RADCOM

Ensuring mission-critical communications with RADCOM Network Intelligence

Publication Date: May 2020

Web Site:

http://www.radcom.com

Table of Contents

Introduction 4

The road to PS-LTE 6

Crucial enablers of MC communications in LTE 7

QoS Class Identifier (QCI) updates 7

Mission-Critical Push-to-Talk (MCPTT) 7

Enhanced Multimedia Multicast (eMBMS) 10

Proximity Service (ProSe) – LTE-Direct (LTE-D) 12

Market Status 14

RADCOM Network Intelligence 16

Proactive MC service monitoring 17

Smart, dynamic traffic sampling 18

Advanced filtering 18

Intelligent traffic sampling 19

Packet and session tracing for root-cause analysis 19

Integration with the Policy and Charging Rules Function (PCRF) and orchestrators 20

Summary 21

Glossary 22

Introduction

Over the last few years, there have been many examples of why Public Safety Networks (PSNs) dedicated to enabling and prioritizing essential, resilient communication services to first responders and emergency services are critical. From earthquakes to wildfire seasons, when disaster strikes, network traffic surges as people try to contact family members and friends. At the same time, emergency services are out in the field, providing first response to the crisis and relying on the same communications infrastructure. Pandemics, natural disasters, terroristic attacks all bring home to us why more and more governments are establishing public safety networks for Public Protection and Disaster Relief (PPDR).

Public safety networks have traditionally been deployed according to regional standards, such as Terrestrial Trunked Radio (TETRA), a European standard created by ETSI (later adopted as the worldwide “de facto” standard, except in North America), and Project 25 (P25 or APCO-25), designed for use in North America. These private networks are Land Mobile Radio Systems (LMRS) that utilize Narrowband (NB) technology that has data rates around a few tens of Kbps and make them suitable for voice-centric applications. Some examples of PSNs that use NB technology are; BOS, Germany, a single shared network for all security authorities, and is one of the largest TETRA networks in the world. INPT in France that has been in operation since 1994. JustTop a TETRA network for authorities in Beijing. VIRVE, Finland that has been operational since May 1998.

Overall, these NB public safety networks are deployed in over 100 countries across Europe, the Middle East, Africa, Asia Pacific, Caribbean, Latin America, and North America. These LMRS networks provide reliable voice-centric applications. However, due to their low data rates lack the bandwidth to enable rich multimedia applications such as video streaming and file sharing. They also utilize different frequencies and technologies and make inter-organizational communications a challenge. Broadband (BB) technologies are required to enable more advanced public safety services such as live video streaming, the use of mapping software, database access, file sharing, and even more advanced use cases.

LTE broadband already provides to consumers and businesses high data rates for transferring massive volumes of data using 3GPP global standards. These networks are cost-effective, provide excellent coverage, and capacity, while already delivering voice, data, and HD video services. So, governments are increasingly looking at leveraging commercial networks run by mobile network operators (MNOs) instead of deploying a dedicated public safety network, utilizing the infrastructure that is already in place while maintaining interoperability with legacy LMR networks. In the long-term, LTE will transition to 5G, introducing ultra-reliable and ultra-low latency, network slicing, and edge computing that will translate into even more significant capabilities and applications for public safety networks. Such as first responders, each being equipped with HD cameras and dispatching units with connected drones to capture overhead views.

The road to PS-LTE

Although the foundations for mission-critical communications on LTE began with 3GPP Rel-8, it was pushed significantly in 2015 with Rel-12 when significant gaps in the mission-critical standards were overcome with the added involvement of the public safety community, support from commercial network operators and network equipment vendors.

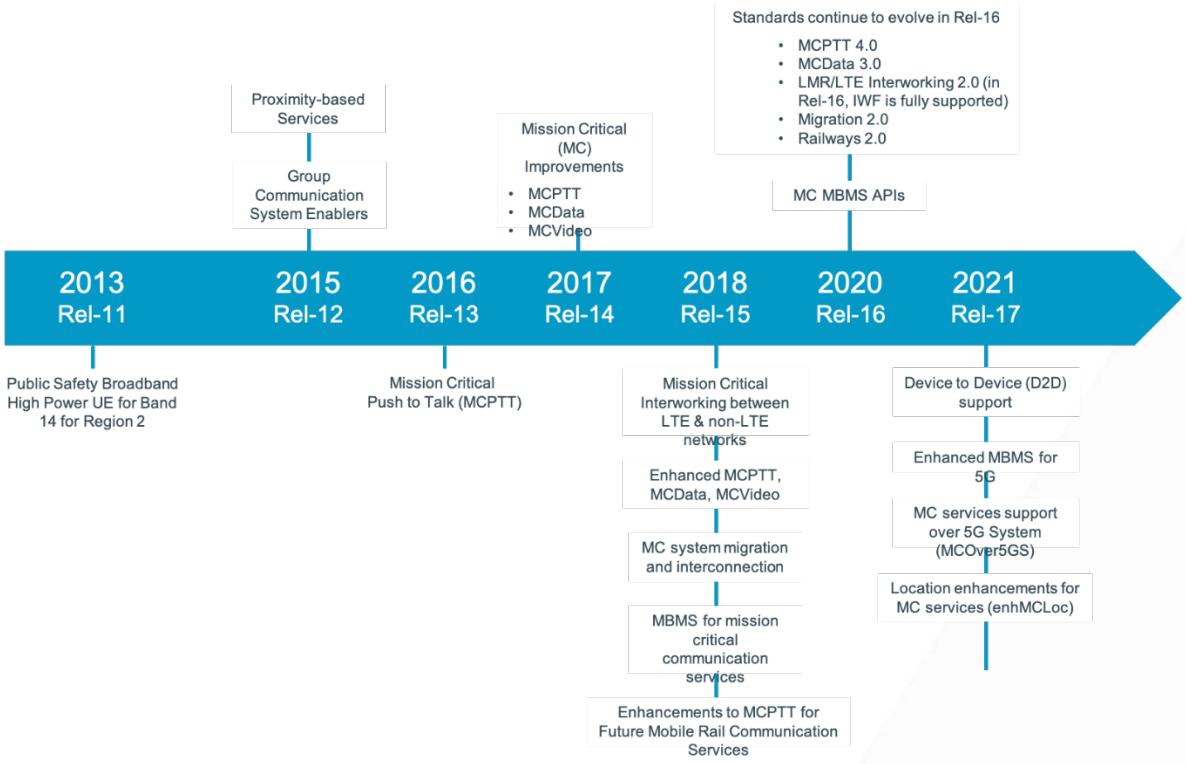


Figure 1 – 3GPP standards for mission-critical communications

Among the other capabilities standardized in Rel-12 were the Group Communications System Enablers (GCSE LTE). In Rel-13 - ratified in December 2015 – 3GPP built on the GCSE to standardize Mission-Critical-Push-To Talk (MCPTT), enabling both on and off-network modes. In Rel-13, Mission Critical communications were limited to voice - via Mission-Critical Push-To-Talk (MCPTT). However, in Rel-14, Video, and Data communications were also made possible.

With Rel 15 being the first release of the 5G standard, mission-critical communications were adapted also work on 5G networks (in addition to 4G/LTE) as well as focusing on the interoperability between legacy PS networks and LTE. This focus on interoperability continues to be a significant focus on Release 16 that is expected to be ratified later in 2020.

As the 3GPP has introduced standards for access barring, bearer pre-emption and bearer-specific packet QoS parameters, device and infrastructure manufacturers released equipment for use in public safety LTE (PS-LTE) agencies and operators have begun trialing and deploying PS-LTE infrastructure. These deployments will only increase as the MC features and capabilities built into 3GPP compliant networks continue to develop.

Crucial enablers of MC communications in LTE

With all the innovation and incremental releases, PS-LTE provides enhanced situational awareness, emergency calls, and priority treatment that provide all the critical elements of a public safety network, while also maintaining interoperability with legacy NB networks. Some of the crucial enablers are:

QoS Class Identifier (QCI) updates

The feature that best defines public safety grade LTE is the use of Quality of Service (QoS) for delivering voice and data to users when the network is loaded. For applications in a 3GPP LTE system, the use of QoS Class Identifiers (QCI) is the mechanism that defines the scheduling treatment of data throughout the network. Different bearer traffic requires different QoS and, therefore, different QCI values. A QCI value nine is typically used for the default bearer of a UE/PDN for non-privileged subscribers.

The QCI is enforced at the air interface between the user equipment (UE) and eNodeB, on the backhaul from the eNodeB to the evolved packet core (EPC) and from there to the application server. With the advent of VoLTE, the use of QCI was mandated to ensure end-to-end voice quality was preserved and as good as or better than circuit-switched voice. The creation of mission-critical applications came after the development of the initial QCI values for LTE. Therefore, modifications to the standard were required to ensure that emergency communications took precedence over commercial traffic. In Rel-12, the QCI was updated to place MCPTT at the top of the food chain. With the signaling layer for MCPTT given the highest priority (a value of 0.5) to ensure that devices are alerted first before data is sent. Then the MCPTT traffic is assigned a value of 0.7.

Mission-Critical Push-to-Talk (MCPTT)

Push-to-Talk (PTT), also known as press to transmit, is the standard form of public safety voice communications today. PTT is a method of voice calls using a half-duplex communications system (in which both parties can communicate with each other, but not simultaneously). Communication is by using a button on the radio or walkie talkie to switch from voice reception mode to transmit mode. Traditionally, PTT was used on LMR networks, but now Push-to-talk over cellular (PoC) is running in parallel to this. PoC has been available for nearly 20 years with MNO solutions, such as iDEN communications from Nextel. Sprint also offered its QChat enabled service, and Kodiak enabled services for Verizon and AT&T.

MCPTT is an international standard set by 3GPP that allows public safety agencies to leverage LTE networks for mission-critical communications. The measure includes high availability/reliability, low latency, support for group calls, and [one-to-one] calls, talker identification, device-to-device direct communications, emergency call, clear audio quality. With the Enhanced Multimedia Broadcast/Multicast Service deployed, MCPTT can also enable thousands of devices to be connected at once to transfer video, images, and voice simultaneously using multicast technology.

MCPTT vendors and variants

The MCPTT solution can be split down into three essential parts that include; the user device, client or user application, and application server. Multiple vendors are offering solutions, some with the whole stack, and others provide partial solutions. Some of the MCPTT vendors are;

Samsung

In June 2015, Samsung produced the first 3GPP based PTT demo using a full LTE network with IMS and eMBMS. Since then, they have created a 3GPP Release 13 MCPTT system. Samsung is the MCPTT service for South Korea's nationwide MCPTT network.

Motorola Solutions

In 2018 AT&T signed a product agreement with Motorola Solutions for its Kodiak carrier-integrated PTT product (Motorola Solutions acquired Kodiak Networks in 2017), along with the eventual MCPTT version of the Kodiak service. In addition to Kodiak, Motorola Solutions offers over-the-top (OTT) MCPTT, MCVideo, and MCData services hosted in the public cloud across the world. Via its cloud-hosted solution Motorola also provides solutions to Verizon and Sprint in the US.

Nokia

In February 2016, they debuted the first 3GPP compliant MCPTT system. It was based on Release 12 due to QCI support in devices, but the infrastructure is Release 13 compliant. This system was a combined effort from Cybertel and Bittium on devices, SK Telecom with application development, and Nokia on infrastructure.

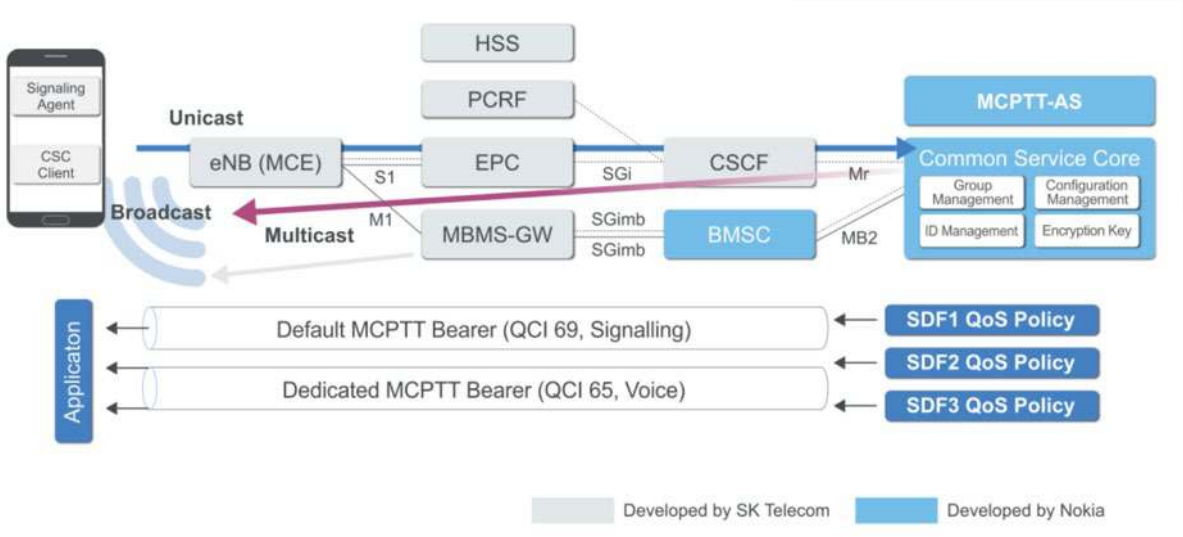


Figure 2 - Nokia & SK Telecom MCPTT Deployment - Source: SK Telecom

From MCPTT to MCX

Standardized in Rel-14 MCVideo enables users to 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, video can allow first responders to share the real condition of the surrounding area with other PSA group members to make more informed decisions. With MCData database inquiries could be made from the frontline, or first responders can make use of features such as event manager sync or robot control, intelligence gathering and dissemination. Users could also distribute files, securely access a public safety cloud, and use messaging service similar to Short Data Service (SDS) from TETRA.

MCPTT network architecture and traffic flow

Service requirements for MCPTT are described in TS 22.179. The MC-PTT architecture defining the several reference points and network nodes involved in the service is discussed in TS 23.179, while the protocols and procedures are described in TS 24.179.

3GPP TS 23.179 specifies that the UE connects to MCPTT specific Access Point Names (APN) to use the MC-PTT service. The signaling is provided over SIP and HTTP, which also leads to using 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 to the same bearer. The following diagram shows how the MCPTT reference points can be mapped to different unicast and multicast bearers.

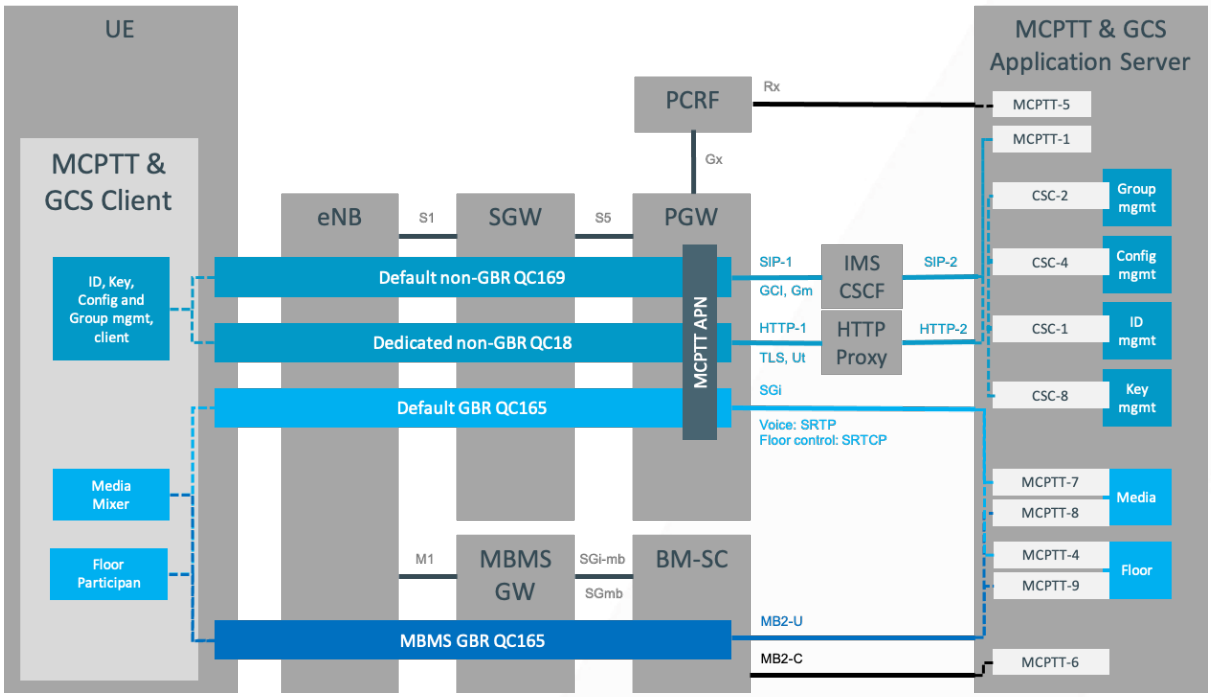


Figure 3 - MCPTT & Group Communications Service Architecture

To use MCPTT, the UE performs authentication and authorization after LTE attach as defined in 3GPP TS 33.179, which consists of three processes:

- MCPTT user authentication (CSC-1)
- SIP Registration and Authentication
- MCPTT Service Authorization

The first two can be performed in any order. For example, MCPTT User Authentication could be achieved 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, where confidentiality and integrity of the Gm interface are using IPSec. MCPTT service authorization is done using the credentials received from MC-PTT user authentication.

Enhanced Multimedia Multicast (eMBMS)

Typical communications in an LMR network are on a broadcast type of communications channel or one to many conversations simultaneously. Users are assigned a talk group with which to communicate in a half-duplex communication system. This form of communication consumes few resources and allows large-scale group communications to happen with ease.

In an LTE network, communication is unicast or one-to-one. This means that a data session needs to be established for each device that is being communicated to individually. eMBMS is a 3GPP-standard that allows mobile operators to use a proportion of their network capacity for a broadcast of content or data. This means they can use the same broadcast stream to serve multiple – theoretically unlimited – customers within a single cell with the same video, TV, or other data services, instead of needing to unicast delivery of the same information to every user individually.

The result is a potentially substantial reduction in the number of network resources used to deliver the content. All kinds of content can be broadcast – linear and live TV and video, linear and live music, static content, software, data, and information. The operator has the flexibility to decide how much of its spectrum resource to dedicate to LTE Broadcast and can allocate proportions of different carriers for either unicast or broadcast content (or more recently, both – see below). Those proportions can be given different profiles at different times of the day. The operator has the option to implement the technology on a cell-by-cell basis so that LTE Broadcast only consumes capacity in areas where the operator wants the service to be offered.

In Rel-15, which was frozen in June 2018, work on stage 2 of MBMS usage for mission-critical communication services was completed. Work on enhancing eMBMS for MCVideo was also undertaken. Rel-16 includes a study on MBMS APIs for mission-critical services. MBMS APIs will enhance interworking with legacy LMR systems.

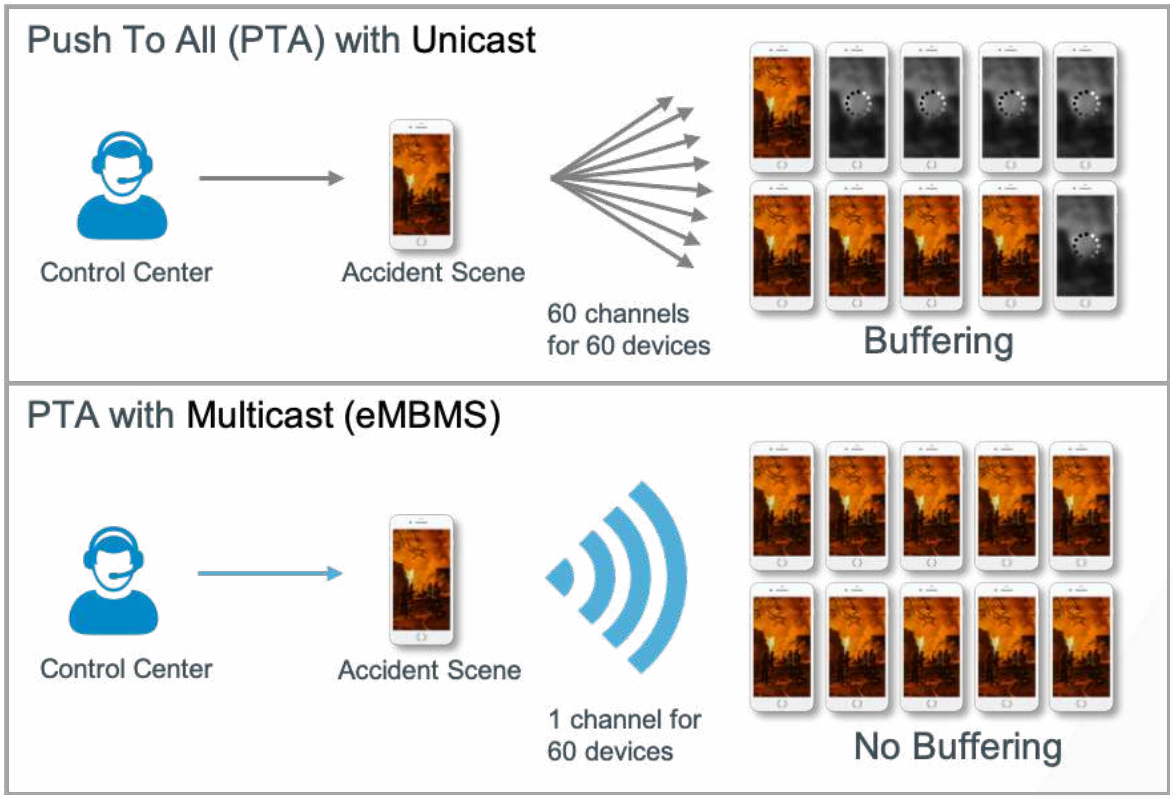


Figure 4 - The advantage of deploying an eMBMS for mission-critical communications

In LTE, the number of users that can be supported on MCPTT is directly coupled to the capacity of the site. If a data stream is 1 Mbps for each user, then a unicast system must support 80 Mbps for 80 users. In an eMBMS solution, a single 1 Mbps stream would be allocated for all users simultaneously, thus allowing more capacity on the cell for other users. The addition of eMBMS support in devices and the network does incur costs and added complexity as an MBMS-GW has to be deployed in the core network. Each eNodeB must have Multicast Coordination Entity (MCE) capabilities.

MCPTT network architecture with eMBMS support

At the end of 2019, there were over forty operators that are known to have been investing in eMBMS, and amongst that group, several are working in the field of eMBMS for MCPTT. One such operator is KT in South Korea that demonstrated the use of eMBMS-based Group Communication Service Enabler (GCSE) capabilities for public safety applications—enabling group communication with a large number of people while using base stations from different vendors (Nokia and Samsung).

The eMBMS can also be used to provide an enhanced Public Warning System (PWS);

- Deliver rich multimedia warnings to subscribers
- Fine control of the granularity of the region where the warning is distributed
- Speed of delivery
- Parallel delivery of multiple warnings (in different languages)
- Reach all subscribers (including roamers)

Proximity Service (ProSe) – LTE-Direct (LTE-D)

The use of simplex mode or device-to-device communications in LMR is a common occurrence, especially for fire departments. Often when arriving on the scene, the firefighters use a vehicular repeater and tune their radios to a simplex radio channel. The simplex radio channel is connected to the repeater and then communicates to the LMR network. This is historically done to ensure coverage between users in a building where they may be in a basement or areas with inadequate external network coverage. Simplex communications are also done to cut down on voice traffic to dispatch that they do not need to hear, and it releases LMR channels for other users.

LTE devices were never intended to directly communicate with each other, as it requires the use of the core network for communications. However, the ability to directly communicate, device-to-device (D2D) was initiated in Rel-12 and has continued evolving in subsequent releases and is essential in delivering robust mission-critical communication services through 3GPP standard mobile networks.

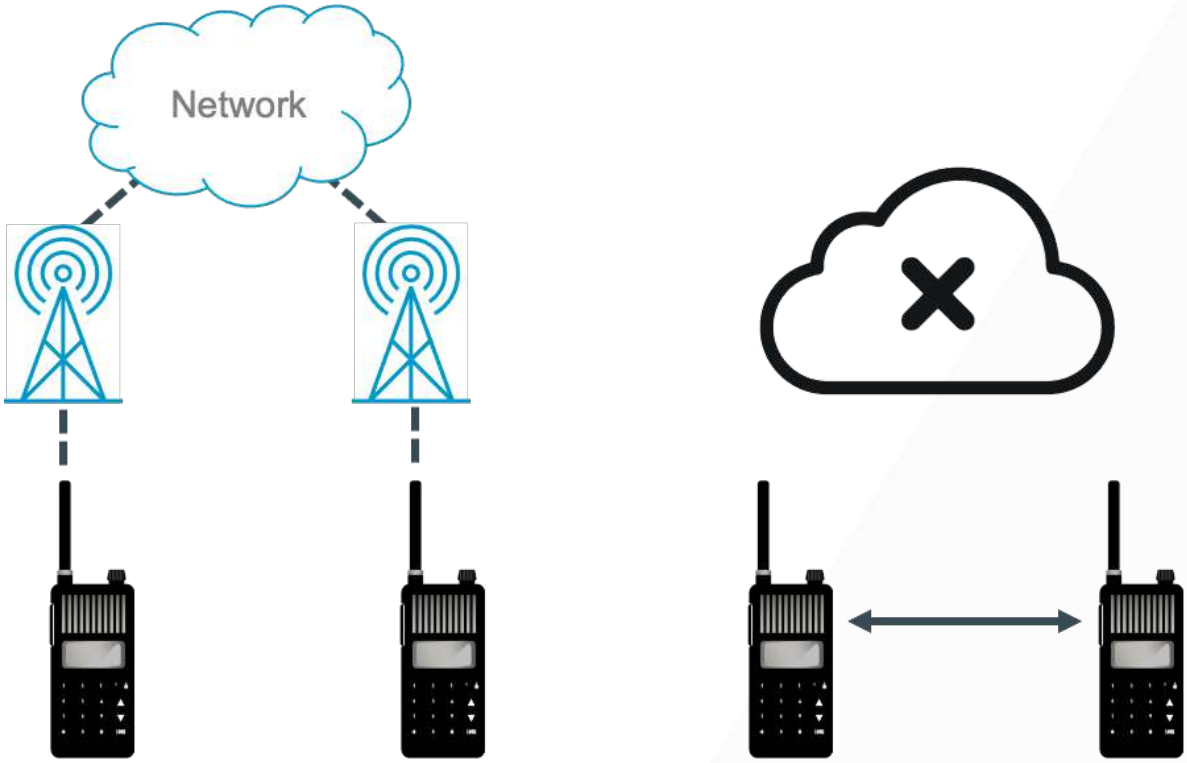


Figure 5 – Proximity services provide direct device-to-device communications off the network

ProSe challenges

LTE-D or ProSe provides direct device-to-device communications off-network for operational support of public safety users that are out of LTE network coverage. The FirstNet Authority in the USA has worked during 3GPP Release 17 discussions to include D2D, and as a result, this feature is added. Release 17 is planned for December 2021. FirstNet explicitly stated that D2D would allow users to communicate directly with each other when they are outside of network coverage areas.

The functionality is similar to operating in P25 simplex or direct mode. Operationally though, the performance of LTE-D devices may vary from P25 subscribers since LTE smartphone power will likely be limited to 23 dBm (transmitting with 200 milliwatts of power). This means that the ability to communicate long distances (e.g., over ½ mile) or through dense building materials will be limited compared to P25 networks (with some LMR devices featuring large external antennas and power levels of 3 watts and 5 watts). While the current 3GPP ProSe might be adequate for direct outdoor mode, providing indoor to-outdoor connectivity may be more of an issue.

Market Status

Worldwide over twenty PS-LTE networks are being trailed, deployed, or already implemented. Some complement existing legacy NB networks and others are meant to replace them. Some of these PS-LTE networks are nationwide, and some are smaller scale, for example, in a city. They include a mix of public and private networks (run by MNOs, but not accessible to the general public, only to emergency services). MNOs are moving from maintaining networks for consumers and businesses to public safety authorities that means a switch in mindset from delivering business-critical services to mission-essential services.

	Commercial Network vs.	Public Safety Network
Critical Level	Mission Critical	Business Critical
Use case assumptions	Works when responsible conditions are in place	Works even when severe congestion occurs
Failure damage	Inconvenience of users	Human lives
Network design principles	• Feature orientated • Minimum redundancy	• Focus on reliability • Full redundancy

Some examples of PS-LTE networks:

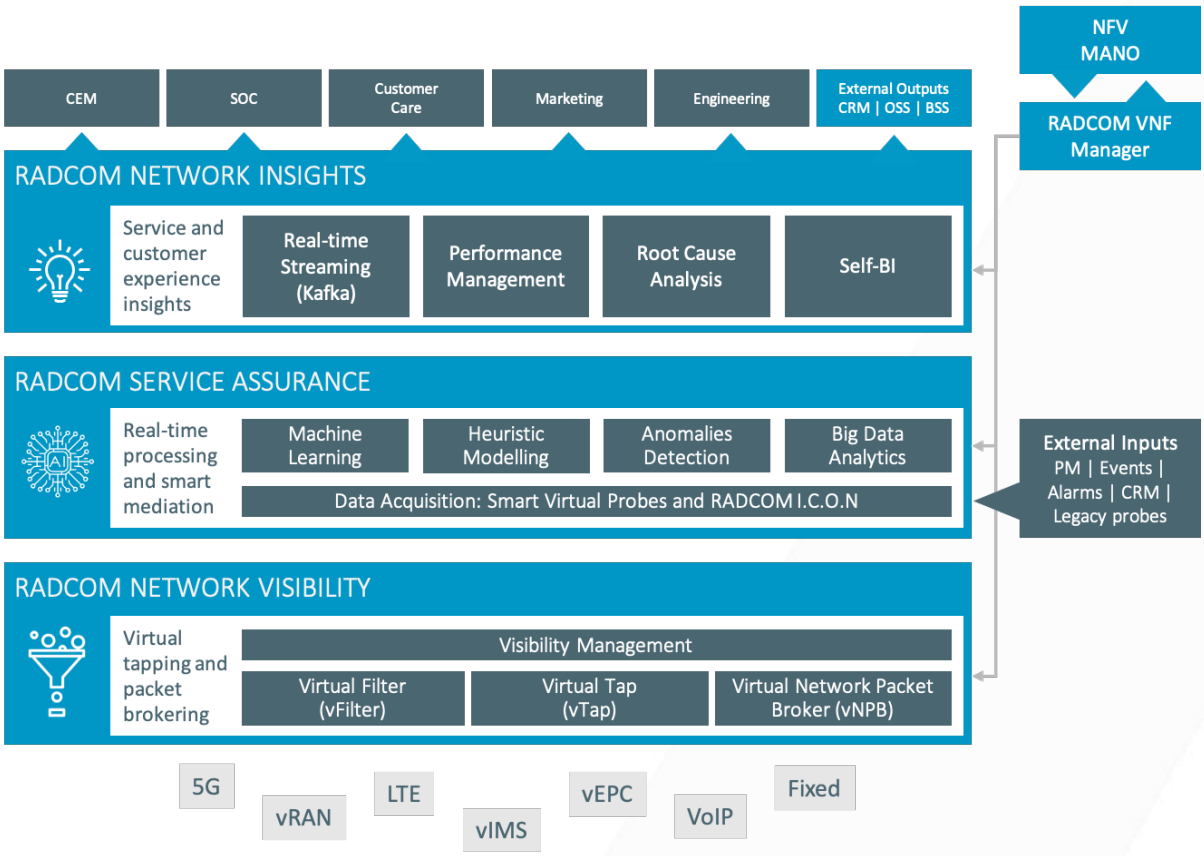
Country	MNO or NEP	Status	Details
Australia	Telstra	Deployed	It launched its LANES PS-LTE network in 2016 on a dedicated 166 MHz of spectrum in the 700 MHz band.
Brazil	Motorola Solutions	Trailing	Brazil held a trial with Motorola Solutions, demonstrating PS-LTE in Sao Paulo and the Federal District. They also held trials during the 2014 FIFA World Cup.
China		Deployed	In 2013, China began building a national PS-LTE network on a dedicated spectrum covering more than ten cities, including Beijing, Shanghai, Nanjing, Shenzhen, and Guangzhou; 256 base stations and over 10,000 terminals are in service in Nanjing. Suzhou Wujiang police have a dedicated LTE-based wireless broadband network. Lijiang is also using Huawei's eLTE for the PS-LTE network. It interconnects with the existing 350 MHz system.
Finland	Elisa	Trialing	Nokia, State Security Networks Group Finland, local operator Elisa, and Helsinki Police Department tested PS-LTE in the Helsinki area in December 2017.
Mexico	Nokia	Planned	Plans are to develop an MVNO for PS-LTE.

Country	MNO or NEP	Status	Details
South Korea		Deploying	South Korea is implementing a public safety LTE called Safenet, which is a separate LTE 700MHz network being rolled out. This follows trials conducted in 2015, 2016, and at the 2018 Winter Olympics.
Spain	Huawei	Deployed	Spanish Canary Islands has a combined TETRA-LTE network. It was launched in 2016. Spain's Bilbao Metro also added PS-LTE to its TETRA network in 2015. Huawei helped install an eLTE PS-LTE network in Rivas Vaciamadrid as an upgrade on its existing TETRA network.
UK	EE (part of BT)	Deploying	EE has been granted the contract to develop and manage the Emergency Services Network (ESN). A deal has been signed with Samsung Electronics to supply 4G handheld devices for the network, which will be using 800 MHz, 1.8 GHz, 2.6 GHz. This network is expected to replace the UK's legacy TETRA network.
USA	AT&T	Deployed	AT&T was awarded a 25-year, $6.5bn contract for building and maintaining the public safety network in March 2017 and was granted 2 x 10MHz of 700MHz (Band 14) spectrum for both public safety and non-public safety use to complement its existing 4G LTE spectrum holdings. FirstNet is being used to support the COVID-19 Emergency Response providing an always-on, 24-hours-a-day priority and pre-emption across voice and data, with multiple priority levels that first responder users can allocate as needed. In May 2020, AT&T had more than 1.3M FirstNet connections across more than 12,000 public-safety agencies.
USA	Verizon	Deployed	Verizon launched its PS-LTE network in March 2018. Spectrum used is 700 MHz, 800 MHz, 1.9 GHz PCS, 1.7/2.1 GHz AWS

RADCOM Network Intelligence

During a large-scale disaster or emergency network traffic surges, which can cause significant challenges such as network congestion, low data rates, and interoperability problems. When emergency services are out in the field, seconds matter, and reliable communications can be a life-or-death issue. So, the importance of QoS for this service is critical.

RADCOM Network Intelligence provides operators with an end to end service assurance solution for MC communications that includes MCPTT, MCVideo, and MCData—covering such network elements as the CSC, CSCF, Presence, MCPTx, ProSe/BSF and the UDC to ensure complete visibility across the MC service quality. RADCOM Network Intelligence includes; RADCOM Service Assurance, delivering probe-based, service assurance using an automated, containerized solution. RADCOM Network Visibility for smart filtering of traffic for a specific MC service or application, as well as load balancing, and sampling. RADCOM Network Insights for business-critical intelligence and real-time information on the MC user and MC service experience.



RADCOM's solution enables the operator to monitor its end-to-end MC network and service quality smartly. While also providing troubleshooting tools for service-affecting issues to ensure MC service quality, during challenging times, whatever the demand. RADCOM monitors ProSe interfaces such as PC1, PC2, PC3, PC4, PC5, PC8, SGi, Ub (for User Authentication), and Zh, MCPTT interfaces like CSC3, SIP (MCPTT-2), and Diameter (MB2 and Sh) as well as ISC-SIP.

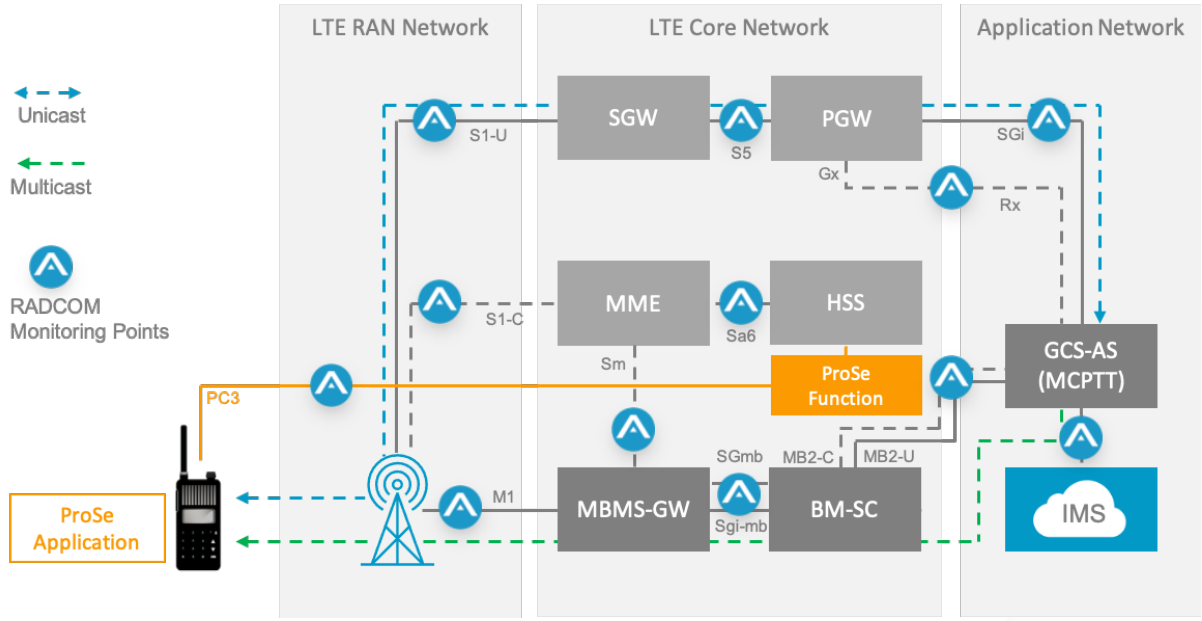


Figure 6 - RADCOM provides end-to-end coverage for monitoring MCx services

As RADCOM Network Intelligence is fully containerized, the solution is elastic and flexible to grow and shrink with the needs of the operator. It is highly efficient when utilizing network resources and adjusting itself to the needs of the operators as the traffic fluctuates. Being cloud-based, RADCOM Network Intelligence is quick to deploy even if the operator has not yet transitioned to a virtual environment.

With full redundancy capabilities and deployed as a distributed cloud solution RADCOM Network Intelligence combines flexible central management and distributed regional deployments that are resource-efficient. RADCOM Network Intelligence provides operators with a rich portfolio for smartly monitoring and troubleshooting mission-critical communications;

Proactive MC service monitoring

With a new set of QCIs specifically for MCx service traffic with stricter latency and loss budgets as well as higher priority assignments, this ensures that even if the network becomes congested, MCx traffic takes priority over all other traffic. While an MCPTT application server can provide PTT service even without these QCIs, mission-critical QoS requires the network and devices to support the new QCIs and for assurance vendors to monitor them.

The set of KPIs defined for MCPTT communications in 3GPP TS 22.179 is intended to ensure that LTE-based MCPTT provides performance that is (at minimum) on-par with existing LMR standards and solutions. The KPIs are as follows;

1. MCPTT Access Time - The time between when an MCPTT User requests to speak and when this user gets a signal to start speaking

2. End-to-End Access Time - Typical case is an MCPTT private call (w/ floor control) request where Rx user accepts the call automatically
3. Mouth-to-ear Latency - The time between an utterance by the Tx user, and the playback of the utterance at the Rx user's speaker
4. Max Late Call Entry Time - The time to enter an ongoing MCPTT Group Call measured from the time that a user decides to monitor such a Group Call to the time when the user's speaker starts to play the audio

RADCOM Network Intelligence ensures your MC communication matches the KPI levels expected and provides engineering teams early warnings about performance anomalies using smart alarms and can also provide AI/ML-based anomaly detection. By identifying issues early, RADCOM Network Intelligence delivers the insights needed to understand and resolve problems before they grow into MC service-impacting events. With RADCOM Network Intelligence, operators gain complete, real-time, and end-to-end visibility into their MC services.

Using RADCOM's solution operators can monitor MC services, based on an architecture that provides:

- Cell sites optimized to deliver maximum radio resources that offer the best possible user service at all times

- 24/7 network health monitoring and proactive capacity management helps to ensure that network issues are addressed before they impact MC service performance

Smart, dynamic traffic sampling

RADCOM Network Visibility solution offers advanced packet brokering functionality that is integrated and synchronized with RADCOM Service Assurance, thus enabling the operator to smartly manage, optimize, and load balance network traffic sent to the assurance probes.

Advanced filtering

Smart traffic filtering allows the operator to filter out or zoom in on specific traffic according to an extensive set of criteria. Traffic matching the rules can be either redirected or dropped. So, for example, if the operator wants to include or exclude traffic from specific applications, it's easy to set up via the web UI.

Using advanced filtering, the operator can filter out the MC service and drop other traffic and only send this critical traffic to the probes. This can be taken a step further by utilizing DPI-based filtering and filtering out different types of data types within an application. RADCOM Network Visibility provides the following smart filtering functionality;

- App-based filtering (MC services such as PTT)
- IMSI/MSISDN-based filtering
- DPI-based filtering (for example, forward encrypted video to target X and not target Y)
- NOT functionality with all fields allowing data to be included or excluded
- Additional logical operations (e.g., and, etc.)
- Filtering by L2, L3 and L4 classifiers
- Provides statistics per filter
- Copy/forward packets for further processing

Intelligent traffic sampling

RADCOM Network Visibility enables traffic sampling in which only a specified amount of traffic (randomly sampled) is passed through the network packet broker to the monitoring tools. The rest of the traffic is dropped. Traffic sampling can be flow or subscriber-based with sampling algorithms, randomly selecting a group of sessions and forwarding only packets that belong to these sessions. Operators can configure the network packet brokers to preserve sessions of either 5-tuple flows or subscribers (MSIP/IMSI/MSISDN). If the overall traffic is higher/lower than expected, the algorithm will reduce/add sessions accordingly.

RADCOM Network Visibility works in unison with RADCOM Service Assurance to optimize network traffic flow, filter unnecessary traffic to reduce overload, enable session-aware load-balancing to distribute across multiple probes as well as dynamic traffic sampling of a specified amount of flows or user data.

Packet and session tracing for root-cause analysis

If issues in MC services are found, RADCOM's packet analysis and call tracing applications can be used to execute root cause analysis of MC sessions quickly. All session legs are correlated and displayed in a single view, with all the various parts of the session from the LTE to the MCPTT interfaces included. Users can filter by MCPTT party ID, MCPTT group ID, and MCPTT granted party ID.

Figure 7 - Troubleshooting MC services using RADCOM's call/session tracing application

Integration with the Policy and Charging Rules Function (PCRF) and orchestrators

A closed-loop approach to monitoring and assuring MC communications is critical to ensure and optimize service performance automatically. RADCOM Network Intelligence provides this approach with integration into the PCRF and the orchestrator.

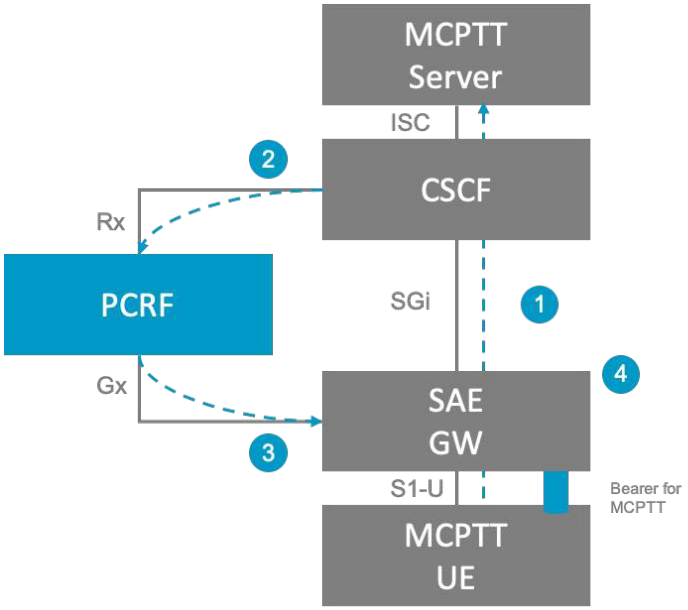


Figure 8 - The role of the PCRF in an MCPTT network

1. MCPTT call establishment request
2. MCPTT service Info.
   [MCPTT ID AVP]
   [Resource reservation AVP]
3. MCPTT QoS enforcement request
4. MCPTT QoS enforcement

With the assignment of a QCI, by the PCRF, to establish a priority level, which determines the order of precedence of traffic sets budgets for packet delay and packet error loss rates and defines whether a given traffic bearer has a guaranteed minimum bitrate or not. Collectively, these criteria are used by the SAE-GW to manage traffic, meet service level requirements, and decide which traffic to deprioritize as the network becomes congested.

The assignment of a QCI, by the Policy and Charging Rules Function (PCRF), establishes a priority level which determines the order of precedence of traffic, sets budgets for packet delay and packet error loss rates, and defines whether a given traffic bearer has a guaranteed minimum bitrate or not.

RADCOM Network Intelligence provides operators with tight integration into the PCRF. Proactively monitoring the operators' end to end MC services and pinpoints network degradations before users are impacted. This data is streamed to the PCRF, which automatically acts to optimize the network and resolve possible degradations, without manual intervention. The seamless combination of RADCOM Network Intelligence with the PCRF expedites and automates not only the detection but also the resolution of network degradations.

RADCOM Network Intelligence also delivers a fully cloud-native, container-based architecture that seamlessly integrates within an operators' cloud orchestrator. Kubernetes (K8s) controls RADCOM's containerized components lifecycle starting from the initial day-0 instantiation and throughout the overall platform lifecycle. Being dynamic and fully integrated with the operators' orchestrator enables operators to take an on-demand, closed-loop approach to assuring and optimizing the network in these challenging times with network usage skyrocketing and subscriber habits changing.

This closed-loop approach is critical for smartly monitoring MC services as manually optimizing the network performance is not viable in particularly during a disaster.

Summary

RADCOM Network Intelligence provides a fully containerized, distributed solution that is resilient during a crisis or emergency – offering full redundancy – while empowering the operator with granular, accurate data about their MC network and services. Offering cloud-based, next-generation troubleshooting tools such as packet analysis and call/session tracing for a low-level examination of the traffic for rapid root cause analysis. RADCOM's end-to-end suite will enable operators to manage and optimize their network to assure MC services are always connected, whatever the demand. For a smart approach to monitoring MC services, choose RADCOM Network Intelligence.

Glossary

Term	Description
D2D	Device-to-Device
DMR	Digital Mobile Radio
dPMR	Digital Private Mobile Radio
eMBMS	Enhanced Multimedia Broadcast/Multicast Service
GBR	Guaranteed Bit Rate
GCSE	Group Call System Enablers or Group Communication Service Enabler
LMR	Land Mobile Radio
LMRS	Land Mobile Radio Systems
LTE-D	LTE Direct
MCPTT	Mission Critical Push-To-Talk
MCX	"X" stands for PTT, VIDEO, and DATA
NXDN	Next-generation Digital Narrowband
PDT	Professional Digital Trunking
PPDR	Public Protection and Disaster Relief
Project 25	P25 or APCO-25 is a suite of standards for digital mobile radio communications designed for use by public safety organizations in North America
ProSe	Proximity Services
PS-LTE	Public Safety LTE
PSA	Public Safety Authority
PSN	Public Safety Networks
PWS	Public Warning System
QCI	Quality Class Indicator
TETRA	Terrestrial Trunked Radio