serving the UE. Three cases are indicated via the eab-Category provided in SIB14 as specified in Subclause 6.3.1 of 3GPP TS 36.331 [Ref 6], listed in order of decreasing size of the set of applicable UEs:
    1. All UEs,
    2. UEs that are neither in their Home Public Land Mobile Network (HPLMN) nor in a PLMN that is equivalent to it, and
    3. UEs that are neither in the PLMN listed as most preferred PLMN of the country where the UEs are roaming in the operator defined PLMN selector list on the USIM, nor in their HPLMN nor in a PLMN that is equivalent to their HPLMN.

NS/EP

As per Annex D.1 of 3GPP TS 24.301 [Ref 8], by virtue of being assigned to a valid access class in the range 11-15, NS/EP NGN-PS is exempt from EAB.

Emergency Services

As per Annex D.1 of 3GPP TS 24.301 [Ref 8], emergency calls are exempt from EAB.

Emergency Services from an NS/EP subscribed UE

As access class membership in a special access class in the range 11-15 does not impact the emergency call exemption, an emergency call from an NS/EP subscribed UE is exempt from EAB.

Relative Priority of NS/EP and Emergency Services

Both emergency calls, and calls from an NS/EP subscribed UE are exempt from EAB.

4.2.2.5 Smart Congestion Management (SCM) and ACB skip

This clause presents Smart Congestion Management and ACB skip, introduced in Release 12. ACB skip is the mechanism which allows certain select identified applications to be exempt from barring by ACB without consideration of access class membership:

- MMTEL voice (i.e., VoLTE) as per 3GPP TS 24.173 [Ref 10];
- MMTEL video (i.e., ViLTE) as per 3GPP TS 24.173 [Ref 10]; and
- Short Message Service (SMS) over IP (not SIP Messaging) as per 3GPP TS 24.341, *Support of SMS over IP networks; Stage 3* [Ref 16], or Legacy SMS (e.g., SMS over NAS) as per 3GPP TS 24.011, *Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface* [Ref 15].

The agreed solution included the following key aspects:

- When there is an IP packet ready to be sent, it is necessary to notify the NAS via some implementation specific means. As the IP layer cannot read the contents of the packet to determine the higher layer

application that generated the packet, in order for the NAS to be aware of the specific application, it is the responsibility of the higher layer application to notify the NAS.

- Applications controlled by ACB skip are responsible for notifying the NAS layer that an instance of a service is in progress via the following service indicators:
  - When a MMTEL call requiring only audio begins/ends and no other MMTEL call requiring only audio is in progress, the MMTEL layer notifies the NAS using the MO-MMTEL-voice-started, or MO-MMTEL-voice-ended indications as specified in Annex J.2.1.2 of 3GPP TS 24.173 [Ref 10].
  - When a MMTEL call requiring video begins/ends and no other MMTEL call requiring video is in progress, the MMTEL layer notifies the NAS using the MO-MMTEL-video-started, or MO-MMTEL-video-ended indications as specified in Annex J.2.1.2 of 3GPP TS 24.173 [Ref 10].
  - When an SMS over IP attempt begins/ends and no other SMS over IP attempt is in progress, the SMS over IP applications notifies the NAS using the MO- SMS over IP (SMSovIP)-attempt-started, or MO-SMSovIP-attempt-ended indications as specified in Annex E of 3GPP TS 24.341 [Ref 16].
  - When a Legacy SMS attempt begins/ends and no other SMS over IP attempt is in progress, the Legacy SMS application notifies the NAS of the need to send an SMS using the EMMSMS-Est-Req, as shown in Annex A, Diagram A9 of 3GPP TS 24.011 [Ref 15].
- Except for emergency and mobile terminated calls, the service indicators defined above are the basis for the setting of the Call Type signaled by the NAS to the RRC layer.
- When more than one mobile originated MMTEL voice call, video call, or SMS over IP session is started, as per Subclause 5.6.1.6 of 3GPP TS 24.301 [Ref 8], it is left to UE implementation to determine the call type indicator sent by the NAS to the RRC layer.
- The RRC layer skips ACB for those services for which ACB skip indication is broadcast in SIB2, which may indicate ACB skip for MMTEL voice, ACB skip for MMTEL video, and/or ACB skip for SMS.

NS/EP

ACB skip does not provide a means to distinguish NS/EP NGN-PS calls from non-NS/EP NGN-PS calls.

The ACB skip capability eliminates the benefits of access class barring for NS/EP NGN-PS operation. The priority of non-emergency non-NS/EP NGN-PS calls are elevated to the priority of NS/EP NGN-PS calls, thus equating the priority of NS/EP NGN-PS with non-emergency non-NS/EP NGN-PS.

Emergency Services

ACB skip has no direct impact on emergency calls. The NAS to RRC Call Type indication marks the call as an emergency call, and as result, the algorithmic logic associated with ACB skip is not applied.

The application of ACB skip to non-emergency non-NS/EP NGN-PS calls eliminates the benefits of emergency access control, as it elevates the priority of non-emergency non-NS/EP NGN-PS calls while providing no advantage for emergency calls.

Emergency Services from an NS/EP-subscribed UE

Emergency calls from an NS/EP-subscribed device, from the point of view of ACB skip, are treated the same as emergency calls from a non-NS/EP-subscribed device.

Relative Priority of NS/EP and Emergency Services

ACB Skip does not impact the relative priority of an NS/EP NGN-PS call vs. an emergency call.

4.2.2.6 Application specific Congestion control for Data Communication (ACDC)

This clause presents Application specific Congestion control for Data Communications (ACDC), introduced in Release 13. ACDC provides a means to limit access from certain applications while permitting access from other applications.

ACDC operation entails a hierarchy of ACDC categories in which applications which should be less restricted are assigned to higher categories, and applications which can be more restricted are assigned to lower categories. An application not assigned to a specific category is denoted as uncategorized.

When an application of a particular category makes a request, and is barred, all subsequent requests at that level or a lower level category, including uncategorized requests, are barred for a duration controlled by a single timer. While conceptually feasible to have a separate timer for each ACDC category at the RRC layer, for simplification, a single timer approach was adopted. In the single timer approach, it is the responsibility of the NAS to not make ACDC requests for barred categories while barring is in effect. If the NAS makes a request for a higher ACDC category, the barring algorithm at the RRC layer resets the running timer prior to performing the barring calculation, then based on the outcome of the test may declare that barring is no longer in effect or may restart the timer with a new value.

A UE is configured with a minimum of 4 ACDC categories as per Subclause 5.3 of 3GPP TS 36.304, *Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode* [Ref 13]. A UE ACDC Managed Object in the ME may have up to 16 ACDC categories as per Subclause 5.4.13, Table 5.4.13 of 3GPP TS 24.105, *Application specific Congestion control for Data Communication (ACDC) Management Object (MO)* [Ref 12], where category 1 is the highest, category 16 is the lowest, and the value 0 is reserved. Also, the USIM ACDC Operating System (OS) configuration in Subclause 4.4.9.3 of 3GPP TS 31.102 [Ref 9], references the coding of 3GPP TS 24.105 [Ref 12].

The SIB2 broadcast by the eNodeB is aligned with UE specifications to have a maximum of 16 ACDC categories as per Subclause 6.3.1 of 3GPP TS 36.331 [Ref 6], but no minimum is provided with regard to the eNodeB broadcast in SIB2.

As per Annex F of 3GPP TS 24.301 [Ref 8], and as enforced by the NAS, ACDC does not apply for the following cases:

- The UE is a member of a valid access class in the range 11 through 15 inclusive,
- The UE is answering to paging,
- The UE is placing an emergency call, or
- An MMTEL voice call is started, an MMTEL video call is started, or and MO SMSoIP message is started.

ACDC operation includes the following key aspects:

- An application wishing to access the network, sends either an application identifier (which the NAS will map to an ACDC category) or “as an implementation option” an ACDC category.
- The NAS is aware of or can obtain ACDC configuration information from the ME as specified in Subclause 5.4 of 3GPP TS 24.105 [Ref 12], or from the USIM as described in Subclause 4.4.9 of 3GPP TS 31.102 [Ref 9]. This provides the information needed by the NAS to determine the ACDC category (or categories) from the application identifier based on UE configuration. As per Annex F of 3GPP TS 24.301 [Ref 8], if an application identifier received from upper layers is not mapped to any ACDC category, an application is described as uncategorized.
- The NAS is aware of or can obtain access class membership from the USIM as described in Subclause 4.2.15 of 3GPP TS 31.102 [Ref 9]. This provides the NAS the needed information to exempt the procedure from ACDC if the UE is a member of a valid special access class.
- If ACDC applies, as per Annex F of 3GPP TS 24.301 [Ref 8], the NAS passes the ACDC category to the RRC, where if multiple ACDC categories are applicable, only the highest ranked category is signaled to the RRC. If on the other hand, no category is assigned, applicability of ACDC is signaled, but no category is specified (case of an uncategorized application).
- If the RRC layer receives either a specific ACDC category, or indication that the application is uncategorized, as per Subclause 5.3.3 of 3GPP TS 36.331 [Ref 6], the ACDC barring evaluation is

performed, and the ACB barring evaluation (including ACB for CSFB, and ACB skip) is not performed. The ACDC barring check details are specified in Subclause 5.3.3.13 of 3GPP TS 36.331 [Ref 6].

- If the RRC layer determines the request is barred, the NAS is notified as described in Subclause 5.3.3 of 3GPP TS 36.331 [Ref 6]. This indication bars requests from the ACDC category of the request and requests from all lower ACDC categories, including requests which are uncategorized. Requests from higher ACDC categories are still permitted.

NS/EP

As per Annex F of 3GPP TS 24.301 [Ref 8], by virtue of being assigned to a valid access class in the range 11-15, an NS/EP NGN-PS subscribed UE is exempt from ACDC.

Emergency Services

As per Annex F of 3GPP TS 24.301 [Ref 8], emergency calls are exempt from ACDC.

Emergency Services from an NS/EP subscribed UE

The emergency exemption is not impacted by membership in a valid access class in the range 11-15.

Relative Priority of NS/EP and Emergency Services

Both emergency calls, and calls from an NS/EP subscribed UE are exempt from ACDC.

4.2.2.7 Access Barring (AB)

This clause presents Access Barring for NarrowBand Internet of Things (NB-IoT), introduced in Release 13.

NB-IoT is a non-backward compatible variant of E-UTRAN supporting a reduced set of functionality. From an RRC point of view this comprised defining a parallel set of NB-IoT RRC messages derived as a simplification of existing RRC messages with limited new IEs, and removal of many features and procedural options. Regarding UE-based access control, all existing mechanisms (including ACB, EAB, SSAC and ACDC) were replaced by the single new Access Barring for NB-IoT mechanism.

To avoid creation of an entirely new capability, 3GPP RAN2 designed Access Barring for NB-IoT based on the existing EAB mechanism, described previously in Clause 4.2.2.4. Rather than repeat much of the EAB discussion, this clause highlights only the differences between EAB and AB first considering procedural aspects, then considering system information broadcast details. The assumption is that the EAB and AB bitmaps are established independently.

3GPP TS 36.331 [Ref 6] provides the procedural description of AB in Subclause 5.3.3.14, based entirely on the EAB procedure in Subclause 5.3.3.12 with only the following changes:

1. Application of AB is contingent upon signaling an “ab-Enabled” indication in the “MasterInformationBlock-NB” broadcast by the eNodeB. No such indication was defined in the “MasterInformationBlock” for EAB.
2. The “mo-ExceptionData” value of the “EstablishmentCause-NB” IE, defined only for NB-IoT operation, when provided by the NAS, provides a barring exemption from AB, when such an exemption is configured by the network and broadcast to the UE in System Information Block Type 14 - NarrowBand (SIB14-NB). No such value is defined in the “EstablishmentCause” IE, so there is no equivalent exemption needed for EAB.
3. A barring exemption for a UE that is a member of a valid access class in the range 11 through 15 is coded within the RRC procedure. For EAB, the exemption was the responsibility of the NAS layer. This change localizes the decision process within the RRC and implies the RRC needs to check the USIM for access class membership, rather than the NAS checking the USIM as was required for EAB.

The system information broadcast information for AB is provided in SIB14-NB as specified in Subclause 6.7.3.1 of 3GPP TS 36.331 [Ref 6]. SIB14-NB is based on the SIB14 used for EAB and differs only in the inclusion of two additional fields:

1. An indication of whether ExceptionData is subject to barring is provided in ab-ExceptionData. As the concept of ExceptionData is unique to NB-IoT, this indicator is not required for EAB.
2. The applicability of AB for the special access classes 11-15 is provided in ab-BarringForSpecialAC. The network can configure a particular access class to be subject to, or exempt from AB. In the case of EAB, the AC 11-15 exemption applies at all times.

As per Subclause 4.1 of 3GPP TS 36.331 [Ref 6], NB-IoT does not support real time services (e.g., voice, video), including emergency calls.

NS/EP

As neither voice, nor video calls (or any real time services) are supported on NB-IoT, neither NS/EP NGN-PS Voice nor NS/EP NGN-PS Video are supported.

However, the NS/EP NGN-PS Data Transport Service, as defined in ATIS-1000065 [Ref 3], is supported.

As per Subclause 5.3.3.14 of 3GPP TS 36.331 [Ref 6], by virtue of being assigned a valid access class in the range 11-15, the system can configure the UE to be exempt from AB. This is accomplished via information broadcast in SIB14-NB in the ab-BarringForSpecialAC as defined in Subclause 6.7.3.1 of 3GPP TS 36.331 [Ref 6].

Emergency Services

Emergency Services are not supported on NB-IoT.

Emergency Services from an NS/EP subscribed UE

Emergency Services are not supported on NB-IoT.

Relative Priority of NS/EP and Emergency Services

Emergency Services are not supported on NB-IoT.

4.2.2.8 eNodeB-based Access Control

This clause presents eNodeB-based access control mechanisms which signal the UE to not initiate access to the system for an indicated time:

- The Reject case of RRC Connection Establishment, introduced in Release 8; and
- Backoff signaled as part of RRC Connection Release, introduced in Release 10.

The eNodeB may reject a request to establish an RRC connection and instruct the UE to not submit another request for a specified time. In times of overload the eNodeB may employ this mechanism to limit the signaling load received from UEs.

Subclause 5.3.3.8 of 3GPP TS 36.331 [Ref 6] specifies the actions to be taken by the UE upon receipt of a “RRCConnectionReject” message. The contents of the “RRCConnectionReject” message are specified in Subclause 6.2.2 of 3GPP TS 36.331 [Ref 6].

The “RRCConnectionReject” message includes a “waitTime” which specifies the time that the UE must wait before reattempting to establish an RRC connection. The “waitTime” is an integer between the values 1 and 16 seconds inclusive. The UE sets the value of the T302 timer to be the value received in the “waitTime” IE.

When timer T302 is running, the UE may not request the Establishment of an RRC connection unless the request is to initiate an emergency call. This emergency call exemption is specified in Subclause 5.3.3.2 of 3GPP TS 36.331 [Ref 6].

> NOTE: The location of the requirement that other reasons for access are subject to T302 was found in Subclause 5.3.3.2 in Releases 8 and 9, then all were moved to Subclause 5.3.3.11 beginning in Release 10, except for the case of an access for a mobile terminated call which remained in Subclause 5.3.3.2.

The introduction of “delay tolerant” in Release 10 and NB-IoT UEs in Release 13 added some further complexities. These complexities were added in a careful manner to not impact NS/EP NGN-PS or Emergency Services as follows.

Beginning in Release 10, to accommodate the needs to further restrict access attempts from “delay tolerant” UEs beyond the 16 second maximum backoff, the “extendedWaitTime” IE was defined and introduced into the “RRCConnectionReject” message, and also into the “RRCConnectionRelease” message. The “extendedWaitTime” is an integer between 1 and 1800 seconds (30 minutes) inclusive. This IE does not impact the RRC layer but is passed to the NAS layer if the UE supports delay tolerant access. Within the NAS layer, as per 3GPP TS 24.301 [Ref 8], under certain conditions (an Attach, Tracking Area Update, or Extended Service Request contains a “NAS signalling low priority indicator” set to “MS is configured for NAS signalling low priority” or a Service Request is sent from a UE configured for low priority) the value contained in the “extendedWaitTime” is used to start the mobility management backoff timer T3346. UEs with valid AC11-15 (which includes UEs with a subscription to NS/EP NGN-PS), and emergency calls are both exempt from T3346. See also the discussion of MME overload control in Clause 4.2.3.2 for other usage of T3346.

Beginning in Release 13, NB-IoT was introduced into 3GPP specifications. The NB-IoT messages “RRCConnectionReject-NB” and “RRCConnectionRelease-NB” adopted use of the “extendedWaitTime” IE, with the values defined above. Again, the IE does not impact the RRC layer. It is passed to the NAS layer when the UE is operating as an NB-IoT UE. NAS layer treatments are as described above with the addition that T3346 is also started if the UE is operating in NarrowBand S1 (NB-S1) mode.

Beginning in Release 14, to provide more granular control of access from NB-IoT UEs, and specifically related to support of Cellular Internet of Things (CIoT) optimization, the “extendedWaitTime-CPdata” IE was defined and included within the “RRCConnectionRelease-NB” message, as per Subclause 6.7.2 of 3GPP TS 36.331 [Ref 6]. The RRC layer within the UE will pass the “extendedWaitTime-CPdata” IE upward to the NAS layer only if the UE only supports Control Plane CIoT optimization, as per Subclause 5.3.8.3 of 3GPP TS 36.331 [Ref 6].

Within the NAS layer, as per Subclause 5.5.3.2.6 paragraph “ka” and Subclause 5.6.1.6 paragraph “la” of 3GPP TS 24.301 [Ref 8], if the UE is operating in NB-S1 mode, the “extendedWaitTime-CPdata” IE is copied to timer T3448, if the UE supports the control plane back-off timer T3448, else it is copied to timer T3346. Previously described exemptions for T3346 still apply. AC 11-15 exemptions for T3448 to support the needs of MPS are specified in Subclause 5.5.3.2.6 paragraph “la” and Subclause 5.6.1.6 paragraph “o” of 3GPP TS 24.301 [Ref 8]. As T3448 applies only to control plane data transfer, which does not support Emergency Services, no emergency exemptions are provided.

NS/EP

While an NS/EP NGN-PS subscribed UE is exempt from the NAS timers T3346 and T3448, an NS/EP NGN-PS subscribed UE cannot initiate communication with the network while the RRC timer T302 is running.

Emergency Services

An emergency call is exempt from the NAS timer T3346 and can be initiated while RRC timer T302 and/or T3448 are running.

Emergency Services from an NS/EP subscribed UE

An emergency call can be initiated from an NS/EP subscribed UE while RRC timer T302 and/or NAS timers T3346 and/or T3448 are running.

Relative Priority of NS/EP and Emergency Services

While NS/EP NGN-PS subscribed UEs and emergency calls from any UE are both exempt from NAS timers T3346 and T3448, as an NS/EP NGN-PS subscribed UE is subject to the RRC timer T302 and emergency calls from any UE are exempt from RRC timer T302, emergency calls have priority over NS/EP NGN-PS.

4.2.3 Congestion & Overload Controls

This clause presents congestion and overload control mechanisms in the LTE system applied either at the time of establishment or during a call/session, and highlights those aspects specific to Emergency Services and NS/EP NGN-PS.

4.2.3.1 eNodeB

This clause focuses on the use of the Allocation and Retention Priority (ARP) to influence scheduler behavior and the selection of the DiffServ Code Point (DSCP) for IP packets sent towards the Serving Gateway (S-GW).

These aspects are discussed in detail in ATIS-1000079, *National Security Emergency Preparedness Next Generation Network Priority Service (NS/EP NGN-PS): Transport Level Packet Marking and Packet Scheduling* [Ref 21].

Beginning in Release 15, the ARP Priority Level in addition to the Quality of Service Class Identifier (QCI) Priority Level may be used by the scheduler to determine which packet to serve when the QCI Packet Delay Budget (PDB) cannot be met for all established Service Data Flows (SDFs). See Subclause 4.7.3 of 3GPP TS 23.401 [Ref 7].

Beginning in Release 14, the QCI and optionally the Allocation Retention Priority (ARP) priority level may be used to determine the DSCP value, or other transport specific information element. This allows the transport level packet marking to be set properly for priority traffic, based on the QCI and ARP priority level of the associated Evolved Packet System (EPS) bearer. See Subclause 4.4.10 of 3GPP TS 23.401 [Ref 7].

As per ATIS-1000065 [Ref 3], in Requirement 64, at least 3 ARP Priority Levels are allocated for NS/EP NGN-PS (denoted here as “NS/EP NGN-PS ARPs”). The concept of an “Emergency ARP” in 3GPP TS 23.401 [Ref 7] includes special treatments during Attach in Subclause 5.3.2 and during Tracking Area Updates in Subclause 5.3.3.

The dedicated “NS/EP NGN-PS ARPs” and “Emergency ARP” trigger the required scheduler behavior at the eNodeB and setting of uplink transport level markings by the eNodeB.

NS/EP

The assignment of dedicated “NS/EP NGN-PS ARPs” to EPS Bearers associated with NS/EP NGN-PS triggers the required scheduler behavior at the eNodeB and setting of uplink transport level markings by the eNodeB.

Emergency Services

The assignment of a dedicated “Emergency ARP” for Emergency Bearer Services triggers the required scheduler behavior at the eNodeB and setting of uplink transport level markings by the eNodeB.

Emergency Services from an NS/EP subscribed UE

The assignment of a dedicated “Emergency ARP” for Emergency Bearer Services triggers the required scheduler behavior at the eNodeB and setting of uplink transport level markings by the eNodeB.

Relative Priority of NS/EP and Emergency Services

The relative priority is not specified by 3GPP. The appropriate tools are in place to configure the desired behavior consistent with national regulation and operator policy.

4.2.3.2 MME

Congestion control functionality for the MME is specified in several places in 3GPP Stage 3 specifications. This clause discusses aspects presented within 3GPP TS 24.301 [Ref 8]. It also discusses MME control of overload over S1-AP as specified in 3GPP TS 36.413, Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP) [Ref 17].

TS 24.301 is the NAS specification for signaling between the UE and the EPC, specifically the MME. NAS messages are carried within RRC messages (3GPP TS 36.331 [Ref 6]) over the Uu Interface between the UE and the eNodeB. They are carried within S1-AP messages (as defined in 3GPP TS 36.413 [Ref 17]) over the S1-AP Interface between the eNodeB and the MME.

Overload and congestion control for EPS Mobility Management (EMM) and EPS Session Management (ESM) procedures are found in 3GPP TS 24.301 [Ref 8] in Clauses 5 and 6 respectively. Accordingly, the EMM and ESM materials are provided in separate subclauses below where it is shown that Emergency Services and NS/EP NGN-PS receive comparable treatment from the perspective of MME congestion control. MME control of overload using the “Overload Action” IE is specified in 3GPP TS 36.413 [Ref 17] and is described in an additional subclause below.

4.2.3.2.1 EPS Mobility Management (EMM)

The ability of the MME to reject an EMM procedure request from the UE with cause identified to be congestion was added in Release 10.

When the MME rejects an EMM procedure due to congestion it signals the EMM cause value to #22 “congestion” and also provides a back-off timer T3346 which prevents any further EMM procedure requests from the UE while the timer is running.

Comparable exemptions which are provided for both NS/EP NGN-PS and Emergency Services include:

- a general exemption,
- procedure-specific exemptions, and
- a Service Request attempt counter.

A general exemption for EMM Congestion Control was provided in Subclause 5.3.9 of 3GPP TS 24.301 [Ref 8]. In Release 10 both Emergency Services and “high priority users” were exempt. In Release 11 “high priority users” was clarified as “High priority access AC 11 – 15” users configured to use one of the special access classes 11-15.

Procedural exemptions for each EMM procedure were implemented as an exemption to the restrictions associated with timer T3346 as shown in Table 4.1.

Table 4.1 - Location in 3GPP TS 24.301 where the emergency and NS/EP NGN-PS exemptions to T3346, the EMM backoff timer, are specified.

Procedure Type	Procedure Name	Location of Exemptions	Notes
EMM specific procedures	Attach	§5.5.1.2.6 case m	(Note 1)
	Combined Attach (EPS and non-EPS)	§5.5.1.3.6	Cross reference to §5.5.1.2.6 since Release 8.
	Tracking Area Update (TAU)	§5.5.3.2.6 case l	(Note 1)
	Combined TAU	§5.5.3.3.6	Cross reference to §5.5.3.2.6 since Release 8.

Procedure Type	Procedure Name	Location of Exemptions	Notes
EMM connection management procedures	Service Request / Extended Service Request	§5.6.1.6 case m	(Note 1)
	UL NAS Transfer	§5.6.3.4	Used for SMS (Note 1)
	UL Generic NAS Transfer	§5.6.4.4	Used for protocol messages from application layer (Note 1)

Note 1: Initially added in 3GPP Release 10. Release 12 clarified AC 11-15 to be “in selected PLMN.”

For the Service Request Procedure, beginning in Release 12, there is an attempt counter which is incremented upon expiry of a timer supervising the procedure. The counter allows the UE to make at most 5 attempts. Timer T3417 supervises the procedure except for the case of CSFB to UTRAN/GERAN which is supervised by T3417ext. Two exemptions for Emergency Bearer Services and NS/EP NGN-PS are specified in Subclause 5.6.1.6 of 3GPP TS 24.301 [Ref 8]:

- The counter is not incremented; and
- The maximum try limit of 5 is not observed.

If the Service Request attempt counter reaches 5, the UE is precluded from attempting Service Requests. In a Release 12 system, the duration of this restriction is specified to be 1 minute, while for a Release 13 or later system, the duration is controlled by a configurable timer T3325. In both cases, exemptions are in place for Emergency Bearer Services and NS/EP NGN-PS.

4.2.3.2.2 EPS Session Management (ESM)

The ability of the MME to reject an ESM procedure request from the UE with cause identified to be congestion was added in Release 10.

When the MME rejects a UE-requested ESM procedure due to congestion it signals the ESM cause value to #26 “insufficient resources” and also provides a per-Access Point Name (APN) back-off timer T3396 which prevents any further ESM procedure requests from the UE to that APN while the timer is running.

Beginning in Release 12, another back-off timer, the “back-off timer” is added. It is a per PLMN, per APN, per procedure timer that applies when the rejection is due to an ESM cause other than insufficient resources and prevents further requests for that specific procedure to that particular PLMN and APN.

To avoid confusion between the “T3396” back-off timer, and the “back-off timer” procedural text involving these two timers is always included in separate subclauses, while the applicable timer is signaled to the UE in the “back-off timer value” IE.

There are two types of exemptions specified in 3GPP TS 24.301 [Ref 8]:

- An MME exemption where the MME does not include the timer in a failure response known to be associated with Emergency Services or NS/EP NGN-PS; and
- A UE exemption which allows it to ignore the timer when accessing using AC 11-15 or requesting Emergency Service.

Comparable exemptions are provided for both NS/EP NGN-PS and Emergency Services for each of the timers: T3396 and the back-off timer. The location in the specification is summarized in Table 4.2.

Table 4.2 - Location in 3GPP TS 24.301 where the "emergency" and NS/EP NGN-PS exemptions to the ESM T3396 and "back-off timer" timers are specified.

3GPP Release	T3396		back-off timer	
	MME exemption	UE exemption	MME exemption	UE exemption
Release 10	§6.5.1.4	§6.5.1.4	N/A	
Release 11				
Release 12	§6.5.1.4.1	§6.5.1.4.2	§6.5.1.4.1	§6.5.1.4.3
Release 13 (Note 1)		§6.5.1.4.2 for "emergency" §6.5.3 for NSEP		§6.5.1.4.3 for "emergency" §6.5.4 for NSEP

Note 1: The Release 13 NS/EP NGN-PS exemptions also apply for the UE requested bearer resource allocation and UE requested bearer resource modification procedures. These procedures are disallowed for emergency connections, so specific emergency exemptions are not required.

4.2.3.2.3 MME control of overload via the Overload Action IE

The MME may signal the eNodeB of the need for congestion control using the S1-AP protocol over the S1-MME interface. The S1-AP "Overload" message from the MME to the eNB provides the type of traffic to be filtered via the "Overload Action" IE. Each "Overload Action" IE maps to either a list of "Establishment Cause" values to be allowed or to a list of "Establishment Cause" values to be rejected.

The RRC "Establishment Cause" IE is defined in 3GPP TS 36.331 [Ref 6]. The S1-AP "Overload Action" IE and mapping rules to "Establishment Cause" values are defined in 3GPP TS 36.413 [Ref 17]. There are differences in Release 8, Release 9, Release 10/11, and Release 12/13/14 that are of interest to NS/EP NGN-PS and Emergency Services.

In the figures that follow the following conventions are used:

- For Overload Actions based on a list of rejected "Establishment Cause" values, an "X" indicates an explicit reject action, and all causes not rejected are implicitly allowed;
- For Overload Actions based on a list of allowed "Establishment Cause" values, a "✓" indicates an explicit allow action, and all causes not allowed are implicitly rejected;
- Allowed Establishment Causes are denoted by a green shaded cell; and
- Rejected establishment causes are denoted by a red shaded cell.

4.2.3.2.3.1 Release 8

The five RRC "Establishment Cause" IE values, three "Overload Action" IE values and the mapping between them is provided in Figure 4.2.

Release 8

Establishment Cause	Overload Action (see key below) 1	2	3
mo-Data	X	X	
mo-Signalling		X	
emergency			✓
highPriorityAccess			
mt-Access			

Key to "Overload Action" IE
1. reject-non-emergency-mo-dt
2. reject-all-rrc-cr-signalling
3. permit-emergency-sessions-only

Figure 4.2 - Mapping of the S1-AP "Overload Action" IE to the RRC "Establishment Cause" IE in 3GPP Release 8.

The Release 8 approach is based on the progression: first, block the flow of data but maintain signaling connectivity so the UE location remains known; and then block both data and signaling. Exemptions from this progression were defined for emergency calls, mobile terminated sessions, and UEs entitled to use the "highPriorityAccess" marking.

NSEP

NS/EP NGN-PS subscribed UEs are members of the special access class set and will therefore always use the "highPriorityAccess" marking when accessing the system. Under all overload actions except under the "permit-emergency-sessions-only" overload action, NS/EP NGN-PS subscribed UEs will be allowed by this overload control. Under the "permit-emergency-sessions-only" overload action, all access from an NGN Priority Service User's UE will be blocked by overload control, including the placing of emergency calls.

Emergency Services

Emergency calls were intended to be allowed under all overload actions. However, if an emergency call is placed from a UE accessing the network using the "highPriorityAccess" value of the Establishment Cause, it will be blocked under the "permit-emergency-sessions-only" overload action. Furthermore, this overload action would block any emergency call back attempt.

4.2.3.2.3.2 Release 9

The five RRC "Establishment Cause" IE values, three "Overload Action" IE values and the mapping between them is provided in Figure 4.3.

Release 9

Establishment Cause	Overload Action (see key below) 1	2	3
mo-Data	X	X	
mo-Signalling		X	
emergency			✓
highPriorityAccess			
mt-Access			✓

Key to "Overload Action" IE

1. reject-non-emergency-mo-dt
2. reject-all-rrc-cr-signalling
3. permit-emergency-sessions-and-mobile-terminated-sessions-only

Figure 4.3 - Mapping of the S1-AP "Overload Action" IE to the RRC "Establishment Cause" IE in 3GPP Release 9.

The overload action "permit-emergency-sessions-only" was replaced by the "permit-emergency-and-mobile-terminated-sessions-only" overload action which solved the emergency call back problem of Release 8.

NSEP

NS/EP NGN-PS subscribed UEs are members of the special access class set and will therefore always use the "highPriorityAccess" marking when accessing the system. Under all overload actions except the "permit-emergency-and-mobile-terminated-sessions-only" value, NS/EP NGN-PS subscribed UEs will allowed by this overload control. Under the "permit-emergency-and-mobile-terminated-sessions-only" overload action, all access from an NS/EP NGN-PS subscribed UE will be blocked by overload control, including the placing of an emergency call.

Emergency Services

Emergency calls were intended to be allowed under all overload actions. However, if an emergency call is placed from a UE accessing the network using the "highPriorityAccess" value of the Establishment Cause, it will be blocked under the "permit-emergency-and-mobile-terminated-sessions-only" overload action.

4.2.3.2.3.3 Release 10 and Release 11

The six RRC "Establishment Cause" IE values, five "Overload Action" IE values and the mapping between them is provided in Figure 4.4.

Release 10, 11

Establishment Cause	Overload Action (see key below)				
	1	2	3	4	5
delayTolerantAccess	X	X	X		
mo-Data		X	X		
mo-Signalling			X		
emergency				✓	
highPriorityAccess					✓
mt-Access				✓	✓

Key to "Overload Action" IE

1. reject-delay-tolerant-access
2. reject-non-emergency-mo-dt
3. reject-rrc-cr-signalling
4. permit-emergency-sessions-and-mobile-terminated-services-only
5. permit-high-priority-sessions-and-mobile-terminated-services-only

Figure 4.4 - Mapping of the S1-AP "Overload Action" IE to the RRC "Establishment Cause" IE in 3GPP Releases 10 and 11.

The "delayTolerantAccess" value of the "Establishment Cause" IE is introduced for control of MTC devices which were viewed as a threat to the service quality of the existing customer base.

Two new Overload actions are added: the "reject-delay-tolerant-access" and "permit-high-priority-sessions-and-mobile-terminated-services-only" values, and the value "reject-all-rrc-cr-signalling" is renamed "reject-rrc-cr-signalling" without change in usage.

Existing Overload actions based on a list of rejected "Establishment Cause" values are modified to also disallow the "delayTolerantAccess" value.

With the "permit-high-priority-sessions-and-mobile-terminated-services-only" value it is possible to give priority to access from NS/EP NGN-PS subscribed UEs, while blocking all emergency calls from non-NS/EP NGN-PS subscribed UEs.

Stepwise Load Reduction is introduced in Release to allow the rejection of a specified percentage of RRC connection requests with a particular set of establishment causes identified using the "Overload Action" IE. The percentage reduction is carried in the newly specified "Traffic Load Reduction Indication" IE as an integer from 0 to 99 inclusive. This reduction applies equally to all identified establishment causes that are subject to RRC overload control.

NSEP

NS/EP NGN-PS subscribed UEs are members of the special access class set and will therefore always use the "highPriorityAccess" marking when accessing the system. Under all overload actions except under the "permit-emergency-and-mobile-terminated-sessions-only" overload action, NS/EP NGN-PS subscribed UEs will allowed by this overload control. Under the "permit-emergency-and-mobile-terminated-sessions-only" overload action, all access from an NS/EP NGN-PS subscribed UE will be blocked by overload control, including the placing of an emergency call. Under the "permit-high-priority-sessions-and-mobile-terminated-services-only" any access from NS/EP NGN-PS subscribed UEs is allowed.

Emergency Services

Emergency calls are allowed under all overload actions, except the "permit-high-priority-sessions-and-mobile-terminated-services-only" overload action which blocks emergency calls from non-NS/EP NGN-PS subscribed UEs but permits emergency calls from NS/EP NGN-PS subscribed UEs.

4.2.3.2.3.4 Release 12, 13, and 14

The seven RRC "Establishment Cause" IE values, five "Overload Action" IE values and the mapping between them is provided in Figure 4.5.

Release 12, 13, 14

	Overload Action (see key below)				
Establishment Cause	1	2	3	4	5
delayTolerantAccess	X	X	X		
mo-Data		X	X		
mo-VoiceCall		X	X		
mo-Signalling			X		
emergency				✓	
highPriorityAccess					✓
mt-Access				✓	✓

Key to "Overload Action" IE

1. reject-delay-tolerant-access
2. reject-non-emergency-mo-dt
3. reject-rrc-cr-signalling
4. permit-emergency-sessions-and-mobile-terminated-services-only
5. permit-high-priority-sessions-and-mobile-terminated-services-only

Figure 4.5 - Mapping of the S1-AP "Overload Action" IE to the RRC "Establishment Cause" IE in 3GPP Releases 12, 13, and 14.

Release 12 adds the "mo-VoiceCall" value of the "Establishment Cause" IE. Overload Action definitions are revised to treat the "mo-VoiceCall" value the same as "mo-Data" value. The treatments afforded to NS/EP NGN-PS subscribed UEs and to Emergency access are not impacted by this addition and are the same as in Release 11.

4.2.3.2.3.5 Summary Observations on the Overload Action IE

Configurations which deny access to NS/EP NGN-PS subscribed UEs, and block emergency calls in some/all cases are described.

To protect the needs of NS/EP NGN-PS, the following configurations are a concern:

- A Release 8 system using the "permit-emergency-sessions-only" overload action blocks all access attempts from an NS/EP NGN-PS subscribed UE including emergency calls; and
- A Release 9, 10, 11, 12, 13, or 14 system which uses use the "permit-emergency-sessions-and-mobile-terminated-sessions-only" overload action blocks all access attempts from an NS/EP NGN-PS subscribed UE including emergency calls.

The above configuration is precluded for a Release 10 system by ATIS-1000065 [Ref 3] requirement [190] which states:

> An MME shall not use the "Permit Emergency Sessions and mobile terminated services only" overload action.

To protect the needs of Emergency Services, the following configurations are a concern:

- A Release 8 system which uses the "permit-emergency-sessions-only" value blocks all emergency calls from NS/EP NGN-PS subscribed UEs, and blocks emergency call back;
- A Release 9 should which uses the "permit-emergency-sessions-and-mobile-terminated-services-only" value, blocks all emergency calls from NS/EP NGN-PS subscribed UEs; and
- A Release 10, 11, 12, 13, or 14 systems which uses the "permit-high-priority-sessions-and-mobile-terminated-services-only" blocks all emergency calls from non-NS/EP NGN-PS subscribed UEs but allows emergency calls from NS/EP NGN-PS subscribed UEs.

4.2.3.3 Packet Data Network Gateway (PDN-GW) Control of Overload

This clause focuses on PDN-GW specific procedures related to rejection of a PDN connection request and the PDN-GW backoff signaled to the MME, introduced in Release 10.

Subclause 4.3.7.5 of 3GPP TS 23.401 [Ref 7] allows a PDN-GW to reject a PDN connection request and provide a PDN-GW back-off time for subsequent requests to a particular APN.

Subclause 7.2.2 of 3GPP TS 29.274*, 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3* [Ref 18] specifies that the "Create Session Response" message optionally contains the "PDN-GW Back-Off Time" IE which indicates the time during which the MME or S4-SGSN should refrain from sending subsequent PDN connection establishment requests to the PDN-GW for the congested APN for services other than Service Users/Emergency Services.

General Packet Radio Service (GPRS) Tunneling Protocol for the Control Plane (GTP-C) overload control, a Release 12 capability described in Clause 4.2.3.4, overlaps with PDN-GW control of overload. As per Subclause 4.3.7.1a.2 of 3GPP TS 23.401 [Ref 7], beginning in Release 12, for a given APN, both PDN-GW back-off and GTP-C overload control are not used by the PDN-GW at the same time. See also Subclause 12.3.8 of 3GPP TS 29.274 [Ref 18].

NS/EP NGN-PS exemptions from the PDN-GW back-off procedure are included in Subclause 4.3.18.5 of 3GPP TS 23.401 [Ref 7]. Stage 3 exemptions for both NS/EP NGN-PS and Emergency Services are in place in Subclause 7.2.2 of 3GPP TS 29.274 [Ref 18].

NS/EP NGN-PS is initially identified via the "highPriorityAccess" value of the "Establishment Cause" IE as specified in Subclause 4.3.18.1 of 3GPP TS 23.401 [Ref 7], and Annex D of 3GPP TS 24.301 [Ref 8], and subsequently verified against subscription data as specified in Subclause 5.2.1.1.2 of 3GPP TS 29.272, *Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol* [Ref 19] via the "MPS-Priority" Attribute Value Pair (AVP). As per Subclause 7.3.131 of 3GPP TS 29.272 [Ref 19], the "MPS-EPS-Priority" bit of the "MPS-Priority" AVP indicates the UE is subscribed to MPS in the EPS.

A request for an emergency call is identified via the "emergency" value of the "Establishment Cause" IE as specified in Annex D of 3GPP TS 24.301 [Ref 8], but the "emergency" value is replaced by the "highPriorityAccess" value when the UE is a member of a valid Access Class in the range of 11-15. When Emergency Bearer Services are requested by a UE, as per 3GPP TS 24.301 [Ref 8], the "PDN connectivity request" message of Subclause 8.3.20 contains the "Request Type" IE of Subclause 9.9.4.1.4. The encoding of the "Request Type" IE is specified in Subclause 10.5.6.17 of 3GPP TS 24.008, *Mobile radio interface Layer 3 specification; Core network protocols; Stage 3* [Ref 20] to be set to the "emergency" value when a PDN connection associated with Emergency Bearer Services is requested.

NS/EP

The "PDN-GW Back-Off Time" does not apply to NS/EP NGN-PS.

Emergency Services

The “PDN-GW Back-Off Time” does not apply to Emergency Services.

Emergency Services from an NS/EP subscribed UE

The “PDN-GW Back-Off Time” does not apply to Emergency Services from an NS/EP NGN-PS subscribed UE.

Relative Priority of NS/EP and Emergency Services

Both NS/EP NGN-PS and Emergency Services are exempt from any back-off signaled in the “PDN-GW Back-Off Time” IE.

4.2.3.4 General GTP-C Overload Control

This clause focuses on GTP-C overload control, introduced in Release 12 as a general overload mechanism which includes a means to signal an overload reduction metric between a pair of GTP-C nodes.

Subclause 4.3.7.1a.2 of 3GPP TS 23.401 [Ref 7] specifies that nodes using GTP-C may support communication of “Overload Control Information” in order to mitigate an overload condition through actions taken by the peer node(s). The “Overload Control Information” may convey information regarding the node itself and/or be specific to one or more APNs.

Subclause 12.3.9.1 of 3GPP TS 29.274 [Ref 18] specifies that a GTP-C entity shall throttle the transmission of messages towards the overloaded peer based on the information received within the “Overload Control Information” IE. Message throttling is achieved by discarding a fraction of the messages indicated in the “Overload Reduction Metric” IE, set in proportion to the overload level of the target peer.

PDN-GW control of overload, described in Clause 4.2.3.3, overlaps with GTP-C overload control. As per Subclause 4.3.7.1a.2 of 3GPP TS 23.401 [Ref 7], for a given APN, both PDN-GW back-off and GTP-C overload control for are not used by the PDN-GW at the same time. See also Subclause 12.3.8 of 3GPP TS 29.274 [Ref 18].

NS/EP NGN-PS and emergency exemptions from GTP-C overload control are included in Subclause 4.3.7.1a.2 of 3GPP TS 23.401 [Ref 7] which recites the need to allow for preferential treatment of MPS users and Emergency Services. Stage 3 exemptions for NS/EP NGN-PS and Emergency Services are included in Subclause 12.3.9.3.1 of 3GPP TS 29.274 [Ref 18] which states that GTP-C requests related to priority traffic (MPS and Emergency Services) have the highest priority, and that subject to regional/national requirements and network operator policy, these requests shall be the last to be throttled, when applying traffic reduction, and this priority traffic shall be exempted from throttling due to GTP-C overload control up to the point where the requested traffic reduction cannot be achieved without throttling the priority traffic.

The identification of NS/EP NGN-PS and emergency call/sessions is described in Clause 4.2.3.3.

NS/EP

NS/EP NGN-PS is exempt from GTP-C overload control.

Emergency Services

Emergency Services are exempt from GTP-C overload control.

Emergency Services from an NS/EP subscribed UE

An emergency call/session from an NS/EP NGN-PS subscribed UE is exempt from GTP-C overload control.

Relative Priority of NS/EP and Emergency Services

Both NS/EP NGN-PS and Emergency Services are exempt from GTP-C overload control.

4.2.3.5 Policy and Charging Control (PCC)

This clause presents the role of PCC in congestion control, specifically the role of the ARP in priority allocation of EPS Bearers.

The Allocation Retention Priority (ARP) as per Subclause 4.7.3 of 3GPP TS 23.401 [Ref 7], and Subclause 6.1.7.3 of 3GPP TS 23.203, *Policy and charging control architecture* [Ref 22] includes three sub fields:

- Priority Level: an integer from 1 to 15, where 1 is the highest priority;
- PVI (Preemption Vulnerability Indicator): marks a bearer as being allowed to be preempted; and
- PCI (Preemption Capability Indicator): marks a bearer request as capable of preempting an existing established bearer.

The ARP provides an indication of the priority to be applied in four situations:

1. In the allocation (establishment or modification) of an EPS bearer, when the system cannot fulfill all requests, higher priority ones are accepted while lower priority ones are rejected;
2. In cases when an EPS bearer needs to be dropped, e.g., when handover occurs and the target cell cannot support all the existing EPS bearers, the priority indicates which are supported and which are dropped;
3. In the preemption of an EPS bearer, when a new bearer (either an initial allocation or handover), marked as capable of preempting, is established by preempting an existing bearer that is both marked vulnerable to preemption and has a lower priority level than the new bearer; and
4. To influence scheduler behavior and the selection of the DSCP for IP packets sent towards the S-GW as described in Clause 4.2.3.1, and the selection of the DSCP for IP packets sent towards the eNodeB by the S-GW.

The ARP for the Default Bearer is downloaded to the MME at the time of Attach. Subsequently (can also be applied at the time of Attach, if so configured) PCC procedures between the Policy and Charging Rules Function (PCRF) and Policy and Charging Enforcement Function (PCEF) may alter this subscription-based ARP.

The ARP for an SDF is provided by the PCRF to the PCEF in a PCC rule. The PCEF is responsible for assigning PCC rules to an EPS Bearer, and establishing new Dedicated Bearers as required to support the SDFs.

The assignment of dedicated “NS/EP NGN-PS ARPs” and the dedicated “Emergency ARP” is described in Clause 4.2.3.1. Use of these special values permits priority allocation of EPS Bearers.

NS/EP

Definition of dedicated “NS/EP NGN-PS ARPs” allows conveyance of the priority needs of NS/EP NGN-PS during the establishment of EPS Bearers.

Emergency Services

Definition of a dedicated “Emergency ARP” allows conveyance of the priority needs of Emergency Services in support of Emergency Bearer Services.

Emergency Services from an NS/EP subscribed UE

Definition of a dedicated “Emergency ARP” allows conveyance of the priority needs of Emergency Services in support of Emergency Bearer Services.

Relative Priority of NS/EP and Emergency Services

The relative priority is not specified by 3GPP. The appropriate tools are in place to configure the desired behavior consistent with national regulation and operator policy.

4.2.4 Summary Observations

This clause provides a summary and high-level conclusion on how access and congestion control mechanisms provide exemptions for Emergency Services and NS/EP NGN-PS. This is based on:

- Access Control mechanisms presented in Clause 4.2.2; and
- Congestion and Overload control mechanisms presented in Clause 4.2.3.

A tabular summary of each of the 15 mechanisms is followed by key high-level conclusions.

Table 4.3 provides a summary of the impact on NS/EP NGN-PS and Emergency Services of access and congestion control mechanisms defined by 3GPP. Column 1 provides an item number (Item No.) and a cross reference to the clause where detailed materials are provided in this report. Column 2 provides the name and a brief description of the capability. Column 3 provides a statement of the key impact of the mechanism on NS/EP NGN-PS and Emergency Services.

Table 4.3 - Summary of the impact on NS/EP NGN-PS and Emergency Services of access and congestion control mechanisms defined by 3GPP.

Item No. and Cross Reference	Name and Brief Description of Capability	Impact on NS/EP NGN-PS and Emergency Services
1 §4.2.2.1	*Access Class Barring (ACB) and High Priority Access (HPA)* A probabilistic mechanism in which access from the UE (without consideration of the access class membership in 0 through 9) is barred with a probability that is signaled over the air interface. Several different thresholds are signaled by the eNodeB, and the one which applies depends only upon the purpose of the access. The duration of barring is also probabilistically determined. Access classes 11 through 15, denoted the special access classes, can be individually marked as being exempt from barring (for a particular purpose of access). These access classes are entitled to High Priority Access.	The E-UTRAN can be configured to give preferential access to NS/EP NGN-PS subscribed UEs, while probabilistically barring a fraction of non-NS/EP NGN-PS subscribed UEs. ACB for Emergency Services works completely differently than normal ACB. There is no way to bar a fraction of emergency calls, i.e., all are allowed, or all are barred. This is explicitly signaled to the UE. For UEs with valid AC11-15, emergency calls are allowed even when the system signals that emergency is barred.
2 §4.2.2.2	*Service Specific Access Control (SSAC)* A probabilistic mechanism that provides a means to manage system load by separately restricting access from VoLTE and ViLTE applications. The duration of barring is also probabilistically determined.	By virtue of being assigned a valid access class in the range 11-15, an NS/EP NGN-PS subscribed UE can be configured to be exempt from SSAC. All VoLTE and ViLTE emergency calls are exempt from SSAC. This exemption does not depend upon access class membership.

Item No. and Cross Reference	Name and Brief Description of Capability	Impact on NS/EP NGN-PS and Emergency Services
3 §4.2.2.3	*Access Control for CSFB* A probabilistic mechanism that provides a means to manage system load by separately restricting access associated with CSFB calls. The duration of barring is also probabilistically determined.	By virtue of being assigned a valid access class in the range 11-15, an NS/EP NGN-PS subscribed UE can be configured to be exempt from access control for CSFB. All CSFB emergency calls are exempt from access control for CSFB. This exemption does not depend upon access class membership.
4 §4.2.2.4	*Extended Access Barring (EAB)* A deterministic mechanism that provides a means to manage system overload by restricting access from UEs that, by virtue of USIM configuration, are associated with particular access classes.	By virtue of being assigned a valid access class in the range 11-15, an NS/EP NGN-PS subscribed UE is exempt from EAB. All emergency calls are exempt from EAB. This exemption does not depend upon access class membership.
5 §4.2.2.5	*Smart Congestion Management (SCM) and ACB skip* A deterministic mechanism that allows certain select identified applications (from the list below) to be exempt from barring by ACB without consideration of access class membership: – MMTEL voice, – MMTEL video, and – SMSovIP (not SIP Messaging) and Legacy SMS.	The priority of an NS/EP NGN-PS subscribed UE is not changed by ACB skip. However, as the priority of non-emergency non-NS/EP NGN-PS calls are elevated to the priority of NS/EP NGN-PS subscribed UEs, NS/EP NGN-PS subscribed UEs lose their relative ACB priority advantage. The priority of an emergency call is not changed by ACB skip. However, as the priority of non-emergency non-NS/EP NGN-PS calls are elevated to the priority of emergency calls, emergency calls lose their relative ACB priority advantage.
6 §4.2.2.6	*Application specific Congestion control for Data Communications (ACDC)* A probabilistic method to limit access from certain applications, while permitting access from other applications. ACDC operation entails a hierarchy of ACDC categories, a mapping of applications to one of these categories, and probabilistic rules for each category to determine barring and the duration of barring.	By virtue of being assigned a valid access class in the range 11-15, an NS/EP NGN-PS subscribed UE is exempt from ACDC. All emergency calls are exempt from ACDC. This exemption does not depend upon access class membership.
7 §4.2.2.7	*Access Barring (AB) for NB-IoT* A deterministic mechanism for NB-IoT that provides a means to manage system overload by restricting access from UEs that, by virtue of USIM subscription, are associated with particular access classes. AB for NB-IoT is based on the EAB mechanism used for eMTC / WideBand Internet of Things (WB-IoT), but provides a configurable, rather than a universal exemption for access classes 11-15. NB-IoT does not support real-time services such as voice and data.	By virtue of being assigned a valid access class in the range 11-15, an NS/EP NGN-PS subscribed UE can be configured to be exempt from AB. Emergency Services are not supported on NB-IoT. Therefore, AB for NB-IoT is not applicable.

Item No. and Cross Reference	Name and Brief Description of Capability	Impact on NS/EP NGN-PS and Emergency Services
8 §4.2.2.8	*eNodeB-based Access Control* The eNodeB may reject a request to establish an RRC connection and instruct the UE to not submit another request for a specified backoff time. When the backoff time is signaled in the "waitTime" IE, the timer (T302) is maintained within the RRC layer. When the backoff time is signaled in the "extendedWaitTime" IE, the timer (T3346) is maintained within the NAS Mobility Management layer. When the backoff time is signaled in the "extendedWaitTime-CPdata" IE, either timer T3448, if supported, else timer T3346 is maintained within the NAS Mobility Management Layer.	An NS/EP NGN-PS subscribed UE is exempt from the NAS timers T3346 and T3448 but cannot initiate communication with the network while the RRC timer T302 is running. An emergency call is exempt from both NAS timers T3346 and T3448, and RRC timer T302.
9 §4.2.3.1	*eNodeB Congestion and Overload Controls* The Allocation and Retention Priority (ARP) may influence scheduler behavior and the selection of the DSCP for IP packets sent towards the S-GW. The ARP Priority Level, in addition to the QCI Priority Level, may be used by the scheduler to determine which packet to serve when the QCI PDB cannot be met for all established SDFs. The QCI, and optionally the ARP Priority Level associated with an established EPS bearer, may be used to determine the DSCP value assigned to IP packets sent by the eNodeB towards the S-GW.	The assignment of dedicated "NS/EP NGN-PS ARPs" to EPS bearers associated with NS/EP NGN-PS triggers the required scheduler behavior at the eNodeB, and the setting of uplink transport markings by the eNodeB towards the S-GW. The assignment of a dedicated "Emergency ARP" for Emergency Bearer Services triggers the required scheduler behavior at the eNodeB, and the setting of uplink transport markings by the eNodeB towards the S-GW.
10 §4.2.3.2.1	*EPS Mobility Management (EMM) Congestion and Overload Control* When the MME rejects an EMM procedure due to congestion, it provides a backoff timer T3346 which prevents any further EMM procedure requests from the UE while the timer is running. This applies to both EMM specific procedures and EMM connection management procedures. For the Service Request Procedure, an attempt counter is incremented upon expiration of a timer supervising the procedure, until the attempt counter reaches a maximum retry limit, at while point the UE must not reattempt a Service Request for a specified time.	An NS/EP NGN-PS subscribed UE is exempt from the EMM backoff timer T3346. An NS/EP NGN-PS subscribed UE does not increment the Service Request attempt counter, and the maximum retry limit of the Service Request counter does not apply. Emergency Bearer Services are exempt from the EMM backoff timer T3346. While Emergency Bearer Services are active, the UE does not increment the Service Request attempt counter, and the maximum retry limit of the Service Request counter does not apply.

Item No. and Cross Reference	Name and Brief Description of Capability	Impact on NS/EP NGN-PS and Emergency Services
11 §4.2.3.2.2	*EPS Session Management (ESM) Congestion and Overload Control* When the MME rejects an ESM procedure due to insufficient resources, it provides a per-APN backoff timer T3396 which prevents any further ESM procedure requests to that APN while the timer is running. When the MME rejects an ESM procedure due to causes other than insufficient resources, it provides a per PLMN, per APN, per-procedure backoff timer, denoted "back-off timer" in the specifications, which prevents further ESM procedure requests for that procedure to that PLMN via that APN while the timer is running.	Two types of timer exemptions are provided in the NAS ESM specification: – an MME exemption in which a timer is not included in a failure response, and – a UE exemption in which the timer is ignored by the UE. An NS/EP NGN-PS subscribed UE is exempt from the ESM timers (T3396 and back-off). Both MME and UE exemptions are in place. Emergency Bearer Services are exempt from the ESM timers (T3396 and back-off). Both MME and UE exemptions are in place.
12 §4.2.3.2.3	*MME control of overload via the Overload Action IE* The MME may signal the eNodeB to apply congestion control actions which reject RRC establishment requests based exclusively on the selected "Establishment Cause" value provided by the UE. The list of rejected "Establishment Cause" values is determined from the "Overload Action" IE signaled from the MME to the eNodeB. Beginning in Release 10, it is possible to specify a percentage of requests meeting the "Establishment Cause" criteria that are rejected.	All "Overload Action" values permit access from NS/EP NGN-PS subscribed UEs, except for one value which permits only emergency and Mobile Terminated (MT) access. Use of this configuration is disallowed by ATIS. While the original intent of the 3GPP specification was to define an "Overload Action" which permits only emergency and MT access, use of this "Overload Action" value blocks all emergency calls from NS/EP NGN-PS subscribed UEs. Use of this configuration is disallowed by ATIS. The "Overload Action" which permits only highPriorityAccess and MT access blocks emergency calls from non-NS/EP NGN-PS subscribed UEs but permits emergency calls from NS/EP NGN-PS subscribed UEs.
13 §4.2.3.3	*PDN-GW Control of Overload* A PDN-GW may reject a PDN connection request and provide the MME a PDN-GW back-off time for subsequent requests to a particular APN. For a given APN, both PDN-GW back-off and GTP-C overload control are not used by the PDN-GW at the same time.	Requests associated with an NS/EP NGN-PS subscribed UE or a Service User are exempt from the PDN-GW back-off time. Requests associated with Emergency Services are exempt from the PDN-GW back-off time.
14 §4.2.3.4	*General GTP-C Overload Control* GTP-C nodes may mitigate an overload condition by requesting specific actions be taken by peer nodes. The requested actions may apply to the overloaded node itself and/or be specific to one or more APNs. The peer node throttles messages towards the overloaded node by discarding the fraction of messages requested by the overloaded node. For a given APN, both GTP-C overload control and PDN-GW back-off are not used by the PDN-GW at the same time.	Requests associated with an NS/EP NGN-PS subscribed UE or a Service User are exempt from GTP-C overload control. Requests associated with Emergency Services are exempt from GTP-C overload control.

Item No. and Cross Reference	Name and Brief Description of Capability	Impact on NS/EP NGN-PS and Emergency Services
15 §4.2.3.5	*PCC and Congestion Control* The Allocation and Retention Priority (ARP) provided through PCC mechanisms provides an indication of priority to be applied in 4 situations: – EPS Bearer allocation, – Dropping of an EPS bearer, – Preemption of an EPS bearer, and – eNodeB congestion and overload controls (see row 9 above).	The use of dedicated "NS/EP NGN-PS ARPs" by PCC to support NS/EP NGN-PS triggers the required priority treatments in the EPS. The use of dedicated an "Emergency ARP" by PCC to support Emergency Bearer Services triggers the required priority treatments in the EPS.

Table 4.3 has presented 15 mechanism standardized by 3GPP to manage congestion and overload, and how NS/EP NGN-PS and Emergency Services are impacted. Several behaviors are observed as follows:

1. *Both NS/EP NGN-PS and Emergency Services are always exempt from a mechanism*:

   This is observed in the following 8 rows of Table 4.3: 4, 5, 6, 10, 11, 13, 14; and the "extendedWaitTime" case of row 8.

   NS/EP NGN-PS and Emergency Services are treated comparably by these mechanisms.

2. *Emergency Services are always exempt from a mechanism, while NS/EP NGN-PS may be configured to be exempt*:

   This is observed in the following 2 rows of Table 4.3: 2 (SSAC) and 3 (Access Control for CSFB).

   For these mechanisms, Emergency Services are provided an advantage over NS/EP NGN-PS unless specific configurations are in place; with these configurations, the services are treated comparably.

   > NOTE: The following converse case does not appear in the table: NS/EP NGN-PS is always exempt from a mechanism, while Emergency Services may be configured to be exempt.

3. *Both NS/EP NGN-PS and Emergency Services may be configured to be exempt from a mechanism*:

   This is observed in the following 4 rows of Table 4.3: 1 (ACB), 9 (eNodeB Congestion and Overload Control), 12 (MME control of overload via the Overload Action IE), 15 (PCC and Congestion Control).

   For these mechanisms, the relative priority (within a mechanism) can be controlled to favor NS/EP NGN-PS or Emergency Services, to support operator policy consistent with regulatory requirements and operator preference.

4. *NS/EP NGN-PS can be configured to be exempt from AB for NB-IoT (row 7), while AB for NB-IoT does not apply for Emergency Services as NB-IoT does not support Emergency Services.*

   > NOTE: Neither NS/EP NGN-PS Voice nor NS/EP NGN-PS Video are supported on NB-IoT, so the AB for NB-IoT configuration only impacts NS/EP NGN-PS data services.

5. *The "waitTime" case of row 8 includes an exemption for Emergency Services, but provides no exemption or means to configure an exemption for NS/EP NGN-PS*.

   This is a disadvantage for NS/EP NGN-PS relative to Emergency Services. Initially this problem carried forward to 5G, but in subsequent revisions, 3GPP avoided this disadvantaged treatment for NS/EP NGN-PS in 5G.

Both the priority of an NS/EP NGN-PS subscribed UE and the priority of an emergency call are not changed by ACB skip. However, as the priority of non-emergency non-NS/EP NGN-PS calls are elevated to the priority of NS/EP NGN-PS subscribed UEs, NS/EP NGN-PS subscribed UEs lose their relative ACB priority advantage. Similarly, as the priority of non-emergency non-NS/EP NGN-PS calls are elevated to the priority of emergency calls, emergency calls lose their relative ACB priority advantage.

4.3 Security Considerations

For NS/EP NGN-PS, currently there are two methods to protect against unauthorized access that are dependent on the specific NS/EP NGN-PS service (a) UE authentication and NS/EP subscription verification, and (b) Service User authentication using PIN verification. Both methods apply from an NS/EP NGN-PS subscribed UE, while only the second method may be used from a non-NS/EP NGN-PS subscribed UE.

For Emergency Services, access from unauthenticated UEs is allowed. Refer to Clause 4.1.1 discussing 3GPP specifications allowing emergency calls from unauthenticated UEs and Clause 4.1.2.2 discussing FCC 47 CFR § 20.18 [Ref 25] indicating that CMRS must transmit all wireless 911 calls without respect to their call validation process.

In general, there are network security threats associated with unauthenticated devices being able to make emergency calls that can negatively impact NS/EP NGN-PS. An example of a security threat needing attention is handling of UEs and devices that are not adhering to applicable standard specifications (e.g., 3GPP) or not following local operator radio access control procedures (e.g., barring procedures) and operator policies (i.e., UEs and devices behaving badly). Another example of security threat is international roaming UEs where the USA operator has no control of the UE operations, but is required to transmit wireless 911 calls without respect to their call validation process.

There are tools and capabilities that could be used by operators to handle (e.g., block or disable) UEs and devices that are behaving badly. However, regulatory rules are not clear. Because of this and other reasons operators are hesitant to take such actions. For example, Clause 6.1 of GSMA SG.24, *Anti-Theft Device Requirements v3.0* [Ref 26] indicates that “disabling of service to a device shall not override regulated mandatory services such as emergency call capability and if supported, emergency numbers programmed by the owner (such as “phone home”).”

In conclusion, operator handling of UEs and devices that are not adhering to applicable standard specifications (e.g., 3GPP) or not following local operator radio access control procedures (e.g., barring procedures) and operator policies (i.e., UEs and devices behaving badly) is an area that needs attention from a regulatory policy perspective.

5 Conclusions, Guidance, & Recommendations

5.1 Conclusions

This technical report analyzed contention issues between different services such as Emergency Services and NS/EP NGN-PS communications during network degradation conditions (e.g., network congestion during certain disaster events) by identifying and analyzing network admission and congestion control capabilities and mechanisms defined in 3GPP LTE specifications. It also takes into considerations other factors such as operational (i.e., network element and resource management) considerations, regulatory rules/policy implications, and security considerations.

The analysis in this report examines all of the network admission and congestion control capabilities and mechanisms defined in 3GPP specifications through Release 14 inclusive independent of whether they are implemented and supported in service provider networks. However, it is possible that not all of the network admission and congestion control capabilities and mechanisms defined in 3GPP specifications are implemented and supported in a given service provider network. Furthermore, the analysis in this report does not imply that all the network admission and congestion control capabilities and mechanisms defined in 3GPP specifications should be supported by service provider networks. The analysis in this report is intended to be a complete analysis of the network admission and congestion control capabilities and mechanisms defined in 3GPP specifications through Release 14 inclusive.

The following is a summary of key conclusions:

General

The 3GPP specifications define a set of admission and congestion control capabilities, but do not provide guidance on how these mechanisms should be implemented by equipment vendors and used by network operators to control

Emergency Services and NS/EP NGN-PS. Since 3GPP specifications are subject to interpretation, it means that there could be differences on how these tools are implemented by equipment vendors and used by network operators to combat various congestion/traffic scenarios in the multiple service provider national network environment. Each network operator is expected to deploy and use the tools provided by their equipment vendors to meet their network specific objectives and policies.

Regulatory policy considerations

3GPP specifications leave relative treatment of the traffic associated with priority services (e.g., Emergency Services, MPS, MCS) up to regional/national regulatory rules and operatory policy. Regulatory rules do not provide clear guidance on how operators are to handle relative treatment between the traffic associated with priority services (e.g., Emergency Services, NS/EP NGN-PS and commercial priority services) under conditions where all traffic cannot be supported (i.e., due to network resource limitations).

This TR endorses the following recommendation documented in CSRIC V WG 8 report [Ref 23]:

> "Policy-makers should reaffirm existing guidance with respect to user classifications (e.g., FCC R&O 00-242), and clear guidelines should be given as to priority assigned to different roles in the face of limited capacity and events that invoke a high density of priority users. Similarly, policy-makers should provide clarification going forward related to pre-emption of communications for non-priority and lower-priority users (on a per application basis), in a congested environment. Relative priority classification of 911 and priority services communications in light of technical capabilities (i.e., LTE) should continue to be assessed."

Mechanism standardized by 3GPP to manage congestion and overload

Analysis of the mechanism standardized by 3GPP to manage congestion and overload, and how NS/EP NGN-PS and Emergency Services are impacted, resulted in the following behaviors observed amongst the set of defined mechanisms:

1. Both NS/EP NGN-PS and Emergency Services are always exempt from a mechanism. This is observed EAB, SCM and ACB skip, ACDC, EMM Congestion and Overload Control, ESM Congestion and Overload Control, PDN-GW Control of Overload, General GTP-C Overload Control, and also for the "extendedWaitTime" case of eNodeB-based Access Control. NS/EP NGN-PS and Emergency Services are treated comparably by these mechanisms.
2. Emergency Services are always exempt from a mechanism, while NS/EP NGN-PS may be configured to be exempt. This is observed for SSAC and Access Control for CSFB. For these mechanisms, Emergency Services are provided an advantage over NS/EP NGN-PS unless specific configurations are in place; with these configurations, the services are treated comparably.
3. Both NS/EP NGN-PS and Emergency Services may be configured to be exempt from a mechanism. This is observed for Access Class Barring (ACB), eNodeB Congestion and Overload Control, MME control of overload via the Overload Action IE, and PCC and Congestion Control. For these mechanisms, the relative priority (within a mechanism) can be controlled to favor NS/EP NGN-PS or Emergency Services, to support policy consistent with regulatory requirements and operator preference.
4. NS/EP NGN-PS can be configured to be exempt from Access Barring (AB) for NB-IoT, while AB for NB-IoT does not apply for Emergency Services as NB-IoT does not support Emergency Services.

   NOTE: Neither NS/EP NGN-PS Voice nor NS/EP NGN-PS Video are supported on NB-IoT, so the AB for NB-IoT configuration only impacts NS/EP NGN-PS data services.
5. The "waitTime" case of eNodeB-based Access Control includes an exemption for Emergency Services, but provides no exemption or means to configure an exemption for NS/EP NGN-PS. This is a disadvantage for NS/EP NGN-PS relative to Emergency Services. Initially this problem carried forward to 5G, but in subsequent revisions, 3GPP avoided this disadvantaged treatment for NS/EP NGN-PS in 5G.

Both the priority of an NS/EP NGN-PS subscribed UE and the priority of an emergency call are not changed by ACB skip. However, as the priority of non-emergency non-NS/EP NGN-PS calls are elevated to the priority of NS/EP NGN-PS subscribed UEs, NS/EP NGN-PS subscribed UEs lose their relative ACB priority advantage. Similarly, as the priority of non-emergency non-NS/EP NGN-PS calls are elevated to the priority of emergency calls, emergency calls lose their relative ACB priority advantage.

Security considerations

There are tools and capabilities that could be used by operators to handle (e.g., block or disable) UEs and devices that are behaving badly. However, regulatory rules are not clear. Because of this and other reasons operators are hesitant to take such actions.

In conclusion, operator handling of UEs and devices that are not adhering to applicable standard specifications (e.g., 3GPP) or not following local operator radio access control procedures (e.g., barring procedures) and operator policies (i.e., UEs and devices behaving badly) is an area that needs attention from a regulatory policy perspective.

5.2 Guidance & Recommendations

Co-existence of NS/EP NGN-PS and Emergency Services depends on proper configuration and use of network mechanisms standardized by 3GPP to manage congestion and overload. Operators and their equipment vendors should consider the information provided in this report as guidance to minimize co-existence issues between NS/EP NGN-PS and Emergency Services during network degradation conditions (e.g., network congestion during certain disaster events).

It is recommended that operators should use the information provided in this report to develop operator specific approaches on how the 3GPP defined tools are to be used (i.e., in the North American national network) to combat various congestion/traffic scenarios for NS/EP NGN-PS and Emergency Services coexistence to meet their network specific objectives and operator policies.

It is recommended that operator handling of UEs and devices that are not adhering to applicable standard specifications (e.g., 3GPP) or not following local operator radio access control procedures (e.g., barring procedures) and operator policies (i.e., UEs and devices behaving badly) is an area that should be investigated.

The information in this document are guidelines and not intended to replace or augment any regulatory requirements for Emergency Services and NS/EP NGN-PS coexistence.