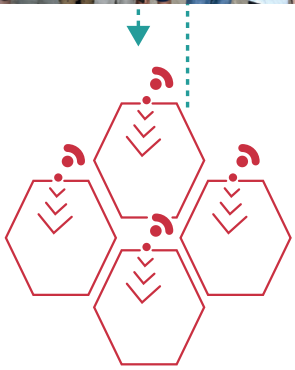
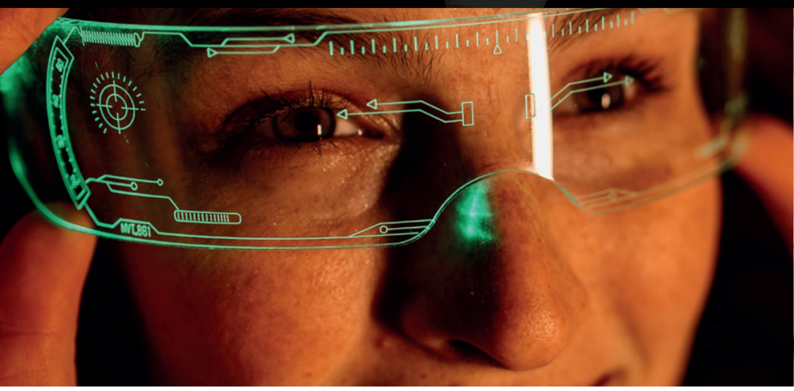
3GPP

Highlights

ISSUE 11
December 2025

the 3GPP Newsletter





NEWS

5G Advanced maturity

Release 19 represents the coming of age of 5G-Advanced. In September 2025, features and core specification work were successfully completed, with the protocols becoming stable in December – allowing the industry to implement Rel-19 effectively.

The MCC is now working on TR 21.919 - Release 19 description, which is a summary of the completed Work Items at its functional freeze.

Major Rel-19 topics bring further advances in:

Artificial Intelligence and Machine Learning (AI/ML) in networks - AI/ML in the NR Air Interface - Extended Reality & Metaverse - eMBB - Massive MIMO – Duplex Evolution - Energy Efficiency & low power solutions - RedCap - Ambient IoT – Sensing & ISAC studies - Improved uplink coverage and reduced latency. . .as well as more on Non-Terrestrial Networks and features for a variety of vertical industries' emerging use cases.

Inside this issue:

We can confidently predict the rise of AI and AI agents. It is therefore worthwhile to consider how to leverage AI to make operator services more flexible and innovative and how to get to "Native AI", to understand the role of data, computing power and algorithms as key elements of AI in 6G.

FORE - WORD

Of course, you know that this could have been written by a 'bot. However, please keep the faith.

This issue of HIGHLIGHTS is still produced by humans for humans, with only a mere suggestion of language and grammar help from the co-pilot. As Queen used to say in their album notes. No synths.

In Issue 11 of the newsletter you will find a series of snap-shots on progress being made across the groups, on topics such as AI/ML, IoT, data, digital twins, 6G Energy Efficiency, sensing and positioning...The articles are not intended to catch-all on the subjects, but more as an expert viewpoint on a particular aspect of the features discussed. My thanks to the experts across seven of our technical groups and to the three Market Partners in 3GPP that have written for you in this Issue.

Alongside the good news on Rel-19 progress, we start to see how Rel-20 has become the new talking point, as the long bridge between 5G-A and the 6G mainland.

As always, we hope that you enjoy this new issue of 'Highlights'. If so, please tell a friend to subscribe. If not, please tell me and I will work to be better next time.

You can subscribe online, via the 3GPP website: **www.3gpp.org**

Kevin Flynn
3GPP Marketing and Communications
kevin.flynn@3gpp.org

Copyright & Contacts

3GPP Highlights is published by 3GPP.

Contact Address: 3GPP Marcom, c/o ETSI, 650 Route des Lucioles, 06921 Sophia Antipolis, FRANCE

Email: highlights@3gpp.org

This publication is supplied free-of-charge.

The PDF version and subscription is online at:
www.3gpp.org/highlights

The Editorial group

Thanks to the following for copy, proof reading and constructive criticism:

Editorial group members:

Editor: 3GPP Marcom Officer, Kevin Flynn

Editorial Group:

- **TSG Chairs:** Younsun Kim, Peter Schmitt and Puneet Jain
- **Head of MCC, PCG Secretary:** Issam Toufik

Editorial guidance: 3GPP PCG Chair and Vice-Chairs

CONTENTS

NEWS ▾ Hot off the press

The latest 3GPP Working Group meetings in Dallas (Nov 17–21) were attended by 1500 experts across TSGs RAN, SA and CT groups. The week's focus was on Release 19 completion and on new Release 20 work for 5G-Advanced and early 6G studies.

Congratulations to 3GPP Organizational Partner ATIS on the success of the week of meetings, and also to the delegates for their work and the creativity they showed in the organisation of two sets of social events.

Two of the groups attended the home of the Dallas Mavericks basketball team during the week and a considerable crowd of delegates watched their colleagues in a concert at the nearby Club DaDa!, Thursday evening - Featuring the WG SA4 band - the Ambisonics and the skilfully titled - RAN2 band.

5G-Advanced XR features as the bridge towards 6G

By Devaki Chandramouli, TSG SA WG2 Rapporteur, Nokia

Exciting times are ahead for 3GPP with 6G studies in full swing within all the key working groups. 5G Standalone system and 5G-Advanced features play a pivotal role as a bridge towards the future 6G standard.

Mobile networks provide connectivity to the Internet where apps and cloud services reside. Massive traffic growth is expected due to advancements in AI technology and the future rise of applications such as video, social media, AR/VR apps, multimodal communication and robotics.

Amongst others, recent success of lightweight and trendy smart glasses with AI features is a notable point. While in the past, applications requiring higher throughput for downlink were dominant, in the future, especially with AI the focus will be more on increasing uplink throughput.

When considering how to enforce QoS in cellular networks, especially when there is competition for resources, cellular networks apply similar traffic management principles applied as on the Internet (e.g., based on traffic differentiation, prioritization and shaping). Furthermore, cellular networks offer the ability to support both guaranteed and best effort QoS.

Cellular networks must go one step further, however, as they need to ensure a minimum QoS offering while also managing the variations incurred due to the volatile air interface and the mobility of end users. Going forward, with emerging AI applications, cellular networks should also facilitate the data availability required for AI applications.

5G-Advanced Features

Release 18 introduced many enablers to enhance the 5G-Advanced QoS framework and support for XR services. These include providing differentiated QoS at the granularity of application data units such as video frames carried in a set of IP packets (PDU sets in 3GPP terminology), and providing additional information to the cellular network on application traffic patterns such as timing and end of data bursts.

The increased application awareness can be used for both QoS and power saving optimizations. These features are building an excellent foundation for optimal treatment of future services in 6G, while at the same time, they help identify those aspects that remain challenging for the current QoS framework.

As the Internet evolves rapidly, e.g., in the area of transport protocols and in policies and business practices, it is crucial to understand the impact these changes will have on cellular networks. As an example, QUIC is an end-to-end encrypted transport protocol providing multiplexing features, meaning traffic with different characteristics or QoS requirements may be carried within the same application traffic flow with no easy way to identify it in the network. Eventually it will be the dominant transport protocol in the Internet, natively supported in cloud environments.

Encryption and multiplexing of traffic without additional identification information will have an impact on MNO offered services:

- **Access control – Blocking traffic, fraud prevention, etc.**
- **Redirection – HTTP, load balancing, etc.**
- **Parental control.**
- **Charging policy – Online, offline, zero-rating, etc.**
- **QoS differentiation – Traffic shaping, bandwidth throttling, etc.**
- **Content enhancement – Media format resolution, etc.**
- **Traffic analytics reporting.**
- **Application and Service awareness.**

Release 19 has introduced additional enhancements to improve traffic detection and QoS flow mapping for multiplexed and encrypted traffic.

In the case of multiplexed traffic flows sharing the same IP 5-tuple (destination and source IP addresses and port numbers, transport protocol) with some visible flow identification information in the application protocol such as in (S)RTP, the application server can provide this flow identification information as additional packet filters with associated QoS requirements as part of the "AF session with required QoS" API to the 3GPP network via NEF [1].

The additional packet filters together with the IP 5-tuple allow the UPF in downlink and UE in uplink direction to uniquely detect each media flow and map it to a specific QoS flow that meets its QoS requirements.

Release 19 also introduced enhancements to enable the application server to explicitly provide per IP-packet (PDU) metadata the UPF can use to detect PDU Set or Data Burst information and to further provide towards NG-RAN, even for protocols such as QUIC which normally do not carry such information in any network-readable header (that is not encrypted) [1]. Release 19 supports three different methods for obtaining metadata in case of e2e encrypted traffic: Media over QUIC (MoQ), Proxy-UDP-in-HTTP/3 [2] and QUIC-Aware Proxying [3], UDP-option [4].

For MoQ [5], the PDU set information is accommodated via metadata in MoQ. For this, the UPF must support the MoQ relay functionality which allows it to see the MoQ metadata.

Proxy-UDP-in-HTTP/3 [2] and QUIC-Aware Proxying [3] operate by introducing a proxy in AS and by UPF acting as HTTP/3 client establishing connections to the proxy and mapping the desired traffic flows to the proxy connections. In Proxy-UDP-in-HTTP/3 the metadata is included in the HTTP datagrams tunneling the proxied end-to-end UDP payload from AS to UPF. In QUIC-Aware proxying where QUIC packets are forwarded rather than tunneled the metadata is added in the QUIC packet itself by a special packet transform. In both cases the metadata is secured between AS and UPF.

For UDP-Option carrying XRM metadata, UPF also connects to the AS side proxy server as in Proxy-UDP-in-HTTP/3, but the metadata is included in a UDP-Option in UDP datagrams carrying the end-to-end payload tunneling HTTP datagrams rather than in the HTTP datagrams themselves. Security keys for UDP-Option are negotiated using HTTP Connect UDP upgrade token between UPF and AS.

Towards the 6G era

Considering the massive traffic growth, capacity, coverage, reliability, spectral efficiency and high performing radio continue to be critical also in the 6G era.

For easy and smooth migration from 5G to 6G, 6G radio should be able to dynamically share spectrum with 5G. This refers to 5G-6G Multi-RAT Spectrum Sharing (MRSS) as the key tool for migration. The use of MRSS looks promising as 6G radio can be designed in a way that allows for optimized spectrum sharing spectrum with 5G, in addition to enabling the support of new frequency bands with larger bandwidth using 6G. 5G-6G MRSS is expected to be much more efficient in terms of performance compared to Dynamic Spectrum Sharing (DSS) used for 4G/LTE-5G spectrum sharing.

MRSS performance will not be limited by interference and overheads imposed by LTE common reference signals (CRS), and 5G-6G MRSS can leverage the forward compatible 5G physical layer flexibility. In addition, 6G can also be deployed in newly available spectrum from around 2030 onwards.

It is imperative to be able to support very high data rates throughout the cell to enable excellent user experience, enhanced uplink and support of low latency services.

Furthermore, understanding the boundaries of the current QoS framework is crucial to determine the improvements needed for relevant 6G day-one use cases. With the emerging NextGen-XR and immersive/cloud gaming and multimodal services, one key challenge to enable best-in-class QoS and Quality of Experience (QoE) considering demanding application needs like changing traffic characteristics, low latency and jitter, high data rates, while considering changing wireless network conditions (e.g., high resources needed in the cell edge).

In 5G, radio resource allocation strategies in cellular networks broadly fall into two categories: best effort or strictly guaranteed QoS offering. The first provides no guarantees, which does not always meet the needs of XR or NextGen-XR applications. The second does provide strict guarantees for data traffic (e.g., strict QoS requirements defined and protected by the cellular network for a service like voice or video), but this approach comes with scalability issues for a wide area network by reserving resources in the network even if not used.

For high data rate and interactive services that can adapt to changing traffic characteristics of XR and AI applications, there is a need to study QoS framework enhancements for 6G that allow for a dynamic adaptation of network resources to the need of (existing and new) demanding - yet adaptive - applications.

[1] 3GPP System architecture for the 5G System (5GS) TS 23.501

[2] IETF RFC 9298: “Proxying UDP in HTTP”.

[3] IETF draft-ietf-masque-quic-proxy-03: “QUIC-Aware Proxying Using HTTP”.

[4] IETF draft-ietf-tsvwg-udp-options: “Transport options for UDP”.

[5] IETF draft-ietf-moq-transport: “Media over QUIC Transport”.

For more from WG SA2: **www.3gpp.org/3gpp-groups**

“In the past, applications requiring higher throughput for downlink were dominant...With AI the focus will be more on increasing uplink throughput

Application Enablement for mobile Metaverse Services

By Arunprasath Ramamoorthy (Samsung), Sapan Pramodkumar Shah (Nokia), Basu Pattan (SA6 Vice-Chair, Samsung), Atle Monrad (SA6 Chair, Interdigital)

The term Metaverse refers to the immersive experiences in a virtual world where users can interact with each other and/or interact with digital objects. Metaverse in diverse industry sectors offers new experiences, products and services that emerge through Virtual Reality (VR), Augmented Reality (AR) and eXtended Reality (XR) technologies.

With metaverse, physical spaces can be converged with virtual spaces through spatial maps and augmented with digital objects like spatial anchors - to provide users with enriched information of objects in physical space.

The users in this virtual world are represented by avatars (which is one of the digital assets of the user). Spatial anchors, Avatars and Spatial maps play a significant role in enabling mobile metaverse services. Healthcare, Consumer Retail, Gaming, Communications and Entertainment are some of the industries which are bound to be benefitted to a larger extent by adopting mobile metaverse services.

Use cases and Requirements

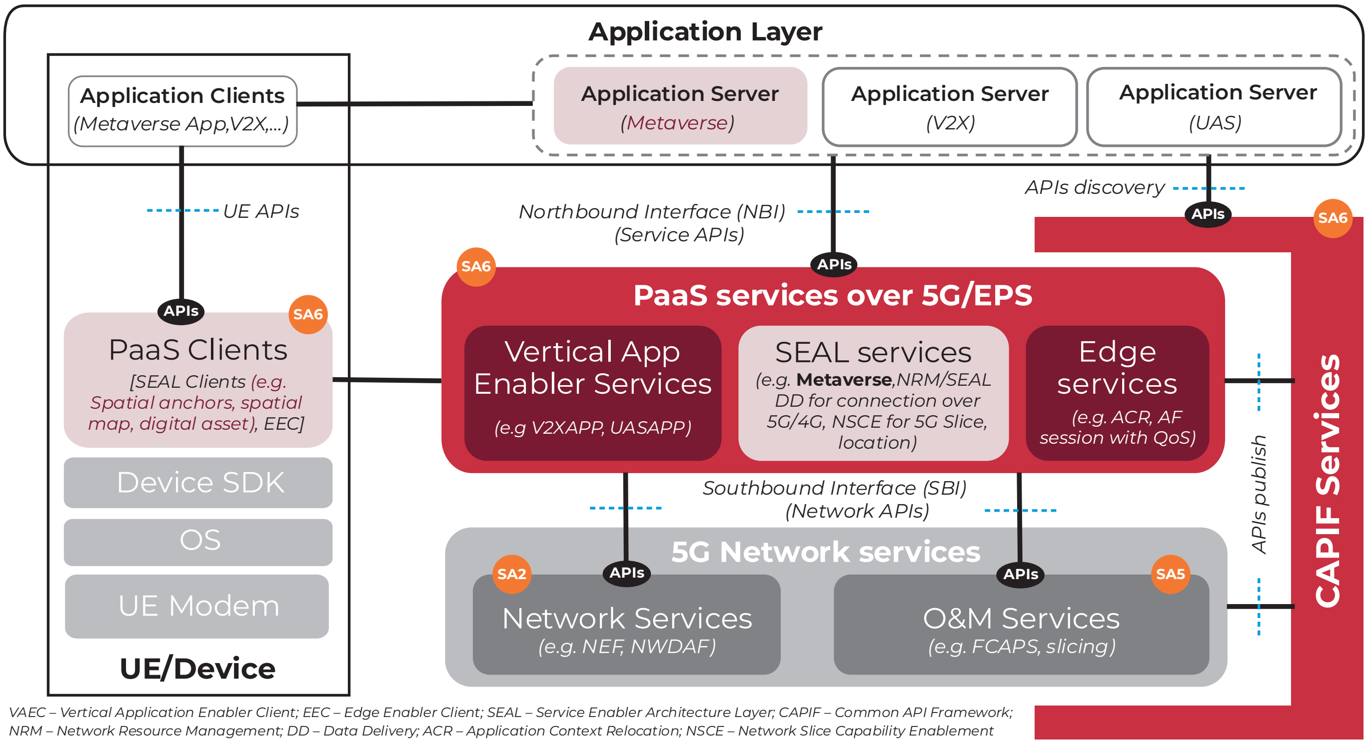
3GPP SA WG#1, as part of FS_Metaverse study in 3GPP TS 22.156, has looked at various use cases and identified the service and performance requirements for diverse service enablers - to enable mobile metaverse services. Some of the application enablement requirements are:

Localized mobile metaverse service – to provide an immersive experience or enriching user experience with contextually appropriate digital layers and media based on the user's location and interest (e.g. spatial anchors).

Support for Avatar as Digital asset service – to manage avatars as the digital representation of users. Requirements related to format, management, and storage of digital assets will improve the interoperability of digital assets across various mobile metaverse platforms.

Exposure of mobile services – meeting requirements related to providing access to spatial anchors, spatial maps and digital assets for mobile metaverse services.

Figure 1: Application Enablement within the 3GPP system



VAEC – Vertical Application Enabler Client; EEC – Edge Enabler Client; SEAL – Service Enabler Architecture Layer; CAPIF – Common API Framework; NRM – Network Resource Management; DD – Data Delivery; ACR – Application Context Relocation; NSCE – Network Slice Capability Enablement

Application Enablement within the 3GPP System

Figure 1 illustrates the service frameworks and application enablers specified by 3GPP SA WG#6, to enable an efficient and simplified adoption of vertical applications over the 3GPP system.

The layered representation illustrates how the services offered at each layer consume the lower layer services to offer added value to the layers above - through service abstraction. The SA WG#6 defined application enablers offer value added services to the application layer, leveraging the core network and OAM & charging services specified by 3GPP SA WG#2 and SA WG#5 respectively. The application enablers, in general, are access agnostic.

Mobile Metaverse Enablers

Mobile metaverse services are immersive and integrated into user's conventional experiences. Such immersive experiences are location-specific (3D locations in the physical world) and enriched with services like spatial maps, spatial anchors, digital assets etc.

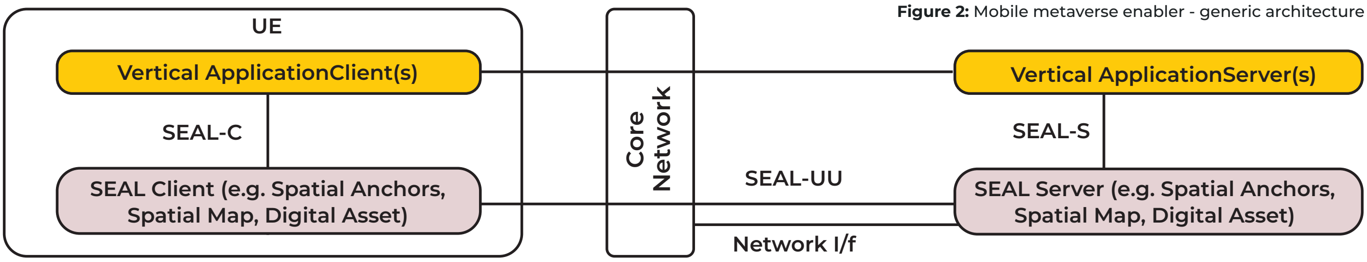
The Spatial map is a collection of information corresponding to the physical space, incorporating the information gathered from sensors concerning the characteristics of the forms in that physical space. Spatial maps enable the creation of the digital representation of the physical spaces.

The spatial anchor is an association between a location in space (three dimensions) and service information for offering immersive experience services. A digital asset is digitally stored information that is uniquely identifiable and can be used to realize value according to their licensing conditions and applicable regulations. Examples of digital asset are avatars, software licenses, gift certificates, tokens and files (e.g., music files), etc. The commonly used digital asset in metaverse services is an avatar. An avatar is a digital representation specific to media that encodes facial (possibly body) position, motions and expressions of a person or a software generated entity. Avatars enable the users in the virtual world to interact with each other for participation or collaboration in various immersive services (e.g, gaming, events).

3GPP SA WG#6 has specified these mobile metaverse enablers to support the metaverse applications, including application layer architecture, procedures and information flows. The Spatial Anchors (SAn) and the Spatial Map (SM) services are specified in 3GPP TS 23.437, while Avatars as Digital Assets (DA) are specified in 3GPP TS 23.438.

The generic architecture of these mobile metaverse enablers is illustrated in Figure 2 below:

Figure 2: Mobile metaverse enabler - generic architecture



This application enabler layer architecture for mobile metaverse services implements the SEAL (Service Enabler Architecture Layer) architecture as specified in 3GPP TS 23.434. Mobile metaverse services specified in 3GPP TS 23.437 and 3GPP TS 23.438 are SEAL services. The VAL (vertical application layer) client and VAL server are the vertical application client and vertical application server respectively providing immersive application services to the user. The SEAL client and SEAL server provides the client and server side functionalities respectively for managing the mobile metaverse services (e.g. SAn, SM and DA) for the vertical applications. The VAL client and SEAL client interact over SEAL-C interface. The interface between SEAL Client and SEAL Server is SEAL-UU. The SEAL server interacts with the VAL server over the SEAL-S interface. The SEAL-UU and SEAL-S implements procedures to manage mobile metaverse services (e.g. SAn, SM and DA).

Details about services offered by mobile metaverse enabler are explained below:

Spatial Anchors (SAn) service

The Spatial Anchors services are offered by the SEAL SAn server to the service consumers (i.e, VAL server, VAL client). The Spatial Anchors services offer the capabilities to manage the spatial anchors belonging to the vertical application layer (VAL) entities that are offering metaverse services. The functional model of Spatial Anchor service is illustrated in Figure 2.

The SEAL client is a SEAL SAn client and the SEAL server is a SEAL SAn server. SAn client and SAn server support the application layer entities that offer metaverse services for managing the spatial anchors. Each spatial anchor is associated with the profile which contains information related to the spatial anchor such as identifier, position information, services information, expiry time, etc of the spatial anchor. Spatial anchors can be grouped, which refers to the collection of spatial anchors based on locations (e.g. Museums in a city) or objects (e.g. items in a shop). Spatial anchor group management services allows organizing the spatial anchors into groups based on logical relationships so owners can manage them efficiently.

The functionalities supported by spatial anchors service are:

- **Management of Spatial anchors:** Provide the operations support for managing the spatial anchors by the spatial anchor providers/owners (e.g, Metaverse Application server). The authorized entities can Create, Retrieve, Update and Delete the spatial anchors. Each spatial anchor has a spatial anchor profile which characterizes the information (e.g. position, service, access control) related to spatial anchor and are maintained at the SAn server.
- **Spatial Anchor Discovery:** Enables the service consumer to discover the available spatial anchors based on the discovery filters (e.g. area of interest, associated service).
- **Spatial Anchor Group Management:** Enables the service consumer to manage spatial anchors as groups.
- **Spatial Anchor subscription:** Enables the service consumer to subscribe to events related to creation, modification, update and removal of spatial anchors, periodically fetch list of spatial anchors fulfilling the discovery criteria filters or discovery of spatial anchors within the range of the UE or discovery of spatial anchors when a UE enters or exits the range of interested spatial anchors provided consumers.
- **Spatial Anchor Usage reporting:** Enables the spatial anchor owners (e.g., VAL server)/providers to receive the insights about the usage of their spatial anchors by the consumers. These insights are helpful to the spatial anchor owners/providers in better planning and management of the spatial anchors.

Application Enablement for mobile Metaverse Services (continued)

Spatial Map (SM) service

The Spatial map service offers the capabilities to the vertical application layer entities (VAL server, VAL client) for managing the spatial maps. The Spatial map management functional model is illustrated in Figure 2.

The SEAL client is a SEAL SM client and the SEAL server is a SEAL SM server. The main functional entities are SM client and SM server which provides client and server side functionalities respectively for managing spatial map for the vertical applications. The spatial map service also supports the spatial localization service through which SEAL SM server, identifies all users/UEs localization along with their three-dimensional location and pose in the spatial map based on the request from the vertical application layer.

For creating and managing the spatial map, it is required to get the data from various sources like cameras or sensors. Spatial map service provides a mechanism for the data sources to register with the enabler layer with the information like the type of data they offer and their availability period etc. Application layer when creating the spatial map can discover the available spatial map data sources through the SM server spatial map services and connect to the data sources to fetch the data required for constructing the spatial maps. Spatial map capable application servers (SMAS) are application servers which can offer spatial map service. SMAS can also register with the SM server with the list of spatial maps they support, coverage area of each of the spatial map, media format of the spatial maps etc. Spatial map service consumers can discover and utilize these readily available spatial maps when required. Below are the functionalities supported as part of spatial map services:

- **Management of Spatial maps:** Provides the operations support for enabling the management of spatial maps by the vertical application layer entities.
- **Spatial map discovery:** The service consumers can discover the spatial maps available, based on certain criteria, such as an area of interest, the location of consumer, based on the spatial map media formats, based on the spatial map layer information.
- **Spatial map subscription:** The service consumer can subscribe to and receive notification of events such as list of objects that are added or deleted, when their velocity or position changes, changes to the spatial map layers associated with the spatial map, spatial map is created and ready to use.
- **Spatial localization services:** Enables the service consumer to identify the users/UEs along with their three dimensional location and pose in the interested area of the spatial map.
- **Spatial map data source registration and discovery:** Entities capable of providing data that is useful for creation and rendering of the spatial map, can register with SM server as spatial map data source. These entities also provide their capabilities, availability and type of data they produce etc. The VAL servers can discover the available spatial map data sources from SM server, based on certain criteria information such as area of interest, availability, mobility of the data source, etc.
- **SMAS (SM capable Application Sever) registration and discovery:** Application servers can register with the SM Server with the information of their spatial maps, their coverage area, availability information and connectivity information. The service consumers can discover the end point information of the spatial map application servers, from the SM server.

Digital Assets (DA) Service

To ensure a seamless user experience across metaverse services, network operators offer digital asset management services that allow users to certify certain information, such as IDs. These services support multiple user identities, each representing different aspects of the user's life, such as their professional role and private life. As a result, each user identity can have its own set of information stored in the associated digital asset profile.

Users can be associated with one or more digital assets like Avatars, software licenses, files, etc. Applications like metaverse services can utilize the digital assets related to users, and the users can benefit from having the use of their digital assets between various metaverse services/platforms in an interoperable way. Digital assets service, as specified by 3GPP SA WG#6 in 3GPP TS 23.438, enables management and usage of digital assets to support metaverse services in a secure and controllable way. Digital asset is represented as a combination of digital asset profile along with associated media. The digital asset profile consists of digital asset specific configuration and parameters (e.g. ID, type, allowed locations and access control) applicable to one or more application(s). A digital asset profile can be associated with one or more VAL user(s). The functional model of Digital Asset service is illustrated in Figure 2. The SEAL client is SEAL DA client, the SEAL server is SEAL DA server. The following functionalities are supported for Digital asset service:

- **Digital asset profile management:** Enables a consumer (VAL server or DA client) of digital asset service to be able to manage (Create, Retrieve, Update and Delete) a digital asset profile.
- **Digital asset discovery:** Enables a DA client to discover digital assets available in the digital asset service.
- **Digital asset media management:** Enables a consumer (VAL server or DA client) of digital asset service to manage the media related to digital asset profile.

Advantages

Generally, the services defined at the application enabler layer supports rapid development and deployment of vertical applications. Mobile metaverse services, which can be offered by several MNOs, aims to support faster development of metaverse services at global scale. Mobile metaverse enablers can ensure a seamless user experience across multiple metaverse services without worrying about the interoperability issues by utilizing the common and standard enabler services specified by 3GPP SA WG#6 to manage digital assets, spatial maps and spatial anchors.

Considering the diversified portfolio (e.g. gaming, healthcare, virtual offices, virtual concerts/events) of metaverse services, the simple mobile metaverse enabler has high potential to attract more application developers and thereby fostering innovation and monetization. It is expected that these metaverse enablers will help accelerate new Service APIs offering of other SDOs (e.g. CAMARA, Metaverse Standards Forum (MSF)) to support Metaverse services addressing customer base beyond mobility.

Future Plan and Next Steps

Currently 3GPP SA WG#6 is discussing the work areas to focus on as part of the 6G release cycle. Digital twins, sensing services, AI / ML are all potential work areas set to play a role in enhancing immersive experiences offered by mobile metaverse services.

For more from WG SA6: **www.3gpp.org/3gpp-groups**

Management and Orchestration Standards for 5G

By Lan Zou, SA WG5 Chair (Huawei), Zhulia Ayani, SA WG5 Vice Chair (Ericsson), Zhaoning Wang, SA WG5 Vice Chair (China Unicom)

Management and Orchestration standards include requirements, management stage 2, management procedures, stage 3 RESTFUL OpenAPI and NETCONF/YANG solution sets to provide complete interoperability capabilities for operators to manage 5G networks in a multi-vendor environment. The purpose of this article is to provide a summary introduction to the related management features.

5G Management and Orchestration Use cases

With more and more new 5G network and service features, operators need to manage network features with multi-vendors' products in a consistent manner and make sure the network and service are stable as much as possible. To manage network in a more efficient way, there are two aspects addressed in standards:

Managing new 5G network elements and new network functions for:

- **Network slicing** (Provisioning, Network Resource Model, performance Assurance, fault supervision, tenancy concept etc.)
- **Non-public networks** (NPN fault management, SLA monitoring and assurance, resource management for NPN, NPN access control, etc.)
- **5G network sharing** (Management support for MOCN and INS scenarios, performance and configuration management in PLMN granularity, management capabilities and architecture based on SBMA, access control for POPs, etc.)
- **Non-terrestrial networks** (management capability and architecture support for NTN, transparent mode feature management, Backhaul feature management, regenerative mode feature management, UE-Satellite-UE communication feature management, etc)
- **Ambient IoT** (gNB reader served A-IoT areas management, reader location management, index for A-IoT capable gNB/reader selection management, etc.)
- **5GC features** (5GC NF management, NWDAF management, 5GLAN management, edge computing management, XRM Service management, etc.)
- **RAN features** (NG-RAN management, MR-DC management, URLLC management, RedCap service management, IAB-node management, WAB-gNB management, NR Femto management, etc.)

Managing and orchestrating intelligence and automation cases including:

- **Management analytics** (Coverage related analytics, SLS analysis, MDA assisted fault management, MDA assisted Energy Saving, MDA assisted mobility management, MDA assisted critical maintenance management, Resource related analytics, Prediction and statistics of Management data, Correlation analytics of Management data, Traffic Steering Analytics etc.)
- **5G Self-organizing networks** (RACH optimization, Mobility Robustness Optimisation, PCI configuration, ANR management, LBO (Load Balancing Optimisation) management, MRO for Conditional Handover (CHO) management, MRO for DAPS (Dual Active Protocol Stack) handover management, MRO for Lower-layer Triggered Mobility (LTM) management, RRM resources optimization for network slice instance(s) management, Centralized Capacity and Coverage Optimization management, LBO (Load Balancing Optimisation) management etc.)
- **Intent-driven management** (delivering radio network, delivering a radio service, delivering a service at the edge, assuring coverage performance, assuring radio network performance, end-to-end network optimization intent, RAN energy saving intent, 5GC network intent, network maintenance intent etc.)
- **Energy efficiency management** (Data Volume (DV) collection, Power, Energy and Environmental (PEE) measurement collection, ES - Capacity booster cell partially overlaid by candidate cell(s), ES - Capacity booster cell fully overlaid by candidate cell(s), Energy saving optimization for multi-carrier RAN scenarios with several partially or fully overlaid capacity booster cells, Energy Efficiency as a Service Criteria etc.)
- **AI/ML management** (ML model training, ML model testing, AI/ML inference emulation, ML model deployment, AI/ML inference etc.)
- **Network digital twins** (Control and life cycle management of NDTs, NDT support for network automation, NDT support for verification, NDT support for data generation, Collaboration between NDTs etc.)

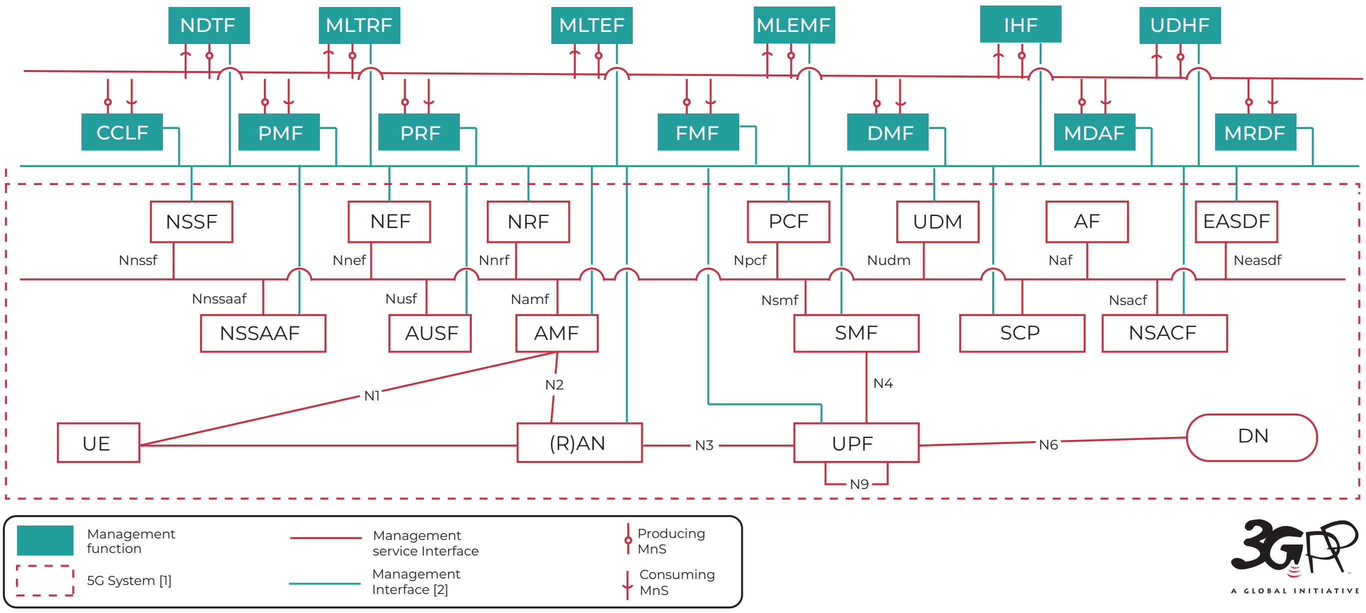
5G Service Based Management Architecture

5G management and orchestration adopts Service Based Management Architecture (SBMA). The fundamental building block of the SBMA is the Management Service (MnS). An MnS is a set of offered capabilities for management and orchestration of network and services. An MnS producer offers its MnS to MnS consumer via a standardized service interface composed of individually specified MnS components.

The flexibility of SBMA allows the 3GPP management and orchestration specifications to be used for different deployment scenarios wherever applies. The following diagram illustrates an architecture reference model for management and orchestration, also shows how the management architecture is integrated with the network architecture. The functions in the management domain are logical, implementation-agnostic entities, defined independently of any specific deployment scenario. More details could be found in 3GPP TS 28.533.

Management and Orchestration Standards for 5G (continued)

Figure 1: Illustrative architecture reference model for management and orchestration



SA WG5 5G Management and Orchestration functional features

The following functional areas in SA5 cover management and orchestration features. They provide complete management and orchestration functionalities for 5G, improve efficiency in management and orchestration, support operators in managing end to end services, both for basic and new network features.

Intelligence and automation: By utilizing new advanced technologies like AI/ML, intent, NDT, closed control loop, operators get the advantage of improving the operational efficiency in their complex networks. In addition, standard also provides various mechanisms for operators to monitor and manage the intelligence and automation features and make sure the features run properly according to operators' expectation and are fully under operators' control.

Support of new services: end to end solution from network to new service needs close collaboration and clear division of responsibilities from multiple players. Standardized solutions could help the players to find appropriate roles, engage domain expert knowledge, setup the work collaboration boundaries and jointly contribute to the service growth.

Management operations / Managing of new network features: generic standardized management operations together with the corresponding network features are specified to manage subnetworks, network elements and network functions, with this approach, operators could keep consistent management behavior for 5G network.

Management data collection: to support operators' management and orchestration purpose, various types of data could be collected via standardized mechanisms across multi-vendor environment.

SA WG5 functional areas and related Specifications

Intelligence & automation	Support of new services	Management architecture & management operations	Management of new network features
• Autonomous Network Levels (TS 28.100) • Management Data Analytics (TS 28.104) • 5G SON (TS 28.313 / .317 / .541) • Plug & Connect (TS 28.314 / .315 / .316) • Policy Management (TS 28.555 / .556) • AI/ML Management (TS 28.105) • Closed-loop SLS (TS 28.567) • Intent-driven Management (TS 28.312) • Network Digital Twin (TS 28.561)	• Energy Efficiency (TS 28.310) • Management Exposure (TS 28.579) • Signalling traffic monitoring management (TS 28.560) • Network and Service Operations for Energy Utilities (TS 28.318 / .554)	• Service based management architecture (TS 28.533) • Network and service management (TS 28.530) • Network and Network slicing management (TS 28.531 / .532 / .540 / .541) • Plan Management (TS 28.572) • Fault Management (TS 28.111) • Performance Assurance (TS 28.550)	• Non-public Network Management (TS 28.557) • Non-terrestrial Network Management (TS 28.540 / .541 / .552) • IAB Node Management (TS 28.540 / .541 / .531) • Redcap Service Management (TS 28.540 / .541/ .552) • 5G RAN Sharing management (TS 32.130) • NWDAF Management (TS 28.541 / .552) • Edge Computing Management (TS 28.540 / .541)

5G Management data collection

Management data collection (TS 28.537 / .622) - MnS Registry and Discovery (TS 28.537 / .532/ .622 / .623) - Notification subscription and Heartbeat notification control (TS 28.537 / .532 / .622 / .623) - File Management (TS 28.537 / .532 / .622 / .623) - Access Control for Management Services (TS 28.319) - SGC/NR/Slice Network Resource Model (TS 28.541 / .622) - Performance Measurements (TS 28.552 / .554 / .558) - Trace & MDT management (TS 32.421 / .422 / .423) - QoE Management (TS 28.404 / .405 / .406)

SA5 5G management services exposure

There are various ways of management exposure depends on different operators' deployment needs. Management service can be exposed to internal MnS consumers (i.e. MnS consumers within the PLMN trust domain) and external MnS consumers (i.e. MnS consumers outside the PLMN trust domain). These consumers can be classified into the following categories:

- **Internal MnS consumer X1:** MnS consumer within the 3GPP management system, e.g. provisioning MnS consumer, fault management MnS consumer and streaming MnS consumer.
- **Internal MnS consumer X2:** MnS consumer outside the 3GPP management system but within the PLMN trust domain, e.g. NWDAF, operator's AFs, Edge Application Server.
- **External MnS consumer Y1:** MnS consumers outside the PLMN trust domain consuming management services directly from the 3GPP management system, e.g., participating operators in RAN sharing scenarios, energy utility verticals, and other verticals.
- **External MnS consumer Y2:** MnS consumers outside the PLMN trust domain consuming management services through CAPIF framework (3GPP TS 23.222), e.g. energy utility verticals, and other verticals.

The exposure of management services to the different types of MnS consumers includes two functional aspects:
discovery of the MnSs and access control.
As a precondition, the discovery of management services assumes that the management services to be exposed have been registered.

Figure 2 illustrates different exposure scenarios, depending on the type of MnS consumer. For MnS consumers X1, X2 and Y1, registered management services are exposed using the mechanisms that 3GPP management system already defines for MnS, discovery and access control in TS 28.537 [2] and TS 28.533 [1]. For MnS consumer Y2, registered management services are exposed using the CAPIF framework, using the mechanisms defined in 3GPP TS 28.579 [3].

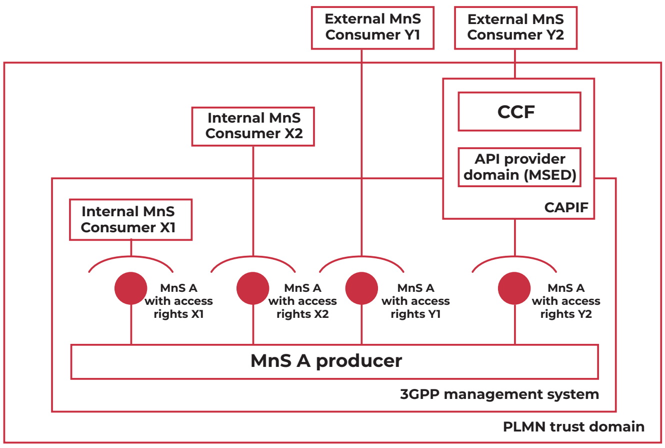


Figure 2: Management services exposure scenarios

SA5 Management and Orchestration Stage 3 solutions

The standardized stage 3 solutions provide two alternative solution sets: RESTFUL and NETCONF/YANG. Operators could select different solution set for integration according to different business needs. The table below shows the management and orchestration features and their corresponding management capabilities. More information regarding Management and Orchestration APIs could be found in TS 28.533 [1] or access 3GPP forge website: **https://forge.3gpp.org/rep/sa5/MnS**

Management Feature	Management Capability
Network and network slicing management	NR Provisioning 5GC Provisioning Network Slicing Provisioning
Edge Computing Management	Edge Computing Provisioning
Performance Assurance	Performance Metric Collection Control Performance Metric Data Report Performance Metric Threshold Monitor Control Performance Metric Threshold Notification
Fault Management	Fault control Fault Notification
Trace and MDT management	Trace/MDT data collection control Trace/MDT data report
Signalling traffic monitoring management	STM provisioning STM streaming
QoE management	QoE data collection control QoE data report
File Management	File Retrieval File Download
Plan management	Configuration plan management
Notification subscription and Heartbeat notification control	Subscription Control Heartbeat Control Heartbeat Notification
MDA	Management Data Analytic
SON	RANSC Management SON policy
Closed-loop	Communication Service Assurance Control Closed control loop management
Intent driven management	Intent Driven Management
AI/ML management	ML model Management
NDT management	NDT Lifecycle Management
MnS Registry and Discovery	MnS Registry and Discovery MgmtData Registry and Discovery
MSAC	MnS Access Control
NSOEU	DSO Rapid Recovery and Threshold Monitoring
External Data Management	External Data Discovery and Request

Summary

SA WG5 management and orchestration takes an important role in the network and service ecosystem and it provides the integrated view in 3GPP including both the network and the management of the network and service. SA5 SBMA standard and interfaces would help operator using generic management framework for multi-vendors integration and could accommodate various deployment scenarios. With introduction of intelligence and automation features, operators could best utilize the new technologies and improve operational efficiency, and build good basis to provide new agile services to their customers.

References

[1] TS 28.533 Management and orchestration; Architecture framework

[2] TS 28.537 Management and orchestration; Management capabilities

[3] TS 28.579 Management and orchestration; Management services exposure to external consumers through CAPIF

For more from WG SA5: **www.3gpp.org/3gpp-groups**

The Network Digital Twin: Enabling Network Intelligence and Automation

By Yushuang Hu, WG SA5 Rapporteur (China Mobile)

The increasing complexity of 5GA networks, coupled with the demand for enhanced service quality and reliability, necessitates efficient management solutions for complex networks. Network Digital Twin (NDT) offers an effective solution by providing deep insights and enabling proactive management.

By simulating scenarios, NDTs help operators predict outcomes, optimize configurations, and prepare for high-risk operations virtually, without affecting the real network. This is essential for 6G, which demands ultra-low latency and high reliability, making NDT crucial for autonomous network management and optimization.

In R19, SA5 initiated a study on “Management aspects of Network Digital Twin” in TR 28.915 [1], marking the first introduction of the NDT concept and technology by 3GPP and subsequently documented the R19 normative work in TS 28.561 [2]. Furthermore, the 5GA R20 work in TR 28.883 [3] is expected to study the NDT enhancements and enable the vertical industry services.

Concepts and Overview

Network Digital Twin is the virtual replicas of mobile network or part of one, that captures its attributes, behaviours and interactions. NDTs can combine hardware, software, and data flows to provide a comprehensive view of the network’s status and potential future states. The implementation of an NDT can rely on simulation, emulation, AI-based modelling, or any other technique that enables the NDT to mimic the behaviours of the network.

NDTs are crucial for enhancing network automation functions by complementing existing capabilities by filling the gap in modelling mobile network behaviours. They can achieve the capabilities by leveraging analytic data from MDA and synchronized data from real networks as needed. Additionally, they can provide modelling capabilities to support network automation functions (e.g., MDA and SON), in achieving their automation goals. NDTs offer flexible deployment options, allowing integration both within and outside existing network automation functions.

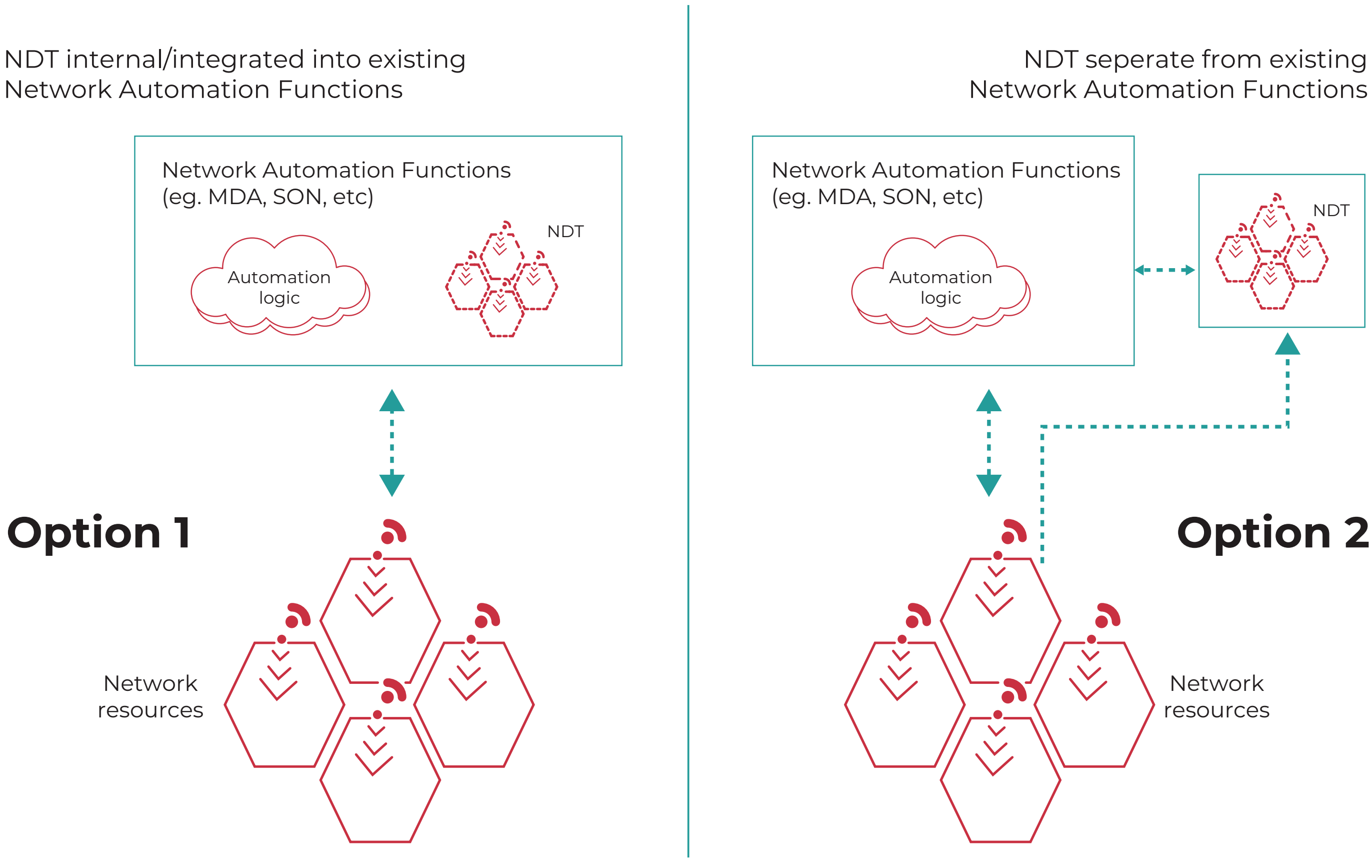


Figure 1: Relation of NDTs with network automation functions

Functions in different domains

The NDT function can be provided by the cross-management domain to support cross-domain simulation/emulation capability or RAN/CN management domain directly to support RAN domain simulation/emulation capability. For instance, the NDT function in RAN domain is responsible for RAN energy saving configuration verification. Figure 2 depicts the scenario when NDT function is deployed in RAN domain.

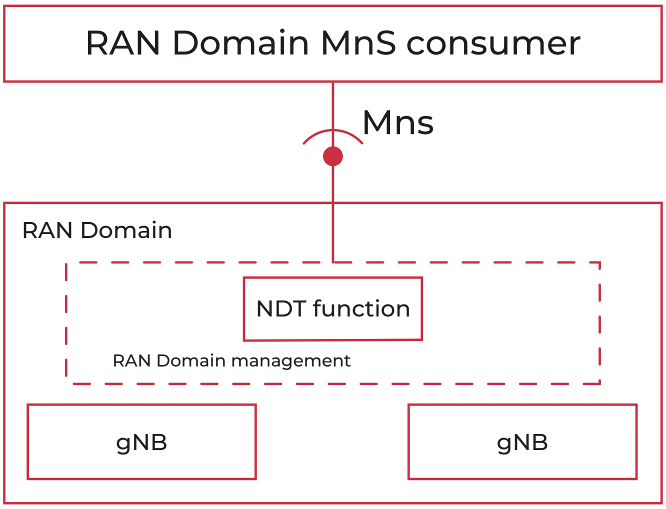


Figure 2: NDT function in RAN domain management

NDT Capabilities and Use Cases

NDTs provide a range of capabilities that enhance network management:

1	Usage of control and Life-cycle management of NDTs.	1) Life cycle management of NDT instances. 2) Control of NDT instances. 3) Synchronization with network.
2	NDT support for network automation.	1) General capabilities on NDT support for network automation. 2) Support for evaluation of high-risk network operations. 3) Support for evaluation of failure events including signalling storm. 4) Network issue inducement.
3	NDT support for verification.	1) General verification. 2) Verification of network response to events. 3) Verification of network configurations. 4) Verification of automation-function configurations.
4	NDT support for data generation.	1) General use case on NDT support for data generation. 2) Using NDT to generate ML training data. 3) Using NDT to generate user experience data.
5	Advanced NDT capabilities.	1) Collaboration between NDTs.

> NDTs are crucial for enhancing network automation functions by complementing existing capabilities by filling the gap in modelling mobile network behaviours.

NDT Management service provisioning

The NDT in 3GPP is defined as a management service (MnS) to provide the digital twin capabilities, including definitions in stage 2 and stage 3 which allows operator to manage NDT in a multi-vendor environment.

For stage 2, the operations (e.g., createMOI operations) and notifications (e.g., notifyMOIcreation) of generic provisioning MnS defined in TS 28.532 [4] can be used for NDT management, including NDT function management, NDT job management and NDT report management. The NDTFunction, NDTJob, NDTReport instances can be treated as Managed Object instances, integrating with existing network management systems and processes, ensuring seamless operation.

For stage 3, the NDT MnS is defined by standardized operations such as the use of RESTful APIs for HTTP-based solutions. The RESTful HTTP-based solution set for generic provisioning management service is defined in clause 12.1.1 in TS 28.532 [4]. Corresponding className are NDTFunction, NDTJob and NDTReport.

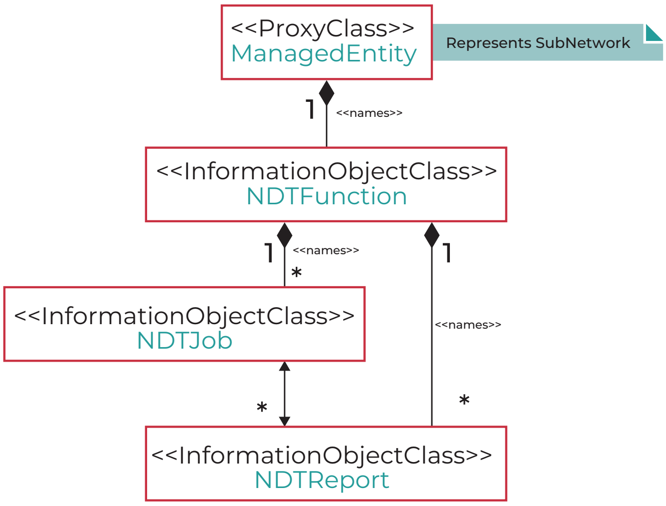


Figure 3: Relationship UML diagram for NDT management

Future developments

Currently, the 6G Network Digital Twin study is being discussed in both WG SA1 and WG SA5, with an emphasis on supporting digital twin capabilities to enable autonomous networks. In SA5, the evolved NDT is considering enhancements to support 6G use cases and optimize network management. This may include NDT enhancements on autonomous capabilities, precise analysis, multi-domain and cross-domain simulations, real-time NDT, data services processing, exposure etc.

In the future, 3GPP SA5 will continue to develop standards for NDT management solutions and meet any new requirements for management aspects from the industry.

[1] TR 28.915 - Study on management aspects of Network Digital Twin

[2] TS 28.561 - Management aspects of Network Digital Twins

[3] TR 28.883 - Study on management aspects of Network Digital Twins phase 2

[4] TS 28.532 - Management and orchestration; provisioning

For more from WG SA5: **www.3gpp.org/3gpp-groups**

Rel-19 Charging Enhancements

By Gerald Görmer, SA5 SWG Charging Chair (Matrixx)

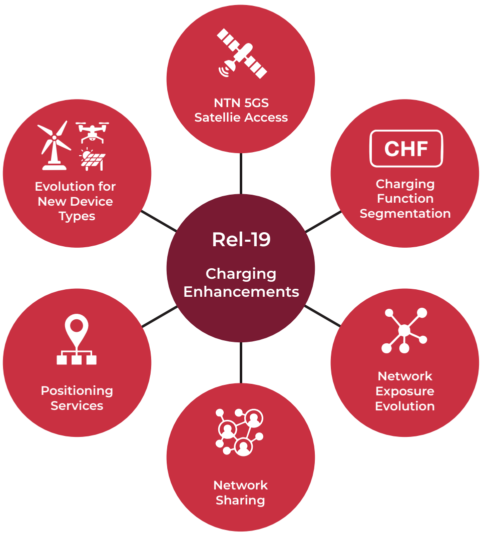
The Converged Charging System remains at the heart of telecom monetization, enhanced at each release to help service providers support evolving business models and new service demands. Building on the foundation of 5G, the charging features introduced in Rel-19 provide operators with new ways to monetize advanced connectivity, vertical industry services, and next-generation applications.

Highlights of Rel-19 Charging Enhancements

NTN 5GS Satellite Access - Satellite access and backhaul, first introduced in Rel-18, are now fully integrated into the charging system. Business cases include Mobile Network Operators (MNOs) offering satellite services—such as service continuity between terrestrial and satellite coverage—and Satellite Service Providers offering network access to MNOs.

Rel-19 expands these scenarios to include MNOs providing satellite services to MVNOs, roaming between operators with and without satellite access, and new service types such as UE-Satellite-UE communication (IMS voice/video with optimized media routing) and Store-and-Forward (S&F) satellite operation. The S&F mechanism supports delay-tolerant services like SMS by extending the relevant Charging Data Records (CDRs).

Charging Function (CHF) Segmentation - The CHF can now be segmented across domains and business contexts based on extended filter criteria, leveraging the Network Repository Function (NRF) framework for CHF instances selection, enabling distributed deployments that align with cloud-native architectures. Operators can isolate individual subscribers and enterprise flows, assign separate responsibilities for wholesale versus retail accounts. For example, using the concept of CHF Group Id, dedicated CHF instance(s) could be assigned to high-priority enterprise contracts, while others to mass-market.



Network Exposure Evolution - Integration with the Common API Framework (CAPIF) brings charging into the heart of network exposure. Charging hooks are added to the CAPIF, allowing operators to bill Service APIs Providers for Management (e.g. publishing service APIs) and Service API invokers for e.g. Service APIs discovery.

In addition, IMS as new exposed network capabilities as well as IMS evolution (data channel application and avatar communication) are covered. This enhances the charging capabilities for monetizing partnerships where network capabilities, such as analytics or AI-driven services, are consumed by third parties.

Network Sharing - Charging capabilities for shared and roaming environments have been refined to improve settlement accuracy. Under Multi-Operator Core Network (MOCN) arrangements, charging is based on RAN performance metrics—such as transferred data volume and number of PDU sessions—collected by the host operator. In indirect network sharing scenarios, where multiple cores connect via an intermediary operator, charging data can now differentiate usage by each participant.

Support for Minimization of Service Interruption (MINT) introduces charging recognition for inbound roamers connecting under disaster conditions, ensuring emergency access remains measurable and recoverable. Together, these updates make cooperative deployments both technically and commercially sustainable.

Positioning Services - Converged charging has been extended to cover both 5GC location services and new ranging and sidelink positioning features. High-accuracy positioning can be monetized in use cases such as connected vehicles requiring centimeter-level navigation, or industrial robots coordinating movements in a factory floor. Charging events capture the type of positioning, accuracy parameters and frequency of updates, enabling tiered offerings. For example, logistics companies could pay a premium for continuous tracking of freight containers, while consumer-level applications might only need periodic updates.

Evolution for New Device Types - Charging is evolving in support of emerging device categories and the services they enable. For Uncrewed Aerial Systems (UAS), operators can charge based on identification, tracking, pre-flight planning, and in-flight monitoring managed through the UAS Service Supplier (USS). Drone-based delivery providers might be billed per flight hour, distance, or airspace usage. For Ambient Power-Enabled IoT, charging covers inventory and command-type services exposed via the Network Exposure Function (NEF). These support ultra-low-power devices that rely on harvested energy and communicate intermittently, enabling scalable, low-cost IoT business models for massive deployments.

Looking Ahead

From non-terrestrial access to positioning services, from shared networks to next-generation devices, charging is evolving to ensure every innovation can be monetized.

These improvements not only secure new revenue streams but also give operators the tools to build sustainable business models in areas ranging from IoT to satellite. As the industry looks toward 6G, charging will remain a cornerstone of commercial success for network evolution.

For more from WG SA5: **www.3gpp.org/3gpp-groups**

6G Architecture to enable capabilities Beyond Connectivity

By Tao Sun 3GPP TSG SA Vice Chair, China Mobile

The Study on Architecture for 6G System (FS_6G_ARC) was approved by 3GPP TSG SA#108 in June this year. It heralds the start of the work on moving ever closer to meeting the critical challenges that have been identified during 5G deployments.

As the industry prepares for a futuristic set of AI inspired digital advances, the TSG SA Study on Architecture for 6G System is shaping up to be a balanced perspective on features and services evolution. There are eight work tasks across the study, with four on ***"Connectivity"***, i.e., baseline architecture for 6G access, inter-working, NTN, cellular IoT and another four tasks moving ***"Beyond connectivity "*** through AI, ISAC, data frameworks and support of computing (coordination between UE, core network and application server).

For each mobile generation, the question arises whether the new architecture is an evolution or a revolution? Networks are evolving quickly from being person centric "2C" *(to Customer)* communications, towards "2B" *(to Business)* in 5G. The trend is now accelerating towards "2A" *(to Agent)* as we plan for 6G. This feels like a revolutionary evolution - with AI at its heart.

This is borne out by the WG SA1 study on 6G scenarios and requirements (TR 22.870) heavy leaning on AI use cases. WG SA1 has defined the AI Agent as: *"An automated intelligent entity that achieves a specific goal (autonomously or not) on behalf of another entity, by e.g. interacting with its environment, acquiring contextual information, reasoning, self-learning, decision-making, executing tasks (independently or in collaboration with other AI Agents)".*

Looking ahead to the next few years, leading up to 2030 and 6G maturity, we can confidently predict the rise of AI and AI agents. It is therefore worthwhile to consider how to leverage AI to make operator services more flexible and innovative and how to get to "Native AI" and to understand the role of data, computing power and algorithms as key elements of AI in 6G.

At the 6G Architecture level, we will consider whether or not to introduce a data framework into the system, for handling *'big data'* through networks and equipment.

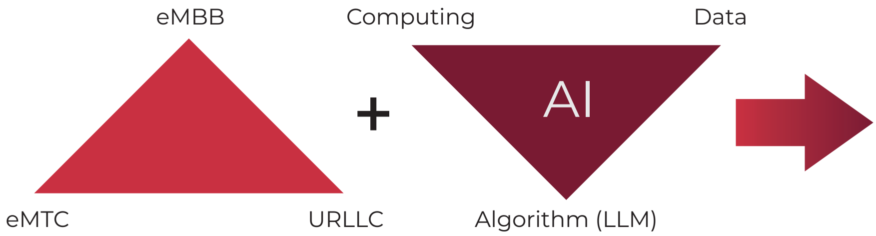
In the 6G era, the network plays new roles: from data pipe to data generator and consumer. This transition brings new data sources and scenarios such as UE AI model data, Sensing and data for digital twins.

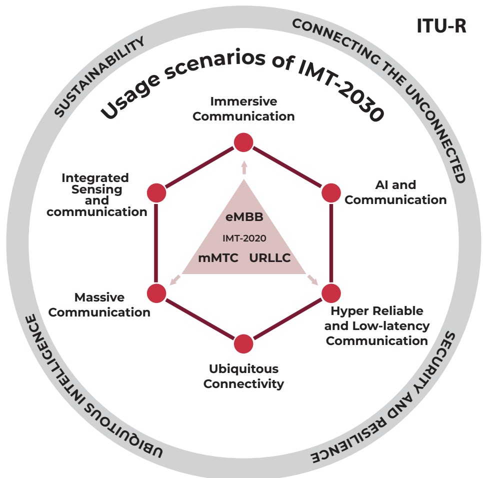
The 6G Architecture shall explore the capability of providing Computing Service. There has been good progress in SA1 where "6G Computing Service" is defined as: *"A service provided by 6G network utilizing computing resources in Service Hosting Environment, which can be used by a subscriber (via UE)/3rd party."* A major opportunity lies in "In-Network Computing", i.e., Deep Network and Computing Coordination.

3GPP and IMT alignment

The 6G architecture is to be aligned with the IMT-2030 vision (From ITU-R), grounded in established design principles, respecting the identified requirements in the 3GPP *Study on 6G Use Cases and Service Requirements* (TR 22.870) and the radio *Study on 6G Scenarios and requirements* (TR 38.914). These studies allow us to proceed with confidence towards the 6G era with secure, resilient and sustainable networks providing 'diverse and novel' services, while interworking seamlessly with 5G systems.

The IMT-2030 goals for 6G are challenging and the 3GPP membership is now – more than ever - collaborating to rise to that challenge. The road is long and time is always limited, but the talent pool within 3GPP is ready and is making great progress on those first 6G studies in Release 20, in preparation for specifications in Rel-21.





The NAS UE policy delivery service

By CT WG1 5G NAS and UE policy Rapporteurs:
Christian Herrero-Veron (Huawei), Zhou Xingxue (ZTE)

The NAS UE policy delivery service provides devices (UEs) with finely-tuned instruction sets of UE policy rules, on access mode and RAT preferences, network slice selection (S-NSSAI), data network name (DNN), address selection, vehicle-to-everything (V2X) or aerial-to-everything (A2X) communication, and gives operators direct and near real-time steering of device behavior - ensuring optimized connectivity and resource management.

This service, available since day one of 5G (Release 15) and at its core, was defined to allow scalability by adding new policy rules into an already defined container (UE policy container). This preserved backward compatibility and resilience - as UEs carry policy rules are cached and stored in the device - even if the network is temporarily unreachable.

The NAS UE policy delivery service is the on-air execution arm of the access & mobility (AM) and UE policy management in 5G (*see [1]*). In fact, it takes policies derived by the policy control function (PCF) for a UE and delivers them via 5G NAS signalling - from the access and mobility function (AMF) to the device (see annex D *in [2], and [3]*), where the policies are enforced in real time.

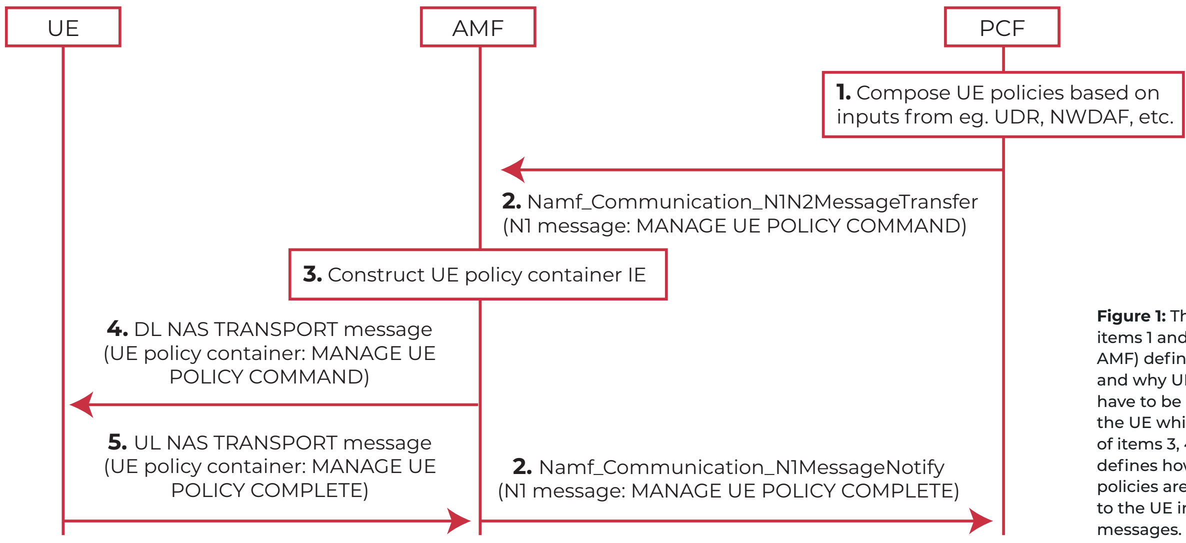


Figure 1: The flow of items 1 and 2 (PCF to AMF) defines when and why UE policies have to be sent to the UE while the flow of items 3, 4 and 5 defines how those policies are provided to the UE into 5G NAS messages.

NAS UE policy delivery service framework

3GPP CT WG1 specified since Rel-15 the NAS UE policy delivery service, providing a unified over-the-air mechanism for delivering operator-defined policies to devices, covering routing of data flows (e.g., IP), access technology selection, V2X resource management, sidelink positioning and other behaviors (*see [4]*).

The policy can be tailor made and pushed from the PCF to the AMF where they are placed and packaged into a "UE policy container" carried by an NAS message (*see [2]*). The "UE policy container" is the core structure which carries a particular message which provides the policies to be used by the UE. 3GPP has defined in Rel-15 through Rel-19 different types of UE policy which can be configured by operators and pushed to UEs (*see [3], [4]*).

1. UE policy types

UE policies define how a UE behaves in the network, governing critical functions such as access technology selection, data network selection, network slice selection, data traffic routing, etc.

These policies ensure that device behaviour stays aligned with subscription information and operator's service requirements.

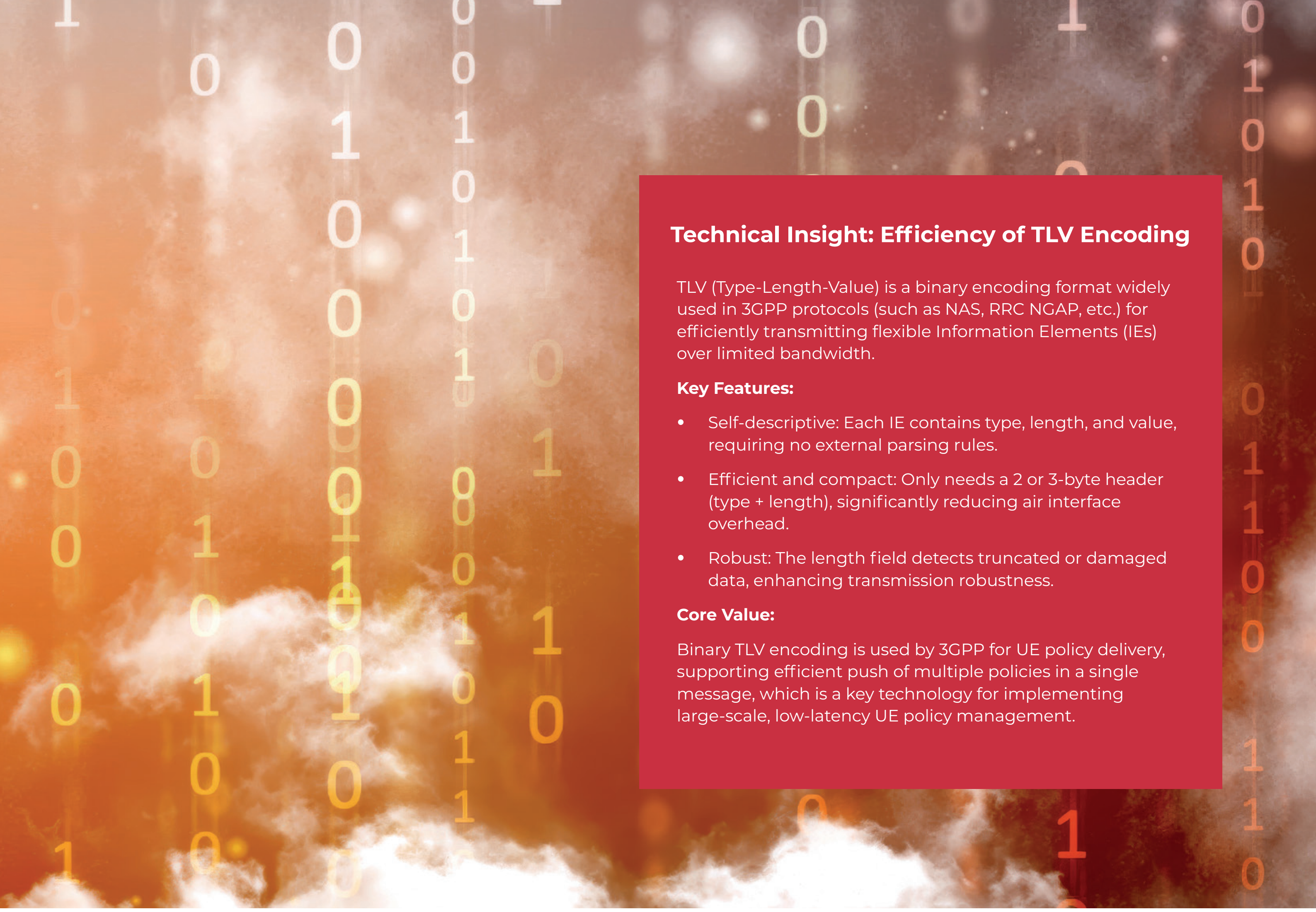
The following are standardized UE policy types defined by 3GPP:

- UE route selection policy (URSP).
- Access network discovery and selection policy (ANDSP).
- Vehicle-to-everything policy (V2XP).
- 5G proximity-based services (ProSe) policy (ProSeP).
- Air-to-everything policy (A2XP).
- Ranging and sidelink positioning policy (RSLPP).

Those policies could be pre-configured at the UE side or provisioned by the network.

New policies merely require a new UE policy type making the NAS UE policy service framework highly extensible for future service policies.

Each policy is encoded as an IE using a consistent TLV format. Policies are sent via NAS messages, allowing the network to push multiple, heterogeneous policy sets in a single, efficient transaction.



Technical Insight: Efficiency of TLV Encoding

TLV (Type-Length-Value) is a binary encoding format widely used in 3GPP protocols (such as NAS, RRC NGAP, etc.) for efficiently transmitting flexible Information Elements (IEs) over limited bandwidth.

Key Features:

- Self-descriptive: Each IE contains type, length, and value, requiring no external parsing rules.
- Efficient and compact: Only needs a 2 or 3-byte header (type + length), significantly reducing air interface overhead.
- Robust: The length field detects truncated or damaged data, enhancing transmission robustness.

Core Value:

Binary TLV encoding is used by 3GPP for UE policy delivery, supporting efficient push of multiple policies in a single message, which is a key technology for implementing large-scale, low-latency UE policy management.

2. UE policy container

The UE policy container is the NAS information element (IE) used to deliver one or more policy rules from the 5G core network (5GCN) (via the AMF) to the UE. It carries a single, extensible TLV-based payload that encapsulates all policies from Rel-15 through the latest release such as URSP, ANDSP, V2XP, ProSeP, A2XP, RSLPP. Rather than separate NAS IEs or RRC re-configurations, all relevant policy types are concatenated as TLVs in one single IE which is delivered to the UE in one message. Hence, a single element (IE) provided in a single message provides multi-policy delivery, all at once. The UE then applies each policy after reception.

The mechanism defined since Rel-15 can deliver very large or complex policy sets (e.g. hundreds of URSP/ANDSP, ProSe/V2X entries) in a single UE policy container (up to ~64 KB of TLVs carrying different policy sets) included in one NAS message (i.e., MANAGE UE POLICY COMMAND carried in a DOWNLINK NAS TRANSPORT message). New policy types can be introduced without breaking existing implementations (unrecognized types are simply skipped).

Key characteristics:

- **Security:** delivered over NAS (control plane) and therefore protected between the AMF and the UE (by NAS security context).
- **Supports full lifecycle operations:** install, update (delta or full), and remove policy entries are supported.
- **Extensibility:** new types of policies can be introduced without breaking old implementations (unrecognized types are simply skipped).
- **Simplicity:** no complex grammar or pointers are needed just a generic and simple parser that reads a type and length, then value (looping until the IE is exhausted). This linear, deterministic processing avoids complex string parsing or JSON tree-building, cutting CPU load and power consumption on battery-constrained devices.
- **Order independence:** TLVs need not follow a strict sequence (the receiver finds the elements it cares about by scanning).
- **Compactness:** binary format keeps overhead very low compared to text-based encodings reducing radio resource usage and speeding up transmission.

3. NAS UE policy delivery service procedures

The NAS UE policy delivery service operates through two procedures:

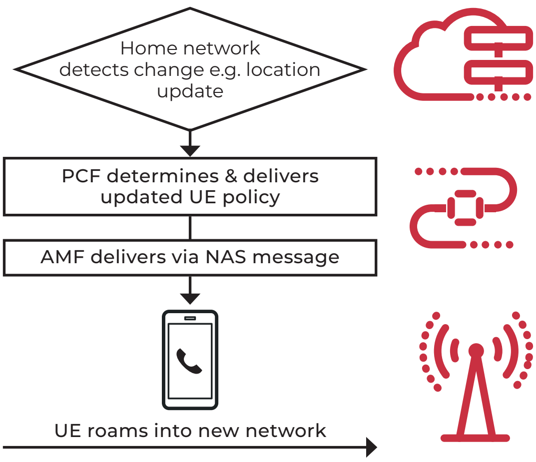
1. **Network-requested UE policy management:** the network uses this procedure to push policies (URSP, ANDSP, V2X, ProSe, A2X, RSLPP, etc.) to the UE.
2. **UE-initiated state indication:** the UE uses this procedure to inform the AMF of its local UE-policy state (stored policies) so that the network detects out-of-sync, missing or invalid policy sections and triggers refreshes when needed.

By leveraging two simple and complementary procedures, 3GPP ensures tight, efficient synchronization of network-computed UE policies and the UE stored policies to maintain correct and complete policy configuration with minimal-overhead policy distribution.

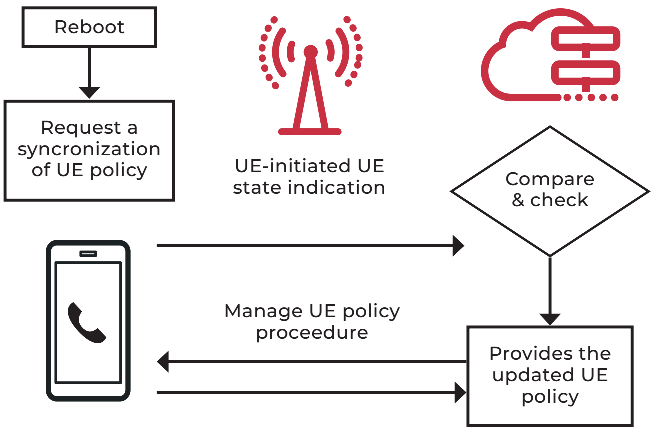
The NAS UE policy delivery service (continued)

Examples:

A UE roams into a new network and needs updated URSP or ANDSP rules (e.g., it enters a new network slice). The HPLMN then sends new or update routing policies to ensure traffic flows through preferred slices or access networks (e.g., updated URSP rules to guide traffic routing).



After a reboot or SIM change, the UE may lose stored policies. The UE triggers a UE-initiated state indication procedure to notify the network that it needs fresh policy provisioning. The network then reacts by triggering the network-requested UE policy management procedure to (re-)send policies.



Examples of UE policies: use cases

Use case 1: A battery-powered environmental (water/electricity) sensor uses constrained application protocol (CoAP) over UDP to report telemetry to the operator's IoT platform.

The operator wants to route all sensor traffic on the UDP port for CoAP to a particular DNN for IoT data traffic, using a massive IoT (MIoT) slice, and preserve the sensor's IP address across re-anchors.

UE policy container content

A UE policy part of type URSP carrying one URSP rule with:

Traffic descriptor to protocol identifier "17" (UDP), remote port range "5683" (start) "5683" (end) (CoAP). Route selection descriptor with precedence "100": DNN = "miot". S-NSSAI: SST="3" (mIoT slice) and SDD set to "3", SSC mode type with value "1" (IP preserved across re-anchors). SSC 1 preserves the IP address on re-anchor, vital for CoAP's UDP associations unless the sensor implements full DTLS session renegotiation on every IP change.

Use case 2: ANDSP-enabled WLAN supplementary services

Operators deploy trusted WLANs in busy venues (e.g., airports, shopping malls, enterprise campuses) and provision ANDSP (containing WLAN selection policy (WLANSP) rules) to guide eligible UEs in a seamless and secure manner discovering, selecting and reselecting operator-trusted WLANs or partner hotspots, reducing load on the 5G RAN.

UE policy container content

A UE policy part of type ANDSP carrying one WLANSP rule with:

Validity area "3GPP location: Tracking Area List = TAIs in downtown zone (e.g., MCC 310, MNC 260, TAC range 100–199)"; time of day "time start: 06:00, time stop: 22:00, day of week: Monday to Friday"; preferred SSID list "Operator_WiFi, Transit_Free_WiFi".

Why operators should make use of the NAS UE policy delivery service

Deploying the NAS UE policy delivery service gives operators a direct, near real-time way to steer device behaviour, optimize resource use, and unlock new revenue streams while keeping control-plane load in check. Note that the NAS UE delivery service allows operator to push slice-selection rules, access technology preferences, and service-specific policies (for V2X, ProSe, A2X, RSLP) into the UE. This ensures that the device makes optimal connectivity and resource decisions.

- **Fine-grained, near real-time control:** operators are provided with a powerful enabler of fine-grained per-flow control, access selection, sidelink timing and positioning settings at near real-time updates and can eliminate much application-layer signalling.
- **Reduced core-signalling load:** by offloading policy enforcement directly to devices (UEs), the AMF, SMF, UPF avoid repetitive reconfiguration loops, freeing control-plane resources for session management and analytics.
- **Scalability:** a single, unified policy fabric, i.e., the "PCF, AMF and UE" path, replaces multiple functions (ANDSF in 4G/EPS access selection and steering, device configuration, e.g., OMA-DM), simplifying network topology and scaling to millions of devices.
- **Dynamic service-level agreement (SLA) enforcement and monetization:** real-time policy to devices support service-tier guarantees, time-limited promotions, slice-based charging and specific packages (customized IoT, V2X, A2X).
- **Multi-access integration:** the same UE policy container can carry Wi-Fi offload instructions, service rules, and others enabling seamless multi-access selection and steer traffic across 3GPP and non-3GPP accesses.
- **Resilience and extensibility:** UEs cache and enforce policies even during core-reachability issues. New service-specific IEs are just plug in via new TLV tags, preserving backward compatibility.

Conclusions

The mechanism defined by the NAS UE policy delivery service centralizes all dynamic policy control (e.g., on network slicing, IP-flow routing, multi-access steering, V2X, A2X or sidelink positioning communication) into a single, standardized NAS container that scales from Rel-15 through any future release of the 3GPP 5G system. New policy types can be easily added without altering core NAS, in a backward compatible manner. In fact, WG CT1 has added new policies in every release; V2X policies in Rel-16, A2X and ProSe policies in Rel-17, RLSPP in Rel-18.

Whether an operator is looking to IoT, enterprise private networks, collaborative vehicle and drone platooning, or immersive consumer applications, the NAS UE policy delivery service is a key enabler of the 3GPP system that ensures device behavior stays aligned with operator wishes and subscription entitlements - enabling interoperability, efficiency and for the simple implementation of future enhancements.

[1] "3GPP AM and UE Policy Management in 5G". Pages 14-15, 3GPP Highlights Newsletter, Issue 10, June 2025.

[2] 3GPP TS 24.501.

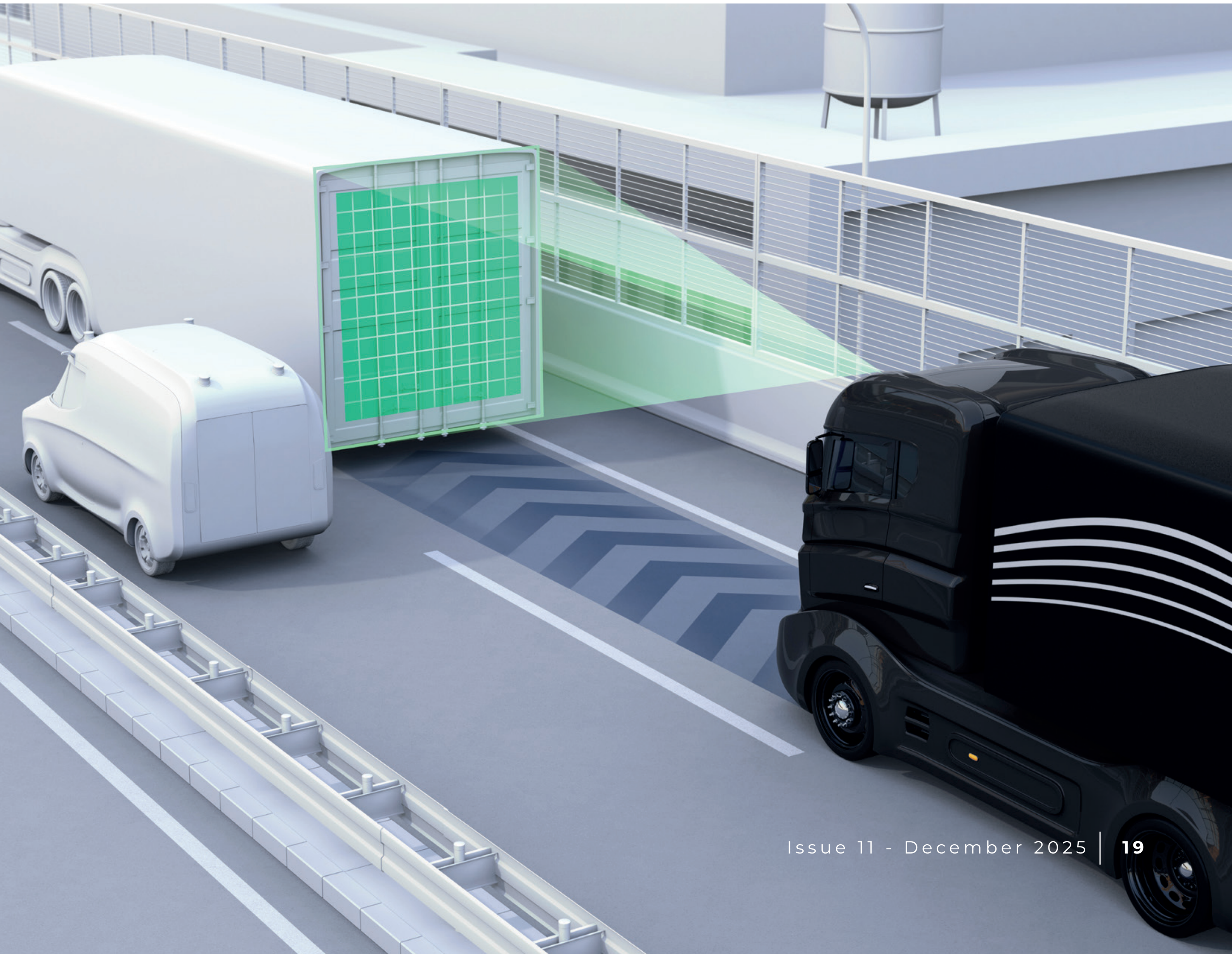
[3] 3GPP TS 24.526.

[4] 3GPP TS 24.578 (A2X policies), 24.588 (V2X policies), 24.555 (ProSe policies), 24.514 (RLSP policies).

Acronyms:

A2XP	Aircraft-to-Everything policy
AM	Access & mobility
AMF	Access & mobility function
ANDSP	Access Network Discovery and Selection policy
CoAP	Constrained application protocol
DNN	Data Network Name
DTLS	Datagram Transport Layer Security
HPLMN	Home Public Land Mobile Network
JSON	JavaScript Object Notation
OMA-DM	Open Mobile Alliance - Device Management
PCF	Policy control function
ProSeP	5GProximity based Services policy
SLPP	SideLink Positioning protocol
S-NSSAI	Single Network Slice Selection Assistance Information
TLV	Type-Length-Value
UE	User Equipment
URSP	UE Route Selection policy
V2XP	Vehicle-to-Everything policy
WG CT1	3GPP Core network and Terminals Working Group 1

For more from WG CTI: **www.3gpp.org/3gpp-groups**



Rel-19 work on Low power wake-up signal and radio

By Xin Qu (vivo), Xueming Pan (vivo)

5G User Equipment (UE) power saving technologies have been studied and specified since Rel-16 in 3GPP.

Although Rel-16 & Rel-17 specified the wake-up signal, i.e., downlink Control Information of Power Saving (DCP) for RRC connected state and Paging Enhancement Indicator (PEI) for RRC idle/inactive state, both of the wake-up signals are based on PDCCH for carrying wake-up information and rely on coherent detection. As a result, they rely on high time-frequency accuracy for demodulation and decoding, offering limited power saving gain.

The Rel-19 low power wake-up signal/wake-up receiver (LP-WUS/WUR) is based on DFT-s-OFDM, generating a superposed signal of OOK and OFDM sequences in the time domain, which provides a common LP-WUS signal design for OOK-based WUR and OFDM sequence based WUR. Thus, non-coherent detection is allowed for LP-WUS detection, such as envelope detection for OOK-based WUR and sequence correlation detection for OFDM sequence based WUR to obtain wake-up information.

Non-coherent detection has lower requirements for time-frequency accuracy compared to coherent detection, thereby relaxing the hardware and baseband processing requirements for LP-WUS reception and achieving much higher power saving gain. The Rel-19 LP-WUS/WUR applies to both RRC idle/inactive state and RRC connected state, and the corresponding detailed power saving gains studies are summarized in later section of this article. The target coverage for Rel-19 LP-WUS is the same as Message-3 PUSCH.

An illustrative description on LP-WUS generation is given in Figure 1, for each OOK "ON" symbol (denoted as 1 in Figure 1), one out of a set of predefined OFDM sequences is overlaid in the time domain. "OFF" symbol (denoted as 0 in Figure 1), corresponds to zero signal or no transmission in baseband. One OFDM symbol could comprise of 1, 2, 4 OOK symbols depending on configuration, among which each OOK "ON" symbol is overlaid with one OFDM sequence. The OFDM symbols go through DFT and transform to complex symbols in frequency domain and cyclic shift operation is performed after DFT which ensures that the phase of the time domain OFDM sequence remains unchanged. Then, such complex symbols in frequency domain are mapped to the resource elements (RE) in the LP-WUS bandwidth, and the adjacent bandwidth can be used by other NR signals. At last, IFFT is applied to LP-WUS and other NR signals, to get the over-air signal in time domain.

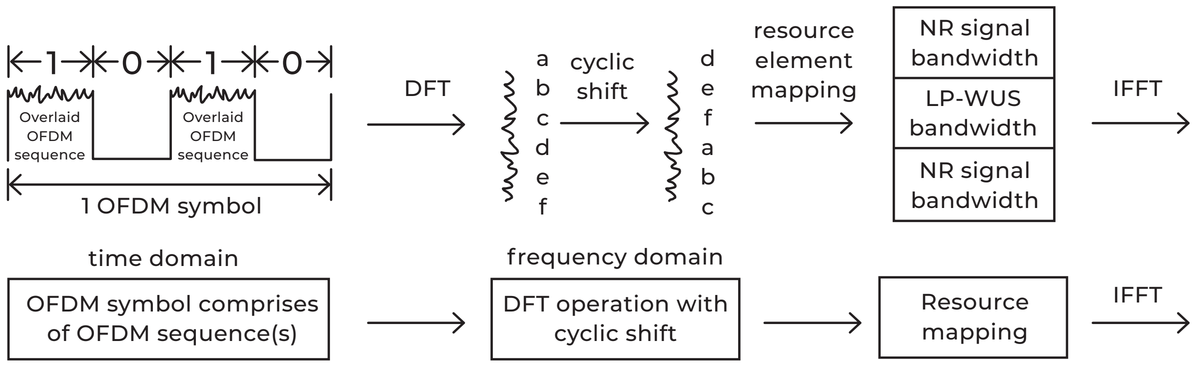


Figure 1: DFT-s-OFDM based LP-WUS generation: OOK with overlaid OFDM sequence

LP-WUS/WUR operation in RRC idle/inactive state

Low Power-Wake Up Signal (LP-WUS) is used to wake up the UE for paging monitoring which helps reducing the unnecessary paging monitoring to reduce UE power consumption.

Before being woken up, the UE main radio may stay in ultra-deep sleep or deep sleep to save power, where a time gap between LP-WUS reception and paging monitoring is required for UE main radio to get ready for paging monitoring from sleep.

Time offset(s) between LP-WUS and paging can be configured by network according to the UE capability on the required time gap. Furthermore, RRM measurement can be relaxed or offloaded to LP-WUR, which can further reduce UE power consumption.

According to [1], compared with existing I-DRX operation, significant UE power saving gain (up to more than 90%) is observed by using LP-WUS/WUR to trigger UE MR paging monitoring compared with existing I-DRX operation (with and without PEI), if sufficient RRM measurement relaxation is applied, i.e., RRM measurement relaxation with relaxation factor of at least 8 or offloading RRM measurement to LP-WUR.

Prior to 3GPP Rel-19, only neighboring cell RRM measurement relaxation is specified, while serving cell RRM relaxation is not supported. In the Rel-19 LP-WUS/WUR, since the LP-WUR is capable of performing serving cell RRM measurements, it is possible to further relax neighboring cell measurement and relax or offload serving cell measurement. Specifically, for UE enabled with the LP-WUS feature, the following two RRM relaxation / offloading types are supported, as shown in Table 1.

For ***1) RRM measurement offloading***, the entry condition is: the legacy serving cell measurement(s) shall be above the configured entry threshold(s) of RRM measurement offloading, and if the entry threshold(s) of RRM measurement offloading for LP-WUR is configured, the serving cell measurements based on LP-WUR shall be above such configured threshold(s). Since the threshold(s) of the entry condition for serving cell RRM measurement offloading is higher than or equal to the threshold(s) to stop neighboring cell RRM measurement, legacy neighboring cell RRM measurement would stop once the entry condition for serving cell RRM measurement offloading satisfies.

The exit condition is the serving cell measurement(s) based on LP-WUR is below the exit threshold(s) of RRM measurement offloading for LP-WUR based measurement.

For ***2) RRM measurement relaxation*** for serving cell and neighbouring cell, the entry/exit condition is: the legacy serving cell measurement(s) are above/below the configured threshold(s) of RRM measurement relaxation; and if the threshold(s) for LP-WUR is configured, the serving cell measurements by LP-WUR shall be above/below the configured threshold(s) for LP-WUR based measurement.

RRM measurement relaxation/offloading type	Legacy serving cell measurement	Legacy neighboring cell measurement	Serving cell measurement by LP-WUR
1) RM measurement offloading	Not performed	Not performed	performed
2) RRM measurement relaxation	relaxed	Not performed or relaxed	performed

Table 1: RRM measurement relaxation and offloading based on Rel-19 LP-WUS/WUR

LP-WUS/WUR operation in RRC connected mode

Low Power-Wake Up Signal (LP-WUS) is used to wake up UE for PDCCH monitoring which helps reducing the unnecessary PDCCH monitoring to reduce UE power consumption. Before waked up, UE main radio main stay in deep sleep, light sleep, or micro sleep to save power, where a time gap between LP-WUS reception and PDCCH monitoring is required for UE main radio to get ready for PDCCH monitoring from certain sleep state. Time offset(s) between LP-WUS and PDCCH motoring can be configured by network according to the UE capability on the required time gap. Furthermore, UE can indicate through UAI (UE Assistant information) a longer preferred time gap to allow main radio a deeper sleep.

There are two options of LP-WUS operation in RRC connected mode, depending on whether LP-WUS trigger PDCCH monitoring via triggered to start C-DRX on-duration timer or not.

Option 1: Among the configured LP-WUS monitoring occasions (MO), the UE monitors only the first Z LP-WUS MOs before the time duration indicated by drx-onDurationTimer, where the start of LP-WUS monitoring is determined by a predefined time offset (LPWUS-Offset) relative to the drx-onDurationTimer. Within each C-DRX cycle, depending on whether LP-WUS targeting for the UE is detected or not, the UE determines whether to start the drx-onDurationTimer and PDCCH monitoring in the current cycle.

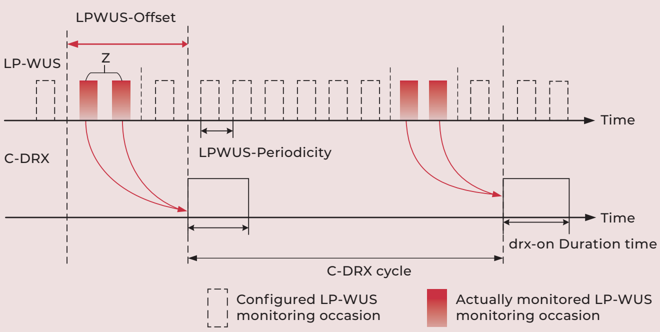


Figure 2 ***Option 1:*** LP-WUS operation in RCC connected mode

Option 2: Among the configured LP-WUS monitoring occasions (MO), UE monitors LP-WUS MOs outside the Active Time to trigger PDCCH monitoring, and the LP-WUS monitoring cycle is configured irrespective of C-DRX cycle. When LP-WUS targeting for the UE is detected successfully, the UE starts the timer LPWUS-PDCCH_Monitoring_Timer after a predefined time interval and monitors the PDCCH while this timer is running.

In Option 2, while LPWUS-PDCCH_Monitoring_Timer is running, the UE is considered in Active Time and monitors the PDCCH; otherwise, the UE exits Active Time and PDCCH monitoring, and returns to the LP-WUS monitoring state. Compared with Option1, Option 2 provides latency reduction while keep the UE power consumption low. Furthermore, option 2 enables gNB to wake-up and schedule the UE almost “at any time”, if the LP-WUS monitoring cycle is configured to be small, e.g. (10~20ms).

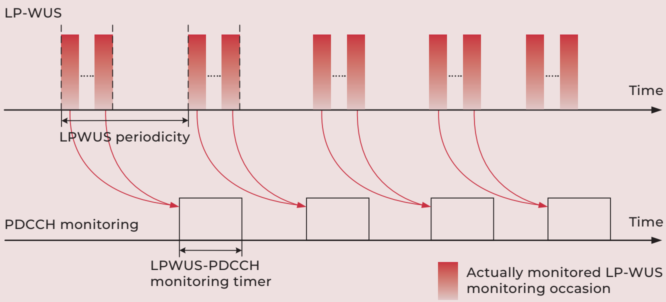


Figure 3 ***Option 2:*** LP-WUS operation in RRC connected modeoption 2

According to [1], in RRC connected mode, for XR traffic, moderate UE power saving gain (up to more than 10%) across different types of XR traffic and system load scenarios can be observed, larger UE power saving gain can be observed if the UE MR can enter light sleep instead of micro sleep during LP-WUS monitoring by LR; for FTP and IM traffic, compared with existing UE power saving techniques, significant UE power saving gain (up to more than 60%) and moderate UPT improvement (up to more than 10%) when the UE MR enters deep sleep state during LR LP-WUS monitoring, larger UPT improvement (up to more than 180%) is observed for traffic with small packets, e.g. IM. Relatively lower or no UE power saving gain can be observed when the UE MR enters light sleep during LR LP-WUS monitoring, but the UPT improvement is higher (up to more than 50%).

At last, LP-WUS is also one of the candidate schemes for 6G UE energy efficiency, especially for DL WUS of OFDM based sequence, the following aspects has been agreed by 3GPP Working Group RAN1 to be studied and evaluated for 6G EE improvement: coverage target for DL WUS (e.g., same as PDCCH, common sync signal, or other), measurements and/or synchronization, system overhead and network energy consumption/UE energy saving for UE operation with the DL WUS, RRC states, and other functionalities [2].

[1] 3GPP TR 38.869 V18.0.0 (2023-12)
[2] RAN1#122bis Chairman notes (2025.10)

For more on TSG RAN and WG RAN1 see:
www.3gpp.org/3gpp-groups

WG CT3 Rel-19 AI/ML features

By Abdessamad El Moatamid and Xuefei Zhang (Huawei), Yizhong Zhang (vivo)

The efficient and extensive use of Artificial Intelligence (AI) related technologies is one of the key enablers for future 3GPP mobile networks. Starting from 3GPP Rel-18 and building on the network automation and preliminary AI capabilities - specified since Release 15 the first release of 5G [1] - 5G-Advanced now further expands the usage and influence of AI towards fully AI-enabled mobile networks on the road to 6G.

The 5G AI/ML Framework in a nutshell

The 5G-Advanced AI/ML framework defined by CT3 from Rel-18 allows AI/ML technologies to be leveraged, such as ML data collection and ML Model training/inference, so as to enhance and optimize the operation of the mobile networks. The framework takes advantage of existing network automation and data analytics capabilities defined in Rel-15, and further broadens their scope and areas of action.

The main AI/ML capabilities supported by 3GPP include the following

- Enhancements to the existing NEF (Network Exposure Function) enabled network analytics exposure capabilities (e.g., network performance analytics) to enable 3rd party AI/ML-enabled applications to benefit from a tailored monitoring of the utilization of the network resources associated to them.
- Exposure of 5GC (5G Core Network) internal information to authorized 3rd party AI/ML-enabled applications (e.g., the candidate UEs to be used to form the group of UEs used in Federated Learning operations).
- Enhancement of the 5GC application-related parameters provisioning framework to support the provisioning of the necessary parameters to assist the operations of the 3rd party AI/ML-enabled applications (e.g., change or influence the aggregated QoS parameters for a group of UEs that are part of a Federated Learning group) together with the improvement of the corresponding underlying 5GC Policy and Charging Control framework and QoS management capabilities (e.g., report the planned changes in QoS / network conditions / etc.).
- ML Model training/inference involving, triggered by and/or in collaboration with 3rd party AI/ML-enabled applications.

AI/ML Rel-19 Enhancements

The major 5G-Advanced AI/ML Rel-19 enhancements include the following functionalities:

AI/ML-based Positioning (see also Use Case #1 below), enhancing the LMF (Location Management Function) to derive UE location based on ML Models, not on signalling measurements exchanged between the UE and the network as is currently supported. The ML Models used for this purpose can be trained either by the LMF or an NWDAF (Network Data Analytics Function) containing the MTLF (Model Training Logical Function) functionalities.

Vertical Federated Learning (VFL), another federated learning paradigm that enables joint model training without exposing raw data, wherein the local data set in different VFL participants (i.e., VFL Server, VFL Client) for local model training have different feature spaces for the same sample. Each entity retains ownership of its ML model, there is no requirement for a uniform model architecture across the involved entities. The NWDAF, NEF and AF (Application Function) are thus enhanced for this purpose with a set of new service APIs [2] [3] [4] [5] to support VFL procedures and capabilities, including ML Model preparation, training and inference.

NWDAF-assisted Policy Control and QoS Management (see also Use Case #2 below), enhancing the NWDAF to support to provide the PCF (Policy Control Function) with a set of network data analytics and predictions in the form of QoS and policy assistance information (e.g., predictions of a set of QoS parameters) for one or several UE(s), so as to enable the PCF to fine tune the QoS and network policies to be applied for the traffic of these UE(s), thus allowing for a more intelligent optimization of network performance.

Signalling storm mitigation and prevention (see also Use Case #2 below), enhancing the NWDAF to provide the other 5GC NFs (Network Functions), here referred to as consumer NFs, with network data analytics and recommendations for signalling storm mitigation and prevention based on the information collected from other NFs and/or network entities. These analytics assist the receiving consumer NF to identify the sources and/or causes of the signalling storm and trigger the necessary actions to return to the nominal network operation.

Use Case #1: AI/ML-based Positioning

When registering at the NRF (Network Repository Function), the NWDAF indicates its support of ML Model training for the purpose of LMF-based AI/ML positioning. Then, if the LMF decides to make use of this functionality, it can discover and select a suitable NWDAF that supports the LMF-based AI/ML positioning during the NF discovery procedure with the NRF.

Afterwards, the LMF subscribes to the selected NWDAF and retrieves the required trained ML Model(s) from it, or in case the required ML Model(s) have not yet been trained, the NWDAF may start the training based on the input data collected from the LMF. Once trained, the NWDAF provides one or more ML Model(s) to the LMF, allowing the LMF to perform the AI/ML-based positioning.

The NWDAF can further provide either a newly trained ML Model or a re-trained ML Model to the LMF for ML Model improvement. In case ML Model performance monitoring is requested by the LMF, the NWDAF evaluates the ML Model performance based on the location measurement data, ground truth data and inference outputs. Based on the outcome of the evaluation, if the ML Model accuracy thresholds are not satisfied, the NWDAF can re-train the ML Model or trigger the LMF to use another positioning method.

Use Case #2: QoS and Policy Assistance

The PCF requests analytics data to the NWDAF by providing a collection of input parameters including the corresponding Analytics Identifier, a list of potential QoS parameter sets (e.g., 5QI (5G QoS Identifier), QoS characteristics, Guaranteed/Maximum Flow Bit Rate), the identifier of the targeted application, and optionally the expected QoE (Quality of Experience).

The NWDAF collects the relevant input data from various data sources, including the SMF (Session Management Function), AMF (Access and Mobility Management Function), UPF (User Plane Function), AF and OAM (Operation, Administration and Maintenance), etc., such as the applied QoS parameters, UE location, observed service experience and network performance measurements.

Based on the collected data, the NWDAF derives and delivers analytics data containing a list of candidate QoS parameter sets and their predicted QoE for the application during specific time slots. The output can include detailed QoS values (e.g., Packet Delay Budget, Guaranteed Bit Rate) and the associated filtering information such as spatial/temporal validity information. This empowers the PCF to make informed, customized and predictive policy decisions, by selecting the QoS profiles that are expected to meet the application's quality requirements, thereby enhancing network efficiency and user experience.

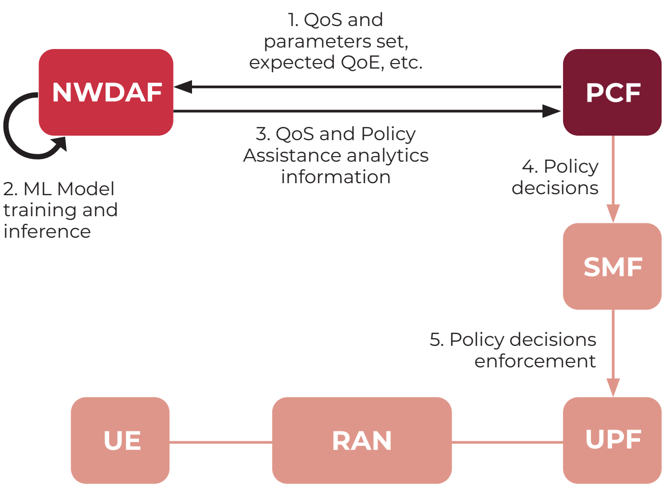


Figure 1: NWDAF-assisted Policy Control and QoS

Use Case #3: Signalling Storm Mitigation and Prevention

The Signalling Storm Mitigation and Prevention Analytics enables the NWDAF to support the mitigation and prevention of network abnormal behaviours. This capability is crucial for maintaining network stability and reliability, as signalling storms — characterized by an abnormal and excessive increase in signalling messages — can overwhelm key 5GC NFs and lead to a degraded QoS for end users and potentially also disruptions of services.

The consumer NFs/entities (e.g., AMF, SMF, SCP), can subscribe to be notified of such analytics data at the NWDAF by providing a collection of input parameters including the corresponding Analytics Identifier, the target for the reporting (e.g., specific NF instances or the whole network), and the target cause (e.g., whether the storm originates from UEs or other NFs).

The NWDAF collects input data from various sources, including UE-related context, NFs' load information and performance metrics, and application data from the AMF, SMF, NRF, AF and OAM, to derive the analysis data. It can also train ML Models to automatically detect and isolate the root cause, e.g., identifying which UEs or RAN nodes are generating the abnormal signalling.

The output provides statistics or predictions regarding the abnormal signalling rate condition. This empowers consumer NFs to trigger proactive actions, such as temporarily barring problematic UEs or redistributing load within the network, so as to prevent the storm from severely affecting the whole network and ensure operational resilience.

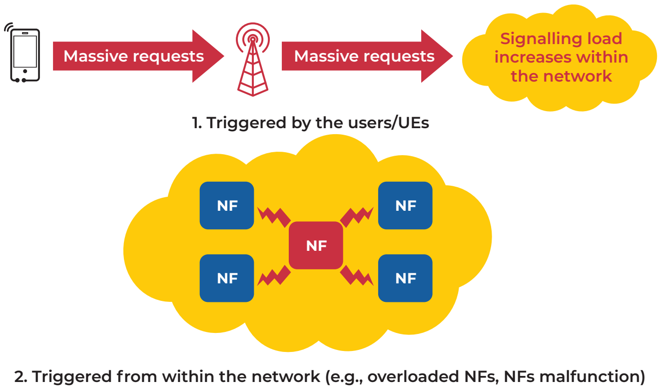


Figure 2: Main Signalling Storm causes in Mobile Networks

Conclusion

5G-Advanced positions itself hence as a cornerstone in establishing and enlarging the usage and influence of AI technologies in mobile networks, with the goal of progressively transitioning into autonomous, dynamic and intelligent network management, thus preparing the way for AI-Native (e.g., using AI Agent based Agentic AI) and intent-driven mobile networks in future generations of mobile networks.

This is expected to allow for optimized and tailored experiences for end users, especially with the increasing new types of devices connected to mobile networks (e.g., IoT devices, sensors). With these new functionalities, enablers and use cases, mobile networks are thus expected to also play a pivotal role in driving the development, strength and adoption of AI technologies.

[1] "Network Automation Enablers in 5GS", Pages 20-21, 3GPP Highlights Newsletter, Issue 09, December 2024

[2] 3GPP TS 29.520: "5G System; Network Data Analytics Services; Stage 3"

[3] 3GPP TS 29.530: "5G System; Application Function Artificial Intelligence/Machine Learning (AI/ML) Services; Stage 3"

[4] 3GPP TS 29.522: "5G System; Network Exposure Function Northbound APIs; Stage 3"

[5] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services"

See also:

- **3GPP TS 29.552:** "5G System; Network Data Analytics signalling flows; Stage 3"
- **3GPP TS 29.513**: "5G System; Policy and Charging Control signalling flows and QoS parameter mapping; Stage 3"
- **3GPP TS 23.501:** "Technical Specification Group Services and System Aspects; System Architecture for the 5G System"
- **3GPP TS 23.502:** "Procedures for the 5G System; Stage 2"
- **3GPP TS 23.503:** "Policy and Charging Control Framework for the 5G System"

For more on CT3 WG: **www.3gpp.org/3gpp-groups**

GSA: Private Mobile Networks Continue to Scale

By Joe Barrett, President of Global mobile Suppliers Association (GSA)

Private mobile networks, also known as non-public networks, are increasingly transforming the way enterprises, industries and governments operate. GSA defines these as 3GPP-based 4G LTE or 5G networks intended solely for private use.

They can use only physical elements, such as the RAN and core, or a combination of physical and virtual elements, for example, hosted by a public land mobile network. But as a minimum, a private mobile network needs to implement a dedicated network core.

Our definition also includes MulteFire and the Future Railway Mobile Communication System. Networks must use 3GPP-defined spectrum and serve business-critical or mission-critical operational needs. GSA's database tracks customer references with contracts above €50,000, filtering out small demonstration networks.

Rising Demand for Private Mobile Networks

Demand for private mobile networks has grown in recent years, driven by their potential to transform existing operations, increase automation and efficiency or deliver new services, using data and analytics. Coupled with LTE or 5G, these networks can be deployed in a variety of environments, be they remote sites or highly secure facilities.

This evolution in mobile technology has been made possible by the arrival of LTE-Advanced systems, which boosted network capacity, throughput and latency. Introduced in 3GPP Release 10, LTE-Advanced enhanced LTE networks, while LTE-Advanced Pro in Releases 13 and 14 took this a step further, adding the ability to share licensed and unlicensed spectrum. The advent of both technologies significantly improved the capabilities of LTE, making it a viable foundation for private mobile networks.

Support for non-public networks started as a study item in 3GPP Release 15, establishing the initial framework for enterprises to deploy private 5G networks. 5G brings increased densities of users and devices, even greater capacity and further improvements to latency that enable the use of mobile technology for time-critical applications. This last point is particularly crucial to private mobile networks as it guarantees a reliable and continuous high-speed connection.

However, it was Release 16 that brought formal definitions and specifications for non-public networks — including both standalone and public network–integrated models — enabling organisations to deploy secure and isolated mobile networks based on standardised 5G technology.

Release 16 also enhanced features such as ultrareliable low-latency communications (URLLC), time-sensitive networking and positioning accuracy, all important capabilities for industrial and enterprise applications.

Market Snapshot

As of GSA's latest update on the private mobile network market, in August 2025 there were 1,846 total customers with a private mobile network in 80 countries around the world, up 7.7% from 1,714 customers in 2024. In the second quarter of 2025, 74 new references were added, up from 62 for the same period a year earlier.

Our research shows that most private networks (51.1%) are on LTE networks, with 28.5% using 5G and 19.0% using a mix of LTE and 5G networks, as shown in Figure 1.

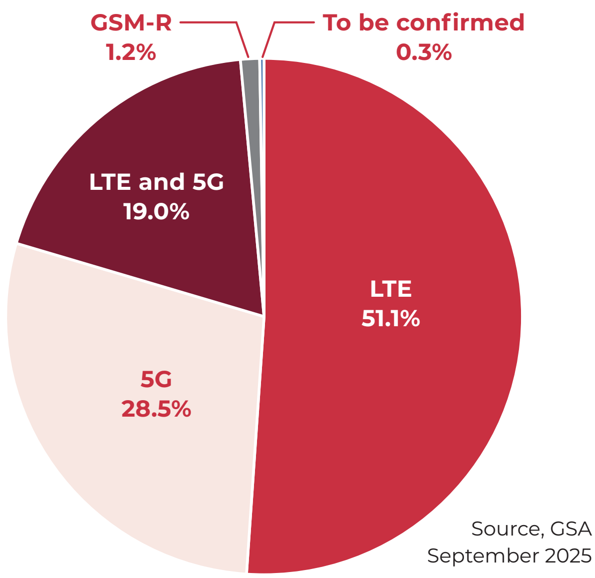


Figure 1: Private mobile network customers, by technology used (base: 1,846 catalogued customers deploying private wireless networks with revenue greater than €100,000)

Private 5G networks are often long-term trials and deployments in education and test-bed or validation facilities, with only a small number in real operation in industrial settings.

However, the type of technology used varies by sector. Industries like oil and gas and mining tend to prefer LTE, whereas hospitals and temporary sports, media and events typically favour 5G networks because of the greater bandwidth. Some industries are split evenly between LTE and 5G networks, like water utilities and power plants.

Looking at the roll-out of private mobile networks by sector, highlighted in Figure 2, the manufacturing sector leads with 359 deployments, followed by education and academic research with 164 and mining with 134. Defence and peacekeeping, with 122 deployments, and device testing and lab-as-a-service, with 111, round out the top five.

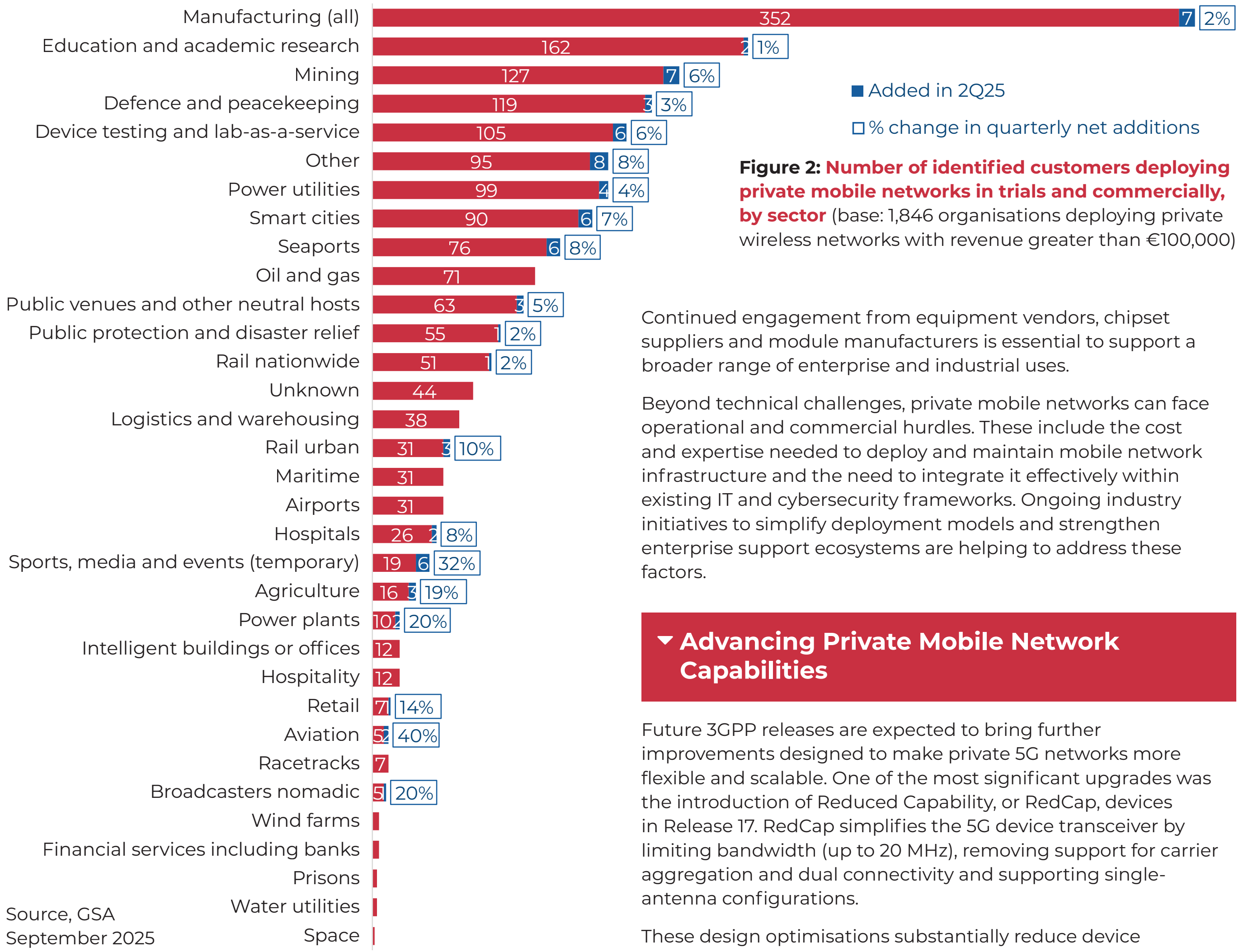


Figure 2: **Number of identified customers deploying private mobile networks in trials and commercially, by sector** (base: 1,846 organisations deploying private wireless networks with revenue greater than €100,000)

Note that although these figures provide an indication of the number of customers deploying a private network, they do not reflect market value or the total number of deployed networks.

We also see variation in the technologies used in different countries: 5G is dominant in Germany and the Republic of Korea, whereas LTE is prevalent in Latin America. This is often influenced by regulators' allocations of dedicated enterprise spectrum, which have been central to widening adoption.

Challenges on the Path to Scale

Despite strong momentum, several challenges could slow the expansion of the market. Many of these reflect the natural maturity curve of an emerging technology segment rather than fundamental barriers.

Although we continue to see progress in the allocation of dedicated enterprise spectrum, access remains uneven across markets. Licensing processes and costs vary widely by country, and harmonising frequency bands between regions is complex. This creates obstacles for multinational organisations seeking to deploy consistent private network operations in several countries.

The device ecosystem and interoperability are also major considerations. GSA has identified more than 31,000 LTE and 5G devices compliant with 3GPP standards, but most are designed for consumer applications. The availability of industrial-grade cellular and, in particular, 5G devices remains limited.

Continued engagement from equipment vendors, chipset suppliers and module manufacturers is essential to support a broader range of enterprise and industrial uses.

Beyond technical challenges, private mobile networks can face operational and commercial hurdles. These include the cost and expertise needed to deploy and maintain mobile network infrastructure and the need to integrate it effectively within existing IT and cybersecurity frameworks. Ongoing industry initiatives to simplify deployment models and strengthen enterprise support ecosystems are helping to address these factors.

Advancing Private Mobile Network Capabilities

Future 3GPP releases are expected to bring further improvements designed to make private 5G networks more flexible and scalable. One of the most significant upgrades was the introduction of Reduced Capability, or RedCap, devices in Release 17. RedCap simplifies the 5G device transceiver by limiting bandwidth (up to 20 MHz), removing support for carrier aggregation and dual connectivity and supporting single-antenna configurations.

These design optimisations substantially reduce device complexity, size and power consumption, while maintaining peak data rates of up to 226 Mbps in the downlink and 120 Mbps in the uplink. This is set to play an important role in lowering the cost of industrial 5G devices and expanding the ecosystem for IoT and machine connectivity.

Release 17 also improved network slicing, with more flexible and efficient partitioning of network resources, allowing mobile network operators to offer dedicated, isolated slices for enterprise users. Such capabilities can support hybrid or virtual private networks that combine the benefits of public network coverage with the control and security required by enterprises, helping to reduce cost and deployment complexity.

Looking ahead, 3GPP Releases 18 and 19 will further enhance energy efficiency, uplink performance, advanced positioning and sensing, and AI-driven automation in network management.

Integration with non-terrestrial networks is another notable development, enabling private networks in remote or hard-to-reach environments to connect through satellite systems. This will enhance resilience, support remote asset tracking and improve continuity for enterprises operating in dispersed or mobile locations.

Together, these successive 3GPP releases continue to strengthen the technical foundation for private mobile networks, expanding their capabilities, improving cost efficiency and underpinning a wider range of enterprise and industrial applications. These improvements will continue to aid the adoption of private mobile networks as they expand into mainstream adoption.

Mission Critical standardised interworking

This article is based on material from TCCA's white paper IWF - Interworking of LMR networks with 3GPP Mission Critical Services. Lead author: Sylvain Allard, Capgemini.

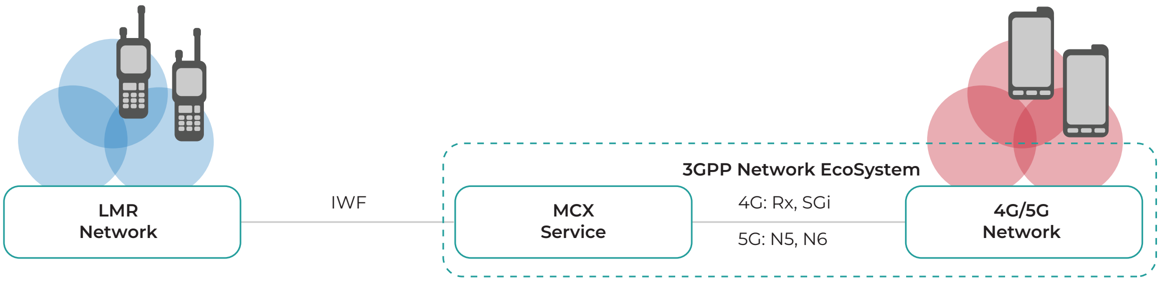
The Interworking Function (IWF) is a function defined by 3GPP to enable seamless communication between next-generation Mission Critical Services (MCX)—delivered over LTE and/or 5G broadband networks—and legacy narrowband technologies such as TETRA, APCO P25, and GSM-R.

As public safety agencies, transport operators, and critical infrastructure providers embark on the migration from traditional Land Mobile Radio (LMR) systems to broadband MCX platforms, the IWF stands out as a key enabler for interoperability during this transitional phase. This migration is not instantaneous. Many user groups will continue to rely on narrowband networks for years, while others move ahead with broadband MCX solutions.

The IWF ensures that these groups can communicate and collaborate effectively, maintaining operational continuity and safety until full migration is achieved.

Standardisation is essential for enabling a smooth and reliable transition from legacy radio systems to next-generation broadband solutions. By establishing a consistent and open framework —exemplified by the IWF as specified in 3GPP standards— the objective is to ensure continuity of key services such as voice and data, while optimizing cost-efficiency and aligning with the evolving requirements of mission-critical communication.

The IWF is not just a technical bridge; it is a strategic tool for managing risk, cost, and user experience during migration.



Technical Foundations and Integration Models

Implementing the IWF poses several challenges, especially for TETRA, currently being addressed by TCCA's Interworking Function Working Group. *The IWF - Interworking of LMR networks with 3GPP Mission Critical Services* white paper produced by the IWF Working Group offers a comprehensive overview of interworking capabilities and technical requirements, comparing standardised and proprietary interfaces for linking TETRA networks with MCX services. While TETRA is used as the primary example, the principles apply equally to technologies like APCO P25 or GSM-R.

A key gap identified in the TETRA ecosystem is that the TETRA IWF specification does not define an internal interface to the TETRA system. This omission places the burden on TETRA vendors to implement the IWF interface themselves. Recognizing that not all vendors may be willing or able to do so, the paper outlines alternative integration models to connect TETRA with MCX systems.

These models all use the standardised IWF interface and other available interfaces on the TETRA side, such as proprietary APIs or the TETRA ISI (Inter-System Interface) which is still under consideration by the ecosystem due to the related vendor implementation approach.

Key Integration Challenges

The TCCA white paper highlights several integration challenges, market dynamics, and use cases that illustrate the gradual extension of LMR services to non-critical, business-critical, and mission-critical users.

Some of the most significant challenges include:

- **Bandwidth Constraints:** The limited bandwidth of LMR restricts its ability to support the full range of MCX's broadband functionalities. As a result, interworking is generally limited to voice, messaging, and location services.
- **Latency and Reliability:** Ensuring low-latency, high-reliability communication —especially for emergency operations— can be complex when linking narrowband and broadband technologies. The IWF must be carefully designed to avoid bottlenecks and maintain mission-critical performance.
- **Cost and Implementation Complexity:** Deploying IWF involves capital investment in hardware, software, and integration, along with the ongoing effort to manage and maintain the solution throughout the transition period.
- **End-to-End Encryption:** Security is paramount. For example, TETRA End-to-End Encryption can be terminated in the IWF, with 3GPP encryption used on the MCX side. However, this

breaks true end-to-end encryption. Some authorities may accept this, while others require strict end-to-end encryption, which is possible but requires implementing the narrowband codec and encryption algorithm on the broadband device.

Market Dynamics and Use Cases

MCX solutions are primarily targeted at the public safety and emergency response sectors but are also increasingly relevant across various industries that demand secure, reliable, and prioritised communications. The key market segments include:

- **First responders:** Police and law enforcement, fire and rescue, emergency medical services.
- **Government and Defence:** Military forces, border security and Coast Guard.
- **Utilities and Critical Infrastructure:** Energy sector, water & waste services, transport & logistics.
- **Commercial and Industrial applications:** Private security, mining & construction, major events.

The TCCA paper categorises and prioritises the key use cases that guide LMR – MCX integration via the IWF.

Status of Standards and Industry Adoption

Since Release 12, 3GPP has actively developed MCX standards, with IWF specifications introduced in Release 15. The IWF specification is considered functionally complete (finalised in 3GPP Release 16 and Release 17 and continuously refined through Release 18), and the ecosystem is evolving to support new features and broader interoperability.

Despite the availability of MCX solutions, IWF adoption by both MCX and LMR vendors has lagged. Early and proactive implementation of IWF is essential to gain the trust of LMR operators and to support a seamless, staged migration to MCX.

The IWF has been demonstrated in ETSI MCX and FRMCS (Future Rail Mobile Communications System) Plugtests™. Interworking between TETRA and MCX systems and between GSM-R and MCX systems was tested and shown in past interoperability events and will be in scope for future MCX Plugtests.

Implementation Options and Recent Developments

While Plugtests have demonstrated the so-called native IWF implementation—where the TETRA system vendor has implemented the IWF on the TETRA system—other implementation options have been showcased in 2025.

One alternative is to connect the IWF to the TETRA system via a proprietary API. These APIs exist on all TETRA systems but are not standardised. Another alternative is to use the standardised TETRA ISI, originally designed to interconnect TETRA systems, to connect to the IWF. Both options allow a third party to develop the IWF, reducing reliance on the TETRA system vendor.

Implementations for other narrowband technologies are progressing as well. For example, FirstNet, the public safety network in the USA, has announced the implementation of IWF for P25 systems, allowing local and regional public safety P25 systems to connect to the FirstNet broadband network. For railways, the IWF is important to connect FRMCS to current GSM-R networks, enabling a smooth migration from GSM-R to broadband FRMCS.

Recently, the DMR Forum announced plans to explore the IWF. A DMR IWF standard would allow DMR systems to connect to MCX in a standardised way, further expanding the reach of interoperable mission-critical communications.

Benefits and Opportunities

Key opportunities discussed in the IWF white paper include:

- **Seamless Voice Communication:** LMR users can join MCX group calls and make private calls across systems, preserving critical voice services during migration.
- **Integration of Data Services:** Real-time exchange of data, including SDS messages and location information, enhances situational awareness and operational decision-making.
- **Priority Access and Multicast Support:** Guarantees that high-priority communications are maintained during emergencies through prioritised access and multicast delivery.
- **Support for Hybrid Operations:** Agencies can maintain legacy voice services while adopting broadband applications, minimizing disruption and maximizing investment.
- **Standards-Based Interoperability:** The IWF adheres to internationally recognised standards, promoting vendor independence, scalability, and security.
- **Control Room Integration:** Unified dispatching and situational awareness across LMR and MCX domains.
- **Future-Proofing:** The IWF is designed to evolve with 3GPP releases, supporting new features such as augmented reality, IoT integration, and advanced railway communications (FRMCS).

Practical Recommendations - For agencies and operators considering migration to MCX, the following recommendations are essential:

Adopt a Phased Migration Strategy	Begin with hybrid LMR–MCX deployments, leveraging the IWF for interoperability
Prioritise Standards-Based Solutions	Ensure vendor neutrality and future scalability by adhering to 3GPP and ETSI standards
Invest in Training and Change Management	Support user adaptation and maximise operational benefits through targeted training and ongoing support
Monitor Industry Developments	Participate in Plugtests, certification programs, and standards forums to stay abreast of evolving best practices

The IWF plays a pivotal role in enabling hybrid communication environments that combine LMR systems with broadband solutions. The various use cases outlined throughout the *IWF Interworking of LMR networks with 3GPP Mission Critical Services* white paper clearly demonstrate the value of interworking during all phases of integration and migration. IWF is positioned to be a key enabler in the broader adoption of broadband communications across public safety, industrial sectors, and critical infrastructure domains, where hybrid LMR–MCX solutions will serve as both a complement and a steppingstone to full migration.

As the ecosystem matures, the IWF will continue to support the evolution of mission-critical communications, enabling agencies to deliver secure, reliable, and efficient services in an increasingly connected world.

TCCA https://tcca.info

Thanks to TCCA's IWF Working Group co-chairs Harald Ludwig and Michel Duits for their help on this article.

TCCA's IWF white paper can be found here: https://tcca.info/documents/Interworking-Function-IWF-Interworking-of-LMR-networks-with-3GPP-Mission-Critical-Services.pdf/

Enabling Local 3GPP Networks

Spectrum Pricing Frameworks and Regulatory Recommendations

By Seppo Yrjölä, Principal Engineer, Cloud and Network Services, Nokia on behalf of the Alliance for Private Networks

The success of 3GPP-based mobile communication networks depends not only on technical specifications but also on timely and affordable access to spectrum. This article identifies and characterizes spectrum pricing frameworks adopted by regulators worldwide for local mobile networks, highlighting their implications for 3GPP technology deployment and is based on the output of the study – A Global Overview of Spectrum Pricing Frameworks in Local Mobile Communication Networks*.

The paper recommends regulatory approaches that balance auction-based population density pricing (€/MHz/Pop) with localized models (€/MHz/km²), ensuring that business capability and willingness to pay are considered. By fostering accessible spectrum frameworks, regulators can strengthen the 3GPP ecosystem, enabling broader uptake, innovation, and sustainable deployment of next-generation networks.

The diversity of both the demand and supply of services and resources within mobile communication networks has increased. Meanwhile, the traffic distribution in volume and quality of service is uneven across geographic areas, indoors & outdoors and across time-of-the-day.

This may lead to inefficient spectrum and energy use if all cases are required to be covered by traditional macro cell based public land mobile network deployments. Location specific approaches are needed to complement the evolutionary approach grounded on the reuse of existing site infrastructure—with the end goal of delivering economically sustainable mobile broadband services to the end users.

Local 4G and 5G networks implemented by various stakeholders are serving the specialized needs of different user groups directly or serving mobile network operators' customers in specific locations. Specific regulatory frameworks for local and or private mobile communication networks are in place in around 52 countries. The characteristics of the selected spectrum regulatory model covering sharing framework, stakeholders, and pricing have a major impact on the feasibility and attractiveness of a deployment and business case.

The pricing of spectrum in the local mobile communications context is a complex and multifaced phenomenon emphasized and approached in different ways across markets and spectrum bands worldwide. Spectrum pricing models in regulation typically consist of the following elements:

- **Opportunity cost**
- **Location**
- **Frequency**
- **Service**
- **Area**
- **Bandwidth**

While the opening of the spectrum access market to new stakeholders and competition can improve efficiency, transparency, fairness, and simplicity, several market failure mechanisms have been found that are relevant for the spectrum pricing for local networks:

- **Information asymmetry**
- **Risk - related to business model and technology**
- **Externalities**
- **Monopolies**

Characteristics of Locally Licensed Spectrum Pricing

Spectrum pricing in the analyzed cases is based on the administrative incentive pricing model. From the data, it is obvious that the designated spectrum bands, pricing frameworks and price levels are country specific. In most frameworks, the annual fee is based on required bandwidth and size of the deployment area. Other parameters include extended area—where the required deployment area is extended with a specified distance margin—area type or classification, population in the deployment area, maximum transmit power, service type, number of base stations and number of user equipment as summarized in the below table.

Table: Parameters identified in different national pricing frameworks.

	Fixed fee	Bandwidth	Area	Ext Area	Area Class	Pop	Tx Power	Serv Type	BS nr	UE Nr
Australia n257, n258		x				x				
Canada n77,n257, n258,n260		x	x		x					
Czech Republic n78		x	x							
Denmark n78, n258		x	x	x						
Estonia n258	x									
Finland n40, n258		x				x				
France n38		x	x							
Germany n78, n258		x	x		x					
Hong Kong n261		x								
Ireland 10.5 GHz		x								
Japan n41, n79, n257, n261									x	x
Lesotho n7, n38		x								
Netherlands n78									x	
New Zealand n38, n78		x				x			x	
Norway n77		x					x			
Poland n77		x			x			x		
South Korea n79, n257		x	x		x					
Spain n40		x	x		x					
Sweden n78, n258		x								
Switzerland n78		x								
UK n3, n40	x									
UK n77, n258		x								
UK local access license	x									
UK offshore mobile license	x									

*Referenced Study: Ojanen, P., Yrjölä, S., & Matinmikko-Blue, M. (2025, May). Global Overview of Spectrum Pricing Frameworks in Local Mobile Communication Networks. In the IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN) (pp. 1-10). IEEE.

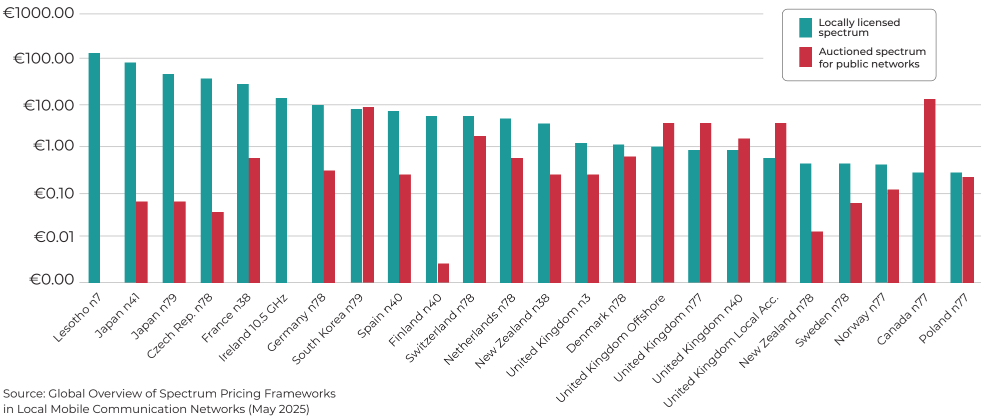
In some frameworks, the fee is fixed. The general price level is determined on a national basis by the local regulatory authority, based on various factors, including the spectrum supply and demand, certainty (sharing), spectrum price levels paid for spectrum for public mobile networks and overall goals related to national spectrum utilization policy.

Spectrum pricing frameworks were assessed by calculating annual spectrum fees for locally deployed networks utilizing sub-6 GHz spectrum bands. The parameters were selected for a typical industrial campus use case requiring 20-40 MHz of exclusive spectrum.

The annual fees of the locally deployed networks were also compared with the auction-based public mobile networks spectrum prices paid by mobile network operators. To compare the spectrum prices of locally deployed networks with the spectrum prices of nationwide public networks, the calculated annual fees are normalized to annual fees/MHz/km2.

The same is done for the auction prices addressing the same countries and as similar bands as possible for the locally deployed networks. If auction-based prices for the same bands are not available, prices in adjacent bands or bands in the same spectrum range are used.

Figure 1: Annual spectrum license fee (€/MHz/km.)



Source: Global Overview of Spectrum Pricing Frameworks in Local Mobile Communication Networks (May 2025)

Figure 1 shows that in 16 countries, the normalized spectrum price (€/MHz/km^2) for local networks in bands below 6 GHz is higher than the normalized price for the auctioned spectrum. In six countries, the price of the auctioned spectrum is higher. There are no auction prices available for Lesotho and for the 10 GHz band in Ireland. Japan has traditionally used administrative allocation instead of auctions for assigning spectrum to the mobile network operators. Therefore, the comparative spectrum prices are calculated from the annual fees.

The Discussion

The pricing frameworks were found to promote efficient utilization of spectrum resources in several ways. Pricing based on ***bandwidth*** is an incentive for avoiding reservation of unnecessarily wide bandwidths, thus improving the overall spectrum efficiency. Pricing depending on the ***deployment area*** acts as an incentive to reserve geographical area only for the area served, which can improve the overall geographical spectrum efficiency.

Different pricing for ***transmit power*** levels is an incentive for using lower transmit power and thus minimizing potential interferences, which can improve the overall spatial efficiency. Pricing based on the ***number of base stations*** may lead to technical and operational solutions aiming to minimize the number of base stations, instead of optimizing the spatial and frequency efficient use. Compared to the block license model, the ***device license*** approach may increase cost, which reduces infrastructure investments and results in inefficient use of assigned spectrum resources.

Regulated leasing aims to increase the overall spectrum utilization efficiency while facilitating spectrum access for local networks at reasonable cost through conditions defined by the regulator. The eligibility requirement related to ***property ownership*** or control can incentivize quality of service. Publicly available regulatory ***information*** facilitates transparency and fairness, mitigates principal and agent conflicts, and reduces transaction costs. The ***recurring payment*** model facilitates new business and encourages a licensee to continuously access the value created with the spectrum license holding.

Recommendations

Grounded on the findings of our study*, several recommendations on spectrum pricing can be made to stimulate the deployment of local mobile communication networks.

- ***Fairness and objectivity*** require level and fair treatment of the stakeholders and the objectivity of the fee characteristics and factors. Eligibility issues to be considered include the eligibility of private entities and mobile network operators for accessing the bands and their specific regulatory conditions, while avoiding potential spectrum hoarding and concentration.
- ***Administrative costs*** can be reduced via consistent, simple, and transparent allocation, assignment and pricing rules and processes.
- The ***public availability and transparency*** of the spectrum fee calculation basis is essential for the overall cost-benefit business case analysis.
- ***Certainty and foresight*** regarding the opportunity cost of spectrum supports economic sustainability. Certainty requires sufficiently long licensing periods or simple renewal mechanisms with long-term stability of the spectrum availability, required especially by industrial applications.
- ***Spectrum pricing*** should consider a balance between auctioned spectrum population density pricing (€/MHz/Pop) and a local use pricing and business actors' capability and willingness to pay. Long-term governmental objectives such innovation and sustainability can be promoted via free/affordable, timely available test licenses to explore problem-solution fit. Further research is needed to explore a proxy for the population density, such as the use of commercial rental prices.
- ***Quality*** of spectrum-related technical risk and potential interference when multiple networks need to be deployed in high-demand areas should be addressed in the future pricing models.
- ***Efficient and full utilization*** of the spectrum resources locally can be promoted via scalability and flexibility of the spectrum license conditions driven by typical local use cases and business models.
- Spectrum ***amount-based pricing*** enables operators to reduce their payments by adjusting their spectrum holdings based on need.
- Automated ***marketplaces*** could facilitate shorter-term assignments to stimulate reuse of unused spectrum resources and reduce transaction costs associated with spectrum sharing and/or trading.

IALA joins 3GPP as MRP

The International Organization for Marine Aids to Navigation (IALA), an intergovernmental organization dedicated to the promotion of safe, economic and efficient movement of vessels - through harmonised Marine Aids to Navigation, has joined 3GPP as a Market Representation Partner (MRP).

Since 2018, collaborative efforts have been increasing between 3GPP and IALA. Initially through the Rel-16 Maritime Communication Services over 3GPP system study (TR 22.819) and more recently during the discussions around and prioritization of 3GPP Rel-18 and Rel-19 features, with IALA participation as a 'vertical' industry representative.

The arrival of the coastal states' Ministries and Regional authorities, alongside their respective Industrial Members will help to ensure that Marine Aids to Navigation contributions are now driven even more effectively through 3GPP standards.

The 3GPP OP#54 meeting approved the MRP request from IALA unanimously, on November 14, 2025.

www.iala.int

IALA

RAN WGs in Bengaluru

The attendance at TSG RAN Working Group meetings, 25 – 29 August 2025, has been hailed as the largest standards meeting to have taken place in India, with over 1500 experts onsite, in person. Congratulations to TSDSI and DoT India on the event and their sustained engagement in the 3GPP 6G vision.

Running for good

There have been two charity runs in 2025, organised by the MCC's Emmanuelle Wurffel. The first was in Malta's Pembroke Natura 2000 parklands, after the close of the RAN group meetings on Wednesday, May 21.

This run in the sun raised over €7000 for **hospicemalta.org**.

The second run of the year took place in the early evening of Wednesday August 27, when delegates ran in memorial of Peter Hedman collecting over €10,000 for Hjärnfonden – A Swedish research body to which Peter was himself a regular donor (**https://www.hjarnfonden.se/**).

Broadcast show IBC features WG SA4

The leadership of 3GPP WG SA4 (Multimedia Codecs, Systems and Services) were recently under the spotlight at IBC2025, Amsterdam (Sept 12–15), with their presentation that covered a wide range of technologies, including:

- **Immersive Voice and Audio Services (IVAS)**
- **Next-Generation Audio & Video**
- **Advanced Media Delivery over 5G**
- **XR and Metaverse-Oriented Services**

These developments are part of 3GPP since Rel-18, enabling 5G Advanced media services to serve the TV industry.

Election update

2025 has been a year of Technical Specification Group and Working Group elections, with 17 of the 18 Chair positions and 30 of the 38 Vice-Chair posts decided this year.

Congratulations to our re-appointed and newly elected officials – For the next two years.

Setting the bar high for continuity was TSG RAN WG5 who appointed Jacob John for a sixth term as the group's Chair.

TSG				Role	Company
CT	**Plenary**	**Peter**	**Schmitt**	**Chair**	**Huawei**
		Hiroshi	Ishikawa	Vice-Chair	NTT DOCOMO
		Biao	Long	Vice-Chair	China Telecom
		Francois	Piroard	Vice-Chair	Airbus
CT	**WG1**	**Lena**	**Chaponniere**	**Chair**	**Qualcomm**
		Behrouz	Aghili	Vice-Chair	Apple
		Sung Hwan	Won	Vice-Chair	Nokia
CT	**WG3**	**Susana**	**Fernandez**	**Chair**	**Ericsson**
		Apostolos	Papageorgiou	Vice-Chair	Nokia
		Yue	Sun	Vice-Chair	China Telecom
CT	**WG4**	**Yue**	**Song**	**Chair**	**China Mobile**
		Anders	Askerup	Vice-Chair	Cisco Systems
		Zhijun	Li	Vice-Chair	ZTE
CT	**WG6**	**Heiko**	**Kruse**	**Chair**	**IDEMIA**
		Ly-Thanh	Phan	Vice-Chair	Thales
RAN	**Plenary**	**Younsun**	**Kim**	**Chair**	**Samsung**
		Enrico	Buracchini	Vice-Chair	Telecom Italia
		Jerome	Vogedes	Vice-Chair	T-Mobile
		Xutao	Zhou	Vice-Chair	vivo
RAN	**WG1**	**Xiaodong**	**Xu**	**Chair**	**CMDI**
		Sorour	Falahati	Vice-Chair	Ericsson
		Hiroki	Harada	Vice-Chair	NTT DOCOMO
RAN	**WG2**	**Diana**	**Pani**	**Chair**	**InterDigital**
		Kyeongin	Jeong	Vice-Chair	Samsung
		Erlin	Zeng	Vice-Chair	CATT
RAN	**WG3**	**Sean**	**Kelley**	**Chair**	**Nokia**
		Lixiang	Xu	Vice-Chair	Samsung
		Xudong	Yang	Vice-Chair	Huawei
RAN	**WG4**	**Yang**	**Tang**	**Chair**	**Apple Inc**
		Gene	Fong	Vice-Chair	Qualcomm
		Shan	Yang	Vice-Chair	China Telecom
RAN	**WG5**	**Jacob**	**John**	**Chair**	**Motorola Mobility**
		Xiaozhong	Chen	Vice-Chair	CATT
		Pradeep	Gowda	Vice-Chair	Qualcomm

He takes the record for longevity from Phil Brown, who served five terms from 2005 – 2012.

"Following on from Phil's long and fruitful Chairing of the group I did not expect to match that longevity. I feel that the continuity we have had in the RAN5 leadership serves this group very well. I am honoured to carry on, I never chased the record, but I am very proud to have been given a sixth term." Said Jacob John, WG RAN5 Chair.

An up-to-date list of all of the group Officials can be found at **https://www.3gpp.org/3gpp-groups**

Jacob John at RAN5#108

TSG				Role	Company
SA		**Puneet**	**Jain**	**Chair**	**Intel**
		Johannes	Achter	Vice-Chair	Deutsche Telekom
		Laeyoung	Kim	Vice-Chair	LG Elec.
		Tao	SUN	Vice-Chair	China Mobile
SA	**WG1**	**Vasil**	**Aleksiev**	**Chair**	**Deutsche Telekom**
		Yusuke	Nakano	Vice-Chair	KDDI Corp.
		QUN	WEI	Vice-Chair	China Unicom
		Feifei	Lou	Vice-Chair	Nokia
SA	WG2	Andy	Bennett	Chair	Samsung
		Dario Serafino	Tonesi	Vice-Chair	Qualcomm
		Wanqiang	Zhang	Vice-Chair	Huawei
SA	**WG3**	**Rajavelsamy**	**Rajadurai**	**Chair**	**Samsung**
		Marcus	Wong	Vice-Chair	OPPO
		Alf	Zugenmaier	Vice-Chair	NTT DOCOMO
SA	**WG4**	**Gilles**	**Teniou**	**Chair**	**Tencent**
		Mary-Luc	Champel	Vice-Chair	Xiaomi
		Tomas	Jansson	Vice-Chair	Ericsson
SA	**WG5**	**Lan**	**Zou**	**Chair**	**Huawei**
		Zhulia	Ayani	Vice-Chair	Ericsson
		Zhaoning	Wang	Vice-Chair	China Unicom
SA	**WG6**	**Atle**	**Monrad**	**Chair**	**InterDigital**
		Basavaraj (Basu)	Pattan	Vice-Chair	Samsung
		Jukka	Vialen	Vice-Chair	Airbus

NEWS

CALENDAR OF MEETINGS

Here is a snapshot of upcoming TSG (Bold) and WG meetings until the end of 2026

The 3GPP quarterly Technical Specification Group (TSG) plenary meetings (TSG CT, TSG RAN and TSG SA) are co-located over a one week period in March, June, September and December each year.

In the lead up to the plenaries, the Working Groups meet to make progress on the specifications and studies that will be approved at the TSG level.

The full calendar is online at: https://portal.3gpp.org

Meeting	Start date	City
Working Groups CT, SA and RAN	17-Nov-25	Dallas
Plenaries CT / RAN / SA - TSGs#110	**08-Dec-25**	**Baltimore**
Working Groups CT and SA	09-Feb-26	TBC - India
Working Groups RAN	09-Feb-26	Gotenborg
Working Group CT6	17-Feb-26	La Ciotat, FR
Plenaries CT / RAN / SA - TSGs #111	**09-Mar-26**	**Fukuoka**
Working Groups CT, SA and RAN	13-Apr-26	Malta
Working Group SA4	11-May-26	Montreal
Working Groups CT, SA and RAN	18-May-26	TBC - China
Plenaries CT / RAN / SA - TSGs #112	**08-Jun-26**	**Singapore**
Working Groups CT and SA	24-Aug-26	Prague
Working Groups RAN	24-Aug-26	Maastricht
Plenaries CT / RAN / SA - TSGs #113	**14-Sep-26**	**Madrid**
Working Groups CT and SA	12-Oct-26	Prague
Working Groups RAN	12-Oct-26	TBC - South Korea
Working Groups CT, SA and RAN	16-Nov-26	Calgary
Plenaries CT / RAN / SA - TSGs #114	07-Dec-26	Boston

ARIB atis CCSA ETSI tsdsi India's Telecom SDO TTA TIC Telecommunication Technology Committee

The 3rd Generation Partnership Project unites seven telecommunications standard development organizations, known as Organizational Partners, providing their members with a stable environment to produce the Reports and Specifications that define the 3GPP system.

- **856 Member Companies and Organizations**
- **176 Meetings in 2025**
- **27,000 Delegates registered for meetings in 2025**

A full listing of 3GPP Members is online at: www.3gpp.org/about-us/membership

TSGs#112

The 112th Plenary meetings will be held in Singapore, June 8-12, 2026. The meeting host, Keysight Technologies has recently sent the invitation letter to 3GPP delegates and registration is now open for the three TSGs' meetings to be held at the Sands Expo and Convention Centre.