Research Collaboration

Design of an FRMCS 5G E2E System for Future Rail Operation

Study Report

October 2021

Authors

Bastian Cellarius (Ericsson)
Richard Fritzsche (Digitale Schiene Deutschland, DB Netz)
Thorsten Lohmar (Ericsson)
Fang-Chun Kuo (Digitale Schiene Deutschland, DB Netz)

About Ericsson

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans the business areas Networks, Digital Services, Managed Services and Emerging Business. It is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's innovation investments have delivered the benefits of mobility and mobile broadband to billions of people globally. Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York. www.ericsson.com

About DB Netz

With more than 33,000 km of track, DB Netze Track operates the largest rail network in Europe. More than one billion train-path kilometers are traveled each year on the tracks in Germany. DB Netze Track is also responsible for managing infrastructure operations as well as for securing long-term infrastructure quality and availability, and non-discriminatory access to train-paths and service facilities. This includes preparing schedules in close cooperation with customers, operations management, construction management and maintenance. www.dbnetze.com

Contents

1 Introduction

Less traffic, less congestion, less particulate matter – and more people and more goods on the rails: The rail sector in Europe is on the verge of a technological leap into the digital future. The sector initiative "Digitale Schiene Deutschland" is taking advantage of this opportunity and bringing future technologies into the rail system. This benefits not only passengers, but also the climate and Germany as a business location. And all this without having to construct a single new track.

The foundation for this is being laid with the fundamental modernization and digitalization of the infrastructure through the consistent introduction of digital control and safety technology. In addition, Digitale Schiene Deutschland is working on a far-reaching digitalization of the railway system. For this, a system architecture will detail the tasks of individual components of the railway system, and how they should work together.

On this basis, numerous digital technologies will then be tested and further developed for use in the system: for example, an AI-based traffic and incident management system will provide intelligent and automated control of trains in the future. These will then run fully automatically and at an optimal distance from each other. The latest sensor technology for environment perception coupled with high-precision train location and an automated interruption detection are further technologies that will play an important role in the digitalization of the railway system. Overall, a significant improvement in capacity, punctuality and efficiency of the railway system will be achieved, all of which are requirements for more traffic on the railway and a strengthening of the railway as the climate friendly mode of transport of the future.

The rail system of the future will be characterized by data-intensive applications that must communicate with each other in real time. New connectivity and IT platforms are therefore necessary in order to achieve this goal. This study conducted by Ericsson and Deutsche Bahn (DB) within the sector initiative Digitale Schiene Deutschland (DSD), aims to investigate design aspects of an End-to-End (E2E) Future Railway Mobile Communication System (FRMCS) based on 5G technology, which is envisioned to enable digital rail operation by connecting train and trackside. FRMCS is seen as the successor of GSM-R (Global System for Mobile Communications – Railway), the current system in use. Beside the upcoming GSM-R obsolescence, digital rail operation is a key driver for the introduction of FRMCS due to its demanding requirements on connectivity. This study especially focusses on a selection of digital rail use cases, addressed by DSD, which introduces higher grades of automation into future rail operation. This study looks at various design aspects of FRMCS to serve the connectivity demands together with the current standardization status and further steps to be taken to make FRMCS ready for digital rail operation.

The FRMCS project has been initiated by the UIC (International Union of Railways), while ERA (European Railway Agency) has accepted the mandate by the European Commission for integrating FRMCS into the upcoming update of the TSI CCS (Technical Specification for Interoperability for Control Command and Signaling), which is expected for end of 2022. Within the FRMCS standardization process, basic documents have already been published, e.g., the User Requirements Specification (URS) [1] and the FRMCS Use Cases [2] as well as the ETSI (European Telecommunications Standards Institute) Study on System Architecture [3], working as a basis for this study. The documents System Requirement Specification (SRS) and Functional Requirement Specification (FRS) are in progress at the time of this study as well as several ETSI Technical Specifications (TS), which complement the FRMCS specification mainly based on 3GPP building blocks. This study aims to give insights about relevant 5G system design aspects and recommendations relevant for the FRMCS standardization (w.r.t. ETSI and 3GPP) and deployment options.

Assumptions on FRMCS and future rail operation use cases are presented in Section 0. A reference architecture is given in Section 3, followed by architecture options to be considered for FRMCS in Section 4. Section 5 comprises the analysis and findings and gives insights on open aspect.

2 The Future Rail Operation System

The future railway system shall benefit from several novel rail operation applications. Denser train scheduling shall be achieved by introducing automatically optimized planning and dispatching, technological evolutions of the train control system and fully automated train operation systems. Depending on the Grade of Automation (GoA), additional supporting applications are required , based on the tasks handled manually or automated at onboard, as shown in Table 2.1. More details on the different grades of automation can be found in [4].

Grade of Automation	Description
GoA0: on-sight train operation	manual driving without safety system
GoA1: non-automated train operation	manual driving of the train, with basic train control support
GoA2: semi-automatic train operation	starting and stopping is automated, but a driver operates the doors, drives the train if needed and handles emergencies
GoA3: driverless train operation	starting and stopping are automated but a train attendant operates the doors and drives the train in case of emergencies
GoA4: unattended train operation	starting and stopping, operation of doors and handling of emergencies are fully automated without any on-train staff

Table 2.1: Overview on Grades of Automation

Rail operation applications are envisioned to be situated at mobile and fixed locations within the railway ecosystem. At the trackside, centralized as well as distributed locations are assumed to be available for hosting applications. In addition, the railway infrastructure includes stations, locations for cellular Base Stations (BSs) and potentially centralized RAN (Radio Access Network) processing units. On the mobile side applications will be integrated at trains and via handhelds for mobile railway staff. In addition, the integration of non-3GPP access (e.g. Wireless LAN) as well as public mobile networks to complement the DB operated FRMCS system is considered. A schematic illustration of the overall rail operation system, as it is considered for this study is given in Figure 2.1.

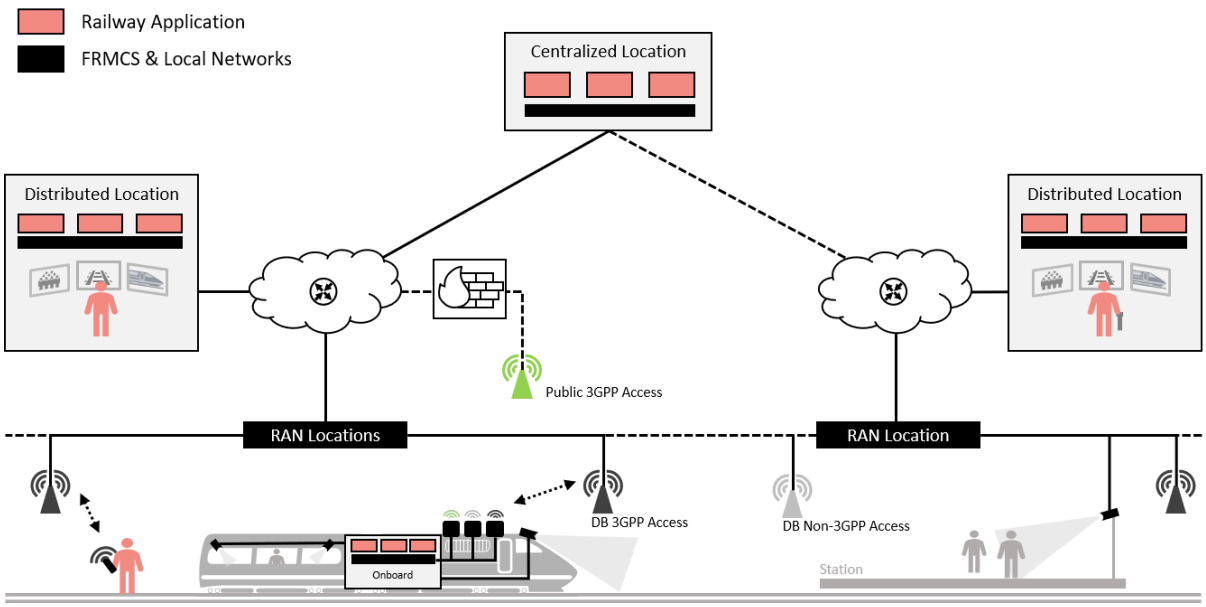

Figure 2.1: Overview of the Considered Rail Operation System

2.1 Use Cases & Requirements

For this study a selection of exemplary railway use cases is utilized for the considerations in the later sections of this report, in particular for analyses in the context of Quality of Service (QoS) management. For that purpose, the use cases Voice, ETCS, ATO, Remote Driving and Video Surveillance are described together with assumptions on the connectivity requirements. In general, this study targets towards fully automatic train operation, referring to GoA4 (see Table 2.1), even though train operation with lower degree of automation needs to be supported by FRMCS as well.

However, GoA4 operation raises more challenging requirements towards the mobile communication system, especially due to the transmission of video data. An overview on the requirements for the described applications w.r.t. data rate, latency and packet reliability are listed in Table 2.2. In there the packet reliability numbers are referring to the number of IP packets, successfully transmitted within the given latency. In addition, there is a general demand on service continuity, i.e., minimizing any interruption time while the train is moving among cells, edge data centers or national borders.

2.1.1 Voice Services

Voice Services are already implemented in the current GSM-R network. Even though, voice services are still present in GoA2 – GoA4 operation (e.g., for communication in incident and emergency cases), its portion on the overall rail operation communication can be assumed to be reduced due to data-based communication among automated entities. Voice communication can happen between various groups of railway personnel, e.g., dispatchers or controllers at the train operation centers, train drivers and maintenance workers at the tracks. The railway voice services comprise several features, e.g., functional and location dependent addressing, group call services, etc., which are assumed to be realized within the service stratum. However, voice related functionalities are not in the focus of this study.

2.1.2 European Train Control System (ETCS)

Today's rail operation is based on block-centric train protection systems, where axle counters are used to ensure that at one point in time only one train can be in a certain segment of track. In the future, a so-called ETCS Level 3 Moving Block approach is envisioned, which operates in a train-centric manner and allows trains to travel in minimum distance through the usage of train-based train integrity information and advanced train-based localization. From connectivity perspective, ETCS involves the signaling of location and train integrity information based on position reports sent from train to Radio Block Centers (RBC) or its evolutions located at trackside. In order to give the permission towards a train to enter a certain rail segment, a Movement Authority (MA) message is transmitted from the RBC. For advanced train-based localization, it is also required to signal digital map and GNSS correction data from track to train. ETCS related traffic is safety-related as the application is categorized as safety-critical. Even though, the safety-aspect is addressed by a dedicated safety layer within the application, its assumed that it’s not allowed to transmit ETCS via public networks. Note that the ETCS system is expected to evolve driven by DSD with more challenging requirements on the connectivity system.
The overall controlling system is typically deployed in a distributed fashion, where the RBCs are responsible for a limited area of the overall rail system of the Infrastructure Manager (IM). In case a train leaves the area of its current RBC and enters the area of a new RBC, an RBC handover needs to be performed. While in circuit switched GSM-R a dedicated modem is used to establish a connection to the new RBC, it is assumed that in FRMCS the connection to the new RBC might be based on a separate communication session using the same modem.

2.1.3 Automatic Train Operation (ATO)

The implementations of GoA2-GoA4 operation is based on the rail operation application ATO (automatic train operation), which is based on “Journey Profiles” including information about the driving behavior of the train. Journey Profiles are transmitted from the centralized ATO trackside system to the train. While the MAs for ETCS indicate the permitted driving behavior, the Journey Profiles are informing about the intended acceleration and breaking. Since Journey Profiles are influenced by the behavior of other trains

it is frequently updated, even though the update frequency is assumed to be below the one for MAs. The ATO trackside system gets information from the train via the status report. The automation functions rely on up-to-date maps and segment profiles including descriptions of the relevant rail segments. At the beginning of the journey, the train obtains the latest version of all relevant maps and segment profiles, which will be traversed during the journey. In addition, it can happen, that relevant updates become available while the journey already started or there is a change in the journey, which requires the download of further data.

2.1.4 Remote Driving

In GoA4 there is no staff on the train that would be able to drive the rolling stock in case of incidents. To provide the capability to still operate the train if automated operation is not possible, remote driving shall be implemented. In this case a remote driver is located, e.g., at a distributed operation center receiving video data from the train front camera (and potentially other cameras). Based on the video and audio data the driver can operate the train remotely on sight. The driver's train control information is transmitted back to the train. The control information I assumed to be transmitted frequently for safety reasons and to better detect transmission interruptions. The remote train driving operation is considered relevant only for train speeds below 40 km/h. Due to latency requirements its assumed that the remote-control system is deployed in distributed locations at specific remote operation centers. Crossing an area border shall result in a handover situation from one train driver to another. For a safe and smooth remote train operation, the remote driver might require multiple video streams in parallel, e.g., to get additional perspectives on relevant track segments as well as to assess the situation within the train.

2.1.5 Onboard Video Surveillance

Due to the reduced number of staff located at the train in above GoA2 operation, video surveillance becomes more relevant, to empower remote staff to identify and act on critical situations inside as well as outside the train. In such cases the remote staff is assumed to be located at a distributed location (e.g., an operation center) potentially co-located with remote operation centers. As can be seen in Table 2.2, the latency requirements in the video surveillance case are less strict compared to remote driving, as no immediate reaction of the remote staff is required. For an adequate assessment of incident situation, also for video surveillance it might be of interest to access multiple train cameras at the same time, for both inside and outside the train.

Use Case	Message Type	UL/DL	Data Rate	Latency	Packet Reliability
Voice	Audio	50/50	24 kbps	100 ms	99.9%
ETCS	Position Report	UL	10 kbps	100 ms	99.9999%
	Movement Authority	DL	10 kbps	100 ms	99.9999%
ATO	Journey Profile	DL	10-50 kbps	100 ms	99.9%
	Segment Profile	DL	100 kbps	1 s	99.9%
	Status Report	UL	1 kbps	100 ms	99.9%
Remote Driving	Video & Audio Stream	UL	1 – 7 Mbps	10 ms	99.9%
	Control Data	DL	10-100 kbps	10 ms	99.9999%
Video Surveillance	Video/Audio Stream	UL	1-7 Mbps	100 ms	99.9%

Table 2.2: Assumptions on requirements for selected rail operation use cases relevant for up to GoA4

2.2 FRMCS Architecture Assumptions

Rail operation use cases and its requirements have been analyzed by UIC and comprised in the documents [1] and [2] (including the applications of the previous chapter). The resulting FRMCS use cases, system principles and interworking aspects have been covered in TR 22.889 [5], the requirements for rail communications on the 5G system have been specified in the technical specification TS 22.289 [6]. To address the given demands, basic principles of the FRMCS architecture have been studied and presented in the ETSI TR 103 459 [3], which is seen as the basis for this study.

The high-level system architecture defines application stratum, service stratum and transport stratum (see Figure 2.2), while the latter two constitute FRMCS. The service stratum includes functionalities like identity and role management, security features, service session management and group communication services, while the transport stratum provides connectivity based on the indicated Quality of Service (QoS).

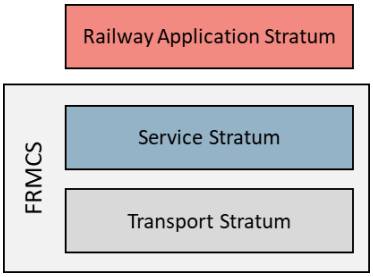

Figure 2.2: High-level FRMCS overview

As stated in [3], service stratum functionality is envisioned to be implemented via the Mission Critical services (MCX) framework on top of the 5G system specified by 3GPP. MCX has its origin in public safety verticals, while railway industry already contributed to the further evolvement for reflecting its requirements. A preliminary study on the architecture of FRMCS in 3GPP (including MCX) can be found in [7] and [8], further analyses are included in [3].

The FRMCS transport stratum concept includes a radio access technology (RAT) agnostic approach, assuming 3GPP 5G core for coordinating the utilized RATs. Especially the capability of using multiple radios (multiple RATs as well as multiple devices of the same RAT) simultaneously is one of the key FRMCS features. The multi-connectivity capability is envisioned to be used for realizing demanding requirements in various situations.

In this study it is assumed that the FRMCS trackside network is owned and operated by the infrastructure manager (IM) DB Netz. For the FRMCS onboard system it is assumed to be operated by the respective railway undertaking (RU), while the IM is able to provide specific configurations. For increasing service quality in dedicated scenarios, some railway applications might be allowed to additionally utilize public mobile network operator (MNO) infrastructure. In these cases, the multi-connectivity functionality of FRMCS provides the option to route data traffic between a train- and a trackside application via two or more parallel user equipments (UEs). More details on the assumed FRMCS architecture are illustrated in Figure 2.3. The functionality for employing multiple UE connections is integrated in the FRMCS Mobile Gateway at the train side, while the need of a corresponding functionality at the trackside is assumed to be subject to a particular solution. Note that the used technology for implementing multi-connectivity is not subject to this study, while an early analysis on candidate technologies has been provided in TR 103 459 [3].

In addition to the usage of multiple parallel connections, a single UE might provide multi-RAT capability itself via 3GPP and non-3GPP (N3G) access. This feature might be relevant for integrating additional WiFi-based connectivity in stations, e.g., for uploading or downloading data.

The FRMCS Service Server is assumed to be located centrally, while some of the railway applications will need to be deployed rather distributed due to low latency requirements (see previous chapter). In order to prevent that data is routed via the centralized service server, future solutions can be considered for allowing to route user traffic directly to the distributed locations. Note that redundant central service server concepts for increasing the reliability of FRMCS are out of scope of this document.

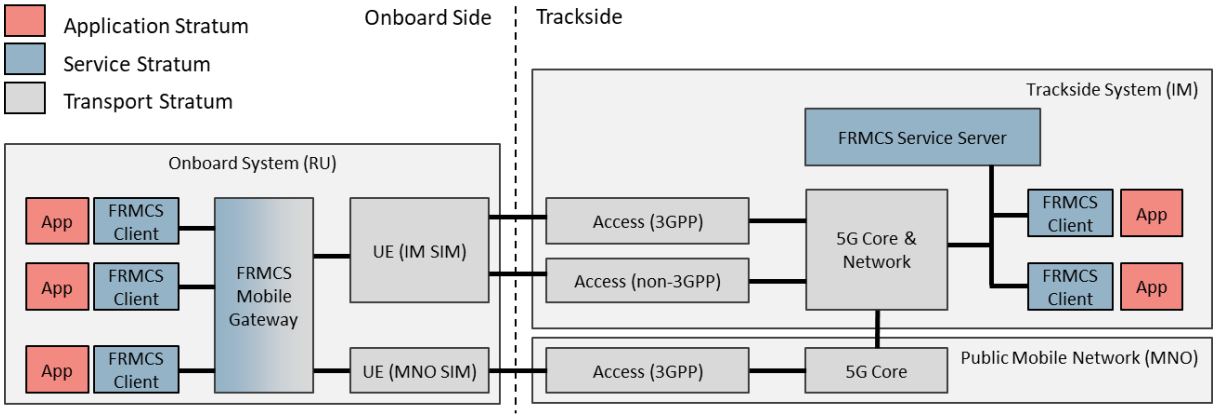

Figure 2.3: FRMCS architecture example (based on [3]), including the indication of the operators: railway undertaking (RU), infrastructure mamger (IM) and mobile network operator (MNO).

2.3 Spectrum and Radio Access Aspects

For the underlying DB infrastructure, the deployment of the cellular communication system as well as the radio spectrum are relevant for assumptions on the supported data rate. The target spectrum for rail operations in Europe is a 5.6 MHz band at 900 MHz (currently partially used for GSM-R) as well as a 10 MHz band at 1.9 GHz. The current available GSM-R spectrum slightly differs among European states, while in Germany the 4 MHz Band 876- 880 MHz (uplink) and 921- 925 MHz (downlink) is reserved and used for GSM-R, while 873-876 MHz (uplink) and 918-921 MHz (downlink) is usable for railways as well [9]. Here it is assumed that some of the radio towers of the current GSM-R can be used for FRMCS as well, while additional radio tower constructions might be required. For the 900 MHz spectrum and rural areas an average inter-site distance (ISD) of 8 km (4 km for the 1.9 GHz band), and for urban areas an ISD of 4 km (2 km for the 1.9 GHz band) is assumed.

3 Reference Architecture

This section introduces selected features of the 5G System (5GS) and the Mission Critical (MC) Framework. The basic user plane architecture and protocol stack, based on Section 2.1, is illustrated in Figure 3.1.

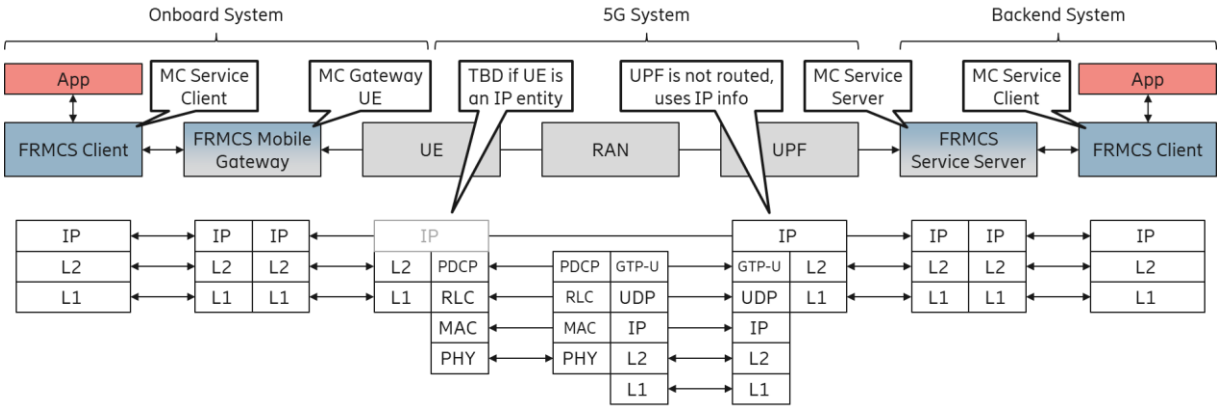

Figure 3.1: user plane architecture and protocol stack of an FRMCS System, comprised of Onboard, 5G, and Backend System.

The 5G System provides a UE with connectivity to a Data Network (DN) for interacting with endpoints in this DN, e.g. the FRMCS Service Server in these. Section 3.1 describes more details on selected 5GS features. In the FRMCS case, multiple applications, potentially running of multiple devices, use the same UE connectivity, summarized as the Onboard System in this case, and implemented using FRMCS clients (based on MC Service Clients from MCX) on the respective clients, and an FRMCS Mobile Gateway as interface to the UEs. The corresponding FRMCS gateway functionality is yet to be specified in UIC TOBA and related activities, e.g., on the MC Gateway UE work item (FS_MCGWUE [10]) in 3GPP SA6. Section 3.2 describes the architecture inside the train in more detail. Finally, the Backend System includes server-side applications with a corresponding FRMCS Client (again based on the MC Service Client from MCX), and an FRMCS Service Server, which among other things builds on an MC Service Server. The FRMCS Service Server acts as a distribution function for peer-to-peer and group calls (e.g. in MCPTT), and is required to always be in the path of user data in the current specification, but further work is planned to introduce UP/CP split for FRMCS. More details on the MCX Framework are described in Section 3.3.

3.1 5G System

In general, a 5G System provides IP connectivity to one or more Data Networks (DNs), identified by Data Network Names (DNNs). A Data Network can be any IP Network, such as an Enterprise Network (IntraNet) or access to the public Internet. In the railway scenario, a UE resides within a train and communicates with one or more Application Servers (ASs), which are hosted in a DN, as illustrated in Figure 3.2. In the FRMCS case, an AS can be the FRMCS Service Server, or the FRMCS Client if the FRMCS Service Server is not in the path.

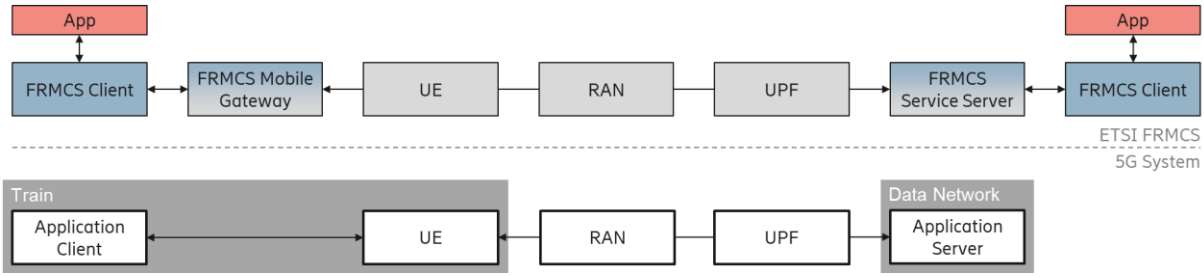

Figure 3.2: The 5G System – including RAN and UPF – connects a UE in the train with connectivity to data networks. Application clients and server use this connectivity to interact.

A train has to connect to Application Servers in different distributed locations during its journey, so the 5G System needs to offer the possibility to provide low latency connectivity to each location, requiring a distribution of multiple UPFs, and certain optimizations in roaming scenarios. Furthermore, the use of QoS is needed to maintain the connection quality required by safety-critical and real-time applications even in high load scenarios. Finally, applications on the train are connected to the 5G System via a Mobile Gateway, which uses one or more UEs for optimal connectivity (and UE redundancy). In complement to connectivity via a dedicated 5G System, additional UEs can be used to connect to public mobile networks.

3.1.1 Functional Architecture

The functional architecture of the 5G System is depicted in Figure 3.3 in service-based reference point representation. The service interfaces in the upper part of the figure (Nnssf, Nnef, etc.) are related to the control plane and are defined using the expected response for specific requests sent using HTTP, for different cases, such as accepting or declining a certain request. While all these interfaces are HTTP-based, the interfaces in the lower part of the figure (N1, N2, etc.), related to the user plane, use various other protocols.

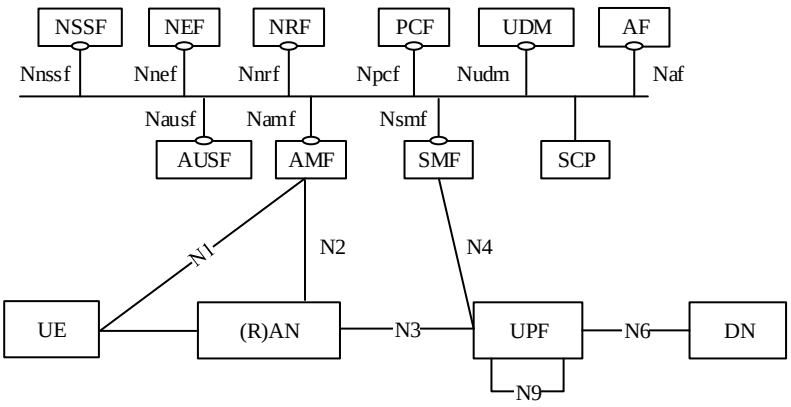

Figure 3.3: 5G System architecture – service-based reference points [11].

The 5G System architecture consists of the following network functions (NFs) and network entities:

- Authentication Server Function (AUSF)
- Access and Mobility Management Function (AMF)
- Data Network (DN), e.g. operator services, Internet access or 3rd party services
- Network Exposure Function (NEF)
- Network Repository Function (NRF)
- Network Slice Selection Function (NSSF)
- Policy Control Function (PCF)
- Session Management Function (SMF)
- Unified Data Management (UDM)

- User Plane Function (UPF)
- Application Function (AF)
- User Equipment (UE)
- (Radio) Access Network ((R)AN)

The AF and the DN are special entities in the sense that they are placeholders for external entities. A DN represents user plane endpoint that the 5GS provides connectivity to, and the AF represents an entity related to an application service offered via the 5GS and responsible for interacting with the 5GS.

Procedure-wise, a UE first follows a tune-in procedure to get radio connectivity, and then follows procedures for establishment of a PDU Session using Non-Access Stratum (NAS) signaling towards the AMF. Figure 3.4 shows a simplified signaling chart of the PDU Session Establishment procedure, where the SMF is responsible for most aspects around the session management policy, including the selection of a UPF and the QoS configuration. The full procedure is described in [12].[1]

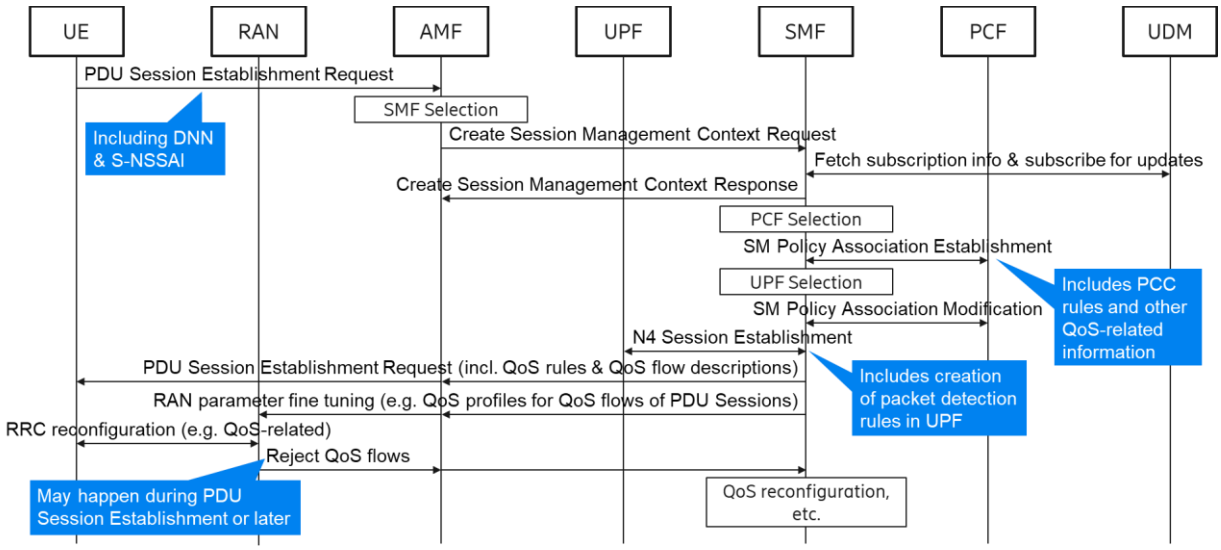

Figure 3.4: PDU Session Establishment procedure (simplified).[2]

During PDU Session establishment, some configurations are already established in different parts of the 5G System, and configuration updates are enabled, either by providing callback URIs (typical for the service-based interfaces), or by establishing bi-directional sessions (typical for the reference points such as N1, N2 and N4). A number of aspects are of particular interest in the scope of this document, which are configured during PDU Session establishment and/or later.

- IP assignment: each UE gets assigned an IP address[3] (per PDU Session) which can be used by communication endpoints in DNs to send IP packets to the UE. The IP is both an identifier on IP layer, and a routing destination. Details on Routing and IP assignment are discussed in Section 4.2.
- UPF selection: all communication between a UE and a communication endpoint outside the 5G System is routed via (at least) one UPF. The Session Management Function (SMF) selects an appropriate UPF for a given UE, based on various inputs such as the indicated Data Network Name (DNN), network slice (identified using a Single Network Slice Selection Assistance

[1] The PCF (and thus interactions with the PCF) is optional in 5GS but assumed to be present in the railway 5GS.
[2] When a QoS Flow is rejected by the RAN after PDU Session, and after the AF has requested a resource allocation (i.e. a QoS Flow to be established) with notifications enabled, the AF can be notified when a QoS Flow is rejected.
[3] To be precise, one IPv4 address and one IPv6 prefix can be assigned to a PDU Session, when dual stack is requested

Information (S-NSSAI)), and possibly the location of the UE in the network to select a UPF in close proximity, usually based on the tracking area of the UE. Details on UPF Selection are discussed in Section 4.1.

- Quality of Service (QoS): multiple QoS Flows might be configured for the UE already during PDU Session Establishment in the SMF based on control rules from Policy & Charging Function (PCF), in which case corresponding rules for traffic mapping and QoS enforcement are provisioned to the UE and to the UPF. Details on UPF Selection are discussed in Section 4.3.
- Mobility: A PDU Session is always anchored at a UPF, and re-anchoring the PDU Session at another UPF requires certain procedures. When moving in the network, the UE may benefit from re-anchoring the PDU Session, where different options are available, and the corresponding configuration is indicated to the UE during PDU Session Establishment. Different Mobility events are discussed in Section 4.5.

The 5G System described so far assumed that a UE is in its UE home country. When a UE moves across any relevant borders, it can connect to a visited network of a local MNO, when a roaming agreement exists between the two mobile operators. The visited network needs to interact with the home network in various ways, where different degrees of integration are possible. Most notably in the scope of this document, there are two fundamental ways on routing user data to and from roaming UEs.

In the home routing case, all data is routed via a home UPF (H-UPF) in the home network (HPLMN), in which case the visited UPF (V-UPF), where the PDU Session is anchored in the visited network (VPLMN), relays data between the UE and the H-UPF. Typically, the H-UPF is a designated UPF deployed in the home country, but in principle it's possible to deploy the H-UPF in a data center within the visited country.[1] The home routing architecture is depicted in Figure 3.5.

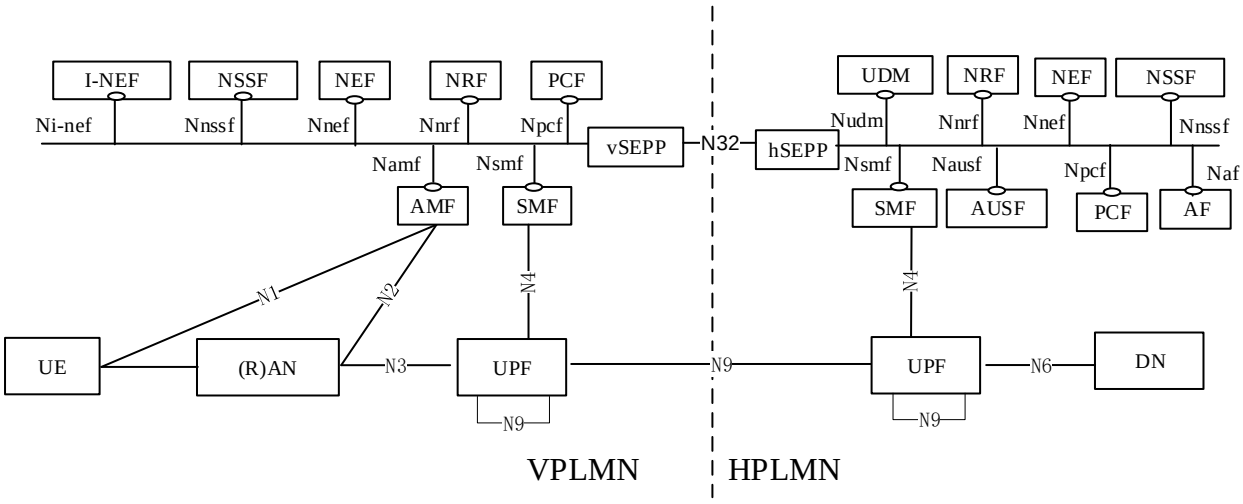

Figure 3.5: Home routing architecture [11].

All interactions between NFs in the HPLMN and NFs in the VPLMN have to pass a security edge protection proxy (SEPP) in each PLMN, which protects control messages, specifically protecting confidentiality and integrity. For configuring QoS for UEs in the VPLMN, interactions between V-SMF and H-SMF are specified so that it is still possible to configure QoS policies in the H-PCF, which the V-SMF only needs to authorize.

[1] The procedures related to configuring and setting up the routing path are quite extensive, but essentially the V-AMF fetches UE data from the V-UDM for the UE-indicated DNN and S-NSSAI, then the V-AMF can determine the H-SMF based on UE data as well as MNC and MCC in the DNN, and also select an H-SMF.

In the local breakout (LBO) case, user data leaves the visited network directly at the V-UPF, only the control plane of the home network is involved with the UE during roaming. The local breakout architecture is depicted in Figure 3.6.

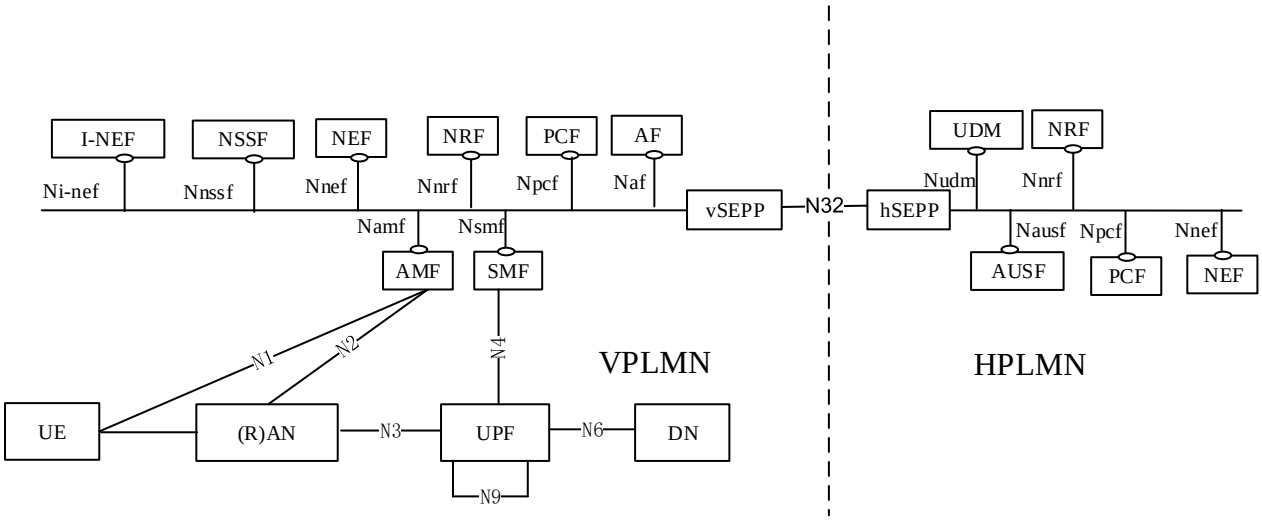

Figure 3.6: Local Breakout in the visited network [11].

All interactions between NFs in the HPLMN and NFs in the VPLMN have to pass a security edge protection proxy (SEPP) in each PLMN, which protects control messages, specifically protecting confidentiality and integrity as well as hides topology on the inter-PLMN interfaces. Configuration of QoS for UEs in the VPLMN can only be done by the V-PCF. There are no interfaces defined to configure QoS (directly or indirectly) from the HPLMN through the 5GC. However, the H-PCF can of course act as an AF towards the V-PCF and influence QoS configuration via Npcf (quite limited capabilities to describe QoS requirements) or use proprietary interactions between V-PCF and H-PCF if needed.

3.1.2 Deployment Architecture

This section describes a high-level deployment concept with assumptions based on the use cases and requirements in Section 0. A real deployment might look different, the purpose here is to provide an understanding of the deployment vision.

For an optimized RAN deployment, fiber infrastructure is already available along a lot of rail tracks, and further build-out is planned. The envisioned RAN deployment is a mix of

1. “baseband hotels”, where baseband units (BBUs) will be aggregated in C-RAN Main Sites, connected to radio heads on the masts via fronthaul, and
2. Stand-alone radio modules (i.e. incl. BBUs) at radio masts.

The maximum recommended fronthaul fiber distance is 15 km, motivated by a maximum fronthaul latency of 100µs given in [13] and deducting 25µs for processing plus safety margin. As the fronthaul is an optical link, a fiber dedicated to fronthaul traffic is needed for connecting one or more radio sites. Multiple radio sites can be connected over the same fiber using Wavelength Division Multiplexing. The complete setup is illustrated in Figure 3.7.

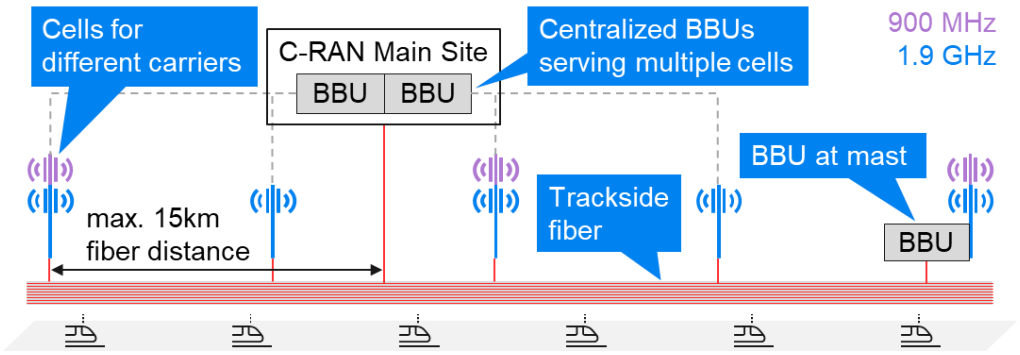

Figure 3.7: Assumed RAN Deployment Architecture for 5GS.

These baseband hotels can typically be installed in outdoor cabinets with limited security mechanisms (difficult to access data directly in the BBUs). For deploying core network functions and application servers, stronger security requirements have to be met, which is why the envisioned deployment targets re-use of existing computing facilities and built-out of additional computing facilities only where necessary due to high operational cost.

3.1.3 Discussion

For the foreseen deployment of the DB-operated 5G Core – as well as the Mission Critical System and the Trackside applications – the deployment assumptions are:

- 10-100 distributed compute sites, which would correspond to a maximum fiber distance of approx. 50 – 200 kms between any RAN site and a compute site
- A central site (including geo-redundancy)

All the different sites are assumed to have excellent fiber connectivity, with an MPLS-based transport system for interconnecting the sites, so that there is no significant transport latency aside from the propagation delay (approx. 1ms per 200km fiber). Each edge compute site contains a UPF and edge compute sites might also contain an SMF and an AMF. The advantage would be to be independent of the link-stability between the distributed site and the central site. However, with fiber infrastructure to inter-connect the different compute sites, this is likely not an issue, especially when deploying a dual link backhaul.

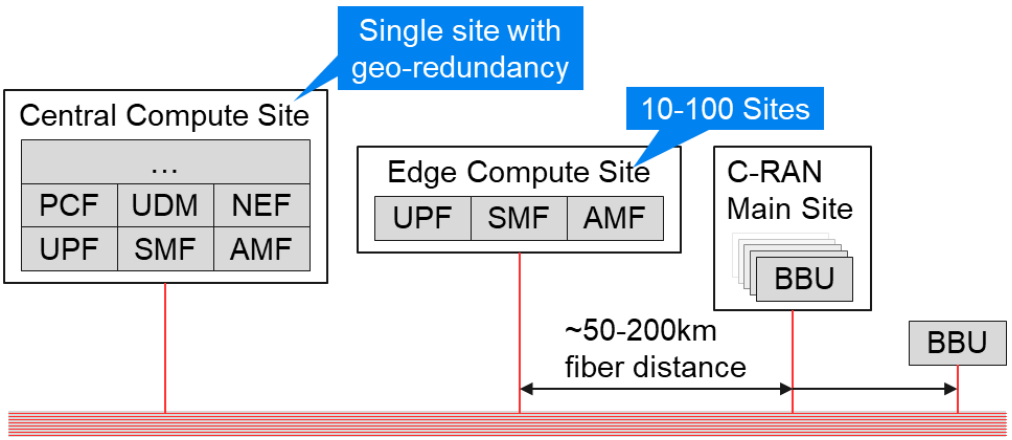

Figure 3.8: Assumed Core Deployment Architecture for 5GS.

When crossing country borders, the UE will attach to a RAN of a locally deployed network, roam into that network. For optimizing the communication path between a UE in the visited country and an application server in the same visited country, it should be avoided to route all data through a UPF in the home country (typical home routing roaming scenario). There are three approaches to optimize this.

1. Use a local breakout in the visited network, where the V-UPF acts as PDU Session anchor and all data leaves the 5GC directly from this V-UPF. This option is resource-efficient but suffers from some complexity if connections are metered, i.e. UEs are supposed to be charged based on consumed data. Furthermore, this option offers limited possibilities to control QoS policies in of UEs in the visited network from the home network.
2. Use home routing, but physically deploy H-UPFs in the visited country, possibly sharing physical infrastructure with the network operator of the visited country to host VNFs. This option is very simple but has a significant deployment overhead.
3. Avoid having national core networks, and instead establish a European core network, potentially with separate network slices corresponding to the respective home countries of UEs. This option avoids all the typical roaming issues but would require much more detailed investigation. Certainly, the responsibility of RAN management would need to be clarified.

Due to the distributed setup and the cross-country movement of trains, different types of hand overs between serving instances in the network are foreseen, as illustrated in Figure 3.9. The various optimization options for these handovers are discussed in Section 4.5.

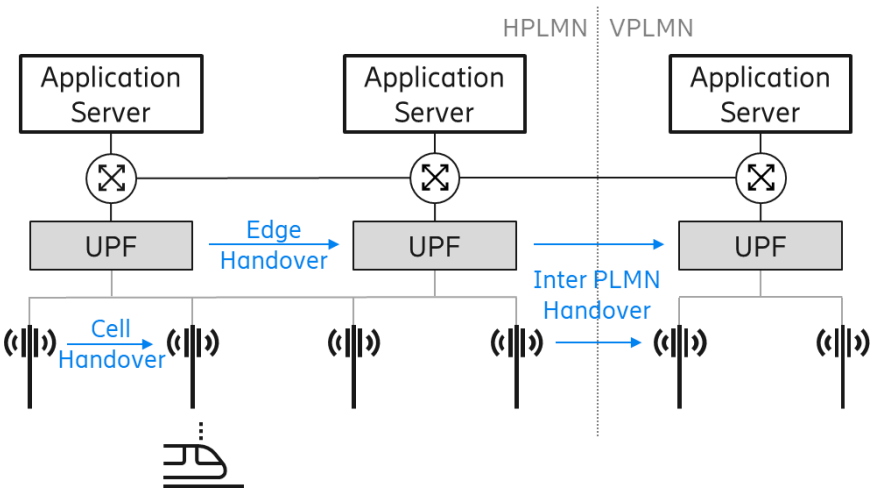

Figure 3.9: Mobility scenarios for 5G-connected trains.

3.2 Onboard Architecture

Inside a train, a number of connectivity options are available. First of all, connectivity to the dedicated railway 5G System is assumed to be available via more than one UE (redundancy against UE failures). Furthermore, connectivity to public networks (5G or other generations) can be used in complement for less critical use cases (e.g. ATO or video surveillance). Finally, dedicated WiFi for FRMCS can be used as complimentary data link at stations and depots . The FRMCS Mobile Gateway manages connectivity via all these links, and in return connects to devices distributed throughout the train.[1] The GW and devices are connected to a common LAN using a bus system on the train, and completely separated from connectivity infrastructure designated to passenger connectivity. This setup is depicted in Figure 3.10.

[1] If ATSSS (see Section 4.4.2) is used, some traffic steering needs to be done in the UE instead of the FRMCS Mobile GW, and a mechanism is required to control this from the FRMCS Mobile GW which has the overall traffic steering responsibility.

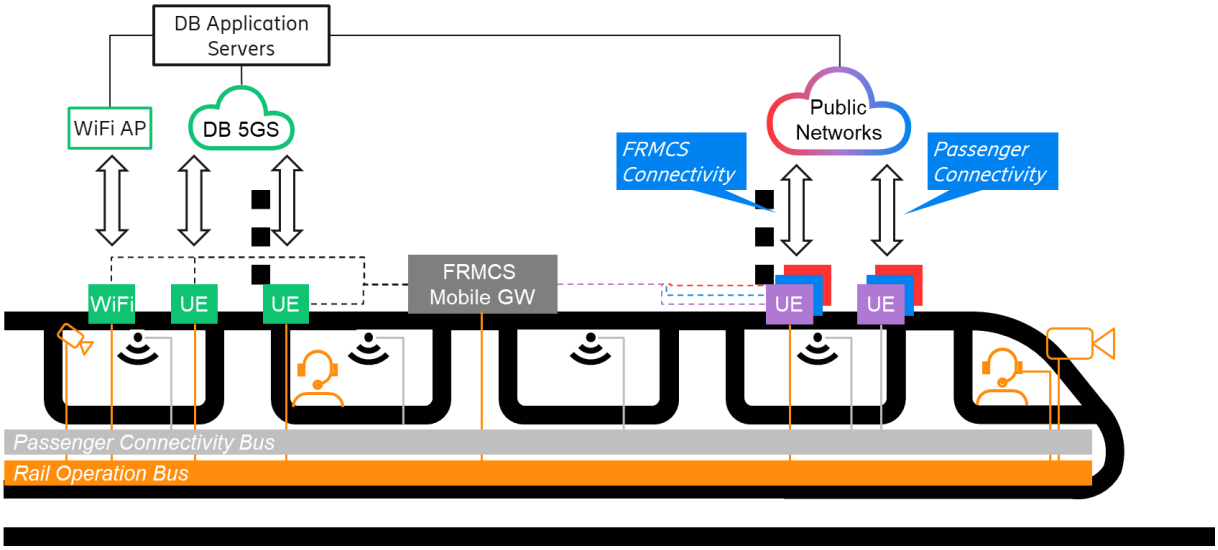

Figure 3.10: High-level architecture of connectivity inside a train, and connectivity to external networks (devices on the train are exemplary).[1]

Figure 3.11 illustrates the connectivity between devices on the train, each containing one or more applications, which again use FRMCS Clients for connectivity via MC Services.[2]. Distinct IP addresses are assigned to the devices, and the FRMCS Mobile Gateway is defined as gateway inside the LAN, i.e. all IP packets are routed to this default gateway (further discussed in Section 4.2). The FRMCS Mobile Gateway then decides where to forward the IP packet, e.g. via 5GS using one of the available modems. In typical setups, a UE (in the form of a modem) is controlled by a device connect via USB or PCI (e.g. smartphones or cars), using a standardized interface for monitoring and controlling the connectivity to some extent.

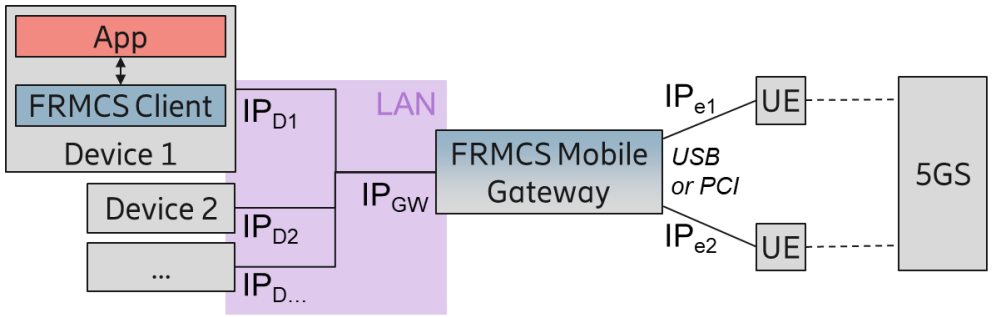

Figure 3.11: Connectivity inside the train using a typical setup.

For the sake of flexibility, UEs might be part of a separate "Mobile Radio" with an ethernet-based connection to the FRMCS Mobile Gateway, allowing a wider distribution of UEs on the train, as illustrated in Figure 3.12. To this end, an IP-based link (e.g. dedicated VLAN on top of the existing physical infrastructure) to each Mobile Radio would be needed.[3] However, further problems arise by separating modem control (in the Mobile Radios) and connectivity decisions and gateway functionality (in the FRMCS Mobile Gateway). Mobile Radios and FRMCS Mobile Gateway would need to exchange a lot

[1] In the figure, WiFi and UE are depicted as two separate entities connected to the rail operation bus. However, integrated WiFi+5GS devices are quite common, and might be used as well.
[2] The FRMCS Client might run on the device with the application, or on the FRMCS Mobile Gateway. In the following, we assume the former case for simplicity.
[3] This requirement comes from link limitations of PCIe (< 1 meter) and USB (~3 meters, with some options to extend range with repeaters etc.), while Ethernet works well for distances of up to 100 meters and can easily be extended. Furthermore, it needs to be studied further whether e.g. a pure ethernet link is preferrable over an IP link in this scenario.

of information for monitoring the connectivity status and controlling the connectivity. If the Mobile Radio units should be “plug-and-play”, such information cannot simply be forwarded between Mobile Radio and FRMCS Mobile Gateway, but significant study and specification work would be needed.[1]

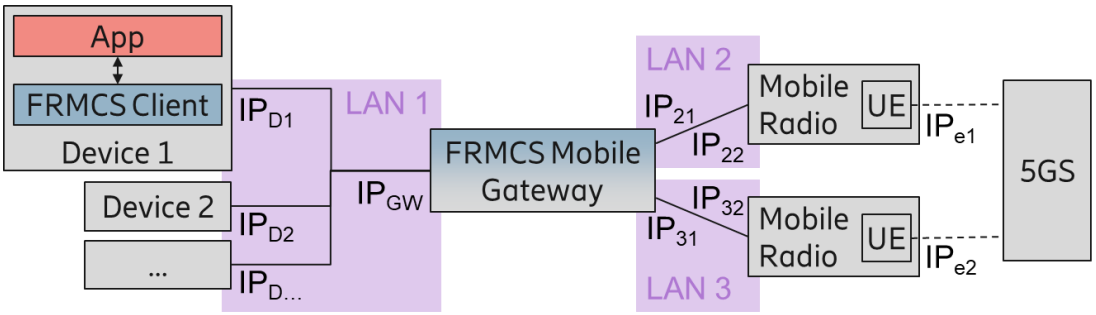

Figure 3.12: Basic connectivity inside a train with multiple UEs.

In a real deployment, several levels of redundancy are foreseen. A lot of deployment options are possible, one of which is depicted in Figure 3.13.[2] This setup includes redundant LANs, each going to an FRMCS Mobile Gateway, both of which would operate in a master-slave setup. Each GW uses (at least) one Mobile Radio for external connectivity but can use Mobile Radios connected to the other GW using a dedicated LAN, either as fallback or complimentary. Different LANs may run as different VLANs on shared infrastructure (e.g. cabling), but for optimal redundancy, at least some LANs should run on different infrastructure, e.g. LAN 1 and 4 on a different infrastructure than LAN 2 and 5.

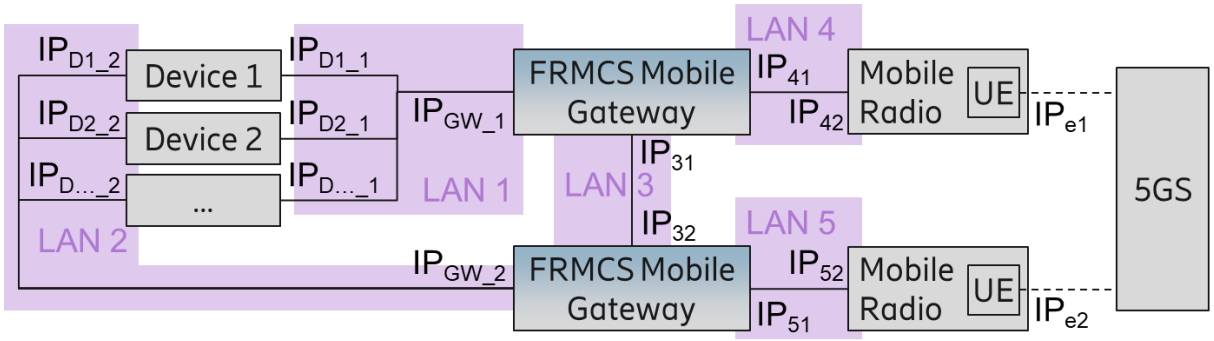

Figure 3.13: Connectivity inside a train with multiple UEs, gateways, and connectivity infrastructure.

3.3 Mission Critical Services

3GPP has specified a functional architecture for the support of mission critical (MC) communications and services over 3GPP networks in recent years, starting with voice communication (mission critical push-to-talk, MCPTT), and later added MCVideo and MCData, as specified in 3GPP TS 23.280 [14], TS 23.281 [15], TS 23.282 [16], and TS 23.379 [17]. The specifications of mission critical services have been initially defined to address public safety use cases but have been later enhanced to include support for railway communications. The support of MCX services has mainly been specified based on the Evolved Packet System (EPS, 4G). This includes interactions with the Evolved Packet Core (EPC) for the management of MCX service resources, e.g. addressing QoS related aspects. However, the support of MCX services over the 5G system is not specified yet. For that, the ongoing study 3GPP TR 23.783 [18] is in progress and it is expected that an initial normative work will be complete by the end of 3GPP

[1] Modems can be controlled using standardized AT-commands, or using more feature-rich proprietary libraries, with dependencies on the operating system using the modem. This makes it difficult to simply relay control to another device for remote control of the connectivity.
[2] If the modem is connected to the FRMCS Mobile GW via USB (which might be feasible in this case), this would also solve the remote connectivity control issue from the previous setup.

Release 17 and continue in Release 18 and later releases. The normative stage 2 work for unicast communication only is already stable and specified in TS 23.289 [19].[1]

MCX specifications include procedures for session initiation, where one MC service client (a "caller") initiates a session with an MC service server, and the MC service server initiates a session with one or more MC service clients (a "callee"), which is why the MC services specifications are usually written separately for the caller and the callee. In the current MCX specifications, an MC service client always sits on a UE. In ETSI FRMCS, the vision is to also have MC service clients behind an MC gateway UE. The assumption is that the MC Gateway UE will contain similar functions like home-router platforms, e.g. a SIP Application Layer Gateway (ALG) as further discussed in Section 4.2, user plane proxy functions and maybe some MCX specific functions. 3GPP SA6 working group has started working on a Release 18 study item to address MC gateway UE aspects, as described in 3GPP TR 23.700-79 [10]. It is expected that the normative work specifying the MC gateway UE functionality will be complete by the end of Release 18. 3GPP Release 18 timeline has not been defined yet, but it is expected to be complete in 2023. Also, for interaction with trackside applications, an MC service client is deployed in fixed infrastructure, without a mobile UE. This architecture is illustrated in Figure 3.14, including the relation to the FRMCS components.

MCPTT and MCData are explained in some more detail in the following sections. MCVideo is quite similar to MCPTT. Note that a single MC UE cannot have multiple sessions of the same type (e.g. MCPTT) in parallel, in the current specification.

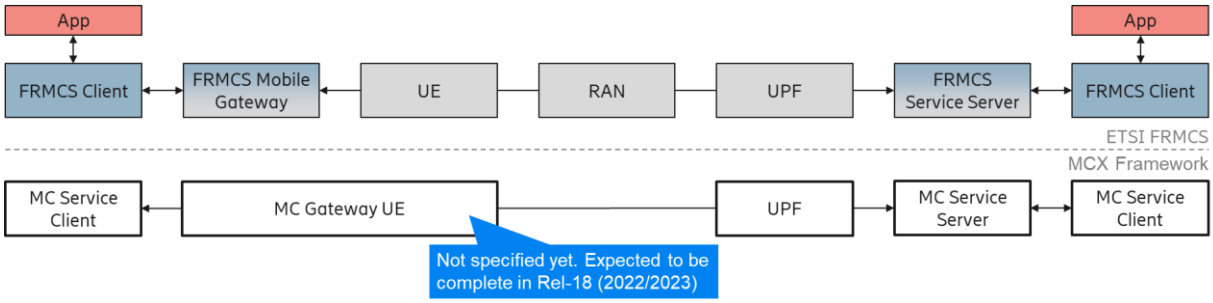

Figure 3.14: MC architecture envisioned for ETSI FRMCS.

3.3.1 Session Initiation

MC service clients interact with a SIP core to initiate a session (cf. Figure 3.15). Procedure-wise, the MC service clients sends an SDP offer via the SIP core to the MC Service Server, which contains a description of the initiated session (listening port, media type, etc.). The MC gateway UE needs to re-write some parts of the SDP, e.g. because a different port is opened on the MC gateway UE than on the MC service client if Network Address Translation (NAT) or an Application Layer Gateway (ALG) are used, further described in Section 4.2. After receiving the SDP offer, the MC Service Server replies with an SDP answer, including information on the MC service server side of the communication. The SIP Core may interact with the PCF for adapting the QoS configuration for the initiated session[2]. Finally, the SIP core might send SDP offers to one or more callees, using basically the same procedure with reverse roles for MC service client and SIP core. The full procedure is depicted in Figure 3.16.

[1] Interactions with the PCF are likely similar to interactions with the PCRF in EPS, as the Rx interface of PCRF is also supported by PCF, and the N5 interface of PCF is basically a service-based, restful, extended version of the Rx interface.
[2] Instead of the SIP core, the MC service server may interact with the PCF for adapting the QoS configuration. This is a deployment choice.

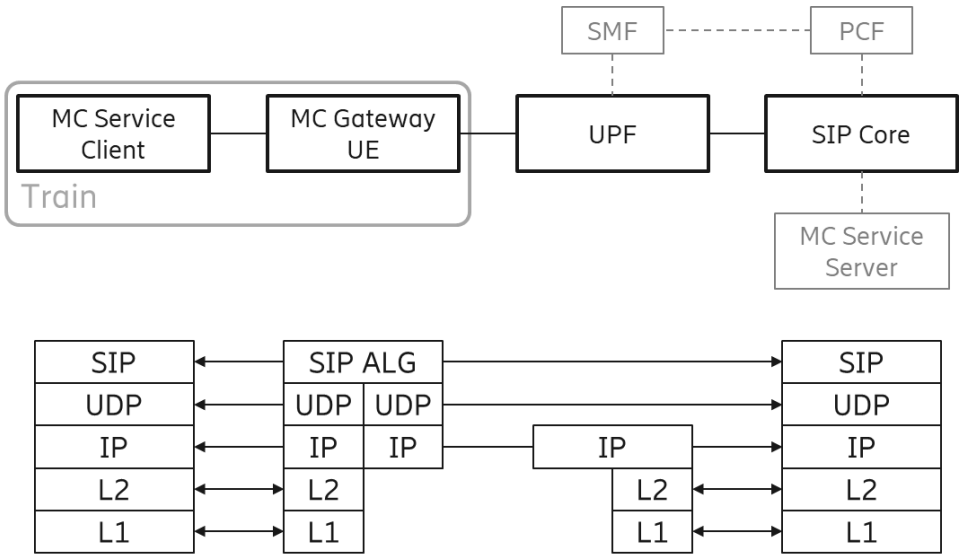

Figure 3.15: Protocol stack for session initiation between MC service client and SIP core, assuming an ALG in the MC Gateway UE.

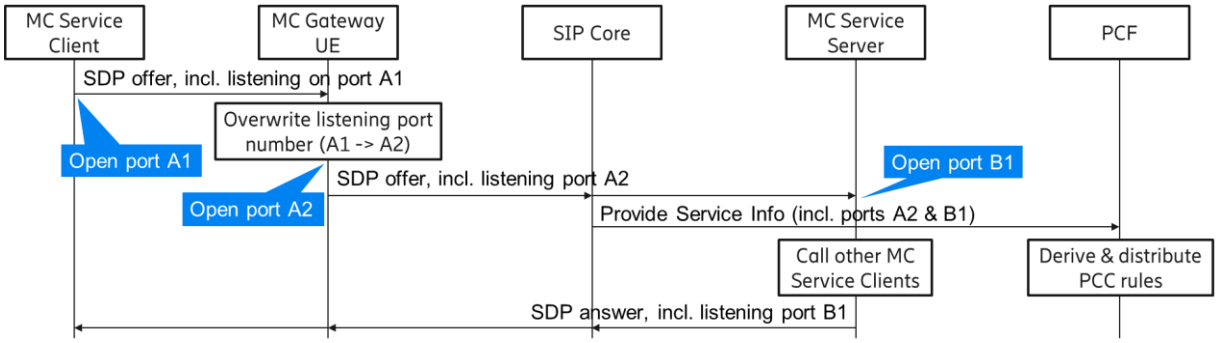

Figure 3.16: Session initiation procedures.

If corresponding functionality from IMS is brought into MCX, it will be possible to set up peer-to-peer connectivity between two MC Service Clients, as explained in Section 3.3.3.

3.3.2 MCPTT

Mission critical push-to-talk (MCPTT) enables voice communication between two (peer-to-peer calls) or more (group communication) MCPTT clients, where the MCPTT server is responsible for establishing sessions with all involved MCPTT clients, as well as distributing media between involved MCPTT clients, as described in 3GPP TS 23.379 [17]. The general MCPTT architecture is depicted in Figure 3.17.

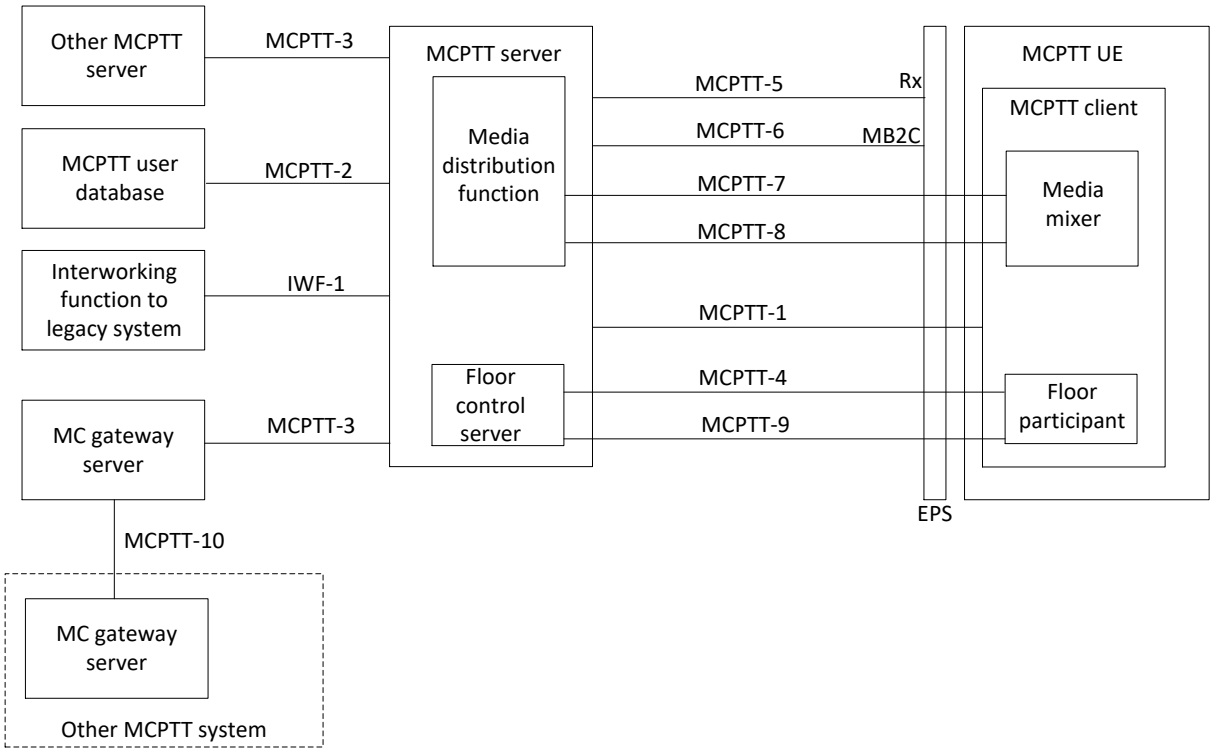

Figure 3.17: Generic application plane functional model for MCPTT [17].

For the voice services use case described in Section 2.1, MCPTT can be used as illustrated in Figure 3.18.

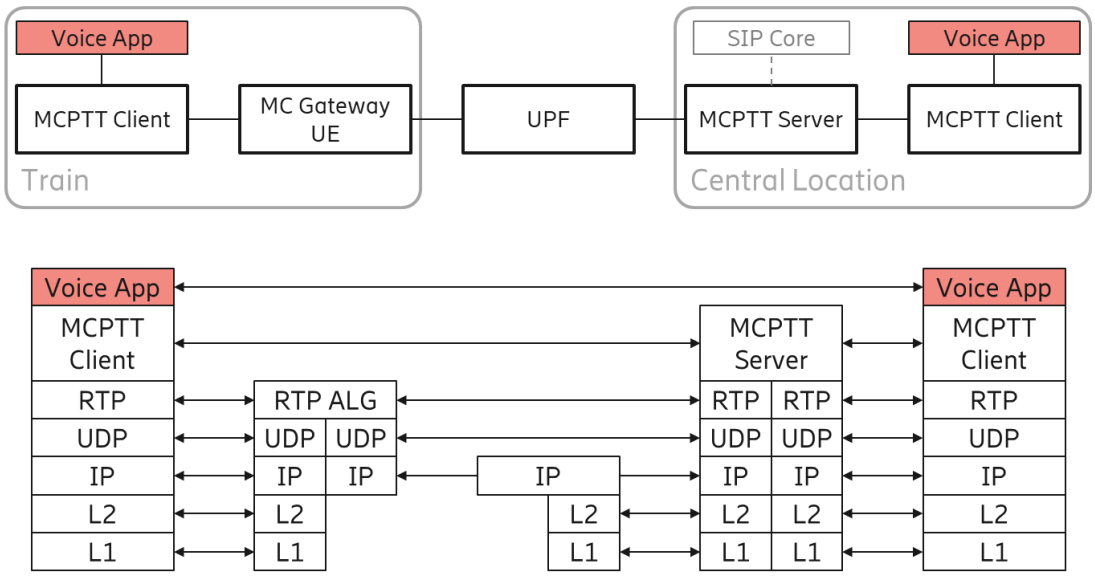

Figure 3.18: Protocol stack when using MCPTT for railway voice services, assuming an ALG in the MC Gateway UE.

3.3.3 MCData

The general MCData architecture, as specified in 3GPP TS 23.282 [16], is depicted in Figure 3.19. The MCData Server supports four different MCData realizations:

- Short Data Service (SDS): The SDS capability shall support messages with a payload of at least 1000 bytes.

- File Delivery (FD): The MCData service shall allow the MCData user to send a file or a URL of a file to another MCData user.
- Data Streaming (DS): The MCData service shall allow the MCData user to send a data stream or a URL of a data stream to another MCData user.
- IP connectivity (IPcon): IP connectivity service enables the exchange of IP Data using MCData transport service and provides the transport of IP Data for e.g. data hosts, servers, etc. that do not have mission critical communication capabilities. The exchange of IP Data is not limited in a transaction.

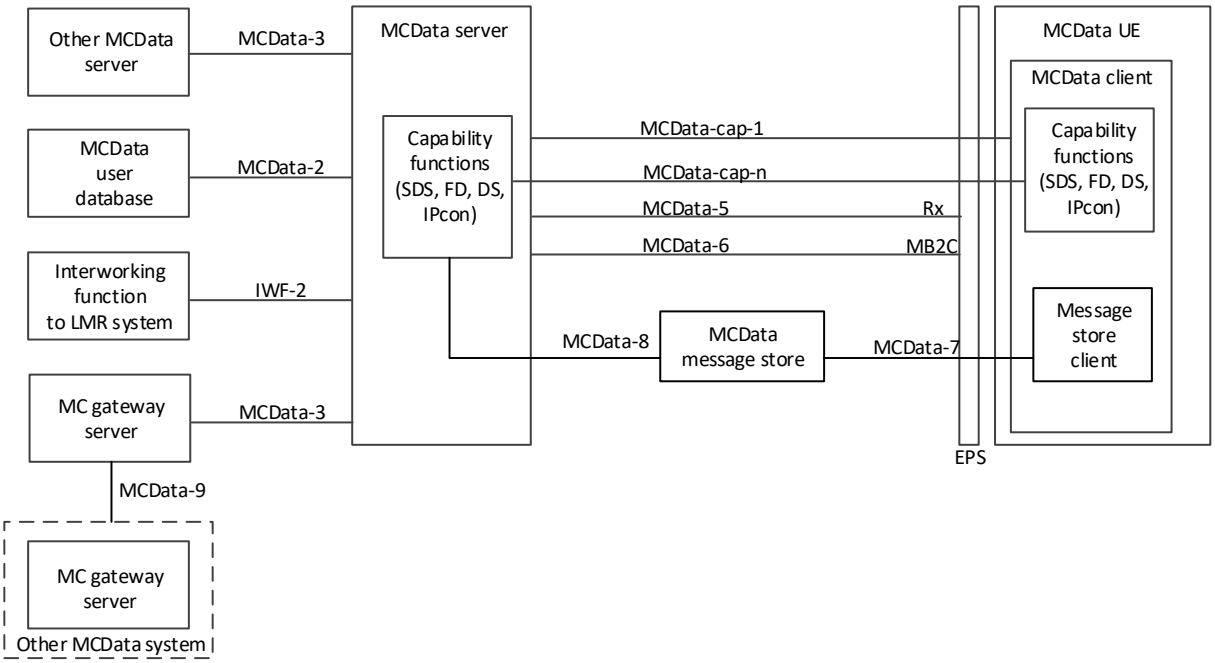

Figure 3.19: Generic application plane functional model for MCData [16].

While DS was introduced to enable exchange of data between two or more MC Data users, IPcon instead enables exchange of data between two or more data hosts, which are normally only accessible through an MC Data client. For FRMCS, the usage of IPcon is of interest for use cases such as ETCS or remote train operations, which require low latency peer-to-peer communication between train and trackside for short messaging type of communication.

The intention of IPcon is the establishment of a generic IP pipe between two MCData clients with specified QoS.

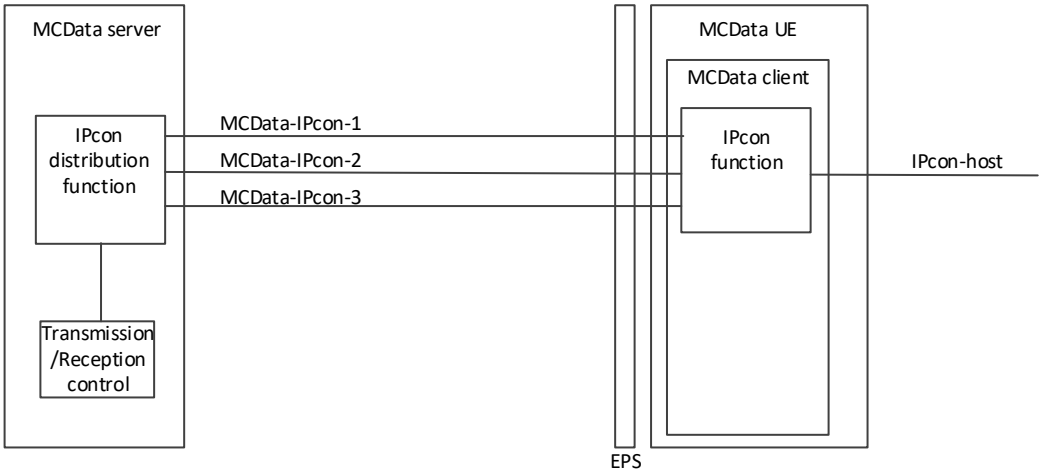

Figure 3.20: Application plane functional model for IP connectivity [16].

- MCData-IPcon-1 reference point is used for MCData application signalling for establishing a session in support of MCData IP connectivity.
- MCData-IPcon-2 reference point carries bidirectional IP Data for point-to-point MCData IP connectivity over the media plane between the U-IPcon distribution function of the MCData server and the IPcon function of the MCData client(s).
- MCData-IPcon-3 reference point is used by the IP-con distribution function of the MCData server to send unidirectional downlink IP Data to the IP-con function of the MCData clients.

The general model is depicted below. Note, special care is needed for terminology usage. A “Server” (see right most box in the figure below) should not be confused with the “MCData Server”. The “Data host” represents the client in normal client server transaction models. IPcon realizes a transparent pipe, similar to the IMS Data channel. Further note, that the MCData transport service (figure below) includes the MC Service Server, as depicted in Figure 3.20.

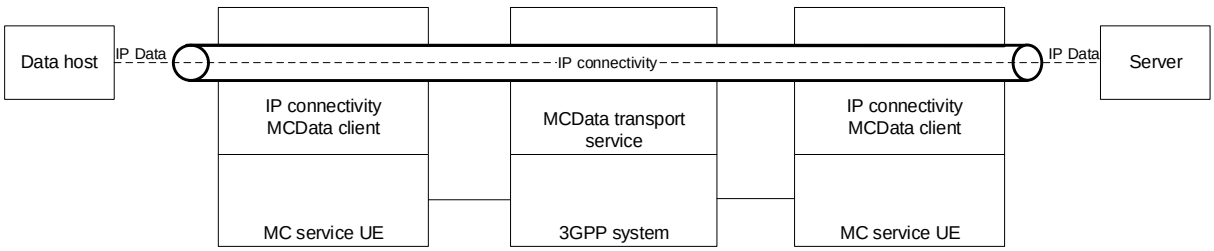

Figure 3.21: Deployment of IP connectivity [16].

In the current specification, the MCData Server is always in the communication path between two MCData clients. ETSI FRMCS intends to support direct communication between MCData clients, for which further study and specification in 3GPP SA6 is required. Note, the MC Service Server combines user plane and control plane into one function. Thus, deployments with distributed MC Service Servers need to consider the distributed control plane. However, further specification work may allow a CP/UP split of MC Service Servers in the future.

There are several possibilities how MCData IPcon can be used by MCData Clients on the onboard LAN of a train. One example making use of the MC service UE is depicted in Figure 3.22, where the MC Gateway UE acts either as router, and potentially as NAT or ALG to allow communication between an MCData Client on the train and an MCData Client on the trackside. Another example, working without an MC Gateway UE, is depicted in Figure 3.23, where the MCData Client sits on the UE and relays IP data to a Data Host via the onboard LAN. It needs to be studied further, which variant is most feasible, especially with the upcoming progress in 3GPP SA6 in scope of the MC Gateway UE WI.

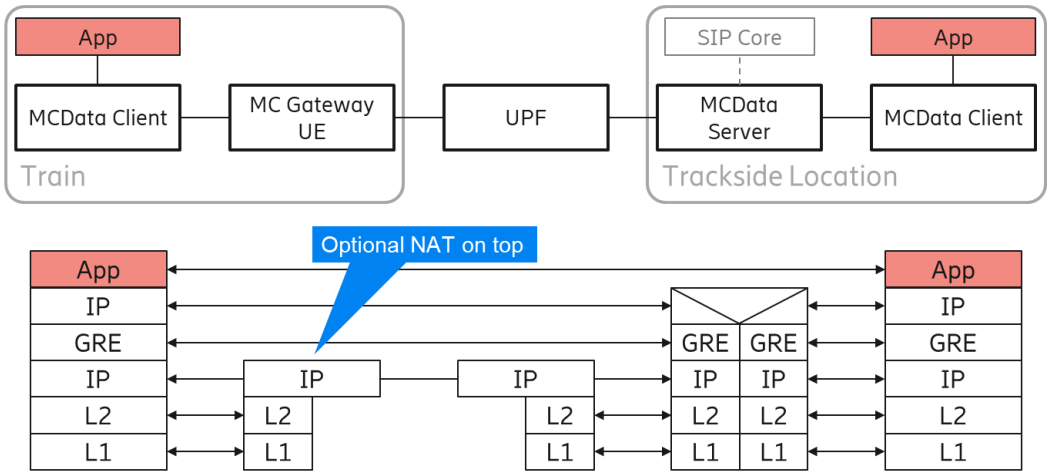

Figure 3.22: Protocol stack when using MCData IPCon for railway data services, assuming that the MC Gateway UE acts as router and optionally as NAT.

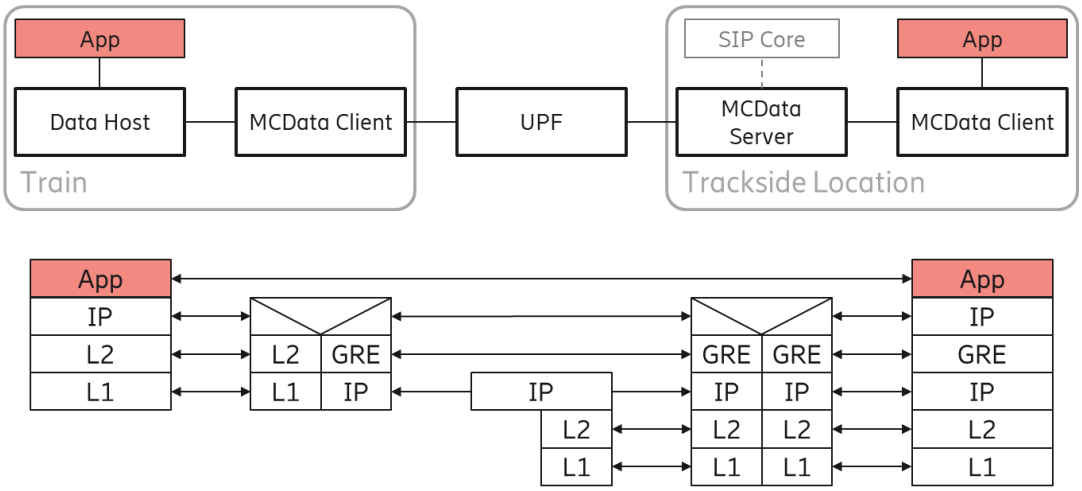

Figure 3.23: Protocol stack when using MCData IPCon for railway data services, assuming that the MCData Client sits on the UE.

4 Discussion of Architecture Options

Several topics are discussed in this section, and multiple alternatives are described.

4.1 UPF Selection

In the 5G System, one UPF is selected as PDU Session anchor (PSA) during PDU Session establishment (cf. Section 3.1) by default. All data delivered over this PDU Session is routed through this UPF, which serves as the gateway between the 5GS and the DN. In the default, most basic configuration, the user data of a PDU Session only passes through a single UPF and is routed to different Application Servers in the Data Network, as illustrated in Figure 4.1.

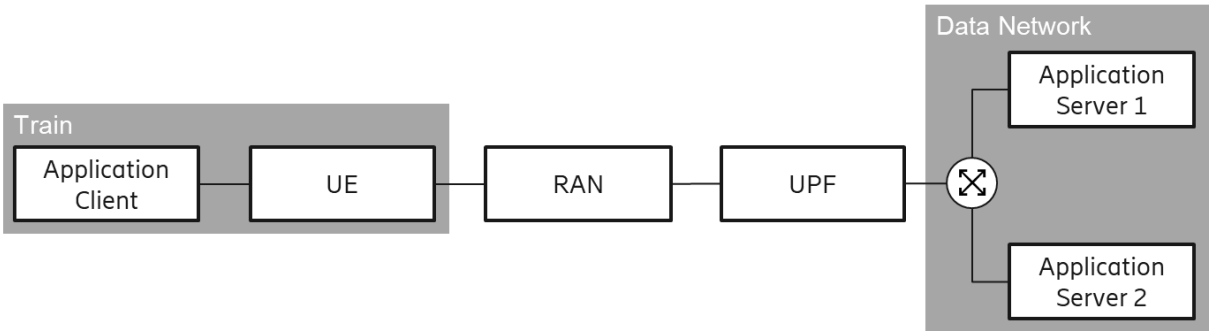

Figure 4.1: User is always routed through a UPF acting as a PDU Session anchor.

The SMF decides on a UPF that is used as anchor for the PDU Session. This decision can be based on a number of criteria, taking into account the information available at the SMF. Typically, in a distributed system, the current location of the UE in the network and the location of UPFs are considered, in order to select a PSA UPF in close proximity to the UE, and the selection algorithm might be specific to DNNs and network slices.[1] However, also aspects such as the UPFs' dynamic load or UPF capabilities might be considered. PDU Sessions can be re-anchored at different UPFs during the lifetime of a PDU Session, as further described in Section 4.5.2.

It's also possible for a PDU Session to have multiple PDU Session anchors in parallel, in which case an intermediate UPF (I-UPF) is needed which takes a decision where to forward data, either based on an uplink classifier, or based on the IPv6 prefix. For the uplink classifier, one more UPF acting as IP anchor may be present, responsible for IP allocation as the UE only gets a single IP[2] for the PDU Session, as illustrated in Figure 4.2. Otherwise, one of the PSA UPFs acts as the IP anchor.

[1] In principle, it's also possible to select the UPF purely based on the DNN in the SMF, and control from the user space in the device handling the UE, which DNN is used, and when PDU Sessions with a specific DNN (corresponding to a UPF at a specific compute site) are established and released.
[2] Or both a single IPv4 address and a single IPv6 prefix.

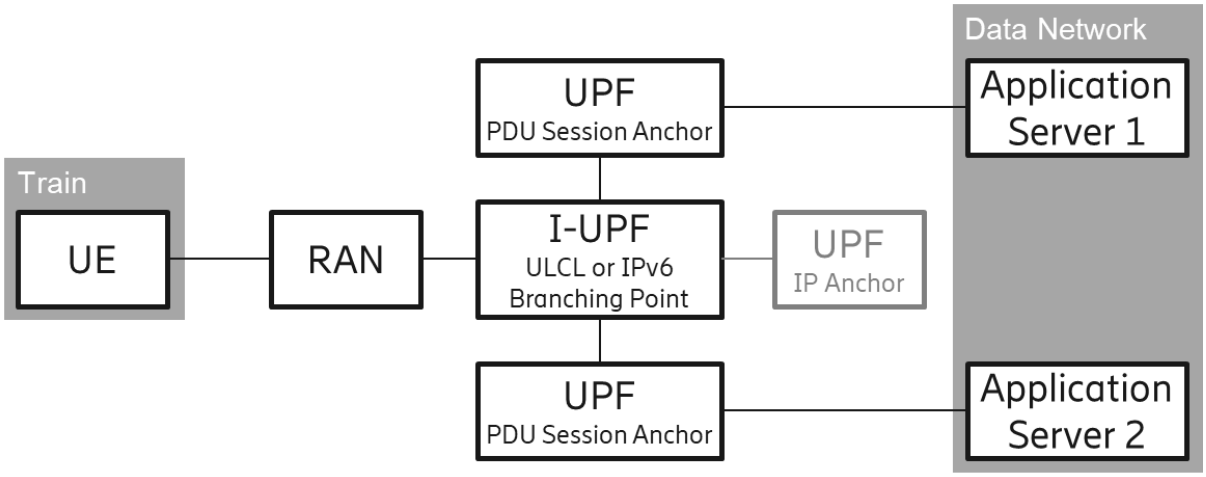

Figure 4.2: PDU Sessions can have multiple PDU Session Anchors, with an I-UPF in the data path of the PDU Session that splits uplink traffic and aggregates downlink traffic.

While the uplink and downlink routing are unambiguous in the scenario with only one UPF, there are some pitfalls in the advanced scenario.

To avoid tromboning in the 5G core (i.e. data being transported back and forth over the same shared link, illustrated in Figure 4.3), the I-UPF must be highly distributed, best co-located with gNBs in the RAN, potentially leading to a significant deployment overhead. This is further elaborated on in context of edge handovers, cf. Section 4.5.2.

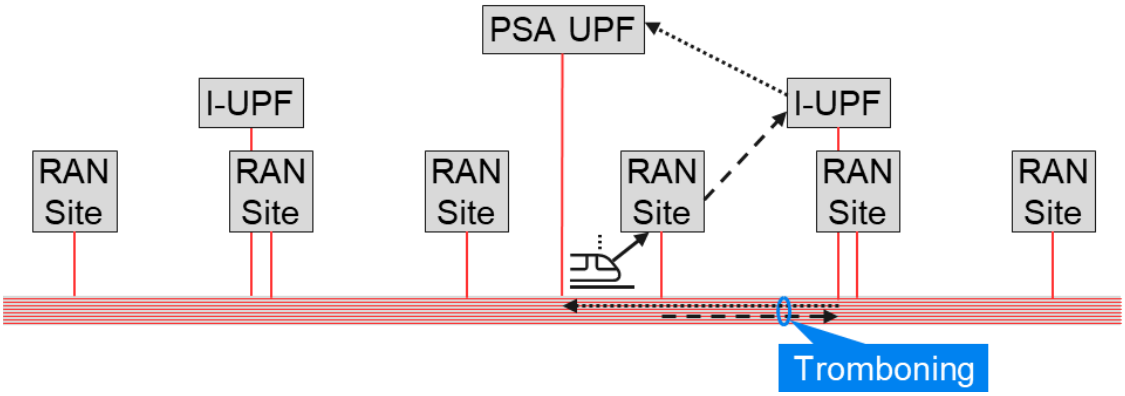

Figure 4.3: Depending on the distribution of RAN sites, I-UPFs and PSA UPFs, tromboning is more or less prevalent.

4.1.1 Uplink Classifier

When an uplink classifier (ULCL) is used, the I-UPF is configured to forward uplink data based on IP packet inspection (e.g. based on destination IP of the packet). The UE only gets assigned a single IP address, and routing of uplink data to one of the PDU Session Anchors happens in the 5G core. This however means that the UE is visible with the same IP from all PSA UPFs, leading to some pitfalls for routing of downlink data, described further in Section 4.2.3.

4.1.2 IPv6 Multi-Homing

When IPv6 multi-homing is used, another IPv6 prefix is added to the PDU Session and sent to the UE. The UE then decides which prefix to use for an uplink IP packet. The I-UPF then forwards packets to PSA UPFs based on the IPv6 prefix in the IP packet. As the UE is visible with different IPv6 prefixes (and thus different IPv6 addresses) via each PSA UPF, routing of downlink packets works just like in the default case.

4.2 Routing & IP Assignment

In the 5G System, the SMF assigns an IP address (or an IP prefix in case of IPv6) to a UE for each PDU Session it establishes, either during or after PDU Session establishment. The SMF may interact with other entities inside or outside the 5G core for deciding on an IP address (or prefix), as further described in Sections 4.2.1 and 4.2.2.

As a train might be connected via more than one UE (and to more than one network), the FRMCS Mobile Gateway needs to handle data to/from multiple IP interfaces. This comes with a significant amount of complexity, especially considering that each link can have varying quality and availability (e.g. WiFi only at stations and depots). Therefore, the FRMCS Mobile Gateway is expected to handle these varying conditions and obfuscate details on the external connectivity from devices on the train. This can be achieved using two different options.

1. Using Network Address Translation (NAT) functionality, in which case data routed to the UE is forwarded to the correct devices on the train based on previously observed uplink traffic. MCX currently does not support NAT, only IMS does.
2. Using WAN IP addresses assigned to devices behind the UE, independent from the network. The UE acts as a normal IP router in this case, and the mechanisms required in the 5G core are framed routing, explained in Section 4.2.4, or IPv6 prefix delegation, explained in Section 4.2.5.

In conjunction with either option, an application layer gateway (ALG) can be used for selected traffic flows (e.g. session establishment), which terminates the application layer session in both directions and take a simple proxy role, or take active decisions to modify, discard, or create new messages. Using an ALG is likely a deployment choice without standards impact that still enables triggering the appropriate QoS flows, which is why this is assumed going forward.

The benefit of option 1 is that there is a very clear separation of concern between railway infrastructure manager and train operator.. However, additional client functions are needed when the user-plane resources are set up separately from the control plane (e.g. RTP/UDP flows, established using SIP) and when different QoS flows are needed to the same destination (e.g. MC Service Service).

Option 2 would require exposing all external connections to these devices, and the need to handle multiple connections and mobility between UPFs in these devices (i.e. new IP addresses for onboard devices when reselecting a UPF). This is not recommended due to high complexity and signaling overhead. Furthermore, when a train is operated by a different entity than the railway infrastructure manager, these mechanisms introduce a dependency between these two entities, since the infrastructure allocates / assigns the “range” of usable onboard IP addresses.

In the following, Option 1 (NAT) is assumed, if not otherwise mentioned. An ALG is assumed where it is mentioned and drawn in a figure.

For downlink IP packets, the destination IP is used by UPFs to determine which PDU Session should be used to forward the IP packet, thus, which UE should receive this packet. The IP address acts here as an identifier bound to the UE (Note, UE may use multiple PDU Sessions simultaneously, thus, have multiple IP addresses). Once the location of the UE in the network is known (might require additional procedures if the UE is in idle mode), the IP packet is sent to the serving gNB via a GTP-U tunnel, identified using a Tunnel Endpoint Identifier (TEID). Outside the 5G core, the destination IP is used for routing the data to the correct UPF in the first place, i.e. routers in the path of the packet are configured so that packets are correctly routed to the respective UPFs. This is typically achieved by associating an IP address pool (e.g. a subnet) with a UPF, where all UEs anchored at this UPF have an IP address from this very pool. Downlink routing is illustrated in Figure 4.4.

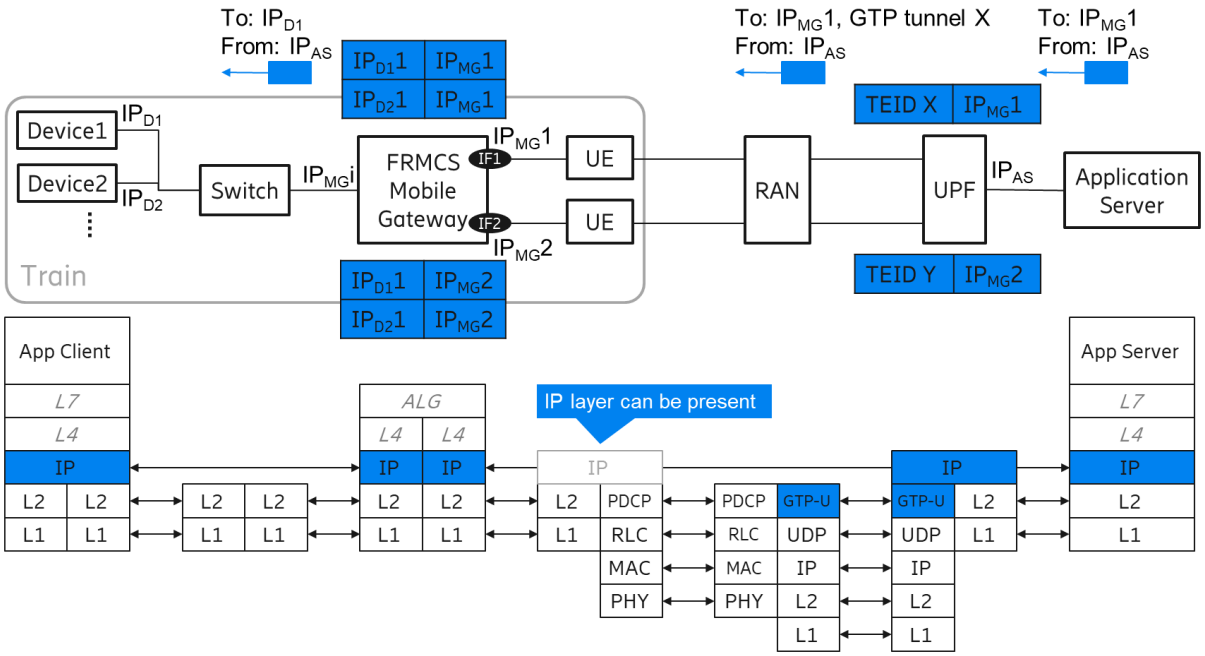

Figure 4.4: Downlink routing of IP packets through a 5GS. L4 and L7 protocol could e.g. be UDP and SIP, or TCP and HTTP.

For uplink IP packets, the FRMCS Mobile Gateway needs to take a decision which network interface to use for an IP packet (e.g. among multiple UEs connected to the same network, or among 5G and WiFi). A somewhat persistent decision is needed for most L4 protocols, as each network interface comes with a different source IP address. Dedicated multi-path protocols can be used to use two different links in parallel. Inside the 5G network, uplink data is routed to (one of) the UPF(s) where the corresponding PDU Session is anchored, where an ULCL or an IPv6 branching point in the data path might take a decision to which PSA UPF the data should be forwarded, if present. After leaving the UPF, the IP packet is forwarded to the destination IP using standard routing. Uplink routing is illustrated in Figure 4.5.

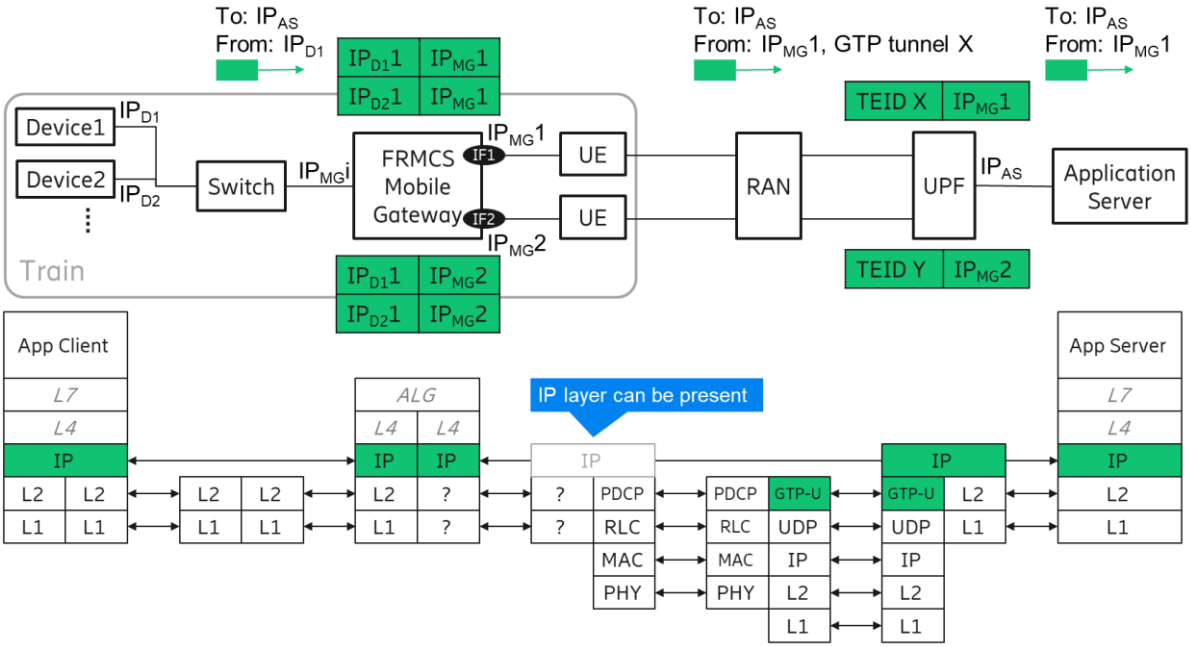

Figure 4.5: Uplink routing of IP packets through a 5GS. L4 and L7 protocol could e.g. be UDP and SIP, or TCP and HTTP.

4.2.1 IPv4

If IPv4 is used for a PDU Session, the IP address is either

a) Sent to the UE during PDU Session establishment (mostly used nowadays), or
b) Obtained after PDU Session establishment using DHCPv4, where the SMF acts as DHCP server towards the UE. In this option, the UPF forwards DHCP requests to the SMF.

Furthermore, the UE may use DHCPv4 to obtain other IPv4 configuration parameters (e.g. DNS server address).

While the SMF assigns the IP address to the UE, there are a number of options on how the SMF decides on the particular IP address.

a) SMF manages IP address pools per UPF and assigns an IP from the pool corresponding to the UPF that is selected as IP anchor (mostly used nowadays).
b) The UPF that acts as IP anchor provides an IP address from its pool and sends this to the SMF over N4.
c) SMF acts as DHCP client towards an external DHCP server (e.g. part of an IPAM solution).
d) Static IP address captured in subscription information in UDM (one single IP address per DNN and network slice).

4.2.2 IPv6

If IPv6 is used for a PDU Session, the interface identifier of the link local address is assigned by the SMF (prefix “fe80::”) during PDU Session establishment. This link local address is only used for communication between UE and SMF.

For the global IPv6 address, the UE uses IPv6 stateless address auto-configuration (SLAAC) to obtain a /64 IPv6 prefix from the SMF after PDU Session establishment. The assigned IPv6 prefix is globally unique, so there is no need for duplicate address detection, the UE can choose any interface identifier (aside from some reserved identifiers defined in [20]) or use multiple interface identifiers. Also, it’s possible to add multiple IPv6 prefixes to a PDU Session, as described in Section 4.1.2.

The UE may use DHCPv6 for IPv6 parameter configuration after PDU Session Establishment (including e.g. DNS address, proxy info, or P-CSCF URI when MCX is used), but support for this is optional, and support by chipsets and operating systems is unclear so far. This in general also allows for allocation of other prefix lengths than 64 bit. In this case, the SMF acts as DHCP server towards the UE. As part of DHCPv6, prefix delegation can be used, i.e. the UE assigns prefixes to devices behind the UE from the prefix assigned by the SMF, as described further in Section 4.2.5.

While IPv6 can also be used in conjunction with NAT or an ALG, as already illustrated for IPv4 in Section 4.2.1, it simplifies the operation without NAT or ALG by allowing multiple interface identifiers for different devices on the onboard LAN with the same IPv6 prefix. As user data in the 5G system is identified using the IPv6 prefix only, some of the problems with IPv4 when using multiple IP addresses behind the UE can be avoided. The FRMCS Mobile Gateway acts as a router in this scenario, announcing all available IPv6 prefixes to onboard devices. Also, duplicate address detection needs to be used locally to guarantee uniqueness of the IPv6 interface identifiers in scope of the assigned IPv6 prefix.

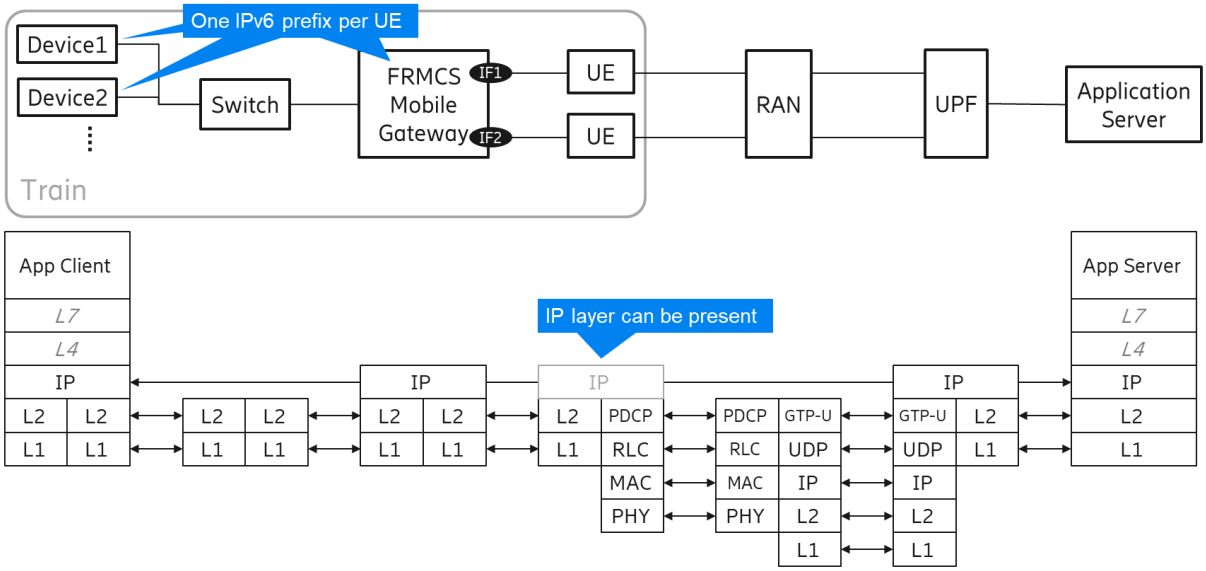

Figure 4.6: Protocol stack when using IPv6 without NAT, where the FRMCS Mobile Gateway acts as router.

While IPv6 offers a range of promising tools, it needs to be studied in more detail, how these tools should be used in the railway setting, e.g. how IP-related functionality is split between FRMCS Mobile Gateway and UE, or how to handle multiple UEs and thus multiple IPv6 prefixes.

4.2.3 Routing with ULCL

Traditionally, routing is done based on the destination IP of a packet, and a set of rules in the router, which describe where IPs from different subnets can be reached. By design, there is a clear 1-to-1 mapping. In the ULCL case, the UE can be reached via multiple points of presence (the PSA UPFs), but only one UE IP, so multiple routes to this UE are available, which would require a routing decision in the router based on the UE location in the network for optimal routings. In a setup where all application servers are co-located with a UPF, this can be avoided by having only a LAN to connect UPF and Edge Server, as illustrated in Figure 4.7.[1] However, as soon as an Application Server can and should be reached via multiple PSA UPFs, the optimal routing decision for downlink traffic depends on the location of the UE in the network. This can certainly be realized (e.g. using an SDN-based system with

[1] Strictly speaking, co-location is not required, and also remote locations can be connected via a VLAN. However, an application server can only communicate with the UE over a single UPF to avoid issues.

interactions between 5G core and SDN controller) but requires dynamic interactions between 5G core and the routing framework (cf. Figure 4.8).

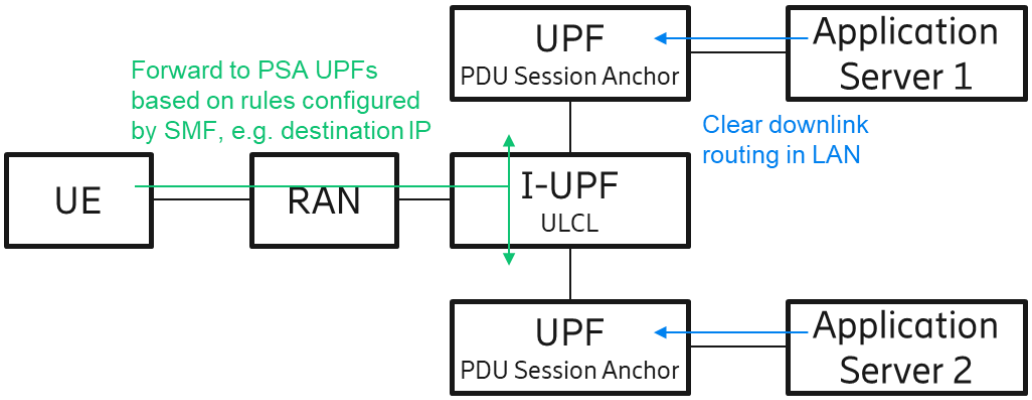

Figure 4.7: An uplink classifier (ULCL) in the data path needs to decide where uplink data is forwarded. If there is a single application server per PSA UPF, routing is clear in both directions.

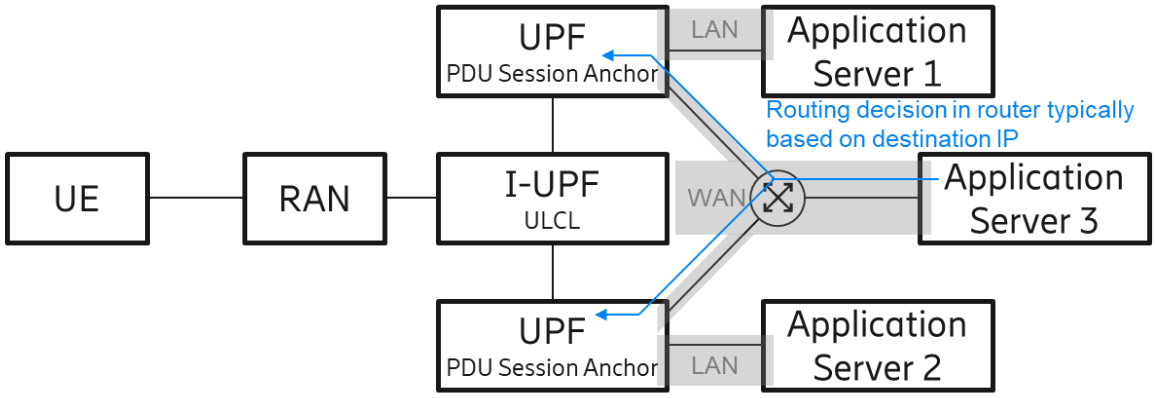

Figure 4.8: When an application server can send data to a UE via multiple PSA UPFs, the routing decision depends on the location of the UE in the network.

One possible way to overcome this issue is to do all routing within the 5G core and instantiate a PSA UPF at every application server that a UE will communicate with (e.g. at every edge and central compute site in the railway case). The drawback is of course the extra capacity needed for the deployment, as well as extra signaling and traffic inspection, and in general smaller routing flexibility. Furthermore, onboarding new services gets more complicated, unless they are not performance-critical, and a single, central PSA UPF can be used as default, as the only UPF connecting to WAN, as illustrated in Figure 4.9.

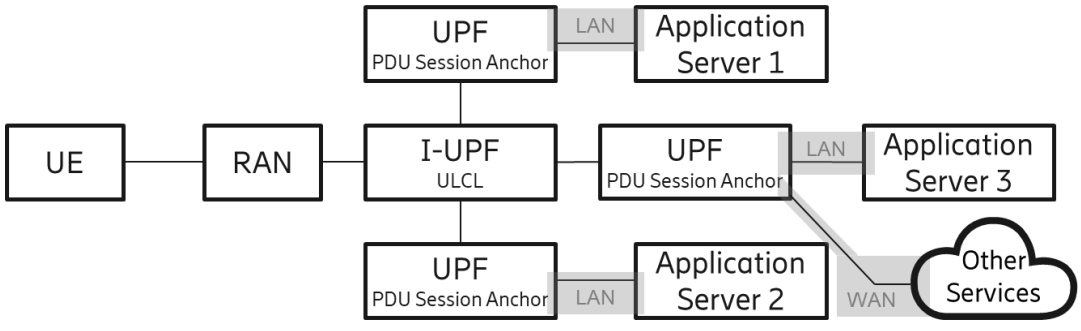

Figure 4.9: To overcome the downlink routing challenges with an ULCL, all routing can be done inside the 5GC, by instantiating a PSA UPF at every designated Application Server, with a single default UPF for other services.

4.2.4 Framed Routing

The 5GS offers the possibility to associate framed routes with a PDU Session. Framed Routing allows to support an IP network behind a UE, such that a range of IPv4 addresses or IPv6 prefixes is reachable over a single PDU session, e.g. for enterprise connectivity. Framed Routes are IP routes behind the UE. Framed Routes essentially allow for configuring the UPF to send DL IP packets designated for a set of IP addresses via a specific PDU Session. In order to do this, secondary authentication/authorization needs to be configured, in which case the SMF contacts a DN-AAA (Accounting, Authentication, Authorization) server after session management context creation. The DN-AAA can then approve of reject PDU Session Establishment based on the parameters received and, if accepted, may provide a list of framed routes to the SMF, which the SMF forwards to the UPF for packet routing decisions, as illustrated in Figure 4.10.

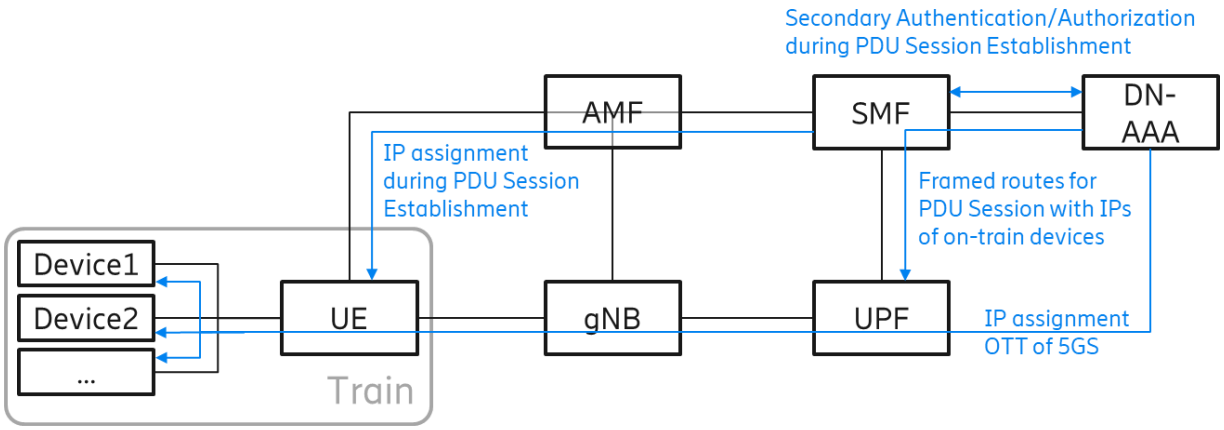

Figure 4.10: IP assignment and framed routing in 5GS.

The UE still only gets a single IP address assigned by the SMF. How the DN-AAA selects the IP addresses, prefixes, or subnets for the devices behind the UE described as framed routes is outside the scope of 3GPP, and there is no integrated mechanism to provision IP addresses to such devices using the 5GS. In principle, the DN-AAA may e.g. act as a DHCP server towards devices behind the UE, allocate an IP address pool during secondary authentication/authorization, and then assign individual IP addresses to the devices using DHCP once user plane connectivity is available. Another option is to use static addresses, but this leads to issues during mobility. Once IP addresses are configured, the device on top of the UE is responsible for forwarding received DL user data within to devices behind the UE.

There are three major challenges with framed routing in the railway context during regular operation:

1. Mobility between UPFs: this topic is discussed in detail in Section 4.5.2, but in principle a train has PDU Sessions anchored at different UPFs during its journey, with different migration options and different challenges w.r.t. framed routes.
2. Multiple UEs on the train: assuming that at least two UEs are connected to the train with PDU Sessions over the same 5GS and anchored at the same UPF, different framed routes must be configured for the same devices behind the UE for an unambiguous PDU Session selection for DL user data at the UPF. Consequently, devices on the train need to handle two (or more) IP interfaces connected to the FRMCS Mobile Gateway, as illustrated in Figure 4.11.
3. Access to additional networks: if the train connects to a public mobile network or to a WiFi access point that is not aggregated in a PDU Session and thus has its own IP domain. This has to be addressed by either adding additional network interfaces to all devices on the train, or by having a mobile gateway on the train that acts as a NAT towards such additional networks and re-use the IP addresses assigned by the DB 5GS as train-internal addresses.

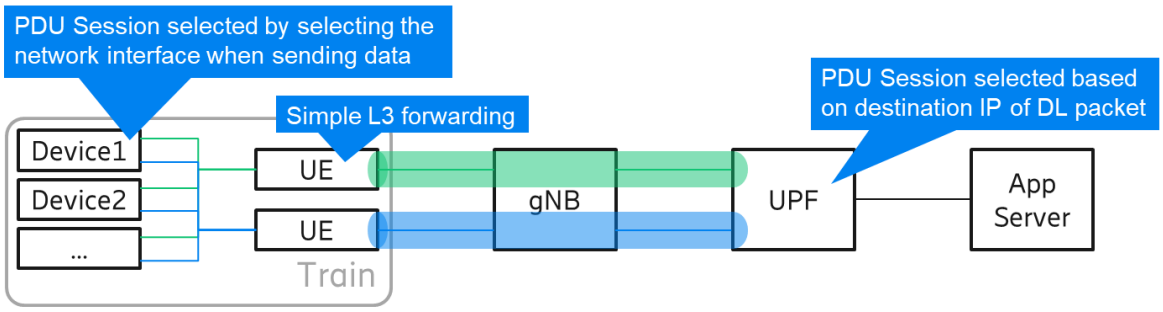

Figure 4.11: Different PDU Sessions must use different framed routes so that data can be routed unambiguously.

On top of this, a fallback mechanism needs to be in place for the event where no connectivity to the DB 5GS is available, e.g. address assignment via another available network or a train-internal DHCP.

4.2.5 IPv6 Prefix Delegation

IPv6 prefix delegation can be used in 5GS to achieve a similar behavior as with framed routing. As described in Section 4.2.2, the SMF assigns an IPv6 prefix to the UE after PDU Session Establishment using SLAAC. Afterwards, the UE, acting as requesting router and implementing a DHCPv6 client, can request prefixes from the SMF, acting as delegating router and implementing a DHCPv6 router.[1] To correctly route data to the designated prefixes that are now assigned further by the mobile router on the UE, the SMF installs PDRs in the UPF, so that IP data addressed to these prefixes are sent to the corresponding UE.

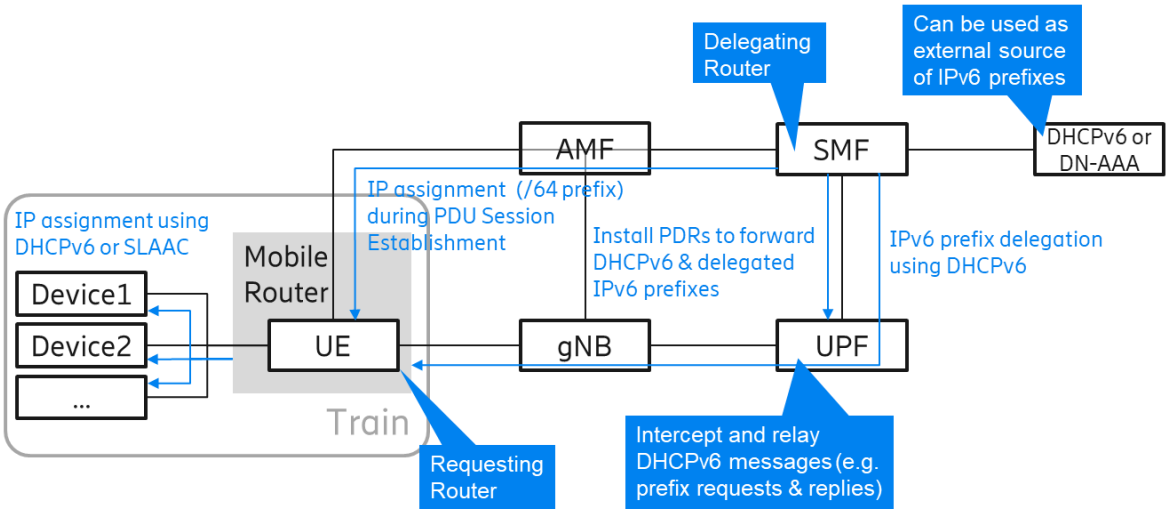

Figure 4.12: Ipv6 prefix delegation

While IPv6 already natively offers some support for multiple devices behind the UE, some challenges could be addressed using IPv6 prefix delegation (e.g. the split between FRMCS Mobile Gateway and UEs, and the presence of multiple UEs and PDU Sessions). However, this also brings new challenges, and it needs to be studied further, how DHCPv6 tools can be used to handle edge handovers and inter-PLMN handovers, when using IPv6 prefix delegation.

4.3 Quality-of-Service

Inside the 5G System, differentiated treatment of parallel service data flows can be enforced. While throttling is enforced in the UPF typically, the most relevant prioritization of certain data flows over others happens in the RAN, specifically on the MAC layer. When a UE communicates over multiple service data flows that require different QoS, these flows can practically be mapped to different QoS Flows

[1] The IPv6 prefix pool can be managed by an external DHCPv6 server or DN-AAA server.

within the same PDU Session, or even mapped to different PDU Sessions with different QoS configurations (cf. Figure 4.13)[1]. In the current specification, a UE can establish up to 15 PDU Sessions in parallel[2], and up to 63 QoS Flows per PDU Session[3][4]. In general, both QoS enforcement and packet detection rely on a number of parameters and rules that are used in the 5G System, which is further described in sections 4.3.1 and 4.3.2.

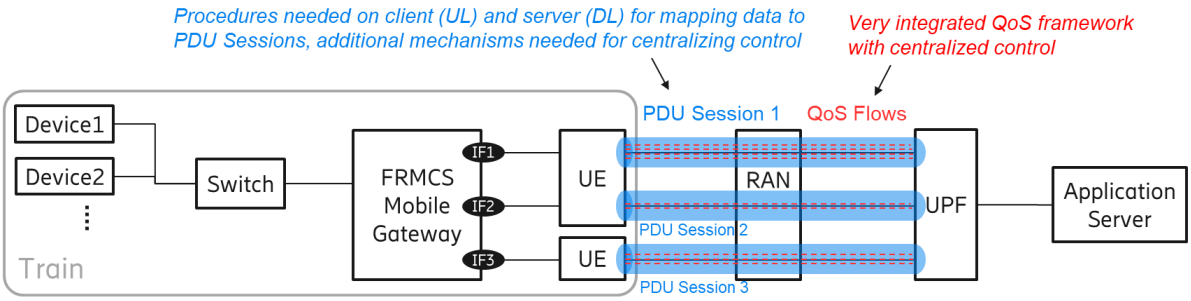

Figure 4.13: Service data flows can receive different QoS treatment by mapping them to different QoS Flows in the same PDU Sessions, or to different PDU Sessions with different QoS configuration.

QoS enforcement is further discussed in Section 4.3.3, while the identification of service data flows and the mapping to QoS Flows, called packet detection here, is discussed in the following.

For mapping service data flows to QoS Flows, the 5G core provisions corresponding rules to the UE (for uplink) and UPF (for downlink), based on pre-configured rules and/or dynamically created rules. These rules enable filtering by e.g. IP-5-Tuples and DSCP (IPv4) or Traffic Class (IPv6) values (cf. Figure 4.14)[5]. As the mapping in the UE is done below the IP stack within the modem (IP packet sniffing in the modem), it also happens behind any NAT or proxy in the FRMCS Mobile Gateway, which is why IP packets originating from different devices on the train appear to come from the same IP, so the source IP cannot be used as a differentiator for mapping a packet to different QoS Flows.[6] More details on QoS in 5GS are described in Section 4.3.1.

[1] Preferably, a single PDU Session is used, but certain limitations may require multiple PDU Sessions, which is further discussed in the following paragraphs and sections.
[2] Limited by PDU Session ID values defined in [27].
[3] Limited by the QFI values in NAS signaling defined in [28].
[4] In practice, a lower number of PDU Sessions and QoS Flows are typically supported, due to hardware limitations.
[5] DL service data flows can also be matched by URIs, captured in packet flow descriptions, but this has several caveats and limitations.
[6] When using Framed Routing or IPv6 Prefix Delegation, service differentiation based on the client IP address might work though.

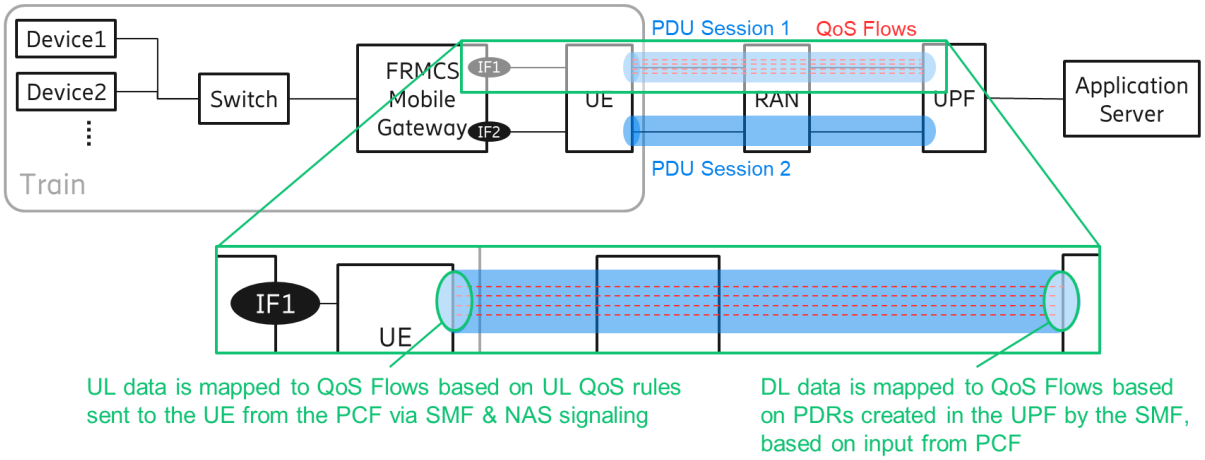

Figure 4.14: The 5GS offers procedures for mapping UL and DL data to QoS Flows with different QoS treatment.

Instead of – or in addition to – differentiating traffic within a PDU Session, the FRMCS Mobile Gateway can also send uplink data over different network interfaces (corresponding to different PDU Sessions) with different QoS configurations. This is either done by configuring the IP routing table of the FRMCS Mobile Gateway to send packets using a specific network interface (cf. Figure 4.15), each of which corresponds to a PDU Session, or by implementing a Layer 4 or Layer 7 proxy in the FRMCS Mobile Gateway (cf. Figure 4.16), which actively selects a network interface over which an IP packet should be sent.

Regarding downlink data, the PDU Session is selected by the UPF based on the destination IP of a DL IP packet. Most communication is client-initiated, and an application server will simply reply to the same IP address, in which case the packet would be sent on the "correct" PDU Session without requiring additional mechanisms. When multipath protocols are used (e.g. MP-TCP), downlink traffic can be dynamically prioritized by deciding which of the paths to use. This could happen in the application server, or in a Layer 4 or Layer 7 proxy in the data path.

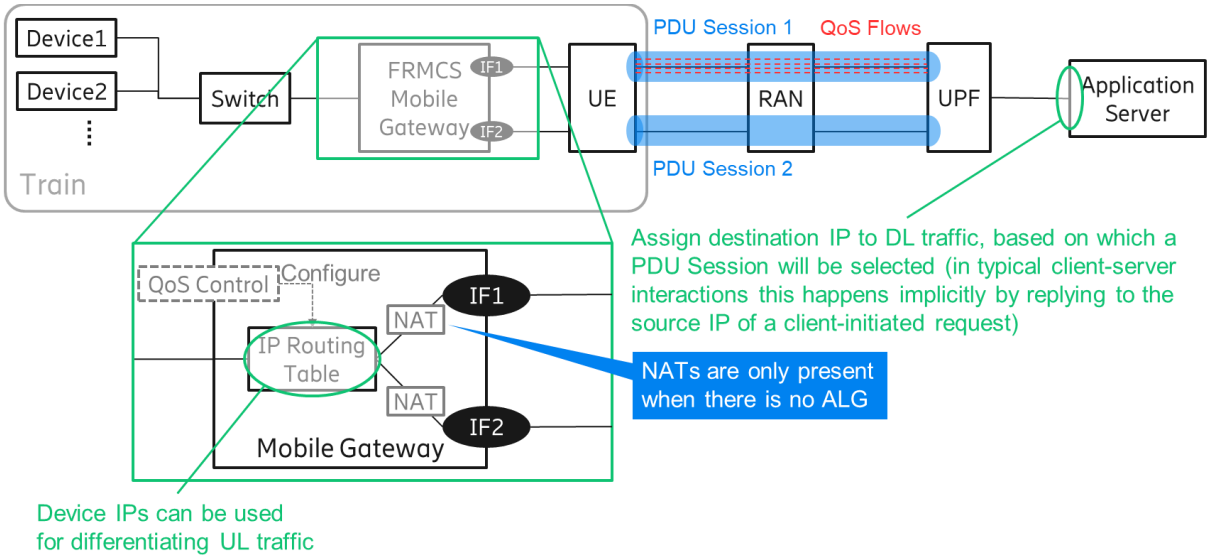

Figure 4.15: Data can be sent via different PDU Sessions using IP Routing configuration for UL data, and by assigning the corresponding destination IP to DL data.

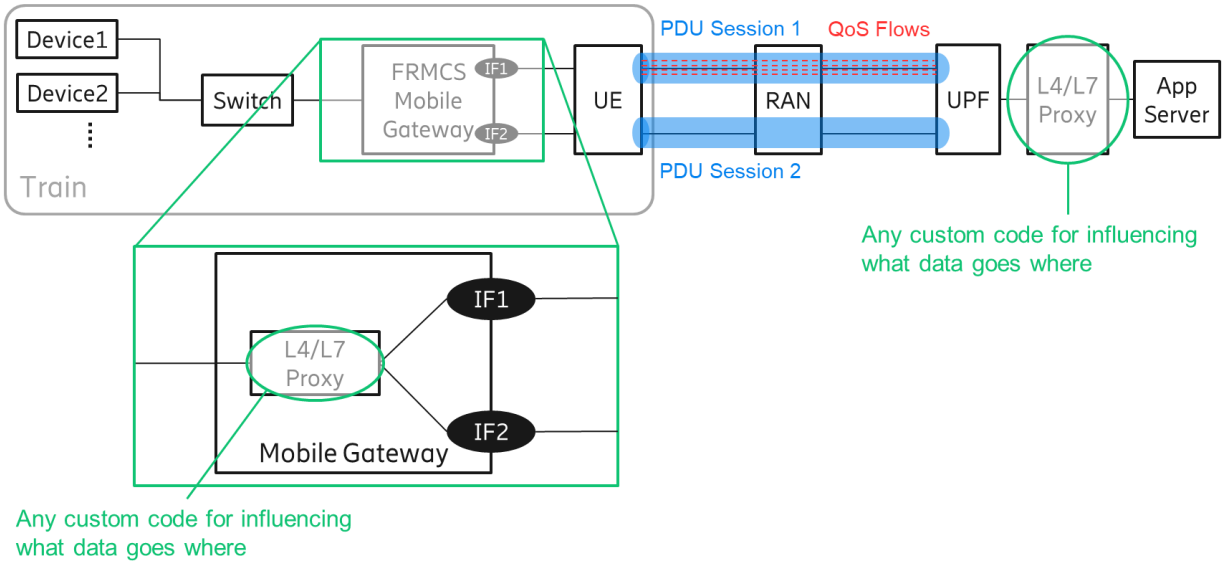

Figure 4.16: UL data can be sent via different PDU Sessions by actively selecting the network interface over which to send data in a proxy on the FRMCS Mobile Gateway.

In general, it is advisable to bundle multiple QoS Flows within a PDU Session, as this gives the most flexibility for schedulers to optimize transmissions, it has the lowest complexity overhead in the client handling multiple PDU Sessions (FRMCS Mobile Gateway in this case), and it has the lowest signaling overhead. Using multiple PDU Sessions only offers more possibilities to distinguish what data packets are sent with what QoS, i.e. more advanced methods for packet detection. Consequently, multiple PDU Sessions should only be used in context of QoS, when packet detection cannot be done as needed within a single PDU Session.

4.3.1 Configuration & Signaling in 5GS

In the 5G System, the PCF is the source of QoS policies, and provisions these policies to the SMF, which distributes parts of that to UEs, gNBs, and UPFs[1]. QoS policies are configured per PDU Session, they are distributed during PDU Session establishment and may be updated later. Which QoS policy the PCF provides for a PDU Session can very well be specific to a DNN and a network slice, i.e. different QoS policies can be configured for different PDU Sessions established to the same UE by using different DNNs or network slices for each PDU Session[2].

For dynamically creating or modifying QoS policies, the PCF offers a service interface that an Application Function (AF, e.g. the SIP core in the MCX case) can use to add additional service data flow descriptions for an already defined QoS policy. This includes both packet filters and QoS enforcement related parameters, which are further elaborated on in Section 4.3.3. Figure 4.17 provides an overview on the QoS-related signaling in 5GS.

[1] In principle, a 5GS also works without a PCF, and a Session Management Policy can also be pre-configured in the SMF. This however does not offer any dynamic policy adaptations (e.g. adding packet filters to existing QoS policies, which is why in this report we assume that a PCF is deployed and integrated.
[2] In general, only a single PDU Session can be established per combination of SIM, DNN, network slice, and IP address type (IPv4 or IPv6).

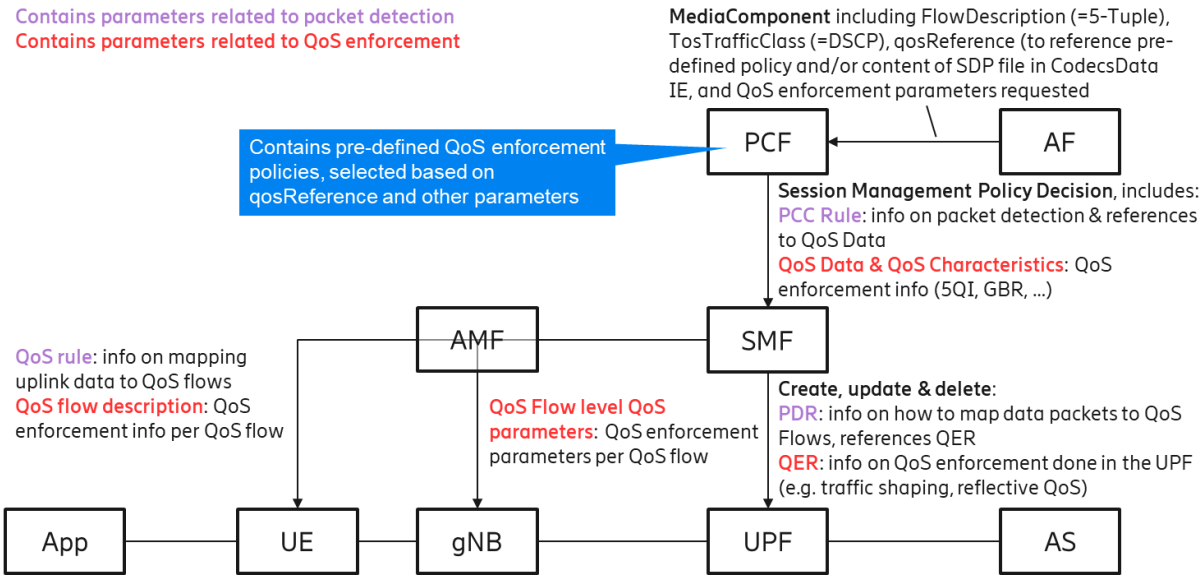

Figure 4.17: QoS-related signaling in 5GS.

4.3.2 Configuration & Signaling in MCX

The mission-critical framework defines interactions with the evolved packet core (EPC, "4G core") on how to configure QoS during MC session establishment. While this is not standardized for 5GS yet, we assume in the following that these interactions will be similar.

During session initiation, the SIP core will request a certain QoS from the PCF for the service data flow (the media plane) described in the SDP offer / answer[1]. The SIP Core processes the SIP messages and extracts the SDP information (e.g. the SDP m-lines) to activate one or more QoS flows with the according characteristics. Note, the SIP Core finds bitrate information in the SDP for some services (like MCPTT or MCVideo). When an MC Gateway UE is in the path, the MC Gateway UE may rewrite the SDP offer / answer information with according IP and UDP information from the MC Gateway UE.

For MCPTT, the protocol stack and content of the SDP during session initiation are well-defined, and it's clear that all service data flows can be clearly identified using only a 5-Tuple in the modem and on the UPF for QoS differentiation (cf. Figure 4.18 and Figure 4.19). However, for MCData IPcon, which has been recently specified in SA6, there is not enough information available to conclude this. More specifically, it is not clear what layer 4 protocols can be used, and whether all needed port numbers are known during session initiation and described in the SDP files.

[1] While the examples in the following assume that the SIP core interacts with the PCF, the MC Service Server can also do this instead.

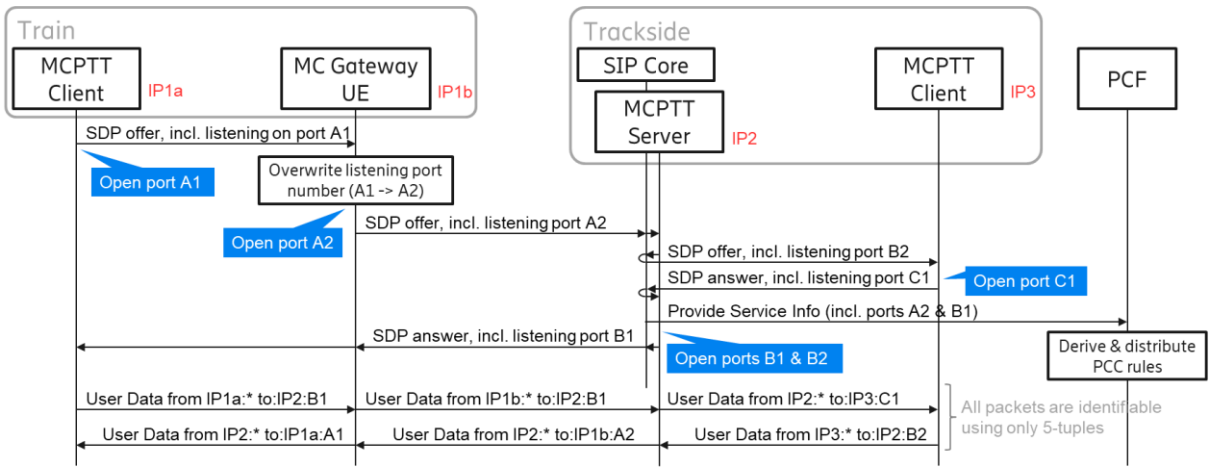

Figure 4.18: Message sequence for initiating an MCPTT session initiated by a train towards a trackside application.

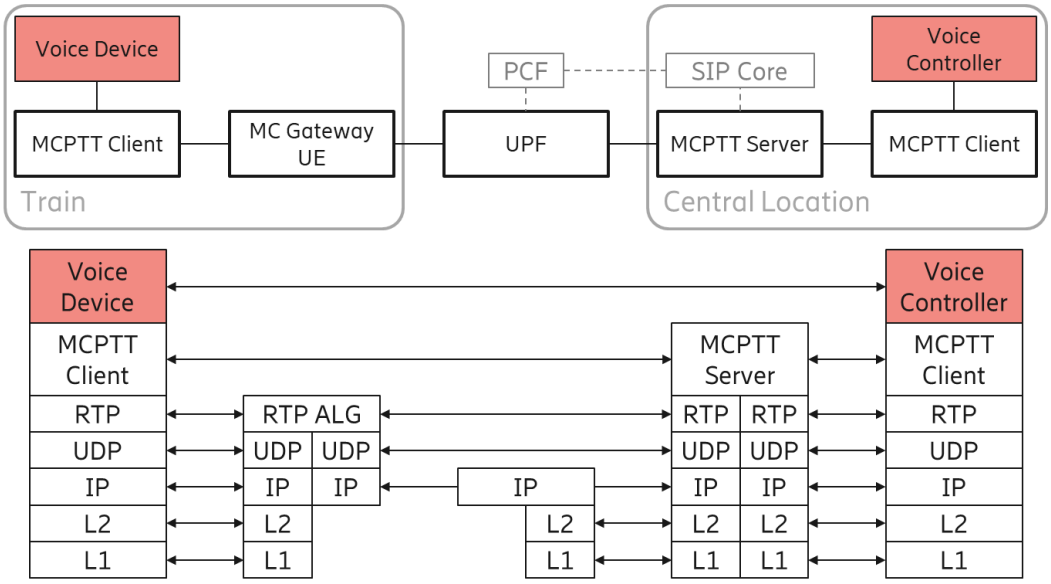

Figure 4.19: Protocol stack of an MCPTT-based call between a device on the train and on the trackside.

If IP-5-tuples are not sufficient to identify all service data flows that need to receive different QoS, the DSCP (IPv4) or Traffic Class (IPv6) field can be used for identifying different Service Data Flows with the same IP-5-tuple in the 5GS. In this case, either the MCX client or the MC Gateway UE needs to set the DSCP / Traffic Class field for each IP packet so that it matches the QoS policies configured in the 5GS. If the MCX client sets this field, the MC Gateway UE might overwrite or at least verify the value of the field.

One issue with DSCP in public networks is that the value might be rewritten by routers in the path, in which case the DSCP value of downlink IP packets assigned by the Application Server might not arrive at the UPF. Routers typically can be configured to not modify the DSCP value. If DSCP rewriting cannot be excluded, extra functionality is needed to potentially rewrite DSCP values, either using a proxy inside the (trusted) rail network, or inside the UPF.

The overall procedure describing how a QoS configuration is signaled through the 5GS when using MC services is illustrated in Figure 4.20.

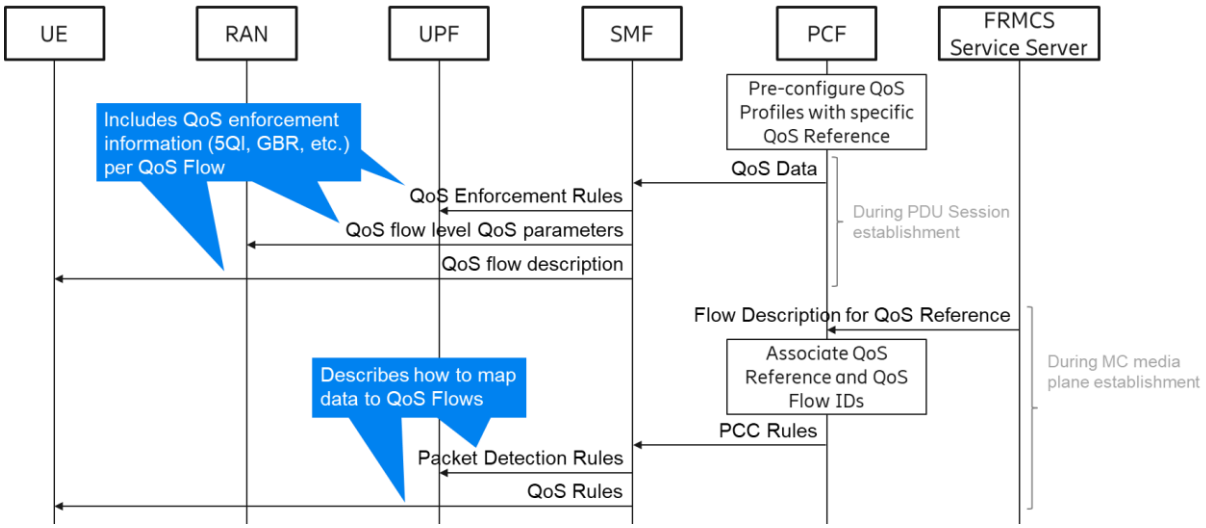

Figure 4.20: QoS configuration procedures for FRMCS (Simplified).

4.3.3 Scheduling & QoS Enforcement

Scheduling in the MAC layer is responsible for prioritizing data radio bearers (DRBs) / logical channels and UEs relative to each other. A DRB / logical channel[1] in the RAN is used to transmit data of all QoS Flows in a PDU Session with the same QoS enforcement configuration.

For downlink transmissions, DL data arriving at the gNB can be scheduled dynamically without prior involvement of the UE, while for uplink transmissions, the UE needs to have a scheduling grant for a set of resources assigned by the gNB. This can happen dynamically using scheduling requests (SR, dynamic scheduling), or by assigning periodic scheduling grants to the UE, in which case the UE can transmit in these resources without a scheduling request (configured grant, CG, successor of SPS (semi-persistent scheduling) from LTE). Furthermore, the gNB only schedules a UE, not the individual logical channels. The UE must then decide which logical channels to transmit over granted resources. This can however be configured by the gNB using the logical channel prioritization framework. As decision baseline for dynamic scheduling (for both UL & DL), the scheduler in a gNB collects several pieces of information from UEs, most notably:

- Channel quality, in the form of periodic and event-based Channel Status Information (CSI) reports. Channel quality is typically predicted on the short term based on these reports. The scheduler uses the channel quality for channel-dependent scheduling, i.e. preferably scheduling UEs when the channel state is good (besides other constraints such as latency requirements and guaranteed bitrates).
- Power headroom, i.e. whether the UE can increase its output power for UL transmissions, as UL is typically power-limited and not bandwidth-limited.
- UL Buffer status, i.e. how much UL data is buffered in a UE (either per DRB or generally).

The SR-grant cycle for dynamic uplink scheduling comes with additional latency. When using configured grant on the other hand, a lower latency is achievable[2], as a UE gets a periodic grant and can transmit data in the periodically allocated resources if there is data in the UL buffer (if no UL data is buffered, the allocated resource remains unused). Practically, to really achieve low latency, the configured grant would need to be synchronized in time with the UL data source. Assuming that this can be done (gNB can e.g. observe UL data availability occasions, configure CG periodical resources accordingly, and

[1] DRBs are on SDAP layer, and logical channels on RLC layer, but there's essentially a 1-to-1 mapping.
[2] The primary benefit of configured grant – besides reduced latency – is improved resource efficiency for periodic data transmissions by avoiding periodic SR and grant transmissions.

adjust in case of clock drifts or other changes to UL data availability), the jitter of UL data arrival should be very small (considering also processing delays, and transport inside the train).

- If UL data arrives early, it is either buffered until the granted resource, or it is dynamically scheduled (additional delay in both cases).
- If UL data arrives late, the situation is the same latency-wise, but the granted resource is wasted (unless other data arrives at this time by coincidence), and the waiting time for the next configured grant is longer.

Assuming ideal conditions the latencies described in Table 4.1 can be achieved for dynamic DL scheduling, dynamic UL scheduling and UL with configured grant (CG). For the 900 MHz band mentioned in Section 2.3, FDD is foreseen, and 15 kHz subcarrier-spacing (SCS) is recommended. For the 1.9 GHz band, TDD is foreseen, and both 15 and 30 kHz SCS can be used. While normal slot durations (14 symbols) are most efficient resource-wise, mini-slots of 7, 4, or 2 symbols duration can be used for urgent transmissions. If a transmission is not successful, up to 3 HARQ retransmissions can be triggered (depends on configuration), in which case this particular packet experiences a higher latency[1]. Finally, the numbers in the table refer to the delay for transmitting a transport block. If a user data packet requires multiple sequential transport blocks in time for transmission (e.g. under bad channel conditions), this needs to be considered separately and depends on the transport block size (TBS). The TBS depends on a lot of dynamic circumstances (e.g. modulation order and coderate based on channel quality) and on configuration choices (e.g. MIMO and reference symbol configuration), but can in general be calculated as described in Section 5.1.3.2 of [21].

Table 4.1: User data latency over RAN (neglecting queuing/buffering) for DL and UL (SR & CG) in FDD (targeting 900MHz band) and TDD (targeting 1.9GHz band, assuming alternating DL-UL pattern) assuming different slot durations (14, 7, 4, and 2 symbols), taken from [22].

Latency (ms)	HARQ	15kHz SCS FDD				15kHz SCS TDD			30kHz SCS TDD		
		14-os	7-os	4-os	2-os	14-os	7-os	4-os	14-os	7-os	4-os
DL data	**1st tx**	2.4	1.4	1.0	0.71	3.4	1.9	1.3	1.7	0.96	0.64
	1 retx	5.4	2.9	1.9	1.4	7.4	3.9	2.4	3.7	2.0	1.2
	2 retx	8.4	4.4	2.7	2.1	11	5.9	3.6	5.7	3.0	1.8
	3 retx	11	5.9	3.6	2.9	15	7.9	4.7	7.7	4.0	2.4
UL data (SR)	**1st tx**	4.5	2.5	1.6	1.4	6.5	3.5	2.2	3.3	1.8	1.1
	1 retx	8.4	4.4	2.7	2.1	11	5.9	3.6	5.7	3.0	1.8
	2 retx	11	5.9	3.6	2.9	15	7.9	4.7	7.7	4.0	2.4
	3 retx	14	7.4	4.4	3.6	19	9.9	5.9	9.7	5.0	2.9
UL data (CG)	**1st tx**	2.4	1.4	1.0	0.71	3.4	1.9	1.3	1.7	0.96	0.64
	1 retx	5.4	2.9	1.9	1.4	7.4	3.9	2.4	3.7	2.0	1.2
	2 retx	8.4	4.4	2.7	2.1	11	5.9	3.6	5.7	3.0	1.8
	3 retx	11	5.9	3.6	2.9	15	7.9	4.7	7.7	4.0	2.4

The numbers in the table are achievable under ideal conditions, but in practice, multiple QoS Flows from the same and from different UEs compete for the same resources. The scheduler needs to implement an algorithm for taking real-time decisions on the allocation of resources. Such algorithms for prioritization are always proprietary in 5GS and previous generations of 3GPP technology. However, when a QoS Flow is established (or policies for the QoS Flow are updated), RAN and core network establish a contract that the defined QoS enforcement requirements of the QoS Flow will be fulfilled. If the RAN cannot fulfil them anymore, the core network is notified. These characteristics are (among others):

[1] Additional latency might come from RLC retransmissions (typically several 10ms) if they are activated (RLC Acknowledged Mod) and all HARQ retransmissions fail, or from retransmissions of protocols on top of IP (e.g. ≥200ms in case of TCP), if the IP packet is not delivered successfully.

- **Priority Level**: when resources are not sufficient for fulfilling the requirements of all QoS Flows, the scheduler tries to prioritize fulfilment KPIs of QoS Flows with higher priority compared to KPIs of QoS Flows with lower priority. Otherwise, the priority is used to distribute resources between QoS Flows (where of course fulfilling GBRs is prioritized). When multiple QoS Flows exist in parallel, the list of QoS requirements and the priority level order should be as straight forward as possible, to avoid unpredictable behavior. In particular for UL transmissions, the scheduler has limited influence on the priority and can only give coarse-grained indications to the UE what data to send.
- **Packet delay budget (PDB)**: the maximum one-way delay between UE and UPF that is allowed for the QoS Flow. It's used for setting scheduler weights and HARQ target operating points. For GBR QoS Flows, the PDB is guaranteed for 98% of the packets, unless it's configured as delay-critical GBR QoS Flow (see below), in which every late packet is considered a packet error. For non-GBR QoS Flows, the PDB is guaranteed for 98% of the packets in uncongested scenarios, and the delay might increase due to congestion.
- **Packet error rate (PER)**: an upper bound for how many IP packets can be lost (i.e. not received). If a GBR QoS Flow is configured as delay-critical, then also packets experiencing higher delays than the PDB are included in the PER. A PER needs to be understood as the packet error rate within the 5GS, of an active QoS Flow. I.e. packet errors outside the 5GS are not considered, and downtimes of the network or dropped QoS Flows are out of scope of this metric.[1]
- **GBR vs. non-GBR QoS Flows**: when a QoS Flow is configured as a guaranteed bitrate (GBR) QoS Flow, the scheduler will try to always assure that a configured guaranteed flow bitrate (GFBR) is maintained over a configured averaging window, even in bad radio conditions and high cell load situations. If the GBR cannot be provided anymore, this is indicated to the core network. For non-GBR QoS Flows, no such guarantee is given.
- **Delay-critical GBR**: if this option is activated for a GBR QoS Flow, every packet that experiences a delay higher than the PDB is counted as a packet error.
- The **guaranteed flow bit rate (GFBR)** gives a guarantee on the supported throughput for the QoS Flow, calculated over a configurable averaging window, while the **maximum flow bit rate (MFBR)** indicates the maximum expected bitrate on the QoS Flow, and excess data does not have to be delivered with the defined QoS requirements (e.g. PDB). Bit rates between the GFBR and the MFBR are treated with relative priority compared to other QoS Flows, corresponding to the configured priority level.

While some of these requirements are specified explicitly (i.e. by number) for a QoS Flow (e.g. GFBR), others (e.g. PDB and PER) are bundled in a 5G QoS Indicator (5QI). Several 5QIs are standardized in 3GPP, i.e. a certain 5QI has standardized values for the various requirements. During configuration of the QoS policies, some values of a standardized 5QI can be overwritten, most notably in this case the priority level.

As an alternative to standardized 5QIs, dynamic 5QIs can be used, where all otherwise standardized values are signaled explicitly to the RAN.[2] As a potential drawback, optimizations in the scheduler for custom 5QIs may be required and should be tested using simulation-based studies.

[1] Downtimes of the network are typically captured under the term "availability" in the telco world. Also dropped/inactive QoS Flows would probably be considered under "service availability".
[2] The procedures are the same for standardized and dynamic 5QIs, but some more parameters are distributed (e.g. "QosCharacteristics" IE sent to SMF by PCF). The extra signaling load is expected to be limited.

The requirements given in Section 2.1 mostly have matching standardized 5QIs, however these 5QIs do not match the 5QIs specified for similar services in most cases[1]. The detailed configuration should be simulated and trialed in the target environments with the corresponding scheduling algorithms to verify that the configuration is working in the given circumstances.

Table 4.2 gives an example on how standardized 5QIs could be used to match the requirements of the railway use cases as much as possible (note that the priority level of standardized 5QIs can be overwritten), and where standardized 5QIs do not address the use case requirements from Section 2.1. As can be seen, the remote driving use case and the ETCS use case cannot be supported using only currently standardized 5QIs. Dynamic 5QIs would have to be configured in the 5GS by the operator, similar to these standardized 5QIs, when needed. Also, harmonization of such dynamic 5QIs between European railway operators would be required, to have well-defined connectivity even for trains roaming in visited networks.

Table 4.2: Example which standardized 5QIs could be used for the various use cases from Section 2.1. The lowest priority level value corresponds to the highest priority. Unfulfilled use case requirements (UCRs) are highlighted in red.

Use Cases			**5QI**	**Resource Type**	**Priority Level**	**Packet Delay Budget**	**Packet Error Rate**
Voice Services	**Audio**	**MCPTT**	65	GBR	15	75 ms (UCR: 100 ms)	10^{-2} (UCR: 10^{-3})
ETCS	**Position Report**	**MCData IPCon**	67	GBR	~~15~~ -> 20	100 ms	10^{-3} (UCR: 10^{-6})
	Movement Authority	**MCData IPCon**	67	GBR	~~15~~ -> 20	100 ms	10^{-3} (UCR: 10^{-6})
ATO	**Journey Profile**	**MCData IPCon**	7	Non-GBR	70	100 ms	10^{-3}
	Segment Profile	**MCData IPCon**	8	Non-GBR	80	300 ms (UCR: 1 s)	10^{-6} (UCR: 10^{-3})
	Status Report	**MCData IPCon**	7	Non-GBR	70	100 ms	10^{-3}
Remote Driving	**Video/Audio**	**MCData IPCon**	82	Delay-critical GBR	~~19~~ -> 30	10ms	10^{-4} (UCR: 10^{-3})
	Control Info	**MCData IPCon**	82	Delay-critical GBR	~~19~~ -> 30	10ms	10^{-4} (UCR: 10^{-6})
Video Surveillance	**Video/Audio**	**MCVideo or MCData IPCon**	67	GBR	~~15~~ -> 80	100 ms	10^{-3}

The gap between use case requirement and 5QI definition for the packet error rate in several use cases could be closed either using higher layer recovery mechanisms (e.g. ACK or NACK-based retransmissions) at the cost of latency or using repetition of messages the at the cost of load.[2]

[1] This is not a technical issue, but it begs the question why an MCPTT call in the railway context requires a different QoS than an MCPTT call in a public safety context.
[2] One concrete approach to improve the PER for messages such as ETCS status reports would be to double the transmission frequency such reports, which quadrates the PER (e.g. 10^{-3} PER for each single transmission gives an overall likelihood of 10^{-6} that both transmissions are not successful, assuming independent transmissions). As this doubles the load, it is only recommended for flows with a very low load and a very high reliability requirement.

While specific 5QIs are specified to be used for MC Services (5QI 65 for MCPTT, 5QIs 67 & 4 for MCVideo, 5QI 70 for MCData [19]), at least MCData may also use different 5QIs. It needs to be studied further, how the distinction between services with different QoS requirements can be indicated to the PCF via Rx/N5 or N33.

On top of the QoS configuration of user data, the IMS signaling should also be treated with specific QoS, so that adaptations can be done dynamically even in congested scenarios. 5QI 5 is specified for this purpose, and 5QI 69 can be used for even faster session establishment and modification. It's recommended to assign a lower priority level value (i,e. higher priority) than for any of the 5QIs used for user data.

Finally, it must be understood that verifying a very low packet error rate like 10^{-6} is really challenging to verify. 10^{-6} means that at most one out of 1 million packets is lost. To verify this with sufficient confidence, a rule of thumb would be to use a factor of 100 for the amount of measurements, i.e. showing that out of 100 million packets, at most 100 packets are lost. Assuming e.g. 10 packets per second for a given use case, this would require 24/7 measurements for more than 17 weeks[1], and this does not yet consider that some use cases might be specific for certain scenarios only (e.g. at stations). One way around this is to verify a lower packet error rate, and then use simple mechanisms (e.g. duplication) to analytically scale up the packet error rate. Another option might be to aim for a lower packet error rate (e.g. 10^{-3} requiring 100,000 measurements, taking less than 3 hours of measurement time for 10 Hz transmissions) and focus on the critical scenarios (e.g. cell edge, high velocity, and high load scenarios) and verify that even in these scenarios, the required packet error rate is not exceeded.

Lastly, there are different ways how a scheduler can assign resources to different UEs.[2] While all of this is an implementation choice, there is generally a notion of fairness, i.e. a scheduler tries to do a "fair" split of resources assigned to different UEs in the same cell. However, channel quality and QoS requirements also play a role in this decision, i.e. a UE with only high priority data can get more resources assigned than a UE with only low priority data. The balance of fairness vs. priority can typically be configured, up to completely neglecting fairness, which can e.g. be useful when having dedicated devices and UEs in a closed system with different responsibilities and different levels of criticality.

As mentioned before, in case of resource shortage, the RAN has to decide, which QoS Flows are dropped, and may furthermore reject the establishment of new QoS Flows (which could also happen in the target cell of a handover). The strategy for this is influenced using the Allocation and Retention Priority (ARP) parameters, which are configured for each QoS Flow. It basically gives a priority to each QoS Flow with an indication which QoS Flows may be dropped or cause other QoS Flows to drop at all. The ARP consists of three parameters.

- Priority level: the relative priority of the QoS Flow, where the flow with the lowest value will receive highest priority.
- Pre-emption capability: indicates whether the QoS Flow may get additional resources that were already assigned to lower priority QoS Flows.
- Pre-emption vulnerability: indicates whether resources assigned to this QoS Flow can be freed, to be assigned to a higher priority QoS Flow.

The difference between the dynamic prioritization framework used by the scheduler and the ARP is that the ARP is only used for resolving resource shortage in the RAN, while the dynamic prioritization is responsible for ensuring that the requirements of all QoS Flows are fulfilled at all times, if possible.

[1] Assuming also the relatively low bitrates of ETCS and control info for remote driving. When having higher bitrates, more packets are sent per second, and the required testing duration is reduced accordingly.
[2] It should be noted that the RAN does not distinguish between multiple PDU Sessions of the same UE, transmissions are handled "globally" for each UE.

4.3.4 Sudden Drop in Channel Quality

Variations in channel quality are quite normal when at least one end of a wireless link is moving (slow fading & fast fading) and the RAN is optimized to handle this with a small quality impact. However, the channel quality can also drop persistently, in which case both throughput and latency are impacted.

When a QoS Flow is configured as GBR QoS Flow, the RAN tries to keep fulfilling the GFBR as configured (given that the default priority level of said QoS Flow is higher than for other QoS Flows competing for the same resources), also in bad channel conditions, in which case more radio resources are utilized, leading to an effective cell capacity reduction for other UEs in the cell. Furthermore, the GFBR can also suffer, and notification control may be used to indicate to the core that the configured GFBR cannot be maintained for a QoS Flow. If alternative QoS profiles are configured for this QoS Flow, the RAN can activate such an alternative profile and indicate in the notification which QoS profile is currently considered instead.

When a QoS Flow is configured as non-GBR QoS Flow, the bitrate will go down in bad channel conditions. To what extend this happens depends on the scheduler implementation (there can e.g. be proprietary parameters for maintaining a minimum bitrate for non-GBR QoS Flows), but certainly the priority of this QoS Flow and other QoS Flows is considered.[1]

Regarding the effect of a drop in channel quality on latency, a chain of effects takes place. Firstly, the modulation and coding scheme (MCS) needs to be adapted, which happens based on channel state information (CSI) sent to the RAN by the UE periodically and during certain events. The periodicity of CSI reports is configurable, where of course more frequent CSI reports require extra radio resources. When the RAN receives such CSI reports, after a certain filtering procedure, the MCS will be adapted. If the drop is very significant, a transport might not be decodable after transmission due to the MCS being too high/optimistic, in which case HARQ retransmissions are scheduled (several ms of extra delay), leading to extra delay for each unsuccessful retransmission. If several HARQ retransmissions fail consecutively, in a typical gNB scheduler implementation an outer control loop will trigger an MCS adaptation for future transmissions. If all HARQ retransmissions fail, either an RLC retransmission might be triggered (if RLC acknowledged mode is configured, several 10ms of extra delay). If all of this is unsuccessful, transport and application layer mechanisms can become active. A TCP retransmission e.g. is triggered after 200ms.

4.4 Multi-Connectivity

The purpose of Multi-Connectivity is to use multiple communication paths in parallel for providing better connectivity. The motivation typically is to add redundancy (in case one communication path fails) or improve the overall performance (throughput, latency, reliability). This can be done using different UEs (for connecting to different networks, or being at different locations on a train), using multiple PDU Sessions with different configurations, or using Multi-Connectivity mechanisms within a PDU Session, built into the 5G System.

One approach to this is to select different communication paths for different services, possibly also dynamically. Another approach is to use multiple communication paths for supporting the same service. Most protocols are designed for a single communication path, which is why dedicated multipath protocols typically hide the different communication paths from higher layer protocols. However, as two different communication paths can have different properties, (e.g. latency and capacity), various problems can arise (e.g. receiver needs to wait for a packet that is stuck in one communication path).

[1] There are proprietary approaches on handling conflicting requirements and priorities (e.g. a low priority GBR QoS Flow and a high priority non-GBR Flow), but it's in general advised to avoid such conflicts already in the QoS design for a set of use cases. An analytical approach on the expected behavior is not feasible due to the complexity, coming from the multitude of relevant parameters and dependencies.

4.4.1 Multi-Connectivity in RAN

In 5G-NR, Multi-Connectivity between RAN and a single UE can be realized on different levels, as illustrated in Figure 4.21 and described in the following.

- Coordinated Multipath (CoMP): A CoMP transmission combines multiple transmission points from a single gNB and/or a single UE, much like MIMO, and may use different means of soft combining to decode the data received over the different paths. CoMP is used within a single carrier and is handled on PHY layer. As BBUs (and thus gNBs) are envisioned to be co-located in many cases in the railway deployment, CoMP could be used to enhance connectivity at cell edges.
- Carrier Aggregation (CA): CA is used to combine transmissions over different carriers between the same UE and gNB. Each parallel transmission has its own HARQ process, both transmissions are decoded independently, and aggregated on MAC layer. For ultra-reliable communication, CA can be used for duplication (i.e. same packet is sent over two carriers), at the cost of doubling the require radio resources. If both carriers described in Section 2.3 (900MHz and 1.9GHz) are used, CA can be used to support the most critical services.
- Dual-Connectivity (DC)/ Multi-Connectivity (MC): MC can be used for combining transmissions between one UE and two or more gNBs. In this case, two separate MAC entities are used, possible also different 3GPP RATs, and transmissions are aggregated on PDCP layer. Also, MC can be used for duplication. In general, MC is more designed for static, industrial settings (i.e. UE is not moving) for the sake of increasing reliability at cell edges, not so much for handover scenarios.

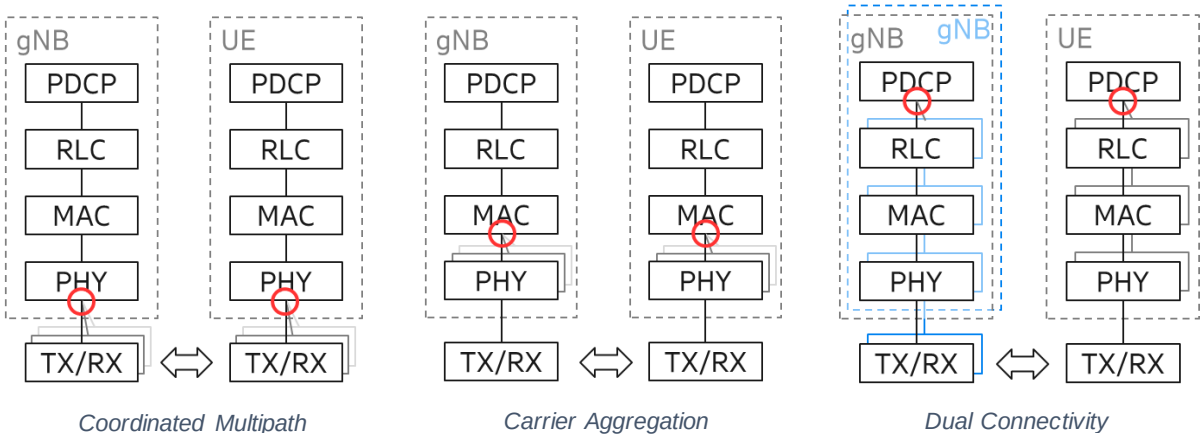

Figure 4.21: High-level illustration of different Multi-Connectivity options defined in 3GPP with corresponding aggregation points (red circles).

Furthermore, 3GPP started working on redundant user plane paths for multiple UEs per device (key word “reliability groups”), but also this is more targeting continuous connectivity to different gNBs by two different UEs in an industrial setting.

4.4.2 Multi-Connectivity above IP

In the railway context, Multi-Connectivity over multiple networks and/or over multiple PDU Sessions in the same network can be of interest, for either redundancy or using another network (WiFi at stations, public mobile networks) as additional bitpipe. These links would be visible as different network interfaces on the UE / Mobile GW, exposed using different IPs to the outside. This topic is not really addressed in scope of the mission-critical services in 3GPP, and some limitations apply when trying to introduce multi-connectivity transparently. Nevertheless, some basic protocols and features are described in the following.

One protocol for aggregating multiple links is multipath TCP (MP-TCP), which supports aggregation of multiple individual TCP connections over different IP connections. Links can be added to and removed from an MP-TCP session, invisible to the service using the MP-TCP session. Furthermore, services can use normal TCP sessions, and MP-TCP and be handled in the protocol stack below, or even on a (possibly transparent) TCP proxy in the path, while the TLS session can still be end-to-end. MP-TCP is of course only applicable to TCP traffic.

A protocol useful for switching between different links is QUIC, which is a Layer 4 protocol implemented in the user space (as opposed to kernel space like TCP and UDP) and reuses simple UDP sockets below. As QUIC uses its own identifiers (connection IDs) different from the IP address, a QUIC session can be maintained while changing the IP session below, e.g. when switching from one network to another in the train (connection migration). As part of this connection migration procedure, a path validation is performed for the new IP address, and no new TLS handshake is required. While QUIC does not support multi-path right now, the expectation is that support for this will be added in the future.

3GPP defines the "Access Traffic Steering, Switching, Splitting" (ATSSS) feature as a means to bundle 3GPP and non-3GPP access, e.g. 5G-NR and WiFi. To achieve this, a multi-access (MA) PDU Session is established with two access networks. The non-3GPP access network needs to be integrated with the 5G Core using an N3IWF (Non-3GPP InterWorking Function) or an ePDG (evolved Packet Data Gateway) if the non-3GPP access network is untrusted, or using a TNGF (Trusted Non-3GPP Gateway Function) or a TWAG (Trusted Wireless Access Gateway) if the non-3GPP access network is trusted.[1] The UE and the PSA UPF then split and merge traffic on both sides of the MA PDU Session. For traffic steering between the two access networks, one option is MP-TCP (UPF may act as a TCP proxy), and the other option is a low layer traffic steering mechanism, which operates below IP layer. In any case, ATSSS rules are used to instruct the UE and the UPF on how to steer traffic over the two access networks, with several options such as active-standby, delay-based, or a load ratio. It needs to be investigated further, whether ATSSS support is required in the chipset, module, modem, or platform, as this determines the expected availability of corresponding client-side products

While ATSSS is integrated into the 5GS specification, MP-TCP, QUIC, and most other multipath protocols operate on top of 5GS and aggregate multiple PDU Sessions from one or more networks. To enable this functionality in FRMCS, the FRMCS Mobile Gateway and the FRMCS Service Server each would need to implement a proxy that splits and combines traffic from the different communication paths and hides the topology from the MCX parts of the system, as MCX specifically is designed for a single communication path. This includes QoS-interactions with the core network. As soon as a second communication path is added, it's not specified in MCX how QoS can be activated for this additional path. The second path can of course be used as a best effort bitpipe, but this can easily degrade the overall channel quality, which is why it's not recommended for latency-critical communication. Further study (and possibly specification) would be needed for supporting multipath with QoS management on both communication paths.

4.5 Service Continuity

Several mobility events during the journey of a train come with an interruption of connectivity, possibly leading to a disruption of the service/application that is using the MC Services and the 5G system. While this section discusses several mobility events – namely cell handovers, edge handovers, inter-PLMN handovers and fallback to public networks – individually, one event may trigger others. A cell handover can trigger an edge handover or and inter-PLMN handover. An inter-PLMN handover will in most cases trigger an edge handover. Consequently, the corresponding quality degradations will happen successively.

[1] When roaming with local breakout in the visited network is used (see Section 3.1.1), an N3IWF or an ePDG is also needed in the VPLMN.

4.5.1 Cell Handovers

During the journey of a train, UEs on the train will be connected to a lot of different cells. While handover procedures between cells are quite optimized already (source and target cell can directly interact to prepare the handover), two main effects on the performance during and after handover can be observed, namely a short interruption of connectivity (several 10ms) and a short throughput dip after handover. The basic handover procedure is illustrated in Figure 4.22.

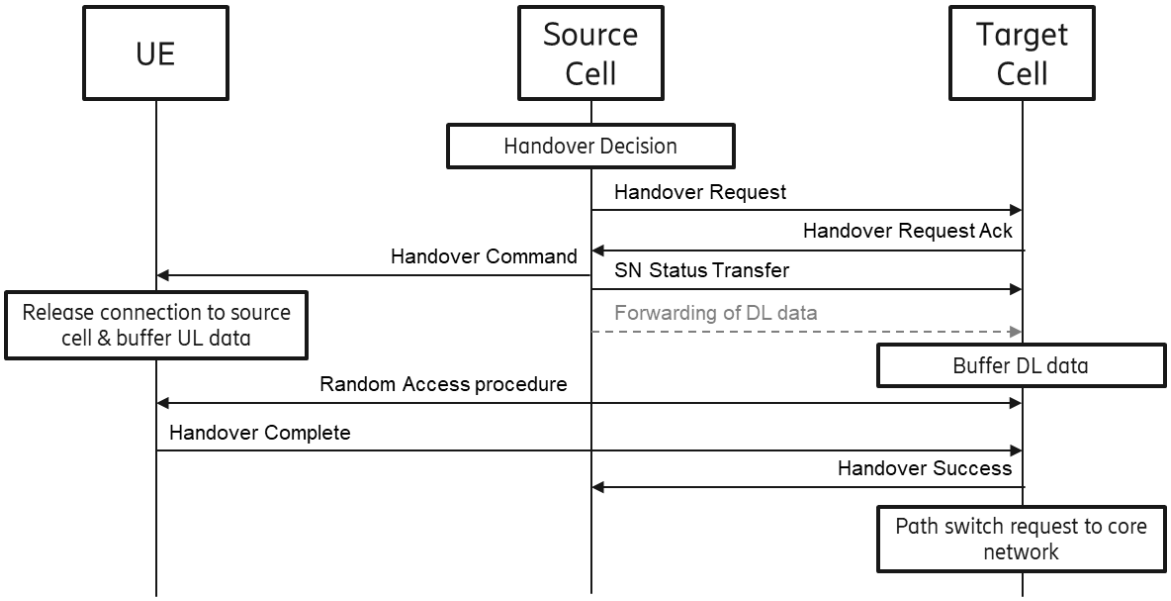

Figure 4.22: Simplified handover procedure.

4.5.1.1 Interruption during Handover

A short interruption is present as a UE first disconnects from the old cell before starting the random access procedure in the new cell. This leads to a handover interruption time of several 10 ms, during which user data is buffered and afterwards forwarded. As a result, user data can experience a maximum additional latency of the interruption time plus the transport delay on the X2 interface between the two gNBs.

If a UE has two transceiver chains[1], the source cell can instruct the UE to stay connected to the source cell until the random access procedure in the target cell is complete (cf. Figure 4.23). Afterwards, UL data transmission is switched from source to target cell, while buffered DL data is still sent in the old cell, before the connection to the old cell is released. As a result, there is no interruption of connectivity. This feature is called dual-active protocol stack (DAPS), which has been standardized as part of 3GPP Release 16.

[1] This has an impact down to the chipset, so it's not possible to simply build a module or modem around a standard chipset. Also, it's unlikely that e.g. chipset support for Dual Connectivity (cf. Section 4.4.1) can be exploited for supporting DAPS, and chipsets are highly optimized for the specific functionality they offer (every millimeter counts).

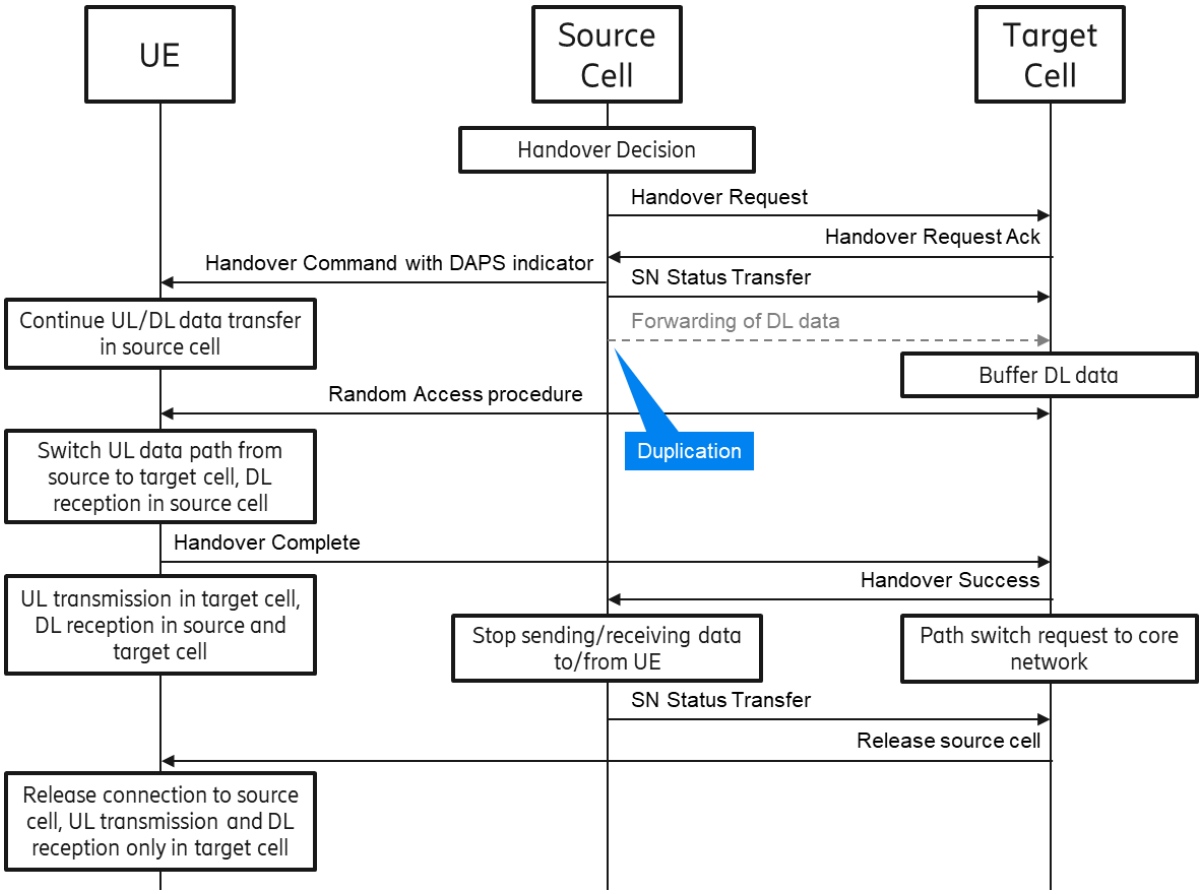

Figure 4.23: Simplified DAPS handover procedure.

Also, as packet duplication of DL data is used in the transition phase, no increased latency is expected from packet forwarding. The connection to the old cell is released only after the path switch is configured in the network.

Figure 4.24 shows the reception delay of UL and DL user data during handover in 5G-NR from a single-user simulation study, with the DAPS mechanism and without (Baseline). In the study, the transport delay between the gNBs is assumed to be 0ms (i.e. gNBs are co-located). The remaining delays in the DAPS case are UE processing delays of up to 3ms. The bad latency performance in the uplink delay that can be observed in the higher percentiles is introduced by issues in the PDCP implementation. While the results would not be as good as the downlink delay, the uplink delay would certainly be lower with DAPS than without. This study did not model the UL path switch, which might cause additional delays inside the UE.

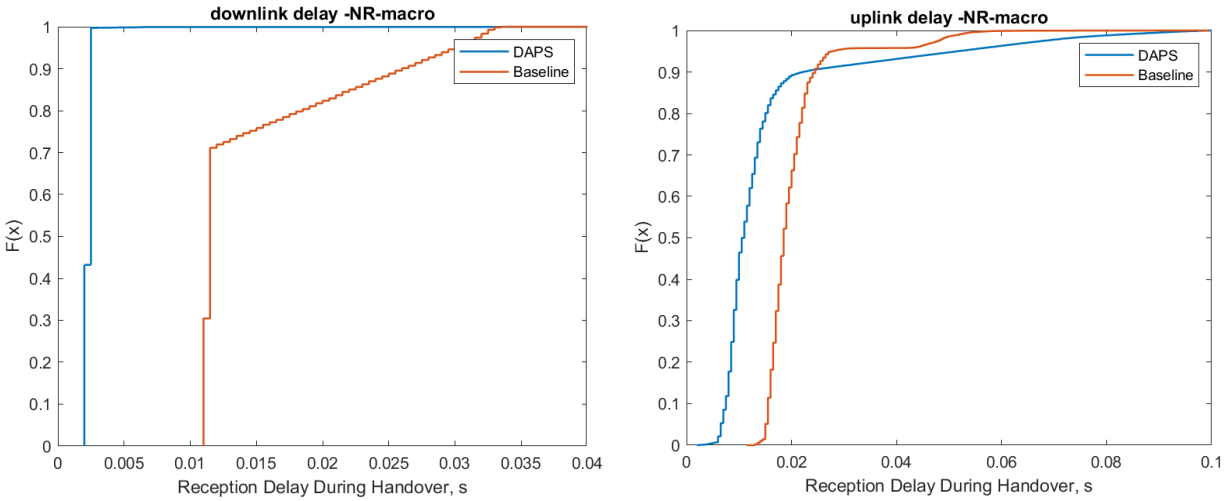

Figure 4.24: DAPS reduces the delay of DL user data down to the UE processing delays in almost all cases. For UL user data, the performance is not as good but in any case lower than for the legacy handover ("Baseline"). The bad performance in the higher percentiles comes from the PDCP implementation in the simulator.

4.5.1.2 Throughput Dip after Handover

During the handover procedure, the target node needs to assume the worst-case radio conditions when scheduling the UE (i.e. pick a low MCS), potentially leading to a significantly lower throughput than what is achievable with the actual channel state. Through link adaption, based on CSI reports by the UE, the MCS is eventually adapted, but this can take some time. As a result of the lower throughput, user data packets might experience additional delay as they are transmitted over more slots than needed. Figure 4.25 shows the potential for improvement, based on a simulation of a legacy link adaptation mechanism, where it takes up to ~20ms for the UE to reach the possible throughput in the simulated scenario.

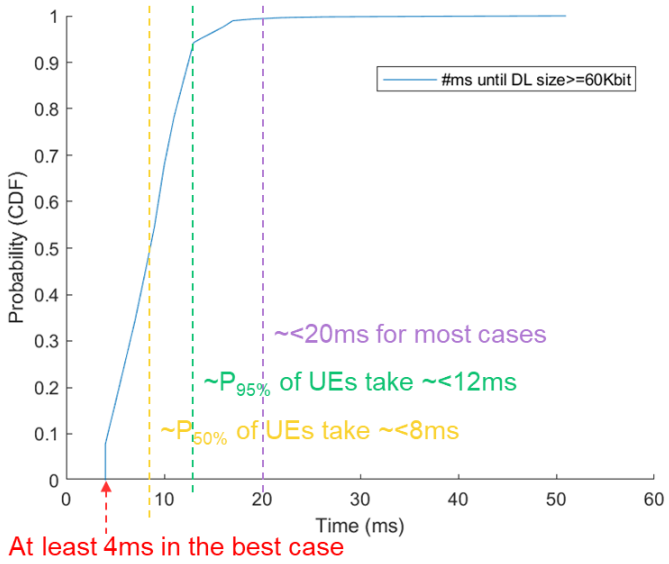

Figure 4.25: Most UEs reach the optimum MCS within 20ms after handover.

A number of improvements are possible to optimize the MCS decision in the target cell after handover, most of which can be realized without impact to standardization. In general, a-priori knowledge helps with optimizing the MCS decision. In the railway scenario, it should be possible to acquire decent a-priori knowledge on the channel state at the cell edge due to the deterministic movement of trains. Consequently, the MCS decision can be configured accordingly, and possibly combined with e.g. conditional handover (handover executed once reaching a certain target SINR for target cell) or blind configuration (useful when knowing a target cell a priori). It's not recommended to hard code MCS values

at the cell edge, to minimize the impact of unforeseen circumstances (e.g. antenna issues, other configuration changes, etc.).

4.5.2 Edge Handovers

During its journey, a train can move over longer distances, where application servers at different edge locations should be used during different sections of the journey. While the application logic for moving to another edge application server is not discussed here, the 5G System offers mechanisms to change the UPF (expected to be co-located with the designated application server) that is used as PDU Session anchor, and through which all user data is passed.

When moving in the network, the PDU Session of a UE will have to be re-anchored to a different UPF at some point. This can be done in a break-before-make manner (SSC mode 2) or in a make-before-break manner (SSC mode 3). In both cases, UPF selection as discussed in Section 4.1 is done as part of the edge handover.

If Session and Service Continuity (SSC) mode 2 is used, the SMF instructs the UE to disconnect from the network and immediately afterwards reconnect, leading to an outage of several 100 ms (cf. Figure 4.26). During the reconnection, the SMF selects a new UPF for the UE, where the new PDU Session is anchored. As a consequence, a new IP is assigned to the UE. For achieving uninterrupted connectivity with SSC mode 2, multiple UEs could be positioned at different ends of the train and aggregated in the FRMCS Mobile Gateway which reconnects over the first UE after edge handover, before the old UE starts the edge handover.

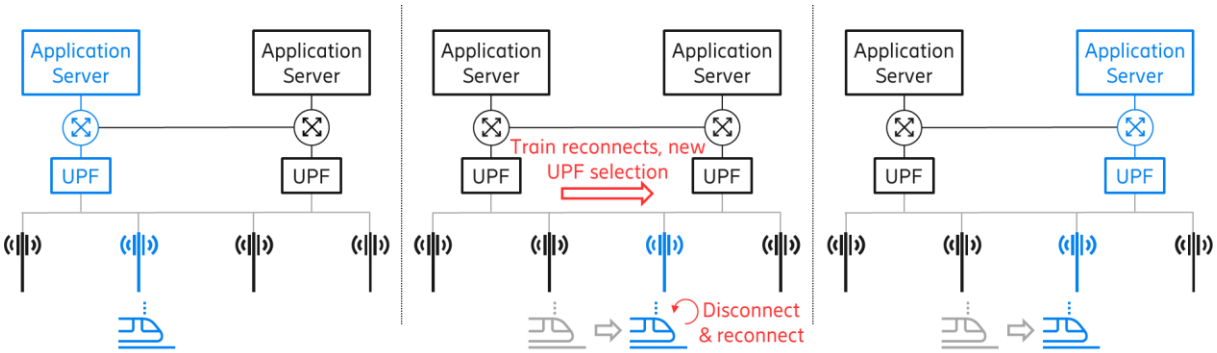

Figure 4.26: When SSC mode 2 is used, a UE first releases the PDU Session and immediately afterwards establishes a new one, as instructed by the SMF.

If SSC mode 3 is used, the SMF instructs the UE to request establishment of another PDU Session (cf. Figure 4.27). This PDU Session will exist in parallel with the old session, leading to another network interface being brought up by the OS that is handling the UE. Consequently, there needs to be functionality on the train for deciding which uplink data is sent via which PDU Session. For optimizing this, a second leg using a different IP link can be added to existing higher layer sessions, to migrate them to the new PDU Session (e.g. in MP-TCP case). Alternatively, higher layer identifiers can be used (e.g. available in QUIC or HTTP) for associating sessions via the older and new PDU Session. The Old PDU Session will time out when not being used anymore. Both PDU Sessions would have the same default QoS configuration, fetched during PDU Session establishment, and dynamic packet detection rules added by the MC Service Server via the SIP core can be added to either PDU session, depending on which PDU session is used to support an MC Service session.

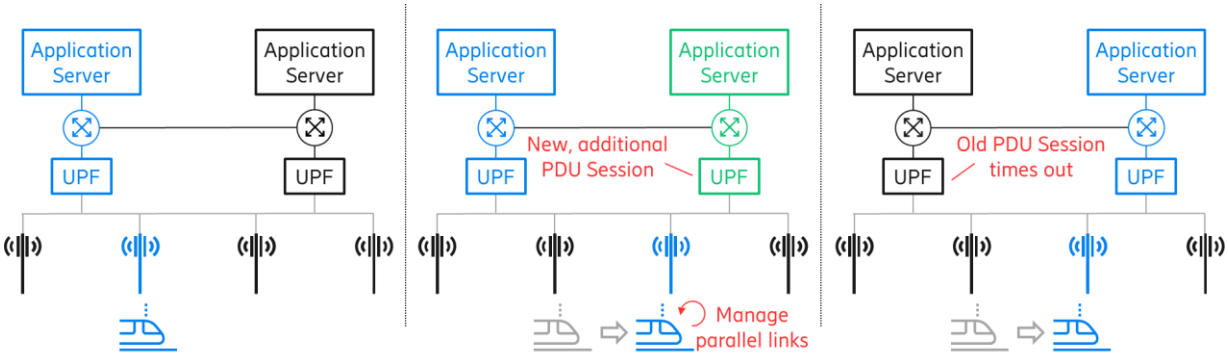

Figure 4.27: When SSC mode 3 is used, the SMF instructs a UE to establish a second PDU Session in parallel, and needs to manage these two sessions for a while, until the old session times out.

Another way to achieve SSC mode 3 is to use PDU Sessions with multiple PDU Session anchors. In this case, a PDU Session at a single UPF is acting as an IP anchor, and multiple UPFs are acting as PDU Session anchors.

One realization of this – possible when IPv6 is used for a PDU Session – is IPv6 Multi-Homing, where an additional IPv6 prefix is added to the existing PDU Session, as described in Section 4.1.2. The new IPv6 prefix is anchored with the new UPF and forwarding based on IPv6 prefix is configured in the I-UPF accordingly (cf. Figure 4.28). The connected device needs to select a prefix when sending an UL IP packet, just like it needs to select an IP address in the multi-session case. Handover between I-UPFs are triggered by and executed after cell handover in a make-before-break manner, i.e. the connectivity of the UE is not interrupted. The old IPv6 prefix and forwarding rules to the old PSA-UPF are removed after a timeout. The FRMCS Mobile Gateway can send a router advertisement for the new prefix to onboard devices, if it acts only as a router and leaves the prefix selection to onboard devices.

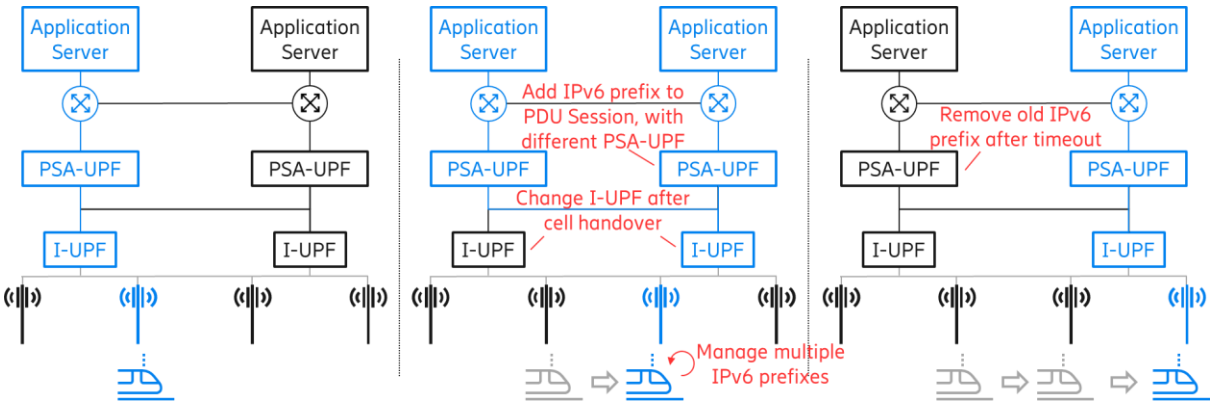

Figure 4.28: When IPv6 multi-homing is used to achieve SSC mode 3, an IPv6 prefix is added to the PDU Session, and an I-UPF in the data path of the PDU Session forwards UL data based on the prefix.

Another realization of multiple PDU Session anchors is using uplink classifiers (ULCLs), where an I-UPF with ULCL functionality is inserted into the data path of the PDU Session, and forwards data to the respective PSA UPFs (described in Section 4.1.1). The ULCL is configured to forward uplink data to the old or new PSA UPF based on destination IP (i.e. of the Application Server) and possibly other parameters. For forwarding data to the old PSA UPF, the I-UPF may either directly forward data to the old PSA UPF, or forward to the old I-UPF which then forwards to the old PSA UPF (as illustrated in Figure 4.29).

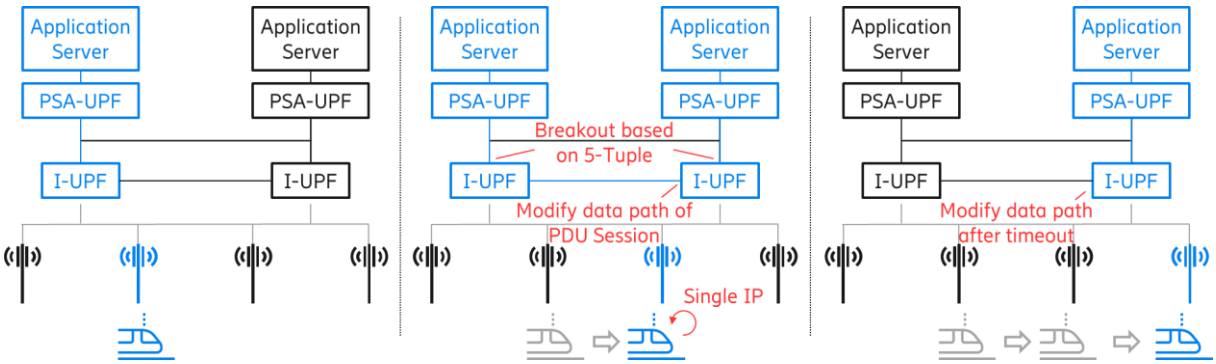

Figure 4.29: When ULCLs are used to achieve SSC mode 3, an I-UPF forwards data based on configured rules and header inspection, while the UE is unaware of this.

In both realizations, the I-UPF can be co-located with (or integrated in) a PSA-UPF, or co-located with the RAN (cf. Figure 4.30), or be deployed anywhere else. Integration with the PSA-UPF is the leanest deployment and has the lowest signaling overhead, but comes with additional latency, as the traffic is always routing via the current PSA-UPF while shorter paths might be available. Co-location with RAN has the best latency performance as the shortest data path can be realized, but another UPF must be deployed (potentially requiring a virtualized environment, housing, different hardware than RAN, etc.). Integration into RAN hardware would be a good deployment option, but it's unclear whether products will support this.

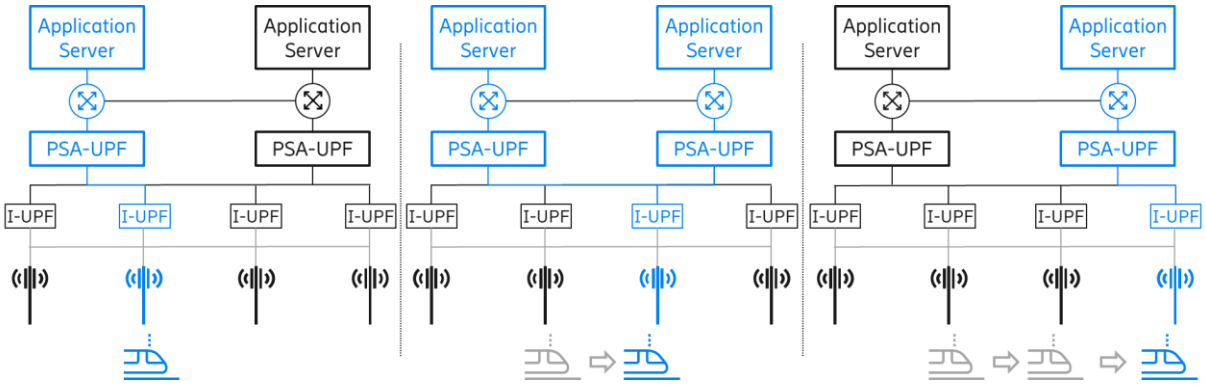

Figure 4.30: I-UPFs can be co-located with or integrated into the RAN for shortest data path, which however requires additional handovers between I-UPFs.

4.5.2.1 Edge Handovers with Framed Routing

Framed routes, as introduced in Section 4.2.4, can be configured for a PDU Session, so that the PSA-UPF knows that DL data to the IP addresses corresponding to the framed routes shall be sent via this PDU Session. IP configuration happens over the top of the 5GS.

During mobility of a PDU Session with a single PDU Session anchor, new device IPs and framed routes must be configured for the new PSA UPF, to avoid ambiguous routing of DL data. Thus, devices on the train must be triggered to request a new IP using DHCP (or similar procedures) when a new PDU Session is established, and potentially handle two network interfaces in parallel for make-before-break connectivity (cf. Figure 4.31). More detailed verification of this approach would be required.

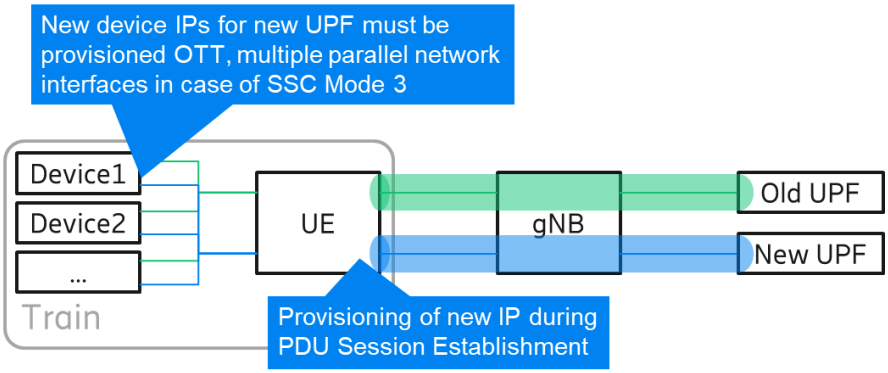

Figure 4.31: Connectivity over PDU Sessions to new and old UPF during an edge handover.

Changing the device IP can possibly be avoided by combining framed routing with ULCL, introduced in Section 4.2.3, where all challenges and solutions for DL routing are also applicable to framed routes. When using ULCL, a UE keeps its assigned IP address even during edge handovers, including the framed routes configured for a PDU Session, and routing between different edges can be done within the core network.

4.5.2.2 Edge Handovers with IPv6 Prefix Delegation

When using IPv6 prefix delegation, as described in Section 4.2.5, the same basic mechanisms are required as for framed routing, and the same problems arise.

4.5.3 Inter-PLMN Handovers

Section 3.1 introduced several options for enabling good connectivity in visited countries. When a network with its own PLMN is deployed in each country (i.e. there is no “EU-wide NG-RAN” with the same PLMN), then a 5G-UE crossing country borders needs to change to a different NG-RAN with a different PLMN.

Such an NG-RAN change comes with an interruption due to context transfers etc. in the network, but several mechanisms exist to optimize this change and minimize the interruption time.

When having no supporting mechanism at all, the UE will run out of coverage of the source NG-RAN and will have to start searching for an available NG-RAN from scratch (starting with looking for a signal in various carrier frequencies). This may include several failed connection attempts. Field tests with LTE showed that it takes several minutes until connectivity over the target NG-RAN is available again.

This can be significantly improved using idle-mode mobility procedures, where the source NG-RAN redirects the UE to the target frequency and PLMN when releasing the connection. Registration and authentication in the target network are facilitated by the source AMF, which the target AMF contacts for fetching the UE context (specified in Sections 4.23.3 and 4.23.4 of [12]). Field tests with LTE using corresponding EPS procedures showed that it takes around 1 second until connectivity over the target NG-RAN available is again.

Another improvement is possible using an N2-based inter NG-RAN handover, which includes a preparation phase between the source and the target 5G System and a shortened execution phase (specified in Section 4.23.7 of [12]). This type of handover is similar to an S1 handover in LTE, for which field trials showed an interruption time of ~0.1 seconds. However, the old PSA UPF is kept during this procedure, and the H-SMF needs to be configured to initiate a PDU Session deletion with reactivation requirement afterwards, i.e. it will essentially trigger the UE to reconnect and force a look-up of LBO configuration in the H-UDM, leading to an LBO configuration in the visited network. The additional interruption time due to this procedure needs to be tested.

In general, 5GS also specifies an Xn-based inter NG-RAN handover (i.e. involving direct interaction between source and target RAN, similar to a normal cell handover), which is even more optimized. However, it requires the two NG-RANs to be handled by the same AMF, which is why it's not applicable here.

All in all, the AMF needs to be changed when moving between networks with different PLMNs, and further optimization than the N2-based inter NG-RAN handover is likely not possible. If the corresponding interruption time is not acceptable, the only options left are to either make use of the length of the train and UEs in the front and in the back to bridge the interruption time, or to have the same PLMN in both countries[1].

One aspect to consider for the interruption time is also the coverage at the country border. Typically, the allowed radiation levels at a given distance beyond the border are regulated by respective national agencies (e.g. BNetzA in Germany). With these constraints, MNOs can then tweak their coverage to have an optimal performance at the country border, which is a typical network deployment optimization task with lots of experience available in the field. Given that neighboring MNOs collaborate on this, good results can be achieved[2], but the regulation needs to allow for this to happen. In the past, coverage gaps on the country borders often existed, due to very low power regulations on at least one side of the border.

[1] This has a lot of implications, starting with operation of the UDM and provisioning of SIM cards. Extensive studying would be needed to assess the full implications of a 5G deployment with such a premise.
[2] The target is to find the sweet spot between too low reception power and too much interference need to be found, at all populated or frequented areas along the cell/country border.

5 Summary and Open Questions

In the study, we highlighted several key aspects to be considered in the FRMCS 5G E2E System design and discussed different solution approaches.

One key topic discussed in the study revolves around controlling the user data path (e.g. by means of User Plane Function (UPF) selection) in the 5G core network, and related IP routing and assignment options. For the UPF selection, it was shown that using uplink classifiers (ULCLs) for routing uplink data to different edges within the core network facilitates the use of the 5G System by higher layer protocols (no IP address changes, flexible & selective uplink routing based on destination), but also can come with substantial drawbacks. When having a very controlled and static deployment with strictly isolated edges, using ULCL can work very well, but it is not recommended for more general deployments, where the deployment of edge servers and core network is not perfectly planned and aligned. On the other hand, using network address translation (NAT) on the FRMCS Mobile Gateway allows for a clean split of responsibility between onboard and trackside infrastructure/network in relation to session establishment with MC Services, which can be addressed using an Application Layer Gateway (ALG) on the FRMCS Service Server. Using framed routing or IPv6 prefix delegation avoids having NAT and ALG functionality on the gateway (i.e. reduced complexity for this component), but on the other hand complicates the integration of onboard components with the network and trackside components for IP management. Also, if framed routes or delegated IPv6 prefixes kept during UPF relocations, the onboard devices can avoid some complexity, but this complexity is pushed to the IP infrastructure in the backbone and integration with the core network, to route downlink IP data to the same IP address via multiple possible UPFs. In general, IPv6 offers more flexibility compared to IPv4 when targeting service continuity and multi-connectivity above IP and is recommended.

Also, for allowing a flexible deployment of UEs on the train, separate from the FRMCS Mobile Gateway, the use of IPv6 Router Advertisements, IPv6 Prefix Delegation and Framed Routes to that end, where UEs are transparent in the IP data path, should be further investigated.

In relation to Quality-ot-Service (QoS), several options to apply different QoS treatment to different service data flows were discussed, and the achievable latencies for several radio configurations were shown. QoS for MC services is already specified quite precisely, including which 5QIs have to be used. While there is some freedom for MCData to apply different 5QIs, it has to be studied further how the specifications can support the indication of specific service types, in order to apply the right QoS policies to the right MC service data flows. Finally, it should be studied further if the given set of use cases can be served with these QoS requirements, given the currently allocated spectrum.

A number of mechanisms exist to make use of multiple connections, either on various RAN layers, or above IP, a recommendation regarding such mechanisms should consider also the deployment and redundancy concept of the train's onboard system, for which alignment with work in TOBA and OCORA workgroups is relevant. A key feature in the 5G system might be the "reliability groups", which can assist in providing fully redundant paths to an onboard device via two different UEs. Also, using QUIC (transparent or non-transparent) should be considered as a transport layer protocol that allows separation of a location identification (i.e., IP address) and session identification.

Service Continuity is an important requirement for rail telecommunications, especially for higher grades of automation, and has to be tackled specifically in different events. While cell handovers are already quite optimized, mechanisms were introduced that can further decrease the performance impact during and after a cell handover, especially when using a-priori knowledge in the relatively well-known rail-specific RAN deployments. For these various features, rail-specific simulations would give better insights on the achievable performance gains.

Also edge handovers (i.e. relocation of a PDU Session to a different UPF, and changing the serving edge server) can be supported by a number of mechanisms in the core network that are already well-studied. While using intermediate UPFs (I-UPFs) with ULCLs can in principle deliver a great performance here, they come with significantly higher complexity in the core network and transport infrastructure and are expected to have a very small market. Using Session and Service Continuity (SSC) Mode 3 with single-homed PDU Sessions requires more intelligence in the UEs, but is otherwise the simpler and more robust solution, and also applicable to a broader set of use cases outside of the railway vertical. Finally, optimizations to reduce the interruption time during border crossing exist already, and only require an integration step between the core networks on both sides of the border, effectively reducing the interruption time to ~100ms, which is definitely recommended. It needs to be studied further how MC Services can best handle these scenarios, building on the studied core network procedures.

In summary, with the joint investigation, some key design trade-offs have been discussed, which can serve as a basis for the FRMCS design, and further steps to be addressed – e.g. within the standardization – have been identified.

6 References

[1] UIC, „FRMCS User Requirements Specification Version 5.0.0," 2020.

[2] UIC, „Use Cases, Version 2.0.0," FRMCS Functional Working Group & Architecture and Technology, 2020.

[3] ETSI TR 103.459, „FRMCS Architecture, V1.2.1," ETSI TC RT, 2020.

[4] International Association of Public Transport, „A global bid for automation: UITP Observatory of Automated Metros," 2011.

[5] 3GPP TR 22.889, „Study on Future Railway Mobile Communication System (FRMCS) v17.4.0," 2021.

[6] 3GPP TS 22.289, „Mobile Communication System for Railways v17.0.0," 2019.

[7] 3GPP TR 23.790, „Study on application architecture for the Future Railway Mobile Communication System (FRMCS) v15.0.0," 2018.

[8] 3GPP TR 23.796, „Study on application architecture for the Future Railway Mobile Communication System - Phase 2 v16.0.0," 2019.

[9] E. D. (02)05, „The designation and availability of frequency bands for railway purposes in the 876-880 MHz and 921-925 MHz bands," 2002.

[10] 3GPP TR 23.700-79, „Study of gateway User Equipment (UE) function for Mission Critical (MC) communications v2.0.0," 2021.

[11] 3GPP TS 23.501, „System Architecture for the 5G System v17.2.0," 2021.

[12] 3GPP TS 23.502, „Procedures for the 5G System v17.2.1," 2021.

[13] ITU-T G Suppl. 66, „5G wireless fronthaul requirements in a passive optical network context," 2019.

[14] 3GPP TS 23.280, „Common functional architecture to support mission critical services v17.8.0," 2021.

[15] 3GPP TS 23.281, „Functional architecture and information flows to support Mission Critical Video (MCVideo) v17.6.0," 2021.

[16] 3GPP TS 23.282, „Functional architecture and information flows to support Mission Critical Data (MCData) v17.8.0," 2021.

[17] 3GPP TS 23.379, „Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT) v17.8.0," 2021.

[18] 3GPP TR 23.783, „Study on Mission Critical (MC) services support over the 5G System (5GS) v1.6.0," 2021.

[19] 3GPP TS 23.289, „Mission Critical services over 5G System v17.0.0," 2021.

[20] 3GPP TS 23.003, „Numbering, addressing and identification v17.3.0,“ 2021.

[21] 3GPP TS 38.214, „NR; Physical layer procedures for data v16.7.0,“ 2021.

[22] Ericsson 3GPP Tdoc R2-1812254, „IMT-2020 self-evaluation: UP latency in NR,“ 2018.

[23] 3GPP TS 24.007, „Mobile radio interface signalling layer 3 v17.2.0,“ 2021.

[24] 3GPP TS 24.501, „Non-Access-Stratum (NAS) protocol for 5G System (5GS) v17.4.1,“ 2021.