Network 2020: Mission Critical Communications

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at www.gsma.com. Follow the GSMA on Twitter: @GSMA.

Network 2020

The GSMA's Network 2020 Programme is designed to help operators and the wider mobile industry to deliver all-IP networks so that everyone benefits regardless of where their starting point might be on the journey.

The programme has three key work-streams focused on: The development and deployment of IP services, The evolution of the 4G networks in widespread use today The 5G Journey, developing the next generation of mobile technologies and service.

For more information, please visit the Network 2020 website at: www.gsma.com/network2020 Follow the Network 2020 on Twitter: #Network2020.

With thanks to contributors:
DISH Network Corporation
EE Limited
Ericsson
Gemalto NV
Huawei Technologies Co Ltd
KDDI Corporation
KT Corporation
NEC Corporation
Nokia
Orange
Qualcomm Incorporated
SK Telecom Co., Ltd.
Telecom Italia SpA
TeliaSonera Finland Oyj
Telstra Corporation Limited
United States Cellular Corporation
Verizon Wireless
Vodafone GmbH

Contents

1

Introduction

1.1 Overview

Many situations arise where human life and other values for society are at risk and where timely and reliable communications between first responders is essential to avoid or at least mitigate damage: we refer to this type of exchange of information as critical communications.

The most typical example of critical communications use is in the so called “blue lights” agencies (police, ambulance fire brigade), however mission critical communications are also applicable to many other sectors of society and industries.

This whitepaper discusses how the capabilities of LTE networks and especially how broadcasting functionality can be leveraged not only to provide mission critical communications at system parity with existing solutions, but to enrich them by allowing users to exchange multimedia content in addition to voice and enjoy access to mobile broadband.

Besides group communications, this paper also proposes to consider exploiting the LTE-Broadcast capabilities for enhancing the delivery of public warnings.

As a testament of the maturity of the technology, a case study of deployment of a mission critical communications system in Telstra’s mobile network is discussed.

1.2 Abbreviations

Term	Description
3GPP	Third Generation Partnership Project
APN	Access Point Name
eMBMS	Enhanced Multimedia Broadcast/Multicast Service
EPS	Evolved Packet System
GBR	Guaranteed Bit Rate
GCSE	Group Call System Enablers
GSM-R	Global System for Mobile Communications – Railways
HTTP	Hypertext Transfer Protocol
IMS	IP Multimedia Subsystem
IOPS	Isolated LTE Operation for Public Safety
ITU-R	International Telecommunications Union, Radiocommunication sector
LMR	Land Mobile Radio
LTE	Long Term Evolution
MC-PTT	Mission Critical Push to Talk
OTT	Over the Top
P25	Project 25
PMR	Public Mobile Radio
PPDR	Public Protection and Disaster Relief
ProSe	Proximity Services
PSA	Public Safety Agency
PSMB	Public Safety Mobile Broadband
PTToC	Push to Talk over Cellular
PWS	Public Warning System
QCI	Quality Class Indicator
RCS	Rich Communication Services
RTP	Real Time Protocol
SIP	Session Initiation Protocol
TETRA	Terrestrial Trunked Radio
VoLTE	Voice over LTE
WRC	World Radio Conference

1.3 References

Ref	Title
[1]	LTE; Mission Critical Push to Talk (MCPTT) over LTE; Stage 1
[2]	LTE; Functional architecture and information flows to support mission critical communication services; Stage 2
[3]	LTE; Mission Critical Push To Talk (MCPTT) call control; Protocol specification
[4]	LTE; Security of Mission Critical Push To Talk (MCPTT) over LTE
[5]	3G security; Access security for IP-based services
[6]	www.firstnet.gov
[7]	www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/telecoms/11958367/EE-wins-landmark-contract-in-controversial-1.2bn-police-radio-replacement.html
[8]	https://blog.networks.nokia.com/public-safety/2016/06/09/nokia-making-future-public-safety-korea-reality-today/
[9]	http://eleconomista.com.mx/industrias/2016/11/17/altan-gana-red-compartida-promete-operar-2018
[10]	Public Warning System (PWS) requirements

2

Market Status

2.1 Demand for enhanced Mission Critical services

Public Safety Agencies (PSAs) utilise for their voice communication specialised systems based on private narrow band radio network systems such as TETRA (Terrestrial Trunked Radio) or Project25 (P25). While these systems offer functionality such as device to device communication, group management, floor control etc. that are essential for critical communications they tend to suffer from low spectral efficiency, limited data transport capabilities, slow evolution and high costs due to lack of economies of scale. For this reason it is not unusual for PSAs to supplement their voice communications through private networks with carrier network voice and mobile broadband data.

As PSAs are by their very nature highly mobile they have gained significant productivity benefits by using mobile broadband. The devices used for attaining mobile broadband connectivity are regular consumer devices ranging from smartphones to tablets and notebooks. It is however cumbersome and inconvenient for operatives to carry multiple devices and they would instead benefit from consolidating all the functionality they need for voice and data communications, as well as the specific capabilities of the two-way radio devices into a single device. That single device operating on a Public Safety Mobile Broadband (PSMB) network can therefore satisfy the Agencies' communications needs.

Moreover, the building and maintenance of a dedicated network such as TETRA or P25 is complex, time consuming and costly, and some PSAs have acknowledged the better ability of carrier networks to meet their communications (voice and data) needs. It therefore becomes attractive to leverage where possible an existing public carrier network. Not only does this facilitate more timely and cost effective introduction of the capability but also offers coverage advantages. The use of LTE as underlying technology for mission critical services removes existing interconnectivity issues between different types of Land Mobile Radio (LMR) networks operating in different geographical regions and, offers significant benefits of a large and sustainable ecosystem of devices available to suit commercial networks that have low unit costs because of global scale and harmonised spectrum usage.

It is vital that a PSMB capability provide for the evolution of its use in new and unexpected ways. Just as the introduction and expansion of public mobile broadband has led to innovative, and sometimes unforeseen uses and to the disruption of traditional operating models, it can be expected that a PSMB capability will also evolve in a similar fashion. The best way to ensure this is to leverage global standards for networks, devices and applications, noting that this global commercial ecosystem for mobile networks is a competitive one that is continuously driving innovation to reduce costs and introduce enhanced performance and new features.

As was the case for traditional mission critical voice services, MC-PTT (Mission Critical Push to Talk) will be primarily targeting PSAs (police, fire brigade, ambulance), however a number of other industries including transport, utilities, industrial plants and nuclear plants can take advantage of this new capability offered by the mobile network.

Besides attaining service parity with the existing systems, Public Safety users have requested multimedia services be adapted to their missions and way of working. Considering the broad use case development for Mission Critical Data/Video over LTE, there is a need for Mission Critical Data/Video communications that leverage the same underlying system enablers defined for MC-PTT. This extends to organisations in the mining, oil and gas industry, as they also have a need for Mission Critical data/video communications to enable remote monitoring and control of their operations.

2.1.1 Mission Critical Video

This set of Mission Critical applications leverages video media. The users can make a video call among groups as in a conference call, video can be streamed to the group members from a robot or drone, a security camera etc. In the context of public safety, the personnel can enrich the voice media with video (Push to Video) allowing first responders to share real condition of the surrounding area with other PSA group members. This information will enable other PSAs to take better decisions.

2.1.2 Mission Critical Data

This set of Mission Critical applications leverages non-voice/video traffic. The customer can use Computer Aided Dispatch, make database enquiries, and make use of features such as event manager sync or robot control, intelligence gathering and dissemination. The customers can also distribute files requiring mission critical transport, securely access public safety cloud and use messaging service similar to Short Data Service from TETRA.

2.2 Demand for non-mission-critical services

The same technology providing mission critical services could also be provided for customers wanting generic non-mission-critical group communications. Generally, any situation where employees use two way radio communications to communicate with each other could be a potential target for commercial PTT services. Examples include security staff in stadiums, train stations, airports etc. The technology is also being studied as a replacement of the ageing GSM-R [x] system currently deployed in many European countries, Australia, India, China and South Africa. The range of addressable opportunities is even larger once the advanced capabilities described in section 2.1.1and 2.1.2 are taken into consideration.

3

Mission Critical Push to Talk Technology Overview

3.1 General considerations

There are many standards-based Push To Talk over Cellular (PTToC) applications that have been developed and are available over commercial mobile broadband networks today. However, the applications fall short for Mission Critical applications under many aspects such as:

- No full service parity with legacy systems;
- No preferential access to radio resources;
- Not natively integrated in devices;
- Reliability cannot be guaranteed;
- Cannot utilise efficient distribution to a group using broadcast technology;
- Don't meet PSA Key performance requirements.

In light of the above limitations of Push to Talk over Cellular, in 2014 3GPP started to work on defining, as part of their Release 13, a mission critical push to talk service [1] that leverages the LTE radio technology, enhanced MBMS (Multimedia Broadcast/Multicast Service) and the IP Multimedia Subsystem (IMS) platform to specify a system that can replace legacy TETRA and P25 systems and that can, over time, evolve in step with new emerging use cases. Developing Mission Critical Push to Talk as an IMS application server allows mobile operators to sweat their investments in IMS made to support for example VoLTE and RCS.

The first version of the MC-PTT specifications, developed in close cooperation with PSAs (e.g. the USA Department of Commerce, the UK Home Office) enables traditional mission critical voice services as well as other capabilities for agencies looking at modernising their public safety communications networks.

The standards for Mission Critical Push to Talk (MC-PTT) capability provide the necessary features to deliver the functionality that is found on traditional narrow band radio networks. The following features are supported:

Group Call System Enablers (GCSE). Traditionally, LTE has been one-to-one communication, GCSE enables the support for the fundamental requirement for efficient and dynamic group communications operations such as one-to-many calling and broadcast capabilities over LTE.

Almost all Emergency services carry out their communications in groups. This feature optimises support in LTE for Group communications and provides appropriate group management to provide a consistent quality of service compared to existing PMR systems.

Proximity Services (ProSe). ProSe enables LTE to identify (discover) other devices in close physical proximity and enable optimised communications to occur between them. ProSe enables communication to occur when there is no network signal available in the area. The functionality introduced as part of Release 13 of 3GPP specifications includes:

- Network assisted discovery/communication - Communications are within LTE network coverage for all mobile services
- Device to Network Relay (Public Safety only) - If one mobile device is out of LTE network coverage but within the proximity of another mobile device that is within LTE coverage the communication can be relayed between the devices
- Direct Communication with no LTE network (Public Safety only) - When mobile devices have no LTE network coverage – ProSe will form a basis for discovery/communication via LTE Direct.

The combination of these capabilities brings MC-PTT at service parity with narrow band private radio systems: communications are possible in absence of coverage using the device in the police car, ambulance, fire truck at the scene to relay traffic to the network using high power communications, or two PSAs to directly communicate with each other. This ensures a very high availability of the service.

As well as public safety, the high availability of the service makes it an attractive proposition for isolated networks such as mining facilities and oil rigs.

Isolated LTE Operation for Public Safety (IOPS). When Public safety officers are out of LTE network coverage, Public safety authorities may deploy dedicated coverage for nearby Public safety devices beyond what is provided by Proximity services in UE-to-UE direct communication mode.

Additional features/functionality specified in Release 13 include:

- Different types of calls (group calls, broadcast calls, private calls, etc.)
- Different types of groups
- Dynamic regrouping
- Late entry to groups

- Bespoke security functions
- Floor control (e.g. queue in priority order requests to speak, limit the time a user talks and so on)
- Override based on priority (e.g. the head of operation can obtain the floor at any time, emergency requests are granted immediate floor access)
- Real time location information (rather than location at call establishment)
- Audio / Voice Quality standards
- Audio call performance standards.

As well as group communications, MC-PTT also supports private calls between pairs of users engaged in MC-PTT group communication with further evolution (in Release 14) to support multimedia capabilities (push to X).

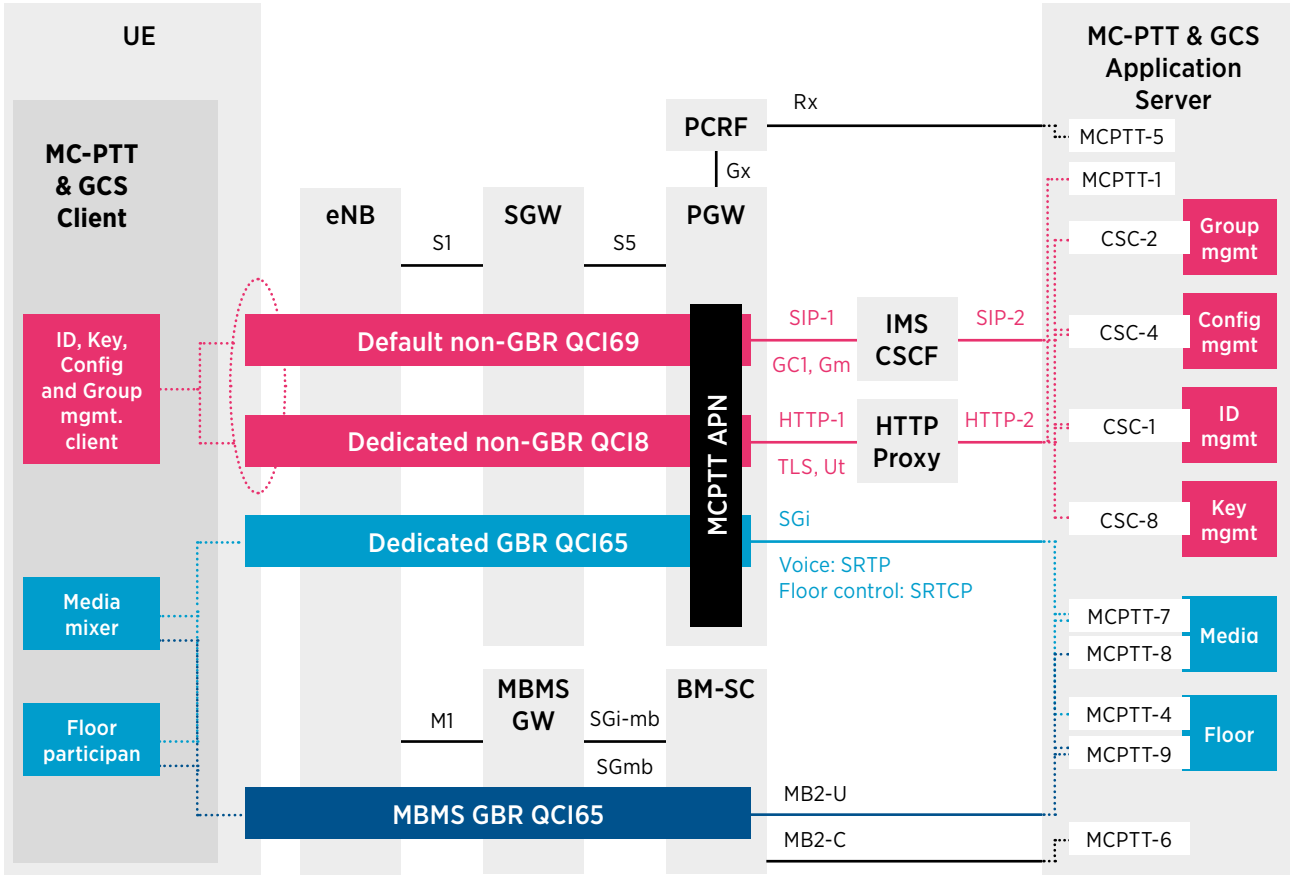
It is anticipated that fully integrated MC-PTT trials may commence in early 2017 with first generation services available from late 2017.

3.2 Mission Critical Push to Talk Architecture

Service requirements for Mission Critical Push to Talk are described in TS 22.179 [1]. The MC-PTT architecture defining the several reference points and network nodes involved in the service is discussed in TS 23.179 [2], while the protocols and procedures are defined in TS 24.179 [3].

3GPP TS 23.179 [2] specifies that the UE connects to MC-PTT specific Access Point Names (APN) in order to use the MC-PTT service. The signalling is provided over SIP and HTTP, which also leads to use of non-guaranteed bit rate (non-GBR) bearers with different Quality Class Identifiers (QCI), specifically QCI 69 for SIP and QCI 8 or better for HTTP. The media is transmitted over secure Real Time Protocol (RTP) either using unicast or multicast GBR bearers with QCI 65. Floor control is also applied on the same bearer. The following figure depicts how MC-PTT reference points can be mapped to different unicast and multicast bearers (description of each individual reference point is given below).

Figure 1: MC-PTT & Group Communications Service Architecture



MC-PTT reference points:

- CSC-1 is used for MC-PTT user authentication between identity management client and server over secure HTTP/TLS
- CSC-4 provides configuration information for MC-PTT services. HTTP is used for non-subscription/notification related signalling and SIP is used for subscription/notification related signalling
- CSC-2 is used for configuration of group management data between server and client. HTTP is used for non-subscription/notification related signalling and SIP is used for subscription/notification related signalling
- CSC-8 provides key material over HTTP/TLS from key management server for end-to-end communication security (keys for SRTP and SRTCP)
- MCPTT-1 is used for MC-PTT session establishment. MC-PTT may also provide location information with respect to multicast service availability. MCPTT-1 shall use SIP and may also use HTTP
- MCPTT-4 is the reference point for floor control over unicast bearer. Secure RTCP (SRTCP) is used for floor control
- MCPTT-5 reference point is used for policy control (QoS)
- MCPTT-6 is used for requesting multicast resources using MB2 control plane
- MCPTT-7 is for media distribution over unicast bearer using SGi interface. Secure RTP (SRTP) is used for media
- MCPTT-8 sends multicast media to MCPTT clients using MB2 user plane and secure RTP (SRTP).
- MCPTT-9 provides floor control signalling over multicast bearer using MB2 user plane and secure RTCP (SRTCP).

To use MC-PTT, UE performs authentication and authorization after LTE attach as defined in 3GPP TS 33.179 [4], which consists of three processes: MC-PTT user authentication (CSC-1), SIP Registration and Authentication, and MC-PTT Service Authorization. The first two can be performed in any order, for example MC-PTT User Authentication could be performed over secure connection TLS without having to register on IMS. SIP Registration and Authentication is based on IMS AKA as specified in 3GPP TS 33.203 [5], where confidentiality and integrity of Gm interface is using IPSec. MC-PTT service authorization is done using the credentials received from MC-PTT user authentication.

GCS AS (GCS Application Server) also provides capability to switch MC-PTT users between unicast and multicast. Since MC-PTT users could be packed in a few cells or sparsely distributed over a wide area, MC-PTT service should provide capability to switch between multicast and unicast respectively for transmission to ensure network efficiency. GCS AS therefore serves the following function:

- Receive location information from MC-PTT users to configure MBSFN area for eMBMS transmission to be used for MC-PTT
- Activate or deactivate eMBMS transmission via BM-SC
- Direct UE that entered a MBSFN area to use eMBMS transmission to receive MC-PTT data
- Or direct UE that left or is going to leave a MBSFN area to use unicast transmission to receive MC-PTT data.

3.3 Deployment scenarios

3.3.1 Sharing models

When deploying a public safety LTE network, several possible alternatives may be considered each with advantages and disadvantages:

- Hosted solution
- Standalone deployment
- Various degrees of sharing with commercial network.

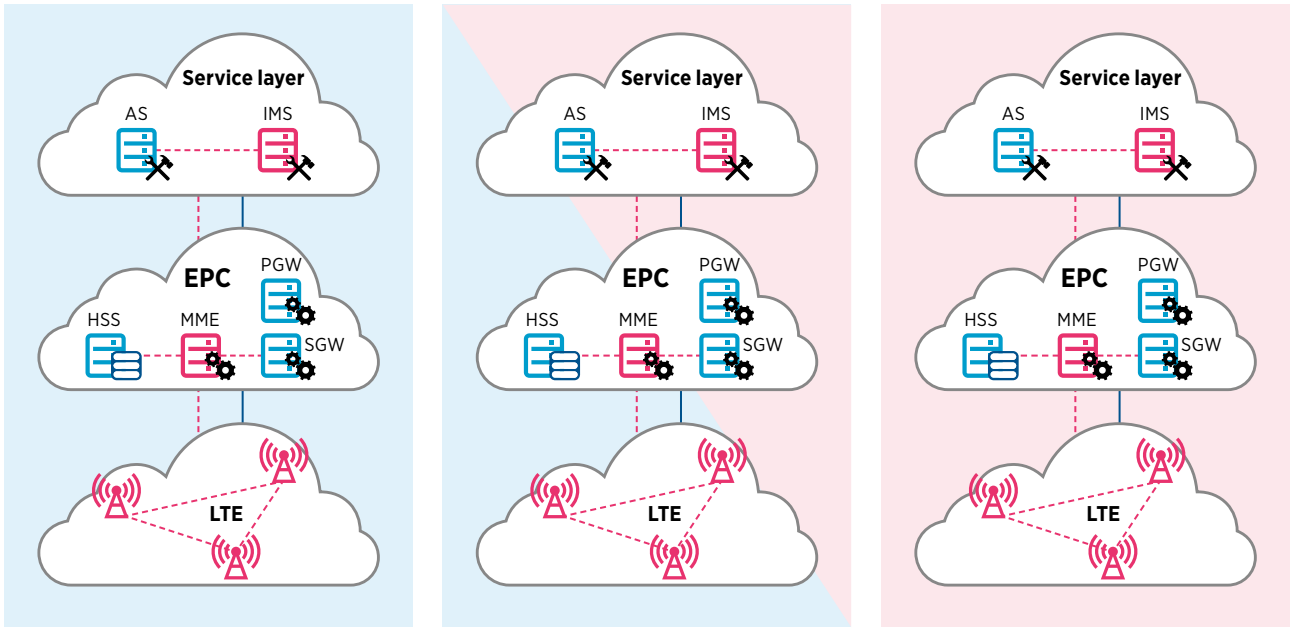
A graphical representation of these scenarios is provided in Figure 2 where the blue background indicates the commercial network while the red background indicates the public safety network.

Hosted solution: In this model the public safety agencies purchase the services required to meet their communications needs. There are several possible commercial models including all layers of the service being from the one operator to each layer being purchased from a different service provider. If the layers are supplied by different service providers then the end to end service could be managed by the PSA or by a lead service provider. The limitation of using different service providers is the lack of seamless connectivity between them and issues of feature parity between networks.

Standalone deployment: in this model the public safety agency deploys a full network covering the service area the agency is accountable for. The spectrum required for this deployment would need to be allocated by the appropriate spectrum management agency and would typically follow Resolution 646 of the ITU-R, which was updated during the recent WRC-15 meeting. While standalone deployment is attractive in terms of PSAs being in control of the resources and subscribers database, it comes with the operational issues and cost of providing a sufficient level of coverage, backhaul capacity, network hardening, technology currency and operational expertise and cost. If the spectrum is reserved for PSA use only it also limits the device economies of scale.

Sharing with commercial networks: there are various levels of sharing infrastructure with a commercial network from a full connectivity solution being provided by the commercial operator and the PSA connecting an application server (Over the Top solution) to only sharing the RAN but provide an own core network and service platform. For the public safety operator, the main advantage of the shared model is the possibility of providing wide coverage area from day 1 (possibly complementing it with its own RAN using reserved spectrum or reserved spectrum hosted on the operators RAN). A PSA needs to ensure that commercial agreements are in place for access to commercial network resources in case of emergency with related service level agreements.

Figure 2: possible deployment scenarios for public safety MCPTT



4

Public Warning Systems

4.1 Introduction

Natural disasters cause the loss of many lives. Some of these losses may be prevented if it was possible for the public agencies to provide the population prompt advice on the nature of the disaster and remedial action. For example, many lives could have been saved in 2004 if the population of Thailand could have been warned of the arrival of a tidal wave.

Besides natural disasters public warnings can play an important role in situations such as terrorist attacks, and other catastrophic events such as the Fukushima Daichi nuclear power plant accident, Tanjin port explosion, and so on.

For this reason, public warnings share many of the characteristics of mission critical communications.

3GPP has specified two solutions aimed at providing public warnings through the mobile network: The Earthquake and Tsunami Warning System (ETWS) included in the Release 8 set of specifications and the Public Warning System (PWS) introduced in Release 9. Neither of the systems make use of LTE broadcasting technology to maximise the efficiency of the delivery of messages to all the users within a certain geographical area and provide limited capabilities in terms of the content that can be delivered, however as discussed in section 4.4, there is no technical reason why the capabilities of eMBMS cannot be exploited to enhance the delivery of public warnings

4.2 Earthquake and Tsunami Warning System (ETWS)

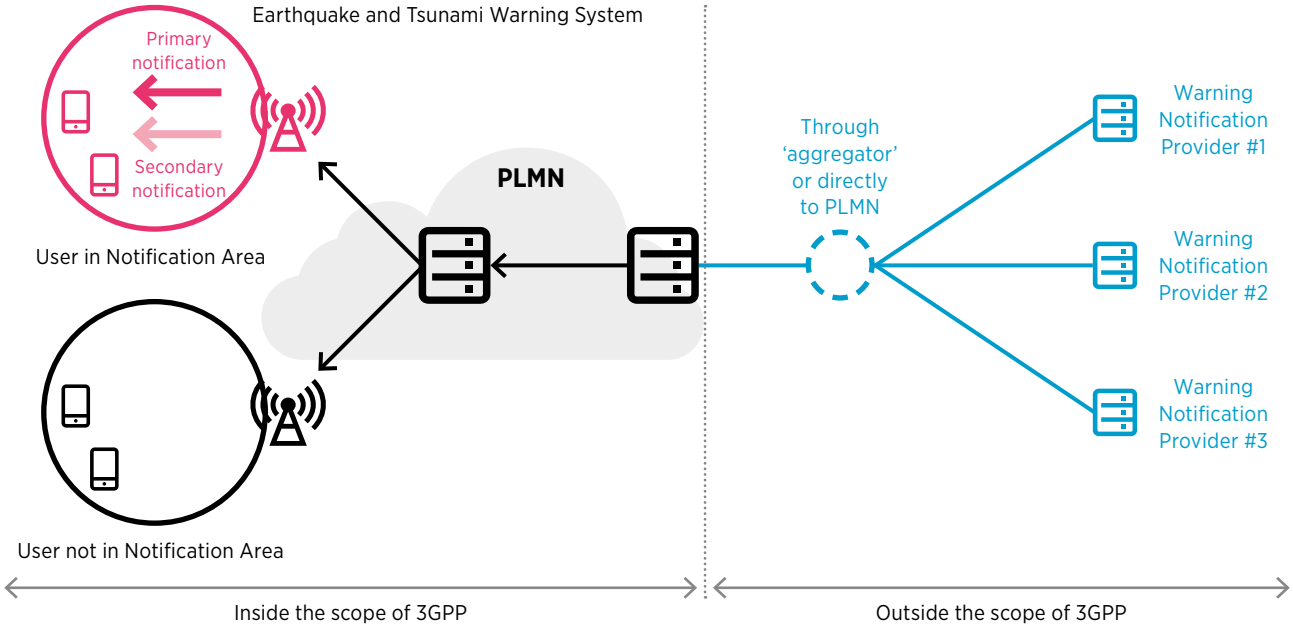
As it can be inferred by its name, this service was specifically targeting Japan and has in fact been developed in advance to the global specification of Public Warning Systems (PWS) as a regional variation. ETWS is now supported by the vast majority of the devices in Japan.

ETWS introduces a means to deliver a Warning Notification simultaneously to many mobile users who should evacuate from an approaching Earthquake or Tsunami. A mobile user receiving a Warning Notification finds out that a nearby threat is approaching or happened already and is able to determine where and when to evacuate.

Given its deployment scenario ETWS is not applicable to the GSM and EDGE Radio Access Network (GERAN), but only to the Universal Terrestrial Mobile System (UMTS), that is 3G, and it requires that devices support and have activated the Cell Broadcast reception functionality.

Reference: 3GPP TS 22.168

Figure 3: ETWS Overview



The most notable characteristic of ETWS is that it delivers two levels of emergency information:

- The Primary Notification contains the minimum, most urgently required information e.g. the nature of the emergency;
- The Secondary Notification includes supplementary, more delay tolerant information such as seismic intensity, epicentre, and so on.

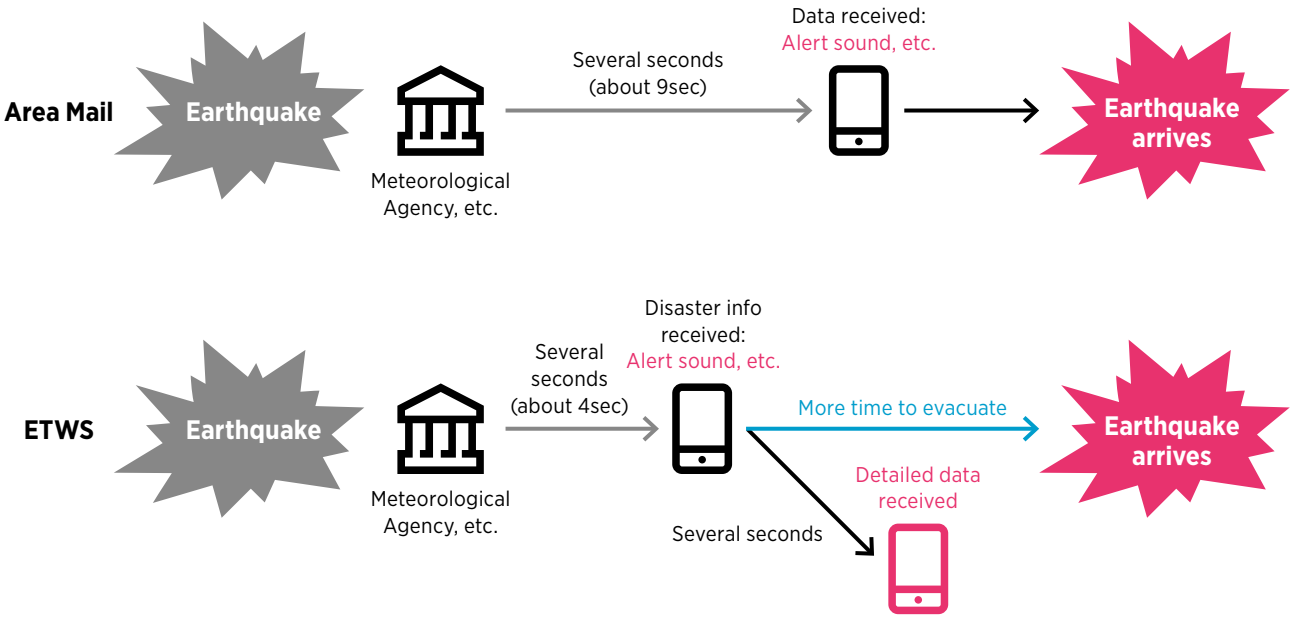
Similar to the existing email based "Area Mail" warning system, the source of the notifications is either a local or national authority, however ETWS greatly improves the performance over such an alternative warning mechanisms and is able to deliver the first notification to mobile terminals within about four seconds of receiving the emergency information from the relevant agency.

The primary notification is designed to be delivered regardless of the state of the mobile device (idle, dedicated, packet idle, packet transfer, dual transfer modes).

The architecture of ETWS is depicted in Figure 5 and is based on the use of Cell Broadcast Service, a functionality that is generally not enabled in devices due to the increase in battery consumption. It should also be noted that ETWS permits to deliver a warning different levels of geographical granularity. While in 3G the Cell Broadcast Centre (CBC) connects to the Radio Network Controllers (RNC) and from there to the all the 3G Base stations (NodeB) reporting to that RNC, in 4G the CBC connects to the Mobility Management Entity (MME) in the Core network which on turn passes the broadcast message only to the relevant eNodeBs.

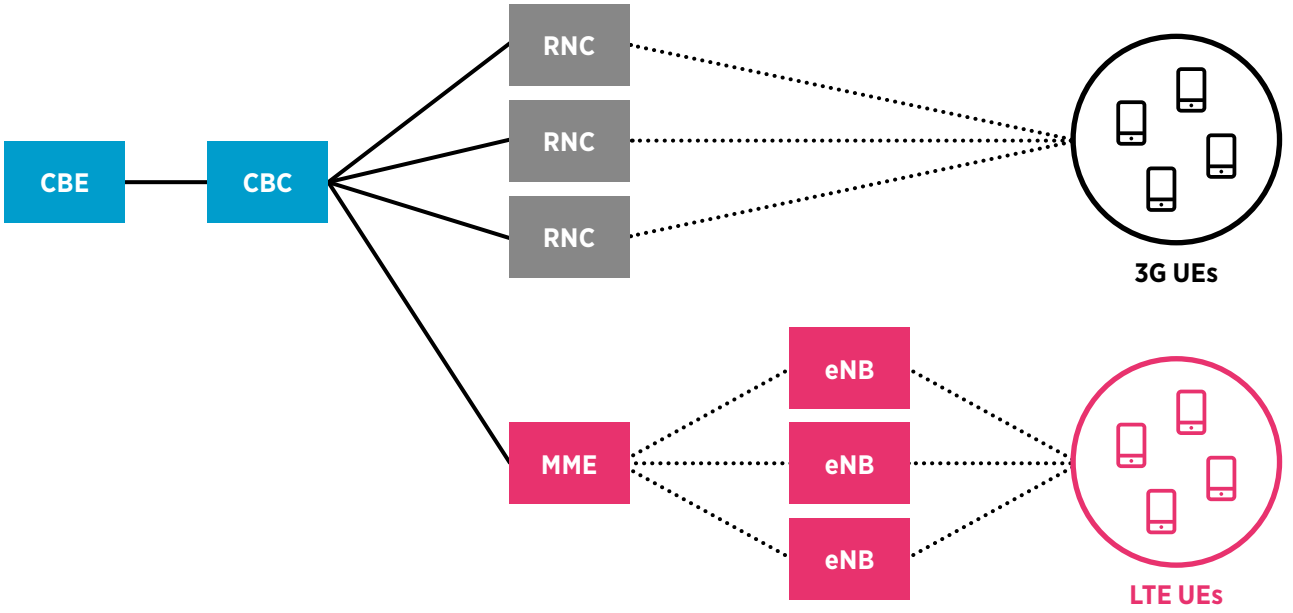
Reference: NTT DoCoMo Technical Journal Vol.11 No.3

Figure 4: Area Mail vs. ETWS



Reference: NTT DoCoMo Technical Journal Vol.11 No.3

Figure 5: ETWS Network Architecture



As a result of the architecture configuration differences, 4G offers a significant advantage over 3G. While in 3G it is only possible to indicate the cells where the message should be broadcast, creating a heavy load on the CBC, in 4G it is also possible to specify either a complete tracking area or an Emergency Area created ad hoc by the operator to cover a certain geographical area.

4.3 Public Warning System

While the study of a generic public warning system was completed in advance of ETWS, the full set of technical specifications were only completed in Release 9, that is a release after the one that included ETWS.

As a result PWS is a generalisation of ETWS.

Figure 6: PWS General Overview

The salient characteristics of PWS (see Figure 6) are summarised in 3GPP TS 22.268 [10]:

- PWS shall be able to broadcast Warning Notifications to multiple users simultaneously with no acknowledgement required
- Warning Notifications shall be broadcast to a Notification Area which is based on the geographical information as specified by the Warning Notification Provider
- PWS capable UEs (PWS-UE) in idle mode shall be capable of receiving broadcasted Warning Notifications
- Reception and presentation of Warning Notifications to the user shall not pre-empt an active voice or data session
- Warning Notifications shall be limited to those emergencies where life or property is at imminent risk, and some responsive action should be taken.

An architecture of the system is depicted in Figure 7.

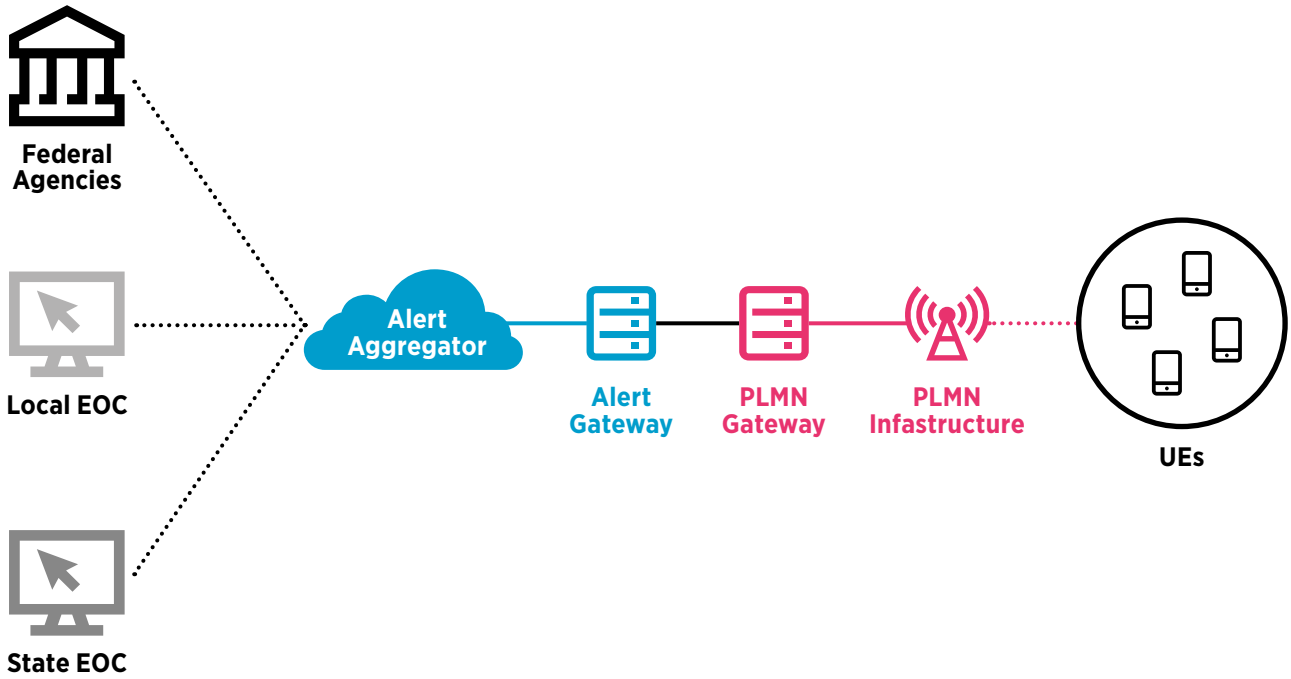
Just like ETWS, PWS is a text based warning system relying on Cell Broadcast technology for the distribution of messages and no additional functionality is required in the UE to support PWS besides the capability of receiving Cell Broadcast Messages.

One of the key component of the CMAS (Commercial Mobile Alert System) is the alert gateway that ensures that warnings come from a trustworthy source and contain a well-defined set of information:

It is expected that Warning Notifications would include the following five elements:

- Event Description
- Area Affected
- Recommended Action
- Expiration Time (with time zone)
- Sending Agency
- Optional Additional elements based on regulatory requirements.

Figure 7: Commercial Mobile Alert System



In terms of system enhancements, PWS adds a number of functionality to ETWS including:

- E-UTRA/E-UTRAN support for multiple parallel Warning Notifications
- E-UTRAN support for replacing and cancelling a Warning Notification
- E-UTRAN support for repeating the Warning Notification with a repetition period as short as 2 seconds and as long as 24 hours
- E-UTRA support for more generic "PWS" indication in the Paging Indication.

Despite such generalisation and advanced functionality, PWS has not been widely deployed.

4.4 Enhancing PWS with eMBMS

If a high level of penetration of devices supporting eMBMS capabilities could be assumed, this technology would provide a number of advantages over the existing public warning systems, namely:

- no need to support cell broadcast;
- capability of delivering rich multimedia warnings to subscribers to support them in disaster situations;
- fine control of the granularity of the area where the warning is distributed;
- speed of delivery;
- parallel delivery of multiple warnings (e.g. in different languages);
- reach of all subscribers, (potentially including roaming subscribers).

5

Deployment challenges

5.1 General considerations

Some of the challenges that arise when utilising a commercial network for mission critical communications are not that different to the challenges faced when building a dedicated network, but are on a smaller scale, and include those such as: how to ensure the network resources are available for mission critical services when needed; how to extend network coverage to remote areas; how to provide service during a power outage; how to provide a range of compatible devices. These challenges are discussed in the following sections.

The rationale for discussing this specific deployment model in more detail is that this approach makes better use of spectrum, and is a far more cost-effective way to support emergency services. In many cases Commercial Operators can meet the reliability and accessibility requirements through a staged approach including introducing spectrum partitioning, priority access and preferential service level introduction for emergency communications.

5.2 Admission control

During emergencies or large scale events, depending on the spectrum assets available, there can be a high demand for mobile services and mobile networks can experience congestion. In order to provide network resources for PSAs during these times, two techniques can be adopted:

- The provision of access prioritisation to PSA services, meaning that in times of high network load, PSA users are admitted to the mobile network as a matter of priority, while non-PSA users may be barred for a short period of time
- The provision of preferential data treatment to PSA services, so that PSA data communications receive priority over non-PSA data communications, and can offer a minimum bit rate.

Working examples of this are seen in Australia where Telstra have developed the LTE Advanced Network for Emergency Services (LANES) capability and in the UK, where EE are deploying a Public Safety Mobile Broadband capability.

5.3 Isolated operations (Network in a box)

Emergencies and large scale events can happen outside the coverage area provided by mobile networks and private radio networks. In some countries, the land mass is so vast, it is virtually impossible to build a permanent mobile network that covers 100% of the land. In order to provide PSAs with mobile coverage where it is needed, temporary coverage solutions can be deployed.

One such solution is a “Network in a Box” concept. Essentially, this is an entire LTE network (RAN and Core) that can be carried around in a “box” and deployed to a remote location to provide localised (isolated) LTE coverage. All the box needs is a power source and the PSAs within the coverage footprint of the network in a box are able to communicate with each other. The PSAs can still use the same mobile devices they use on the permanent mobile network, which saves them having to carry an additional device.

If the PSAs wish to communicate with users on the macro network (the “rest of the world”), then a means of connecting the network in a box to the macro network (backhauling) is required. This is possible today for example via the use of satellite technology.

Other temporary solutions that require backhauling include “Cells on Wheels” (COWs), whereby an LTE cell (i.e. RAN only) is deployed at a location and backhauled via cable or microwave transmission, and “Satellite Cells on Wheels” (SATCOWs), whereby the LTE cell is backhauled via satellite.

Development is currently underway in various markets to provide temporary coverage on-board drones or UAVs. As technology advances and mobile network functionality can be deployed on smaller and smaller infrastructure, mobile coverage solutions will become more and more portable.

5.4 Network Hardening

Commercial 3G and 4G networks with appropriate 'hardening' can provide the performance and reliability sought by PSAs and superior to that achieved by private radio networks. Battery backup capability can be extended, additional sites can be built for greater redundancy and increased capacity and coverage, backhaul bandwidth can be increased and physical security can be enhanced. 'Hardening' the network in this way will increase the resiliency and robustness of the mobile network, such that in the event of a power outage, or network infrastructure is damaged, the network should remain operational for an extended period of time.

Commercial operators also have a proven history of network performance and fast restoration by their national field work force during natural disasters.

5.5 Devices

There are a number of factors involved in the development of devices, key amongst them are the Spectrum bands and number of bands supported, compliance to the 3GPP specifications, and the particular release of the specifications.

For commercial devices the vendors consider all the bands that are in use globally and which bands are used in different markets, then the likely volumes of device sold.

Global and regional harmonisation of the spectrum bands used for Public Protection and Disaster Relief (PPDR) is very important to ensuring a cost effective device eco system development and will greatly increase the device range available and reduce the unit cost.

Volume is also essential for supplying affordable and compatible user devices. Carriers are involved in negotiating the supply of high volumes of user devices and it is also likely to be much more cost effective to ruggedize existing commercial devices rather than developing and acquiring devices that are specifically made for the PSMB requirements.

5.6 Regulatory challenges to spectrum for consumer mobile broadband access

Mission Critical Communications applications, such as PPDR, are vital and must be supported. However, this need not, and should not, threaten affordable, widespread mobile broadband access for citizens and businesses. Any efforts to use part of the 700 MHz band's uplink or downlink channels for PPDR would reduce the amount available for mobile services which in turn can negatively impact the cost, coverage and capacity of mobile broadband. Instead, exclusive spectrum for PPDR services can be found outside of commercial mobile band plans.

6

Parallel opportunities

It is of paramount importance to ensure that the standards for products and services that deliver mission critical communications are of the highest quality since there are situations where the failure of the service may result in significantly serious consequences. To ensure that sufficient efforts are made in building resilient products, it is vital that the use of mission critical communications is not restricted to a relatively small market such as public safety, but rather that benefits from economies of scale are fully leveraged so that the additional development costs necessary for guaranteeing the desired quality are shared across a larger user base.

A Push to Talk service that has been developed to Mission Critical standards would more than satisfy Business Critical standards.

Different levels of QoS, higher than made available for best effort products but not as high as those needed for mission critical can be offered to service Business Critical opportunities. Examples of industries that may benefit from business critical communications include the financial sector (Banking), media as well utilities sectors.

Services that require a specific QoS treatment may be identified based on either the subscription or the application being used.

6.1 Deployment Status

More than 30 countries around the world have started either assessment, planning, or deployment of Mission Critical and Business Critical Services with the primary focus being on Mission Critical services as replacement of legacy systems. The status in some selected countries is as follows:

United States: Developed plans to build a national public security broadband network in 2012 called FirstNet using the LTE 700 MHz spectrum with an overall US$ 10 billion-plus investment. In March 2014, 231 sites were built in Los Angeles as part of the first phase of the project at a cost of US$ 175 million. [6]

United Kingdom: A national public security broadband LTE network has been planned for construction over 6 years (2015 - 2020), which will permit operators to build public-safety networks over LTE public network spectrum. The first phase of the project began in 2015 with an investment of 1.2 billion pounds sterling and the network operator providing the commercial network is investing in expanding the coverage of their network. [7]

South Korea: In 2014, the country began building a national broadband emergency disaster prevention network based on the LTE standard, with a total investment surpassing US$ 2 billion. The first phase kicked off in late 2015 in Pyeongchang County and was completed successfully in June 2016. In this phase, Korea deployed a control centre, 220 base stations (mobile/fixed) and 2,496 devices at a total cost of US$ 40 million. Korea will continue operating the trial and resolve any potential defects of the network. [8]

Mexico: The government has agreed to allow the deployment of a shared LTE network using 700MHz LTE bands that is expected to cover more than 90% of the population when completed. The Red Compartida shall be a platform that provides latest-generation mobile services to its clients, some of which could focus on specialized vertical markets such as public safety, civil protection, health and transportation services, among others [9]

6.2 Enable Critical Communications over Carrier's LTE network

The same architecture and infrastructure that empowers MCPTT can also support business critical communications, a rapidly growing segment especially once advanced functionality such as "push to X" ("X" being video, text, location, etc.) become available.

Figure 8 shows the deployment of an end to end Mission critical communication system running LTE. All interfaces between the network elements are standard open interfaces therefore suitable for multi-vendor support. In the case the operator has already deployed IMS (e.g. for the support of VoLTE), the additional investment in the network is limited to infrastructure for delivering multimedia broadcast services (eMBMS).

At service level, mission critical communications is enabled by an IMS application server (GCS AS) and by a mobile client that could be installed on a regular LTE-enabled device. Provided an operator has already deployed IMS (e.g. for the support of VoLTE), a new application server supporting a different industry segment may be considered a relatively small investment.

Figure 8: Optional architecture of mission critical communications over LTE

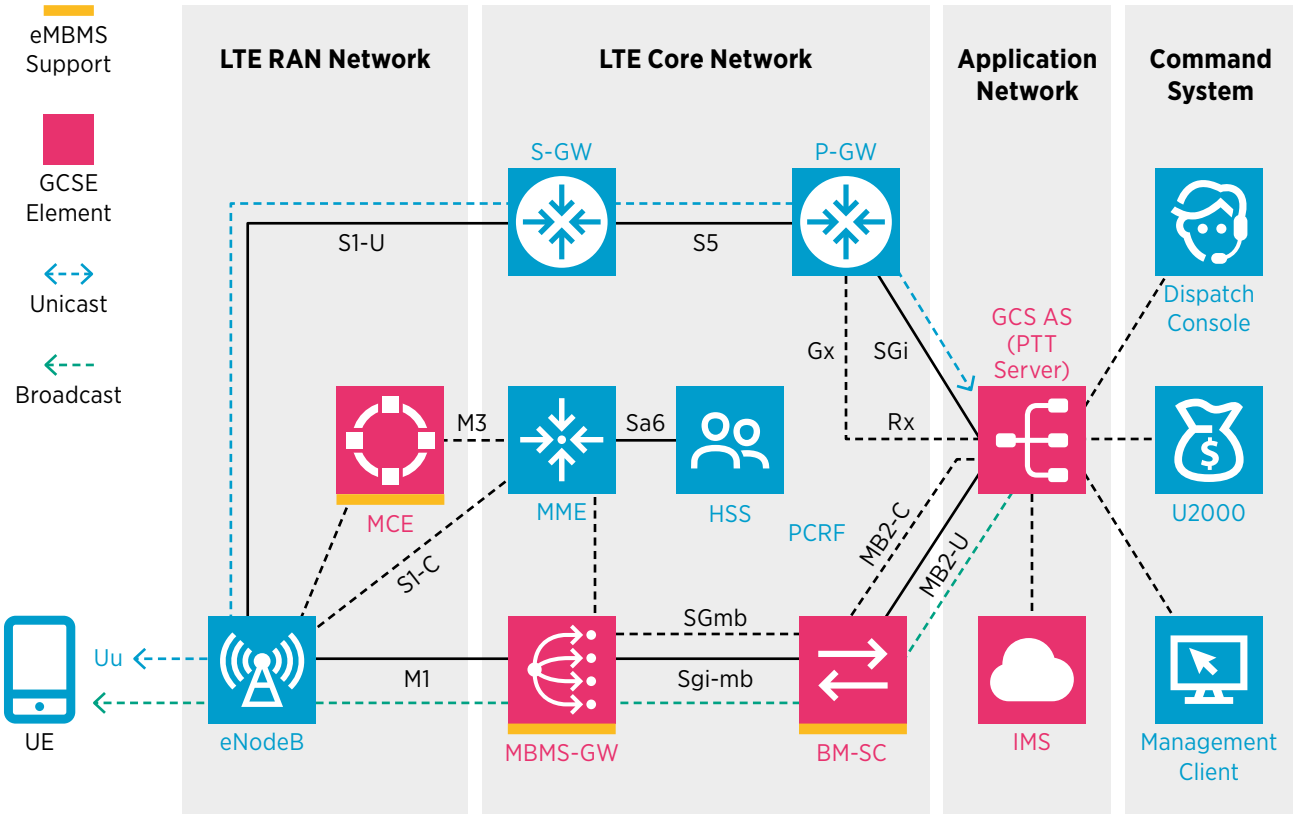
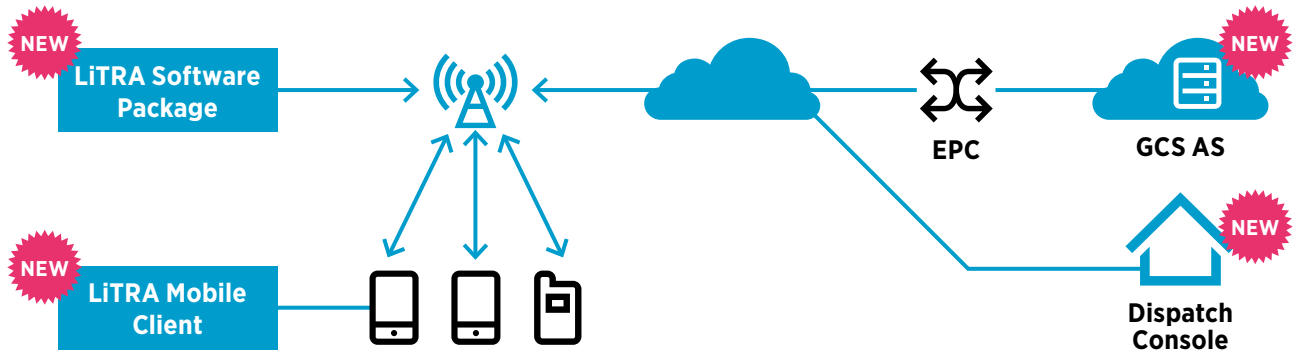


Figure 9: Network Diagram for a generic critical service



7

Case Study: Establishing the foundations of a Public Safety Mobile Broadband Network

Australia is prone to natural hazards such as fire, floods, and cyclones. These natural events have the potential to cause significant loss of life and property. Australia's geographic area covers over 7 million square kilometres of area with a population of 24 million people predominately on the coastal areas of the country.

Consequently, Australia faces unique challenges in enabling a national public safety mobile broadband capability from other nations, which may not exist for countries that have significantly smaller geographic areas or populations. With these challenges Telstra has enabled a national public safety mobile broadband capability utilising its carrier network. This service is known as Telstra LANES for Emergency Services and complements other public safety services provided commercially by Telstra to the police and emergency services including the Wireless Prioritisation System Service, national Community Alerting System – Emergency Alert and mission critical land mobile radio networks.

Telstra has followed a systematic approach firstly releasing two Whitepapers that explore the capacity of utilising a public carrier to provide the next generation of public safety mobile broadband capability:

In February, 2011, Telstra released its first whitepaper on PSMB: Public Safety and Security: Emergency Grade Mobile Broadband for the Public Safety and Security Sector.

The following year, in November, 2012, Telstra released a second whitepaper: Delivering 4G/LTE Mobile Broadband for Emergency Services.

This was followed by a number of trials with the police and emergency services in Australia. In late Nov/early Dec 2013, Telstra piloted LANES® in the live network. Telstra showcased this capability to Government and Industry representatives in Brisbane and Perth through a series of live demonstrations.

Following the success of the Showcase, Telstra LANES® was successfully deployed at the Woodford Folk Festival for use by the Queensland Police Service.

A large scale live trial in Brisbane in 2014 saw Telstra LANES® provide support to QLD Government and Emergency Services during the G20.

In October, 2015, Telstra LANES® was trialled at the Melbourne Cricket Ground (MCG) on Australian Football League (AFL) Grand Final Day with approximately 100,000 people within the stadium. Network traces showed Telstra LANES® services performed as expected for both access prioritisation and preferential data treatment. User experience testing showed that video streaming on a Telstra LANES® device was of a higher quality than on non-LANES devices.

The following diagram in Figure 10 illustrates the primary features of the Telstra's LANES® solution including:

- Prioritised Access for Police and Emergency Services;
- Preferential Data Treatment; and
- Self-Dimensioning Bandwidth.

Making available an unprecedented 166 MHz of LTE spectrum for Australia's first responders.

Figure 10: Telstra's LANES® main features

Prioritised access

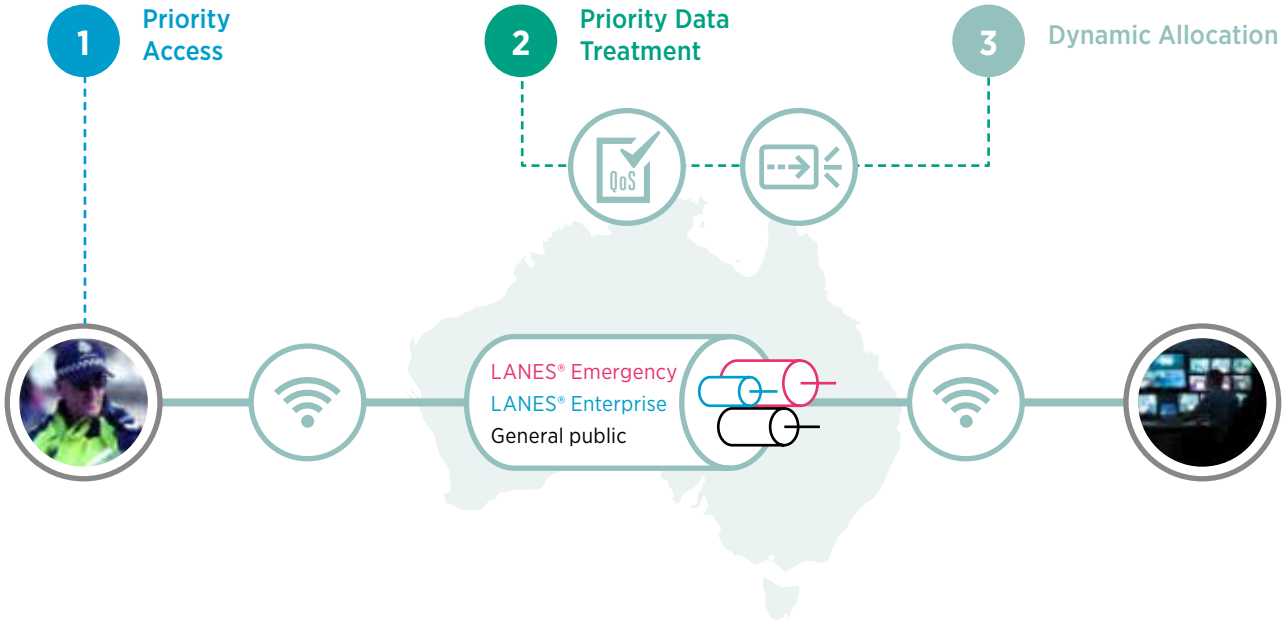
Telstra LANES® Users identified and provided priority access in the event of network congestion

Preferential Data treatment

Enhanced Quality of Service (QoS) to provide preferential data treatment to Telstra LANES® users

Self Dimensioning Bandwidth

Bandwidth allocation to priority users dynamically shaped on demand to meet their needs



The national Public Safety Mobile Broadband Capability is simply accessed by installing a Telstra LANES® for Emergency Services SIM Card.

Telstra's LANES® solution has been enabled nationally and will be available for the police and emergency services to utilise for the forth coming natural disaster season in Australian 2016-17 with the aim of:

- Keeping the Community Safe – The Telstra LANES® strategy is a unified national approach. It's designed to better support our emergency services organisations to protect communities now and in the future; and
- Connecting the Entire community – PSAs gain Australia-wide interoperability enabling them to automatically connect to each other in coverage areas to improve joint response without having to invest in infrastructure.

Find out more at
www.gsma.com/network2020

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601