On the road to MCX: ensuring reliable connectivity for mission-critical communication over public mobile networks

Overcoming congestion, outages, and loss of coverage

Lyfo

Preface by Maurits Zandbergen, CEO of Lyfo

Are you ready for MCX to finally deliver on its promise?

There is a growing realism in the market about the (im)possibilities of mission-critical communication over public mobile networks (MCX). For many public safety organizations, like the police, only one thing is truly critical: a reliable connection with the control room.

This is what the current Tetra network is designed for, and to me, it's the absolute minimum requirement for any replacement technology.

And that's the problem.

Replacement MCX solutions rely on a single mobile network and, despite talk of national roaming, there are many technical, political, and commercial hurdles. The MCX standards don't address:

- Improving network coverage
- Handling congestion
- Dealing with outages
- Dealing with Mobile operators

More is needed, like network priority and backup access to all available mobile networks in the country. If your primary network fails, there needs to be an alternative, without any user-interaction. Only then can mission-critical availability surpass the current Tetra network.

Sounds like the future? It's not.

By combining Lyfo.net's comprehensive network setup with priority in the home operator's core network, we have realized a reliable solution for mission-critical communication over public mobile networks and you can start NOW to improve mobile connectivity for your users. No need to wait for MCX!

Starting NOW creates a natural growth path for both Operators, Public safety organizations and their users towards MCX based services in the coming years, step by step.

You can read all about this unique solution in this whitepaper and would you like more information, meet and discuss? Let's connect!

Maurits Zandbergen
maurits@lyfo.com

Introduction

Public Protection & Disaster Relief (PPDR) organizations all over the world want to transition from traditional, TETRA-based networks to public mobile networks for mission-critical communication. But when using public communication networks, even occasional congestion can't be avoided. Without the right configurations, the impact on users can be significant.

As a mission-critical user in the PPDR domains, it's vital that you experience the lowest impact from any congestion present on mobile networks during your missions. And with Push-to-Talk as the primary mechanism for critical communication, it's especially key to minimize the impact on this specific application — because it's the "lifeline" for first responders.

This whitepaper describes how users can leverage public mobile networks for mission-critical communication by mitigating the main risks of mobile networks: loss of coverage, network outages and severe network congestion.

Read on to learn about:

About Congestion

Congestion, generally characterized as a network that is near or at its capacity limits, may be caused by one or more factors, like:

- Local issues with the radio or antenna;
- Capacity issues with mobile backhaul in the area (especially when combining the traffic of several mobile sites);
- A significant increase in requested capacity during an event like a festival or concert, in spite of presence of a mobile site (Cell on Wheels);
- Unplanned events such as protests, where large amounts of subscribers gather in a small area.

In general, congestion is intermittent and caused by a peak in usage with large numbers of subscribers.

Most carriers operate with a certain level of margin (or overcapacity) on their public networks to cope with peak load while still allowing some congestion during a limited timeframe. But it's always possible for a load to be so excessive that the capacity becomes maxed out, creating sustained congestion for users.

When that happens, a carrier has two measures to ensure that certain users retain access and maintain sufficient capacity on the mobile network:

1. **The Access Class (AC)**

2. **The Quality-of-Service Class Identifier (QCI)**

An Access Class designated for Mission-critical users

Mobile networks are based on 3GPP standards and have a well-defined set of access classes, ARP, and QoS parameters assigned to subscribers.

Access Classes 0 through 9 are intended for normal users (with many carriers opting to map the class number to the last digit of the IMSI). Classes 10 through 15, however, are known as special access classes, with Class 14 designated for mission critical users.

Typically, a cell congested by active concurrent users/devices will start using barring mechanisms to back off some of their excess load requests for new active users/devices per 4G/5G cell. This mechanism initially sheds the load from the normal access class subscribers in Classes 0 through 9, ensuring that users of special access classes can still access the cell to request their services/data-bearers under high (user) load.

The access class method is the first barrier to stop overload due to concurrent users, but it doesn't guarantee data service yet. Even if the mobile network has enough capacity for data-bearers or data-transport, the amount of mobile devices attempting to request a bearer or access could still exceed capacity.

This is where access class differentiation comes into play, helping to manage and prioritize connection based on device classification.

The access class is stored on the SIM card and used when the device tries to attach to the mobile network. During the establishment of a session with the cell, the AC value determines whether the device should attempt to connect under congested conditions.

If yes, the connection is made, the subscriber is identified, and the priority of the requested service is determined using the associated ARP value. Then, the user's traffic is associated with the relevant traffic profile and quality of service for the data-bearer.

However, carriers are hesitant to provide large numbers of subscribers with special access classes, as this could significantly impact the capacity available for regular subscribers. As a result, many PPDR organizations cannot benefit from these classes yet. Carriers would be much more at ease providing these classes to PPDR organizations when these subscribers only use the right set of priority parameters intended for mission critical data — in this case Push-to-Talk (PTT) traffic.

Combined with a high-priority QoS Class Identifier data-bearer

While the access class determines whether a subscriber should be attempting to access the mobile network, and the ARP level (per data-bearer) determines the priority on assigning a data-bearer, the quality-of-service class identifier (QCI) determines the handling of traffic by the data-bearer on a congested cell.

Different types of traffic flows are prioritized based on a set of predefined characteristics. An example of this principle in practice is the handling of access to mobile internet (ISP service) and VoLTE calls.

The signaling traffic for the establishment and maintenance of a VoLTE call uses QCI 5 (which is pretty high), while the voice traffic for the same call is handled using QCI 1 (one of the highest). With this principle, there is almost always capacity available for making voice calls (rather than other forms of data traffic like internet usage). The signaling traffic is less likely to be available with regards to capacity but has a high enough priority in the network to ensure efficient handling of connection requests.

Combining Special Access Class 14 with a relevant ARP and high-priority QCI of the data-bearer ensures that PPDR organizations can use public mobile networks with an almost guaranteed level of access and capacity for mission critical application traffic. It minimizes the impact of congestion on any component along the chain, enabling reliance on public mobile networks as a viable option for PPDR teams.

The Challenges for Mobile Carriers

Carriers are particularly hesitant to provide these priority mechanisms to PPDR users when there is limited control on the usage patterns and data-volume coming up from users (e.g. live video up-streaming with priority).

Historically, all mobile traffic from a device was consolidated into a single data-bearer — often the mobile internet connection. This approach, while convenient, can lead to unexpected and uncontrolled load on the network, especially when resource-intensive applications like the device operating system and app updates are executed without regard to other functions being performed.

Such unmanaged congestion can jeopardize the service quality for all mobile users, including consumers, business users, roaming users, and even public safety personnel.

To address these challenges, mobile traffic separation is essential. Prioritizing public safety (PPDR) applications over generic internet data is a crucial first step. However, it is equally important to ensure that prioritized data remains within reasonable limits to avoid excessive load and costs. Additionally, a portion of mobile capacity must be reserved for public internet users, not only to maintain a positive network experience but also to comply with regulations like the EU Net Neutrality rules.

Until recently, this level of traffic separation was not feasible on mobile devices.

The Challenges for PPDR organizations

A PPDR organization should maintain a purpose-based contract with a large carrier, generally using a specific (IMSI) range of SIMs tailored to the PPDR group/ subscribers. The carrier, then, can manage these SIMs using a special portal and assign Special Access Class 14 and mobile data priority to a subsection of their users. The number of subscribers with priority would be limited under the contract to protect the integrity of the mobile network.

Changing the Access Class in the field (SIM in use) makes use of the over-the-air (OTA) update mechanism of SIM management. For planned events such as festivals, concerts or sports events, it's a cumbersome but manageable mechanism, as the PPDR organization can pre-allocate the special access class and priority to the subscribers that are scheduled to be present at the events.

But it's not a good solution for unplanned events.

Attempting to use an OTA mechanism to provision new parameters to SIMs present in an area under congestion conditions has an increased chance of failure, leading to the PPDR subscribers being unable to access the network when they need it most. Access Class updates also require the phone to read from the SIM card again to be applied (either user or SIM OTA-initiated).

The attempt to provision special access class settings to the PPDR subscribers can even increase the congestion in the area, which leads to an even further degraded experience for the PPDR and other subscribers in the field.

But Lyfo and its carrier partner have developed a unique integral solution which addresses all the challenges above — for both mobile carriers and PPDR organizations alike.

The Integrated Solution

Lyfo and its carrier partner bundled all their practical and technical know-how into a comprehensive, integral and innovative solution that guarantees availability specifically for mission-critical Push-to-Talk (PTT) and other PDDR applications. The solution encompasses three key components:

1) Optimized network access for Push-to-Talk traffic

Using this solution, the carrier can now provide all PPDR teams with SIMs already equipped with Special Access Class 14 to be used for mission-critical PTT communication.

Doing this significantly improves the network access for PPDR subscribers on the carrier partner network and eliminates the requirement for targeted OTA campaigns to pre-assign AC14 to a small subsection of subscribers in preparation for events.

But this doesn't resolve the entire congestion challenge, as the data bearer assignment and the resource scheduling allocation of network resources is no different than a regular mobile subscriber.

To achieve this, the carrier prepares and provisions an alternative data-APN (bearer) for PTT/PPDR traffic with a special QCI/ARP setting. Then, the user's device gets equipped with Lyfo's proprietary technology to request and map only this PTT/PPDR traffic to the special APN.

This ensures that the special APN is only used for authorized traffic, and other generic (often internet) traffic like MS Teams, email, OS updates, etc., are handled via the "regular" internet data-bearer without higher priority.

Lyfo enables this separation of traffic types without the need for extra changes on the device like profiles and EMM enrollment. It also ensures that both the needs of the PPDR organization and the mobile carriers are met: only mission-critical PPDR traffic gets prioritized, reducing extra resource allocation on the carrier network and associated risk and cost for the carrier.

2) Lyfo BackupSim to ensure network redundancy

Using Lyfo BackupSim for all PPDR subscribers automatically enables a fallback solution that leverages other national mobile carrier networks. The patented technology (on both SIMs and mobile phones) scans all available mobile networks and intervenes instantly when needed — without end-user intervention.

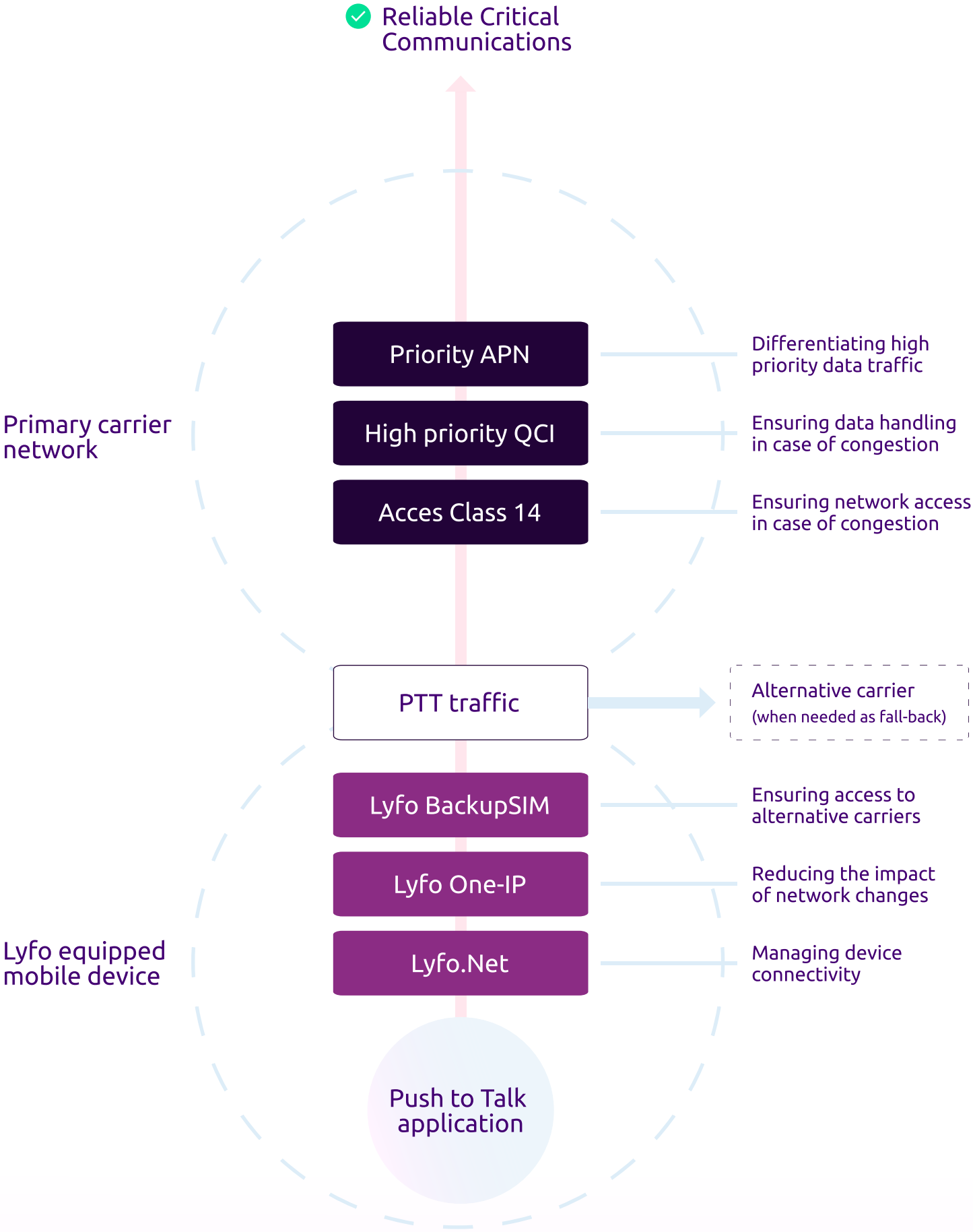
When the primary carrier connection falters, Lyfo automatically switches to the best alternative mobile network available. This ensures that the PPDR subscribers remain connected, even when encountering congestion or outages in the primary carrier partner.

Using Lyfo's BackupSim provides the PPDR organization more than access to any (inter-)national network available. It also establishes a redundancy of the second carrier's core network — resulting in full mobile network redundancy even at country borders.

3) Lyfo One-IP to reduce the impact of network changes

Push-to-Talk applications can take seconds — or even minutes — to reconnect/re-authenticate when the (IP) connection of the device changes or is interrupted for a time (which happens when switching between mobile networks and WiFi or when switching between primary carriers and alternative carriers with BackupSim).

Lyfo One-IP reduces the impact of a network change to an absolute minimum by switching networks without notice to the application.


Reliable Critical Communications
Primary carrier network
Priority APN
Differentiating high priority data traffic
High priority QCI
Ensuring data handling in case of congestion
Acces Class 14
Ensuring network access in case of congestion
PTT traffic
Alternative carrier
(when needed as fall-back)
Lyfo equipped mobile device
Lyfo BackupSIM
Ensuring access to alternative carriers
Lyfo One-IP
Reducing the impact of network changes
Lyfo.Net
Managing device connectivity
Push to Talk application

Conclusion

Transitioning from traditional TETRA-based networks to public mobile networks for mission-critical communication is already feasible. By leveraging mobile priority capabilities, like elevated Access Classes, ARP and QCI designations, without relying on the not-yet-widely-available standardized 3GPP MC-PPT solutions.

PPDR organizations can take advantage of unmatched reliability on their carrier of choice. Together with Lyfo BackupSIM, carrier partners can use all other available carriers for backup without having the need for a contract with other national carriers.

—Lyfo.net is the solution for mission-critical communication.

To learn more about how Lyfo.net can improve MCX for your PPDR organization, reach out to our team today. We're excited to hear from you.

Get started