Grant Agreement N°: 952189

Topic: ICT-53-2020

Next generation connectivity for enhanced, safe & efficient transport & logistics

D5.5: Report on dual SIM for seamless cross border TO

Revision: v.1.0

Work package	WP5
Task	T5.5
Due date	30/11/2023
Submission date	12/12/2023
Deliverable lead	Roboauto
Version	1.0

Abstract

While 5G aims to greatly reduce the connection downtime experienced when border crossing, there is no definite approach on the network level yet. The ICT-18 projects 5G-MOBIX, 5G-CARMEN and 5GCroCo have demonstrated the extent to which service interruption can be brought down leveraging the capabilities of 5G. The times achieved using inter-PLMN handover went as low as 121 ms. This level of connection continuity is sufficient for almost any application including most Connected and Automated Mobility services, and nearly so for teleoperation. It was, however, indicated that to achieve such numbers, a great deal of cooperation between MNOs operating under different legislations is required. Preliminary results of activities within the 5G-Blueprint project indicate that the service interruption time may be reduced even further, becoming sufficiently stable even for teleoperation and remote monitoring of autonomous vehicles. This research may even lead to the modification of the corresponding 3GPP standard, simplifying the communication protocol used for inter-PLMN handover. Even still, the need for cooperation between MNOs presents large difficulties, some of which are not even discovered yet. This deliverable presents our end-device approach that is essentially a multi-SIM/multi-modem solution. Besides requiring little coordination between MNOs, save for sufficient overlap of e/gNB coverage, the use cases that benefit from this solution go beyond border crossings and include a crossing of different network types, or simply increasing the service availability, and/or bandwidth. The devised multi-SIM solution takes learnings from what was already developed in 5G-MOBIX in providing more control over the data flows. In this deliverable, we present a novel approach to multi-modem data transmission implemented on the computational unit using standard toolset available on Linux systems supported by the higher layer protocols.

Keywords: dual-sim, 5G, teleoperation, cross-border, communication, redundancy, latency, load balancing, cellular, iptables, routing.

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	14-08-2023	First version	Jakub Juza (Roboauto), Jan Capek (Roboauto)
V0.2	22-11-2023	Internal review	Ghazaleh Kia (SEAFAR), M.C. Campodonico (Martel)
V.0.3	30-11-2023	Revised version	Oliver Held (Roboauto)
V1.0	12-12-2023	Final version ready for submission	Wim Vandenberghe (MIW)

Disclaimer

The information, documentation and figures available in this deliverable, is written by the 5G-Blueprint (Next generation connectivity for enhanced, safe & efficient transport & logistics) – project consortium under EC grant agreement 952189 and does not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.

Project co-funded by the European Commission under H2020-ICT-2018-20		
Nature of the deliverable:	R	
Dissemination Level		
PU	Public, fully open, e.g. web	√
CI	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to 5G-Blueprint project and Commission Services	

* R: Document, report (excluding the periodic and final reports)
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.

EXECUTIVE SUMMARY

Latest market research reports indicate that the teleoperation market valuation is expected to surpass $530M in 2028 with the market opening up in 2024 [1]. However, any future commercial deployment of remote vehicle operation has a precondition that all safety aspects and implications of the application have been considered. Teleoperation has one of the most stringent requirements on network availability and stability of not only CAM solutions but of all wireless network applications in general. A connection loss or latency spike of even less than 200 milliseconds needs to result in a safety stop manoeuvre as the distance travelled the vehicle travels essentially uncontrolled by the remote operator may result in an accident, especially when taking a turn or making a lane change. The safe stop not only makes the experience of the remote operator less pleasant but also decreases the energy efficiency of the vehicle due to additional stopping and acceleration. Even greater is the impact on the disruption of the surrounding traffic flow and decreased predictability of the vehicle's trajectory, resulting in a greater chance of accident. To increase the network availability and stability has been one of the key areas of focus of MNOs and the whole wireless network industry. Country border crossings are one of the most prominent examples of areas that are still not solved in a standard manner and isn't likely to be widely implemented in the upcoming years during which the teleoperation market is expected to reach a substantial size already. To overcome this obstacle, teleoperation providers and developers need to devise ways these shortcomings of the current state of wireless networks. This deliverable presents one such approach, and while such solutions will likely become obsolete in the years to come, as the wireless networks mature and reach greater technical capabilities, it may become an enabler for a commercial deployment. By enhancing the safety, efficiency and user experience implications of network availability and stability, it will shorten the time to market. It is highly probable that during the early years of teleoperation deployments, multi-SIM solutions will be a requirement, and will only differ in their implementation. The described approach has a great benefit of being vendor and UE independent, allowing the UE most fit for the use case to be used. Due to the ongoing development of the standard and subsequently the UE and its firmware, this is a benefit that cannot be downplayed. Additionally, as the chip-crisis that stemmed from the COVID-19 pandemic proved, solutions that are not reliant on a single vendor may gain a significant advantage.

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

3GPP	*Third Generation Partnership Project*
4G	*Fourth Generation*
5G	*Fifth Generation*
ADAS	*Advanced Driver Assistance Systems*
C-ITS	*Cooperative Intelligent Transport System*
CA	*Carrier Aggregation*
CAM	*Cooperative Awareness Message*
CAV	*Connected Autonomous Vehicles*
CC	*Carrier Component*
CCAM	*Cooperative, Connected & Automated Mobility*
COTS	*Commercial Off the Shelf*
CRS	*Cell-specific Reference Signal*
CSMA/CA	*Carrier-Sense Multiple Access with Collision Avoidance*
D2D	*Device-to-Device*
DENM	*Decentralized Environment Notification Message*
DSRC	*Dedicated Short Range Communication*
DUST	*Distributed Uniform Streaming*
eNB	*Evolved Node B*
ETSI	*European Telecommunications Standards Institute*
GLOSA	*Green Light Optimal Speed Advisory*
gNB	*Next Generation NodeB*
GNSS	*Global Navigation Satellite System*
HO	*Hand Over*
HPLMN	*Home Public Land Mobile Network*
I2V	*Infrastructure-to-Vehicle*
IEEE	*Institute of Electrical & Electronics Engineers*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
IVIM	*Infrastructure to Vehicle Information Message*
KPI	*Key Performance Indicator*
LIDAR	*Light Detection and Ranging*
LR	*Long Range*

LTE	*Long Term Evolution*
MAPEM	*MAP Extended Message*
MEC	*Multi-Access Edge Computing*
MNO	*Mobile Network Operators*
N2V	*Network to Vehicle*
NEF	*Network Exposure Function*
NCM	*NR Sidelink Communication Manager*
NR	*New Radio*
OBU	*On-Board Unit*
OEM	*Original Equipment Manufacturer*
OPLMNwAcT	*Operator controlled PLMN selector with Access Technology*
PBCH	*Physical Broadcast Channel*
PLMN	*Public Land Mobile Network*
RADAR	*Radio Detection and Ranging*
RF	*Radio Frequency*
RSRP	*Reference Signal Receive Power*
RSRQ	*Reference Signal Received Quality*
RSU	*Roadside Unit*
RTP	*Real-time Transport Protocol*
SCM	*Sidelink Communication Manager*
SDR	*Software-Defined Radio*
SIM	*Subscriber Identity Module*
SPAT	*Signal Phase and Timing Message*
SPATEM	*Signal Phase and Timing Extended Message*
SPS	*Semi Persistent Scheduling*
SR	*Short Range*
SREM	*Signal Request Extended Message*
SRTP	*Secure Real-time Transport Protocol*
SS	*Synchronization Signal*
SSEM	*Signal request Status Extended Message*
TCP	*Transmission Control Protocol*
UE	*User Equipment*
UDP	*User Datagram Protocol*
V2I	*Vehicle-to-Infrastructure*

V2I2V	*Vehicle to Infrastructure to Vehicle*
V2N	*Vehicle-to-Network*
V2P	*Vehicle-to-Pedestrian*
V2V	*Vehicle-to-Vehicle*
V2X	*Vehicle to Everything*
VCC	*Vehicular Cloud Computing*
VEC	*Vehicular Edge Computing*
VPN	*Virtual Private Network*
VRU	*Vulnerable Road User*

1. INTRODUCTION

With trucks and other vehicles being driven by remote operators sitting sometimes hundreds of kilometers away from the vehicles themselves during teleoperation, the stability of the connection between the remote operation center and the vehicle is of utmost importance. This places great requirements on the performance of the wireless network. While intra-PLMN inter-gNB handovers are well defined and do not have any noticeable impact on network availability from the application perspective, inter-PLMN handover is an area that is the focus of many ongoing research activities, including the 5G-Blueprint project. While this work is still ongoing and significant progress has been made, the work described in this deliverable is an approach that is fully independent on it and has applications beyond the border crossing use case.

Using multiple data channels to make up for the discrepancies caused by the disruptions in availability in one of the channels seems like a straightforward solution. However, there are multiple approaches to the problem that can be grouped by different parameters. One such dichotomy is between the failover approach and simultaneous data transmission. Another way to differentiate between possible approaches is where the multi-channel approach is implemented. This can be done either at the point of origin of the data (e.g. a computer) or at the UE - typically a router. Each of these approaches has their pros and cons that will be further described in the following sections. The main focus of this deliverable is to describe the multi-SIM solution that was implemented within the 5G-Blueprint project, the results that were achieved during its testing, and a look forward into its practical use cases as well as how it can be further improved and extended beyond what was within the scope of this project.

2. POSSIBLE APPROACHES TO CROSS-BORDER SCENARIOS

With current mobile networks (3G, 4G), users may be disconnected for several minutes when traversing a border. By design, the User Equipment - UE tries to stay connected to an e/gNB and if it loses the connection, it will take some time to search for a new network. When attempting to optimize this behaviour, solutions arise at both the UE and the network side. For instance, the UE can start searching earlier for other PLMNs and switch to the next PLMN before the connection is lost. When using multiple modems in parallel, a connection failure can even be avoided altogether. It is however also possible to resolve this issue with a network handover between bordering networks. Different levels of integrations are possible between bordering networks to limit or even prevent data loss when moving between networks. Although HOs between bordering networks are possible, there are still significant limitations preventing Mobile Network Operators (MNOs) to implement this at scale.

We can break down the methods to limit the disconnect time in two classes:

- UE based measures.
- Network based measures.

2.1.UE based measures

2.1.1. COTS Failover Solutions

As we have established in chapter above, there are no standardized solutions that would guarantee a seamless handover during border crossing during which there would be no noticeable loss of service. The most straightforward and natural approach to deal with service loss is fail-over. Network failover solutions offer a reliable way to maintain connectivity even in the face of unexpected outages or disruptions. These solutions work by providing redundancy in network connections. When the primary network link experiences issues, failover mechanisms seamlessly switch traffic to a secondary connection, minimizing downtime and keeping critical operations running smoothly. Network failover solutions come in various forms, from simple backup connections to more complex setups involving multiple ISPs or technologies. They are not only valuable for maintaining business continuity but also for enhancing network performance and reliability.

A general mark of fail-over systems is that only one connection is used to actively transfer the data at a time. An alternative connection is chosen when a problem with the primary connection is detected.

As we are looking for solutions that would substitute the handover happening on the network level, it makes sense to focus on fail-over approaches available on the user equipment. These can be roughly categorized as follows:

Failover solutions in user equipment are mechanisms or technologies that enable devices, such as computers, smartphones, and routers, to switch seamlessly between different network connections when one becomes unavailable. These solutions enhance connectivity and reduce downtime. Here are some common failover solutions in user equipment:

- **Dual SIM Cards:** Many smartphones and some tablets support dual SIM cards. When one network signal is weak or unavailable, the device can switch to the other SIM card and its associated network.

- **Mobile Hotspot Failover:** Mobile hotspots and routers often support failover between different types of connections, such as switching from a wired broadband connection to a mobile data connection when the primary network goes down.
- **Wi-Fi Failover:** Some devices, especially in the Internet of Things (IoT) realm, support failover between different Wi-Fi networks. For example, a device might switch to a secondary Wi-Fi network when the primary network is out of range.
- **Ethernet/Wi-Fi Failover:** In laptops and some home routers, you can configure failover between Ethernet and Wi-Fi connections. If the wired connection drops, the device can switch to Wi-Fi or vice versa.
- **VPN Failover:** In business settings, VPN clients can be configured to failover between different VPN servers or gateways. If one is unavailable, the client will automatically connect to an alternative.
- **Dual SIM cellular Routers:** Some advanced routers offer failover capabilities. They can switch to a backup connection if one fails.

These failover solutions in user equipment are designed to improve connectivity, reduce downtime, and enhance the user experience, whether for personal use or in a business context. The choice of solution depends on the specific use case and the devices involved.

From the point of view of the teleoperation use case, it makes sense to zoom in on the Dual SIM card fail-over approach as this is the most commonly used one, even if a fail-over to a WiFi connection may make sense in some cases. Even though during the early prototype phases a cell phone can be used on the vehicle side, we will focus on the more advanced stage of using wireless routers.

2.1.1.1. Failover Dual SIM routers

Our examination of dual SIM routers encompasses their hardware design, radio frequency management, network selection algorithms, user interface, software integration, battery management, user experience, adherence to global standards, and secure data storage.

At the core of dual SIM routers lies an intricate hardware design that accommodates two SIM card slots within the device's form factor. These slots are engineered with precision to guarantee proper contact with the device's circuitry, enabling a seamless transition between the two SIM cards. As a further extension, a cellular router may be dual-modem. This means having two largely independent cellular modems with their independent radios, each potentially being Dual SIM. This enables further features, such as load balancing, as traffic can be transferred through two SIM cards simultaneously. However, this will be explored more in detail further down in this deliverable. For now, we will focus on the fail over capability of dual SIM routers.

Dual SIM routers feature advanced radio frequency (RF) management systems, comprising multiple transceivers and antennas. These components are meticulously tuned to distinct frequency bands, ensuring optimal signal reception and transmission. Such an arrangement proves invaluable in maintaining network connectivity even in the presence of disruptive factors.

The heart of dual SIM router functionality resides in the deployment of sophisticated network selection algorithms. These algorithms take into account a plethora of factors, including signal strength, available network types (ranging from 3G to 5G), and user-defined preferences. This intellectual decision-making process governs the seamless transition between SIM cards based on network availability and prioritization.

A seamless user experience is the ultimate objective of dual SIM routers. In the event of signal disruptions, the router's software operates in such a way as to ensure that users remain connected with minimal disruption.

Dual SIM technology in routers adheres to stringent global standards, ensuring compatibility with SIM cards from diverse mobile carriers and network technologies worldwide. This global compatibility empowers users to maintain internet access while traveling internationally or transitioning between carriers.

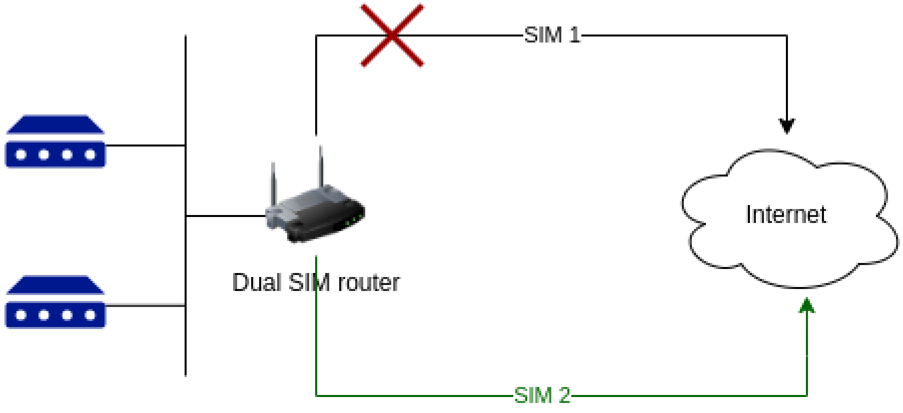


Figure 1: Dual SIM Failover

2.1.1.2. Failover Dual SIM Routers and Teleoperation

In order to be usable for teleoperation in the cross-border scenario, the switch to the back-up network must be done in lower hundreds of milliseconds. There is a possibility to limit the maximum vehicle speed based on its location, however, an interruption in the connection between the vehicle and the remote control station lasting longer than 200 ms must result in the vehicle initiating an emergency stop maneuver. The data on the time it takes to switch between two different SIM cards in a failover dual SIM router that is provided by the manufacturers and distributors is inconclusive so we chose to test the viability of this approach in practice.

From the point of the failover approach, the only thing that matters is the loss of connectivity through the primary SIM card. It does not matter whether it happens at a border crossing or any other place as long as the secondary SIM card has connectivity to switch to. Thus in order to increase our efficiency, we performed the tests using SIM cards from two different Czech MNOs at spots we knew we were consistently losing connection at with one of them, while realistically emulating the cross-border environment.

The tests were performed using two different routers from two manufacturers using the latest available firmware on each one. The first tested router was a Teltonika RUTX09. It is an industrial Dual SIM router with failover capability. We have extensive experience with Teltonika LTE routers, having used the RUT240 since 2018. The second router we used was the Advantech ICR-2834, also a Dual SIM industrial router with failover capability.

Figure 2: Teltonika RUTX09 Dual SIM LTE router

To properly test the failover functionality, the vehicle was not controlled through teleoperation during these trials, as in case the connection between the remote control station and the vehicle is lost, the vehicle performs an emergency stop. We did, however, have the teleoperation system up and we monitored how long the connection loss lasts. Soon after starting the tests, we ran into another issue that we noticed thanks to monitoring the data source. Before the failover happened, we regained connection through the primary SIM card. Thus we had to stop the car in the blind spot to be able to test how long the actual failover takes. Unfortunately, even after various parameter tweaks, we were not able to reduce the downtime below several seconds, reaching the conclusion that failover dual sim routers are not suitable to ensure uninterrupted connection during cross-border teleoperation scenarios.

2.1.1.3. Enhanced UE-based approaches

By default the UE only starts to search and switch to a new network when the network connection is lost. This behavior can be changed with an application, which forces the UE to another network before it loses the connection. This can be achieved by measuring the signal strength: when the signal strength is below a certain threshold an application starts to search for other networks and if there is a better network forces the modem to connect to this other network. This application can run on the SIM, preventing the need of needing extra equipment. Although this method can be very effective in certain cases (e.g. moving from a private network towards a public network), when applied at large it can result in a lot of searches and reconnects at border crossings. Our borders don’t follow a straight line and the signal strength is not always a good indicator to direct a switch. Especially since practical tests show that a switch to a new network can take between 2 and 10 seconds in optimum conditions.

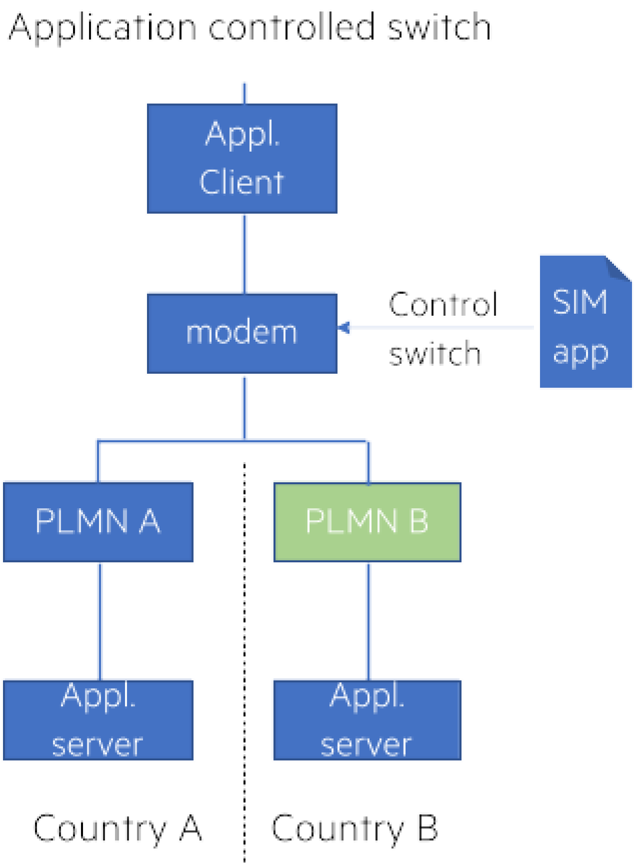


Figure 3: Application controlled switch to the new network

This method can be optimized by applying learnings from previous border crossings using a central prediction function running. In the 5G-Mobix project (see [2] section 3.4) a central prediction function was applied. The UE could query this prediction function and based on its location determine the best moment to handover to the other network. Although in the 5G-mobix test this prediction function was applied on a multi-modem setup to switch between the two modems, the principle of using a central function to predict the best handover location and network stays the same.

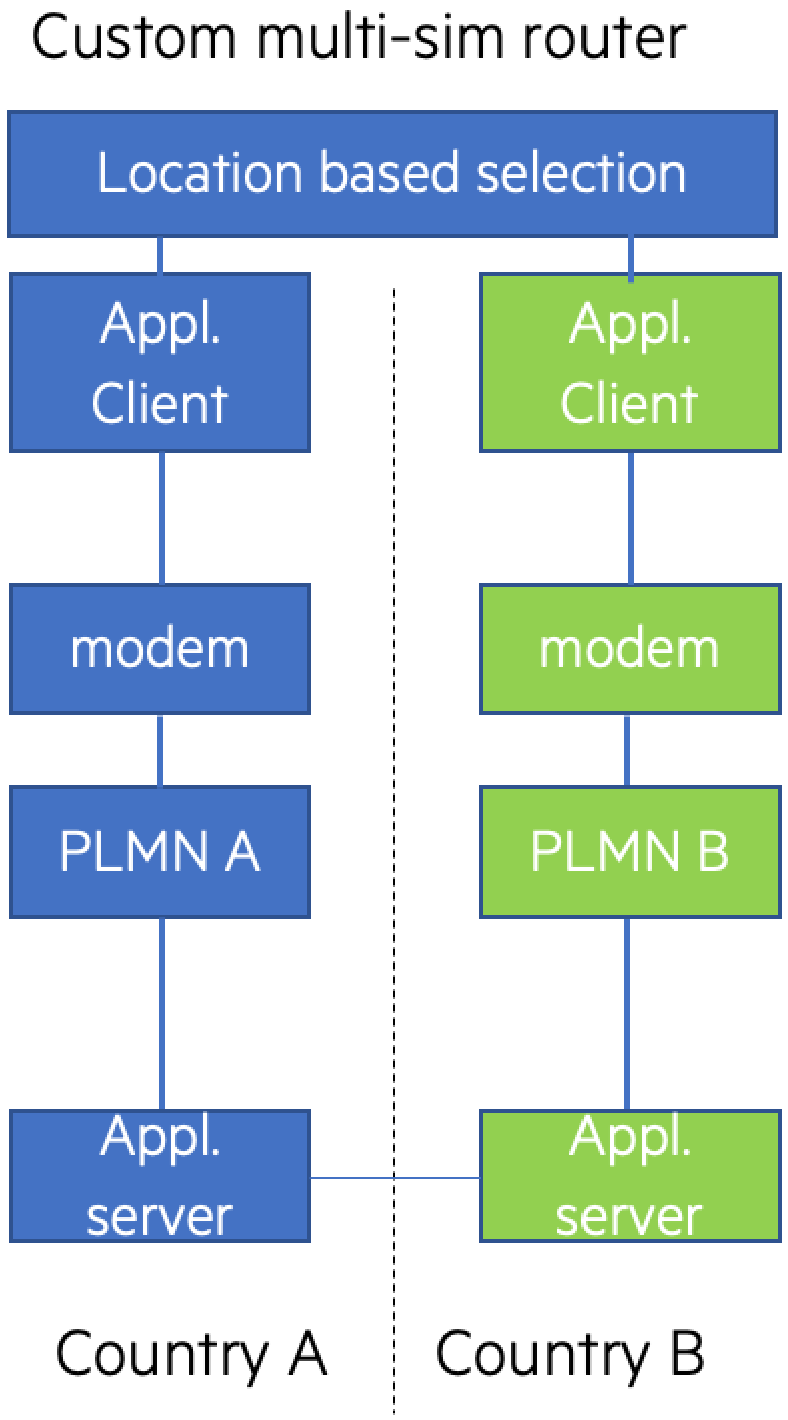


Figure 4: using a prediction function with a custom multi-sim router

This method of using a prediction function was used by the German trial site in the 5G-Mobix project [2]. In this case a prediction function predicted the best location to switch and an application in the vehicle switched to another stack (where a stack consisted of a device and modem with a separate MQTT client). Although the setup was extensive, the principle of using a "prediction function" was interesting. The advantage of using a prediction function is that you can prevent unnecessary switches and the use of different MQTT clients has the advantage that you can always connect to the closest MQTT server on the network (with the lowest latency).

The principle of using multiple modems is not new. There are already off-the shelf routers available which can help in this respect. In each modem of such a router a simcard of a specific network is inserted and the modem is prevented to roam to a new network. With both simcards belonging to the other bordering country, they will always try to stay connected and with enough overlap there will always be a valid connection. In addition to these different modems, multiple VPN tunnels are used (one for each modem) to route the traffic to an internet connected gateway. At this gateway the packets of the different VPN tunnels are re-ordered and merged again. This way multiple modems can work together, enabling extra capacity at a possibly sparsely covered area. This method was tested in the 5G-Mobix project by both the Finish and French trial sites [2]. The disadvantage of this method is that you need a modem/simcard for each country that is traversed. Also the internet connected gateway will stay at one location, inducing larger delays with longer routes.

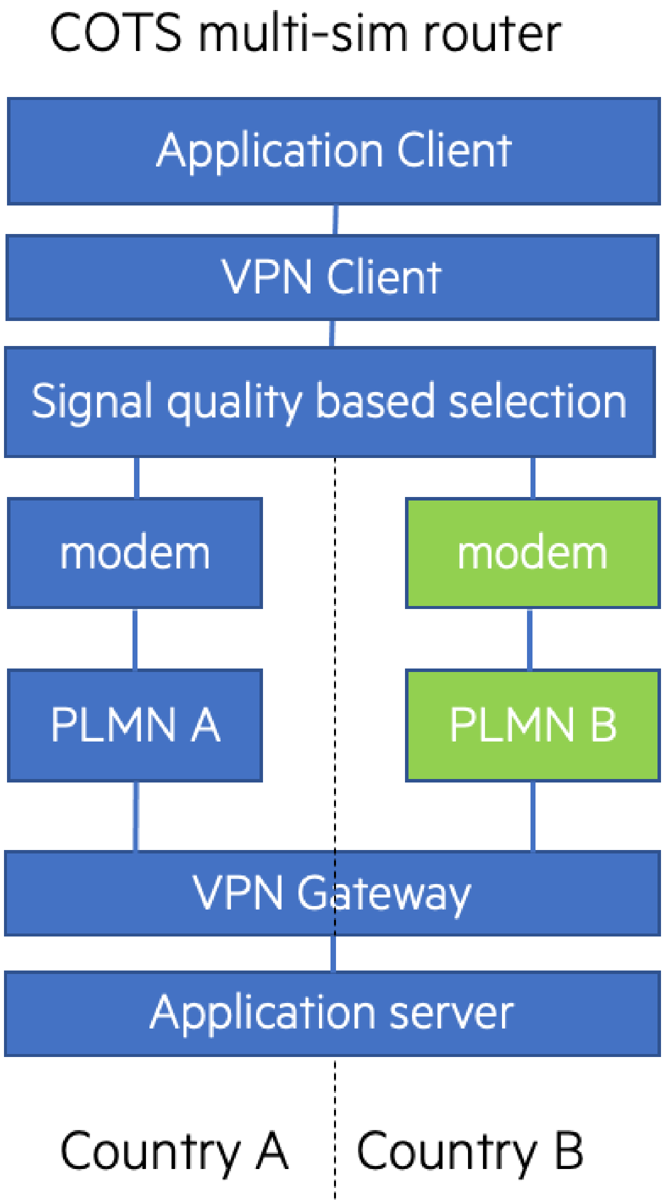


Figure 5: COTS multi-sim router

2.2.Network based measures

Using the network to direct the UE to a new network we see three different available methods that can be applied:

1. Release with redirect
2. N2 handover using the N14 interface
3. Steering of roaming AF

A Release with redirect is essentially a redirect to the new gNodeB without information being exchanged between the gNodeB's. The UE needs to re-authenticate itself and setup a new datasession. In addition the UE needs to consider the new network as an equivalent PLMN. This method has been described by 5G-Mobix in the deliverable D3.7 [2] but has never actually been proven in a test. The advantage of this method is that no interconnectivity between 5G cores and gNodeB's is needed. The disadvantage is that steering of roaming is not possible and still detailed information about signal levels and frequencies of neighboring gNodeB's need to be configured.

With the N2 handover over the N14 interface the bordering networks are interconnected. The gNodeB's will actually handover the UE to the new bordering gNodeB and the datasession will continue to work. This is the method where with a single UE the lowest interruption time can be achieved. This is also the method that has been extensively tested within our 5G-Blueprint project. Initial results show that it takes about 100 ms for the network to complete the handover. The UE is directed to do regular signal measurements and a handover is triggered when the signal level is below a certain threshold while the neighboring network has a signal level above a certain threshold. This is also described in TS 36.331 Section 6.3.5. The advantage of this method is the low interruption time while using only a single modem. The disadvantage is the complex configurations needed of the gNodeB's and extra interfaces between the 5G Cores. Also steering of roaming is not possible using this method.

A steering of roaming application function is a network based method where the UE is steered to another network when close to the border. The application function is triggered by the NEF when a UE is close to the border. When the UE is in the bordering cell the application function gets notified by the NEF. As a result the application function will update the “Operator controlled PLMN selector with Access Technology” (OPLMNwAcT) list on the UE over the air. This will cause the UE to switch faster to the preferred neighboring network. The advantages of this system is that steering of roaming is at the core of this solution, enabling the MNO to select the best network for the required services. The disadvantage is that there will still be a network interruption of at least several seconds and the UE needs to setup a new data connection. Another complexity is that the HPLMN needs to make a NEF connection to all the operators it has a roaming agreement with.

3. PRINCIPLES FOR HANDOVER ON 5G NR

While we described the possible approaches to handling cross-border scenarios at the network level in the previous chapter, this chapter's goal is to describe in more detail the principles and algorithms behind gNB handover and how they differ from the previous generation of wireless networks.

In 5G NR, handover is performed by measuring the signal strength of the serving cell and neighbouring cells, i.e., RSRP or RSRQ.

In LTE, all we rely on are Cell-Specific Reference Signals (CRS). However, in 5G NR, the concept of CRS has been removed to reduce overhead and added the SS/PBCH Block (SSB), which consists of Synchronisation Signal (SS) and Physical Broadcast Channel (PBCH)

The SSB periodicity can be configured as 5, 10, 20, 40, 80, or 160 ms. So no fixed measurement from the UE reducing power consumption on the Mobile Device (UE).

Measurement Control Info

The measurement configuration provides UE with this information through the RRC message under measObjectToAddMod as part of the MeasObjectNR IE. It contains the following information: SSb frequency, subcarrier spacing, Sync offset, periodicity, measurement window.

3GPP specification 38.331 specified following events defined for 5G NR.

- Event A1 (Serving becomes better than threshold)
- Event A2 (Serving becomes worse than threshold)
- Event A3 (Neighbor becomes offset better than SpCell)
- Event A4 (Neighbor becomes better than threshold)
- Event A5 (SpCell becomes worse than threshold1 and neighbour becomes better than threshold2)
- Event A6 (Neighbour becomes offset better than SCell)
- Event B1 (Inter RAT neighbour becomes better than threshold)
- Event B2 (PCell becomes worse than threshold1 and inter RAT neighbour becomes better than threshold2)

A1-A6 are used for Intra-RAT and B1-B2 for Inter-RAT Events.

UE measures source serving cells and target neighbours, reports it to be verified with the threshold defined. The trigger for the event can be RSRP, RSRQ or SINR.

For the roaming showcase we will deepdive in the two events used A2 & A5.

Event A2

The A2 event is triggered when the measurement of the serving cell signal is below a threshold:

Ms + Hys < Thresh.

The A2 event is stopped when the measurement of the serving cell signal is greater than a threshold:

Ms – Hys > Thresh.

Example of Event A2

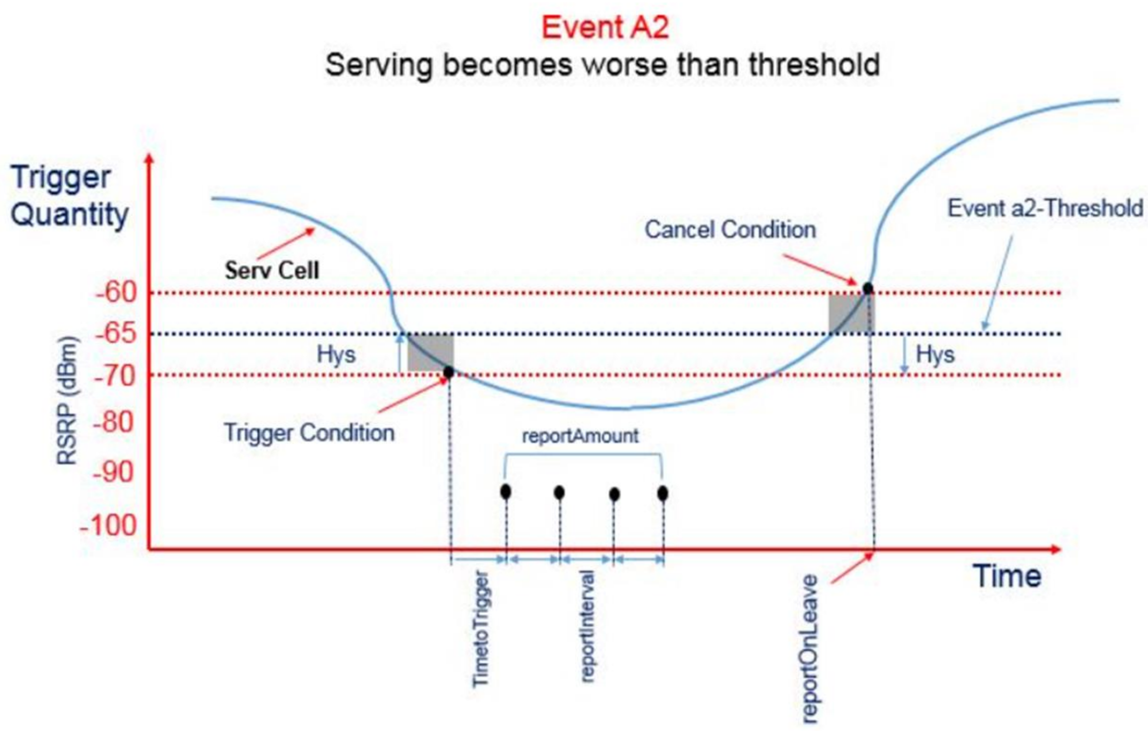


Figure 6: Event A2 visualization

The variables used in the equations above are defined as follows:

- Ms is the measurement result of the serving cell in dBm
- Hys is the hysteresis parameter for the A2 event expressed in dB.
- Thresh is the threshold parameter for this event,

Event A5

Event A5 is triggered when a serving cell becomes worse than threshold 1, while a neighbouring cell becomes better than threshold 2.

The following figure and equations show the trigger and cancel conditions.

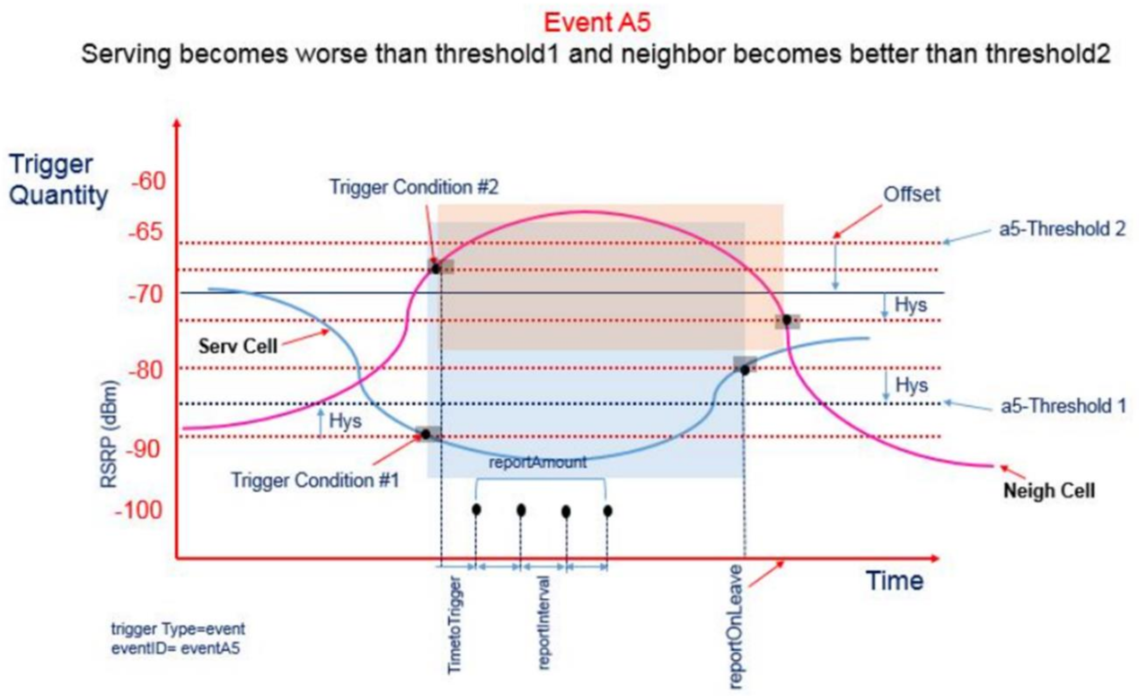


Figure 7: Event A5 visualization

Event Trigger Condition:

- Mp + Hys < Thresh1
- Mn + Ofn + Ocn - Hys > Thresh2

Event Cancellation Condition:

- Mp - Hys > Thresh1
- Mn + Ofn + Ocn + Hys < Thresh2

The variables used in the equations above are defined as follows:

- Mp is the measurement result of the NR SpCell,.
- Mn is the measurement result of the neighbouring cell.
- Ofn is the measurement object-specific offset of the neighbour cell,
- Ocn is the cell-specific offset of the neighbour cell.
- Hys is the hysteresis parameter.
- Thresh1 A5-Threshold1
- Thresh2 A5-Threshold2

4. ROBOAUTO 5G-BLUEPRINT APPROACH

Roboauto has developed a customized solution for ensuring redundant 5G communication. This versatile solution is router-agnostic, allowing seamless integration with a multitude of routers. Single router setup is also possible, provided the router supports the configuration of multiple simultaneous interfaces.

At the heart of this redundancy solution is the Linux operating system, where the vehicle's software stack operates. Linux offers a robust foundation for redundancy through its versatile networking capabilities. A key feature is its capacity to manage multiple routing tables and establish distinct routing rules, effectively creating a virtual network topology.

This solution harnesses primary Linux tools, namely ip and iptables, which communicate with the system kernel using the netlink protocol. Netlink is a socket-based communication protocol for inter-process communication (IPC), making it a powerful resource for configuring network redundancy. Implementation wise it is possible to either utilize the netlink API directly, or use the ip and iptables tools. This solution uses the latter approach.

Using the netlink requires special privileges. To use the netlink directly, the software would need to either run with administrator privileges, or have the CAP_NET_ADMIN capability. On the other hand, when using the tool based approach,the user running the software needs to have the required privileges to run the tool. This is usually achieved by adding the user running the vehicle software to the sudoers file with the required tool commands. Using external commands is the approach used by Roboauto's implementation.

In addition to configuring routing and rules, it's imperative to recognize that a custom communication protocol is essential to fully harness the setup's capabilities. The protocols used by this solution are Roboauto's proprietary protocols, MultiUDP and RoboProto.

4.1.1. MultiUDP Protocol

MultiUDP is a protocol that enables utilization of multiple network interfaces simultaneously by sending passing datagrams to multiple IP addresses. Each stream is uniquely identified by a session ID, which is assigned to each datagram for the duration of the stream. This enables the receiving end to identify the stream and dispatch the datagrams to the original recipient underlying application. Datagrams coming through this layer are sent through selected routes, and each datagram is assigned the aforementioned session ID. Selection of the route is typically controlled by the underlying application, which can disable or enable the route based on the current connection status or other external factors.

This protocol doesn't offer any reliability guarantees, nor deduplication of the datagrams. This is handled by the upstream RoboProto protocol.

4.1.2. RoboProto Protocol

RoboProto builds upon the MultiUDP foundation, offering advanced features for robust and secure communication. While the TCP has proven to be a reliable protocol for communication, it's not suitable for real-time applications on the unreliable networks as they are prone to packet loss and latency spikes, which can cause the TCP connection to stall.

This protocol includes periodic heartbeat signals, enabling real-time health checks of the connection. Clocks of the both ends are synchronized using the inbuilt NTP-like protocol, which is used to calculate the round trip time (RTT) of the connection. This information is used to calculate the timeout for the heartbeat signals. This ensures that the system clock change doesn't affect the connection. Messages within RoboProto can be encrypted using DTLS (Datagram Transport Layer Security) for enhanced security. Encryption in the teleoperation system is always enabled in the production environment.

Furthermore, RoboProto supports both reliable and unreliable data transfer, accommodating various communication needs. Key feature of the protocol is that each message is assigned a unique sequence number. This enables the receiving end to handle situations when MultiUDP delivers the same datagram multiple times, but upstream of the RoboProto layer, it is received only once.

4.1.3. SRTP

SRTP is a protocol that hasn’t been created by Roboauto, however its properties work well within the whole redundancy solution. The protocol itself is based on RTP, or Real-time Transport Protocol, which is a fundamental protocol used for transmitting audio and video data over the internet. While RTP is effective for real-time communication, it lacks inherent security measures. To address this vulnerability, SRTP, or Secure Real-time Transport Protocol, was developed. SRTP enhances RTP by adding encryption, authentication, and integrity checks to the data, making it suitable for secure applications like VoIP and video conferencing, where protecting sensitive information is crucial. In essence, SRTP acts as a security layer for RTP, ensuring the privacy and integrity of multimedia content in real-time communication sessions.

One of the key properties of RTP and SRTP are sequence numbers, which are used to order and identify individual packets within a stream of multimedia data. Each RTP packet includes a sequence number, which is incremented for each successive packet in a stream. This sequence number allows the receiver to arrange the incoming packets in the correct order, ensuring the proper playback of audio or video content. Sequence numbers are also helpful in detecting lost or out-of-order packets, which can affect the quality of real-time communication. That is related to the fact that each datagram can be delivered only once. So when using redundancy, where the same datagram is sent multiple times, the receiver can detect the duplicates and discard them.

4.1.4. Iptables

iptables is a powerful utility for managing network rules in Linux. It operates through various tables and chains, allowing to define and control packet filtering and network address translation. Primary tables and chains of the iptables are described below.

4.1.5. Filter Table (filter)

This is the default table and is used for managing the packet filtering rules. It primarily deals with decisions regarding whether to accept, drop, or reject incoming and outgoing packets. Rules in the filter table are commonly used for enforcing security policies, so it is not required by this solution.

4.1.6. NAT Table (nat)

The nat table is responsible for Network Address Translation (NAT) and is used to modify source or destination addresses of packets. It allows the manipulation of IP addresses, enabling scenarios like port forwarding, source address translation (SNAT), and destination address translation (DNAT). It is used by the cross-border solution to rewrite the destination address of the packets.

4.1.7. Mangle Table (mangle)

The mangle table is used for more advanced packet mangling. It can modify the Quality of Service (QoS) bits in the IP header, and mark packets with special marks for advanced routing and filtering. It is used by a redundancy solution to mark packets with special marks, which are then used for routing.

4.1.8. Raw Table (raw)

The raw table is not used by this solution. It is used primarily for configuring exemptions from connection tracking. It allows packets to bypass the connection tracking system, which can be useful for some specialized purposes.

4.1.9. Security Table (security)

This table is not used by this solution. It is only mentioned here for completeness. This table is used to work with SELinux security policies in some Linux distributions. It allows finer-grained control over packet filtering based on security contexts.

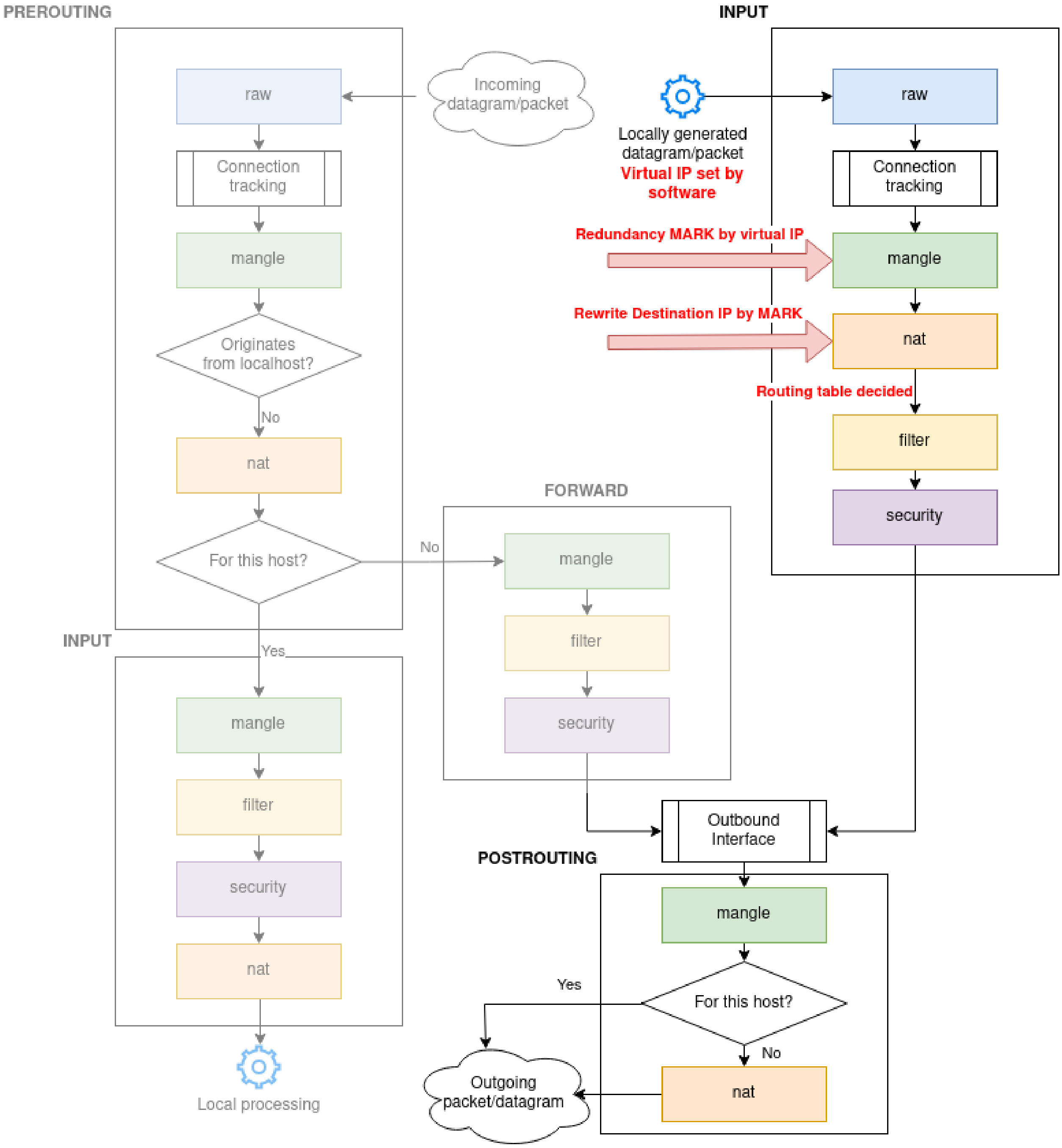


Figure 8: iptables processing flow

4.2.Technical implementation

Each vehicle needs a list of routers or rather router interfaces. This setup is then saved to the parameter file of the vehicle software. When multiple hardware computing units are used, the parameters are distributed to the respective units from the master node.

In the vehicle software itself there is a main component that is responsible for the configuration of the network. This component is called *Network configurator*. At the moment it supports several strategies of how the configuration can be done, however in this document we will focus on the strategy that was implemented for this project. The name of the strategy is “IP Route strategy” as in the name of the iptables of the linux kernel. The software component that is driving the configuration is called **IP Route Configurator** or in short **IPRC**.

When the software starts the parameters are read and the static configuration step is performed. Static configuration means that the configuration is done once per IPRC instance, and is not changed during the runtime. The form of the parameters for IPRC are the ip address or hostname of the gateway, and optionally the network interface name. The default interface is used when the interface name is not provided. The default interface is the network interface that is used for the default route, which is typically the first router in the setup.

Configurator then have to prepare for configuration of each gateway. Each gateway needs a virtual ip address from a pre-selected range, and also a random number whose purpose will be explained later. With the newly generated data, the IPRC can now set up the routing table, which is one of the static configurations. The table gets the name of the random number and the gateway ip address is set as the default gateway for the table. The content of the table can be listed with the command

```
ip route show table <table name>
```

And generally can look like this:

```
default via <ip address of the gateway> dev <interface name>
```

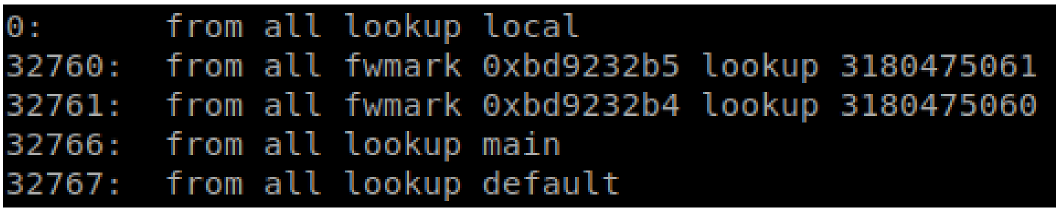
The next static step is to set up the routing rules. The rules are used to determine which table should be used for the routing. Each rule tries to match the packet by special mark and if the packet is matched, the table is determined for the packet. Mark is a numeric value, and how the packets are marked will be explained later. The rules are set with the command

```
ip rule add fwmark <mark> table <table name>
```

For convenience the mark and the table name are the same. The rules can be listed with the command:

```
ip rule show
```

And its output might look like the following figure:



```
0:      from all lookup local
32760:  from all fwmark 0xbd9232b5 lookup 3180475061
32761:  from all fwmark 0xbd9232b4 lookup 3180475060
32766:  from all lookup main
32767:  from all lookup default
```

Figure 9: Routing rules

The rules on the figure states that packets marked with fwmark 0xbd9232b5 and 0xbd9232b4 should use their respective routing tables. Routing table names are outputted in decimal format, but if we viewed the value in hexdecimal form it would be matching the mark.

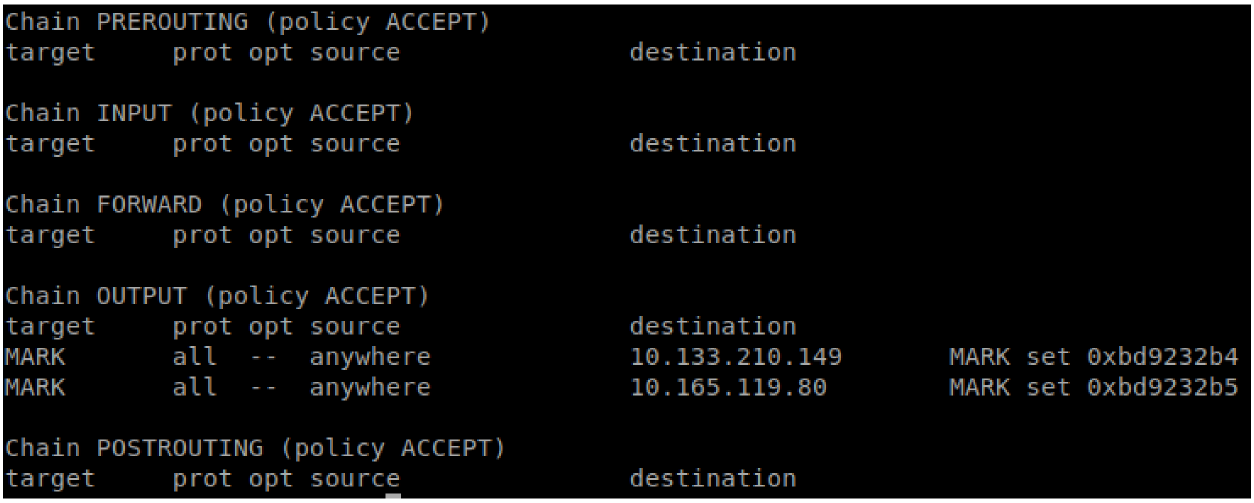
Last step in static configuration is to set up the marking. The marking is done by the iptables tool and is done in the mangle table. The marks are applied to packets whose destination address is the virtual ip address of the gateway. They are used to determine which routing table should be used, and which packets need their destination address rewritten. The marking is done with the command:

iptables -t mangle -A OUTPUT -d <virtual ip address> -j MARK --set-mark <mark>.

Using the OUTPUT chain ensures that the marking is done only for packets originating from the local machine. The PREROUTING chain could also be used, but it would mark all packets, including those that are forwarded by the machine, and since that scenario currently doesn't exist, the OUTPUT chain is used for better performance. Active mangle rules can be listed by command:

iptables -t mangle -L

The output of the command might look like this:



```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
MARK       all  --  anywhere             10.133.210.149       MARK set 0xbd9232b4
MARK       all  --  anywhere             10.165.119.80        MARK set 0xbd9232b5

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
```

Figure 10: Mangle table

The figure shows two virtual gateway addresses 10.133.210.149 and 10.165.119.80 with their respective marking rules.

The dynamic configuration takes place when the vehicle is about to connect to the remote station.

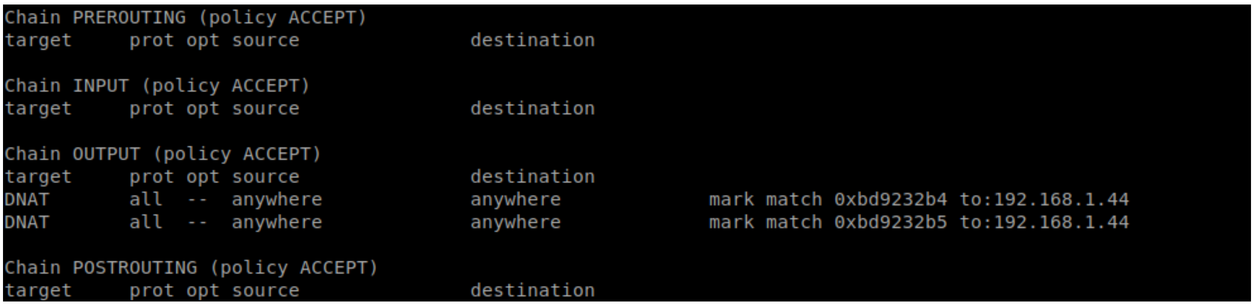
The vehicle software obtains an IP address from the remote station and uses it to configure DNAT (Destination Network Address Translation), for all virtual IP addresses. As the virtual address can be identified by the mark, the DNAT configuration is done by the following command:

iptables -t nat -A OUTPUT -m mark --mark <mark> -j DNAT --to <remote ip address>

The rule says that all packets with the specific mark should have their destination address rewritten to a remote station IP address. Active DNAT rules can be listed with the command:

iptables -t nat -L

The output of the listing command might look like this:



```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DNAT       all  --  anywhere             anywhere             mark match 0xbd9232b4 to:192.168.1.44
DNAT       all  --  anywhere             anywhere             mark match 0xbd9232b5 to:192.168.1.44

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
```

Figure 11: NAT table

After the configuration of the routing, the communication can start. Endpoint with the original remote station IP gets transformed into an endpoint represented by all router virtual addresses. This is then used by the MultiUDP protocol to open channels for all endpoints. The same procedure is used for streaming pipelines. Now it’s up to the higher layer to handle the channel utilization. When more channels are used simultaneously we are talking about data redundancy. In this particular scenario, we can use GPS or roaming to selectively use channels.

After the external condition is met, one or more channels of the MultiUDP/streaming layer are disabled, allowing us to complete various scenarios like the crossborder.

4.2.1. Configuration of routing in distributed system

Vehicle software is currently running as multiple hardware nodes running several processes, that each have their own responsibilities. Since the rules and routes are set for the whole system, it is necessary to synchronize the configuration between the nodes and processes. For this purpose we have a mechanism involving database and file locking. The database is used to store information about the rules set by each instance. The database is deployed along with the software and is located in the directory that is accessible by all processes. We have chosen SQLite 3 database, because it is lightweight and doesn't require any additional software to be installed, but other databases could be used as well. The only prerequisite is that the database supports concurrent access and exclusive locking.

Each instance of IPRC has its own database connection, which is used to store information about the rules set by the instance. When accessing the database the instance acquires an exclusive lock on the database file, which prevents other instances from accessing the database. This ensures that there are no clashes when multiple instances try to randomly generate the same configuration. In the SQLite terms, this is implemented as a block guarded by the *BEGIN EXCLUSIVE* and *COMMIT* statements. Since SQLite doesn't support waiting for the lock, the implementation polls the database until the lock is acquired. In theoretical terms this could lead to a starvation of some instances, but in practice this is not an issue, as each instance accesses the database only once during the startup, during dynamic configuration and during cleanup phase.

The other purpose of the database isn't just to ensure no clashes during the startup, but also to ensure proper cleanup in case that any of the hosting processes exits abnormally. So it's not the actual rules that are stored in the database, but rather the commands that are needed to clean up the rules. Each instance of IPRC has the responsibility to clean up the rules of the process that has exited abnormally. This is when the file locking comes into play. Each instance of IPRC has its own identification number assigned by the database. This number is used to generate the name of the file lock. The file lock is created in the directory accessible by all processes (e.g. /tmp). Each instance of IPRC then acquires an exclusive lock on the file. This way other instances can try to acquire the lock, and if they succeed, it is certain that the instance that created the lock has exited abnormally, so the process can clean up the rules. The configuration is not permanent, so it needs to be reapplied after the reboot of the system, when the vehicle software starts. It's not an issue if any rules are left in the database, as their cleanup is idempotent to current state. Possible DDL for SQLite database is below.

```
PRAGMA foreign_keys = false;

DROP TABLE IF EXISTS "process";
CREATE TABLE "process" (
  "pid" INTEGER NOT NULL,
  "iprc_id" integer NOT NULL,
  "lock_file" text(500) NOT NULL,
  PRIMARY KEY ("pid", "iprc_id")
);

DROP TABLE IF EXISTS "rule";
CREATE TABLE "rule" (
  "rule_id" INTEGER NOT NULL PRIMARY KEY AUTOINCREMENT,
  "pid" INTEGER NOT NULL,
  "iprc_id" INTEGER NOT NULL,
  "rule" TEXT(500) NOT NULL,
  "type" TEXT NOT NULL,
  CONSTRAINT "fkProcess" FOREIGN KEY ("pid", "iprc_id") REFERENCES "process" ("pid", "iprc_id") ON DELETE CASCADE ON UPDATE CASCADE
);

DROP TABLE IF EXISTS "sqlite_sequence";
CREATE TABLE "sqlite_sequence" (
  "name",
  "seq"
);

INSERT INTO "sqlite_sequence" VALUES ('rule', 0);

PRAGMA foreign_keys = true;
```

Figure 12: DDL for software routing

5. TESTING

5.1.Testing setup

For the testing of the cross-border solution we have used real hardware and a virtual border crossing point. In the setup we have used two 5G routers, standard Teleoperation set with four cameras, and as a vehicle we have used a Hyundai I40.

One of the 5G routers that we used on the Czech Site is Sierra Wireless Airlink XR90, which is currently used as a primary router for this use case. The Airlink XR90 is a high-performance multi-network vehicle router that is particularly well-suited for mission-critical applications in transport and emergency services. While it supports two 5G modems, we are currently utilizing only one, and we use a second router as a form of hardware redundancy.

Figure 13: Sierra Wireless Airlink XR90

The second router in the setup is Teltonika RUTX50, which is a compact, cost-effective, and secure industrial 5G router for professional applications. It delivers high performance, mission-critical cellular communication, and supports GPS location capabilities. Like the Airlink XR90, it also supports two 5G modems.

Figure 14: Teltonika RUTX50

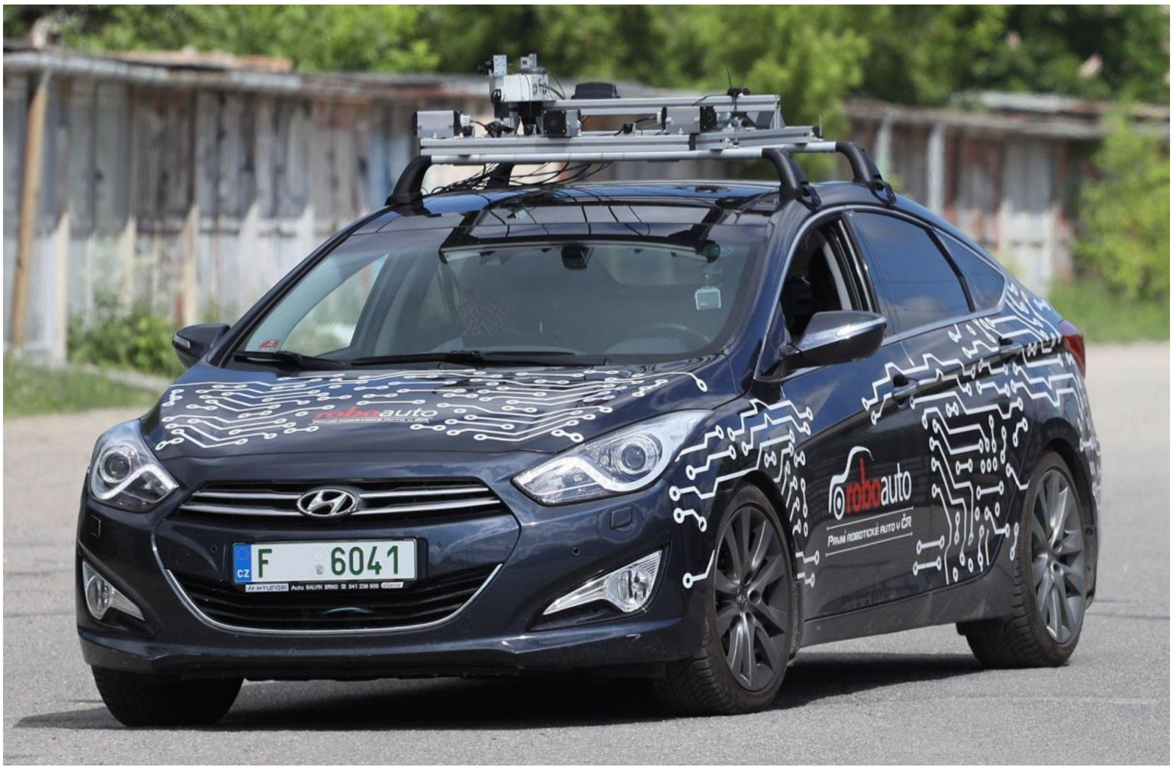


Figure 15: Hyundai I40 used for tests on Czech site

For the trials at the Netherlands site we used two Sierra Wireless Airlink XR90 routers and a Toyota C-HR.

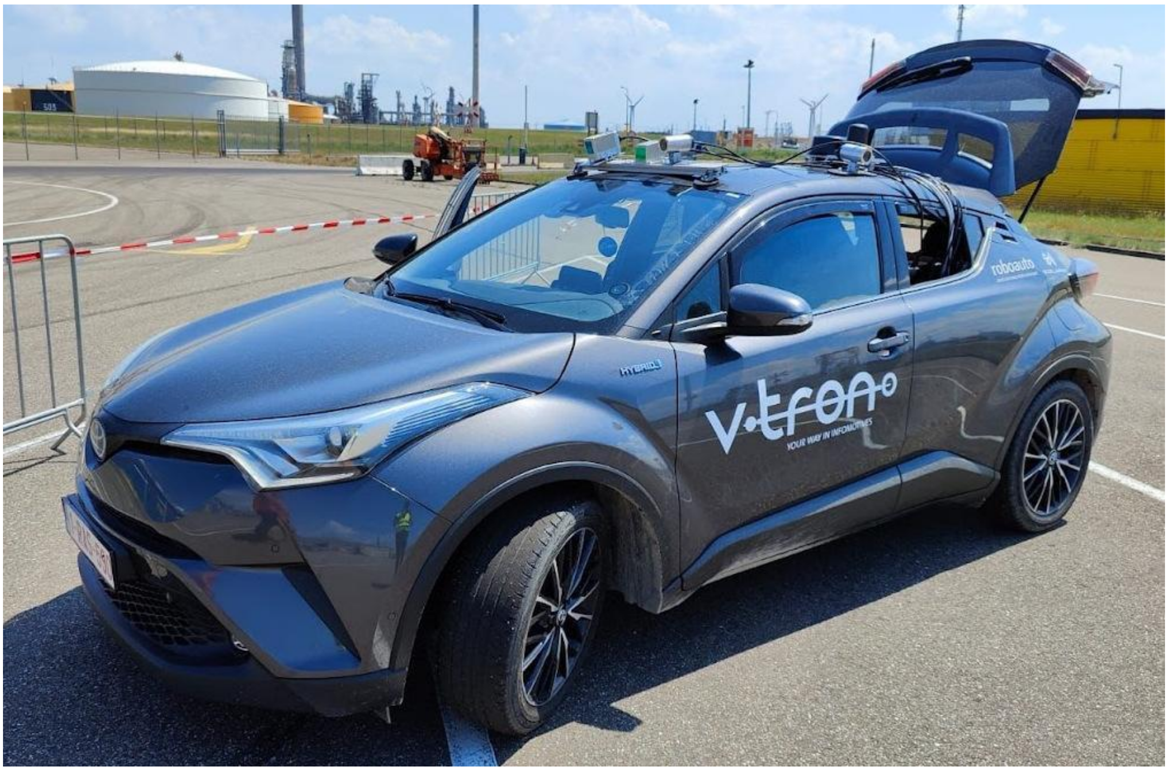


Figure 16: Toyota C-HR used for test on Netherlands-Belgium site

Common hardware for both testing sites are compute units, one gigabit POE (Power over Ethernet) switch, one gigabit switch without POE, two camera modules and drive by wire interface. Remaining hardware components are omitted as these are not important to this use case. The image of the complete vehicle hardware stack can be found below.

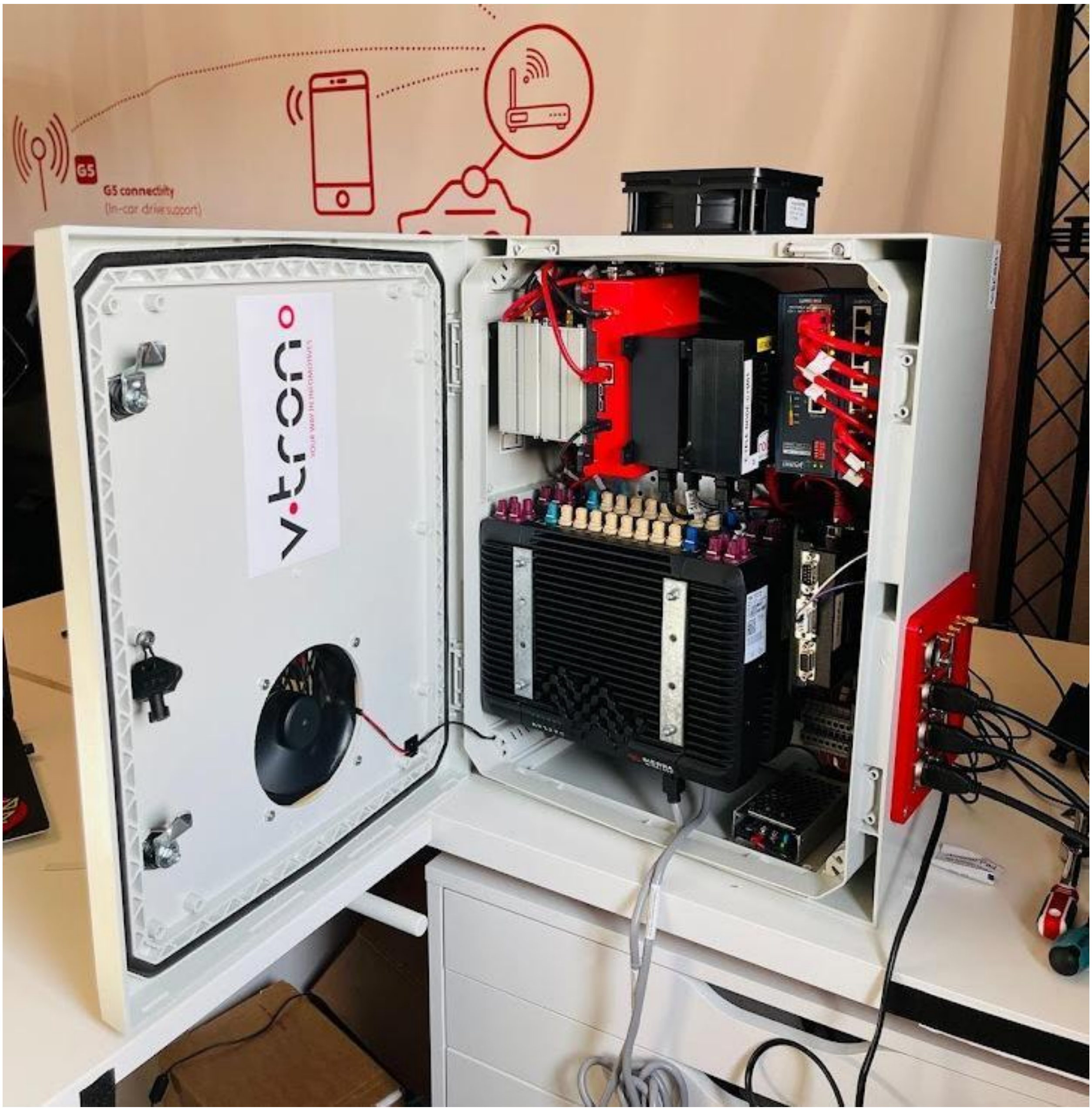


Figure 17: Hardware installed in Toyota C-HR

5.1.1. Jetson Nano Production - Compute Units

The Jetson Nano production modules are compact, powerful embedded computing platforms designed and manufactured by NVIDIA. These modules are specifically engineered to deliver high-performance artificial intelligence (AI) and computer vision capabilities in a small form factor, making them well-suited for a wide range of applications, including camera encoding and streaming.

Jetson Nano production modules offer robust support for video compression standards such as VP8 and H.265 (also known as HEVC), making them highly suitable for the camera encoding and streaming use case. VP8 is a widely adopted video codec known for its efficient compression and compatibility with various streaming platforms. H.265, on the other hand, is renowned for its superior compression capabilities, allowing for high-quality video transmission at lower bitrates. The Jetson Nano's ability to handle these codecs ensures that your hardware solution can deliver optimized, bandwidth-efficient streaming, making it well-equipped to meet the demands of real-time video encoding for teleoperation.

In the current setup, each Jetson Nano production module, also referred to as a "node," effectively manages two cameras independently. To achieve this, each camera is associated with its dedicated and distributed software instance, ensuring efficient and separate control. This distributed software is orchestrated and overseen by a primary vehicle software instance, which is executed on a specific hardware node termed the "master node." The "master node" serves as the central control unit, managing the coordination and communication between the individual camera software instances, resulting in a well-organized and synchronized system for camera handling and streaming.

The primary vehicle software, operating on the designated "master node," takes on the critical role of managing communication across various components of the system. Specifically, it handles interactions with the teleoperated center (also known as remote station), communicates with the main teleoperation gateway, and establishes communication with the drive-by-wire unit.

5.1.2. Camera - Liebherr MDC3

The Liebherr MDC3 is a digital smart camera developed by Liebherr, a company known for its manufacturing of construction and mining machinery. This camera is designed to deliver high-resolution images even in extreme environmental conditions, making it particularly suitable for a wide range of applications including teleoperation.

The MDC3 camera features High Dynamic Range (HDR), which allows it to take multiple pictures simultaneously at different brightness levels and combine them into a single ideal image. This feature enables the camera to deliver up to 40 high-contrast images per second, providing important image details.

The camera also has a high contrast range of 132 dB, which means it can capture a wide range of light intensities, from very dark to very bright conditions. This feature is particularly useful in environments with varying lighting conditions, such as driving through tunnels.

In addition to its robustness, the MDC3 camera has been tested for its reliability and latency. It has proven to deliver images to displays with minimal delays, which is crucial for teleoperation. The camera has also been tested under heavy shock loads and in heavy vibrations, and it has performed well without any failure or impairment.

Camera supports two output formats: MJPEG and H264. In this use-case we are currently using MJPEG format. While the H264 offers higher compression, it also has higher decoder latency and has higher performance requirements. Since the image data gets re-encoded into VP8 or H265 formats when transmitting the image to the teleoperation center, the properties of MJPEG better suit the task at hand.

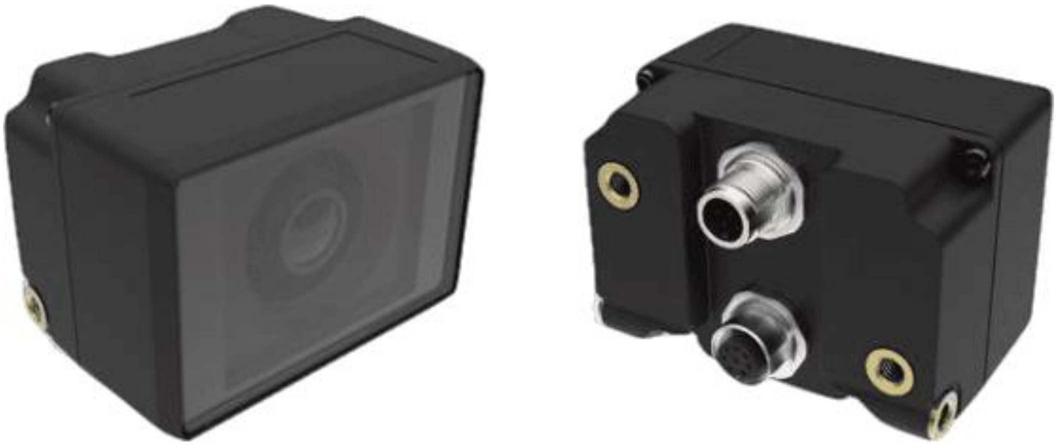


Figure 18: Liebherr MDC3

5.1.3. Drive by wire

The drive-by-wire hardware module serves as the crucial intermediary for communication with the vehicle. Its primary role is to translate abstract commands, originating from the teleoperation system, into commands that the vehicle's internal systems can comprehend and execute. This essential function ensures that the vehicle's electronic components and actuators can interpret and act upon the instructions provided, effectively bridging the gap between human intent or control algorithms and the physical actions performed by the vehicle.

The DBW is based on the STM32F2 microcontroller. STM32F2 is valuable for communicating with vehicles in applications like drive-by-wire due to its robust processing capabilities and extensive range of communication interfaces. Its high-performance ARM Cortex-M3 core can efficiently handle real-time data processing and control tasks. Moreover, its abundant peripherals, including Ethernet, ADC, and namely CAN, facilitate seamless integration with various vehicle systems, allowing for rapid and reliable data exchange. This microcontroller's versatility and adaptability make it a suitable choice for interfacing with in-vehicle networks, enabling precise control of vehicle functions in drive-by-wire applications while ensuring safety and reliability.

The communication with the DBW and the master node is using ethernet, while communication with both Hyundai I40 and Toyota C-HR is performed using CAN bus.

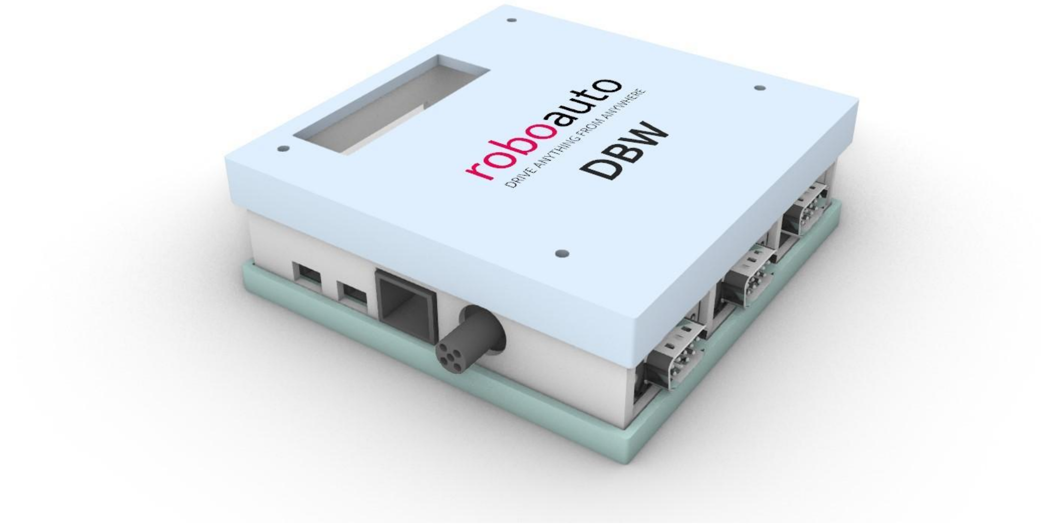


Figure 19: Drive by wire unit model

5.1.4. Testing

For the testing we have chosen two testing scenarios. One scenario is crossing the border and using a GPS to signal MultiUDP to artificially disable one of the channels. The other scenario is simulation of the network outage by disconnecting the router from the network.

For the testing of our cross-border solution, we have devised three distinct testing scenarios. These scenarios are crucial in validating the system's performance and reliability. While we tested the scenarios with dual-SIM setup, it is possible to utilize even more SIMs for redundancy purposes. In the scenarios below we will refer to SIM cards as SIM A for home network A and SIM B for home network B.

5.1.5. Scenario 1: GPS driven scenario

In this scenario, we aim to replicate real-world border-crossing situations where users may transition between different mobile networks seamlessly. Our solution utilizes GPS technology to detect when a device is approaching the border. This, in turn, signals the MultiUDP system to take specific actions in order to optimize data transmission. This scenario is particularly useful when evaluating the software response as it is possible to create virtual borders. Virtual borders then makes the whole process of testing easier as the test participants do not have to approach the real border. The scenario can be divided into three phases.

Initial Phase: When the user is well within the home network's coverage area, the channel using the home SIM A is active.

Near Border Phase: As the user nears the border, the system intelligently switches to a multil-SIM mode, utilizing both SIM A and SIM B for improved connectivity. This transition is governed by the GPS coordinates, ensuring a smooth handover.

Border Crossing Phase: Upon crossing the border and leaving the near border area, the system switches exclusively to SIM B.

During this scenario, MultiUDP plays a crucial role by providing the flexibility to either send data concurrently through both SIM cards or choose a specific SIM (SIM A or SIM B) for data transmission.

The GPS based solution is visualized on the following sequence diagram.

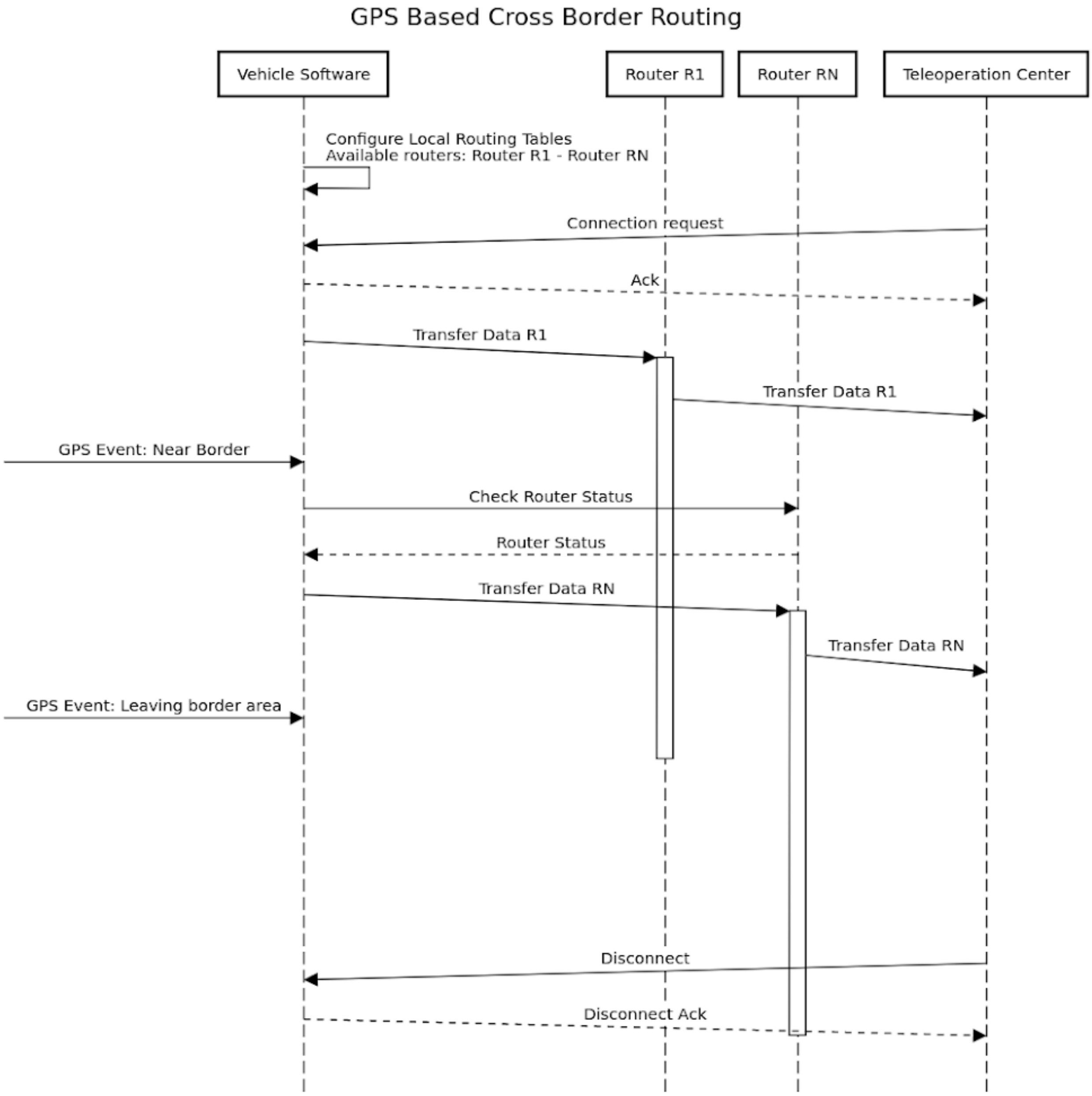


Figure 20: GPS/GNSS based cross-border routing

5.1.6. Scenario 2: Manually disabling hardware

In this scenario, we simulate the cross-border by managing the hardware availability manually. We intentionally disconnect and connect the routers during phases. This test scenario is simplest in terms of performability as there is no need for components that would manage the connection channels. The requirement for this test scenario is having a reliable way to simply connect and disconnect hardware in the moving vehicle. That might be done for example having another tester inside the vehicle to perform the task or by making this task effortless for the safety driver.

Initial Phase: The router with SIM B is disconnected from the system.

Near Border Phase: When approaching the virtual border, the tester inside the vehicle reconnects the router with SIM-B to the network.

Border Crossing Phase: Upon crossing the virtual border and leaving the near border area the router with SIM A is disconnected.

5.1.7. Scenario 3: SIMs with disabled roaming

In this scenario, we aim to simulate cross-border conditions by using SIM cards with disabled roaming capabilities. Unlike the previous scenarios, where GPS technology or manual hardware management was employed to trigger network transitions, this scenario focuses on testing the system's response to the limitations imposed by SIM card settings. By disabling roaming each router has restricted the ability to connect to foreign networks. This scenario requires either crossing the real border, or testing in areas with exclusive preset networks and locked SIM cards.

Initial Phase: At the beginning of this scenario, the system operates within the home network's coverage area, and the active channel is exclusively using SIM A, as the network for SIM B is unavailable.

Near Border Phase: As the vehicle nears the border, the SIM B native network becomes available, and both routers are able to transfer data.

Border Crossing Phase (SIM B): Upon crossing the simulated border and leaving the near border area, the network for SIM A becomes unavailable, and the communication continues solely via router carrying SIM B.

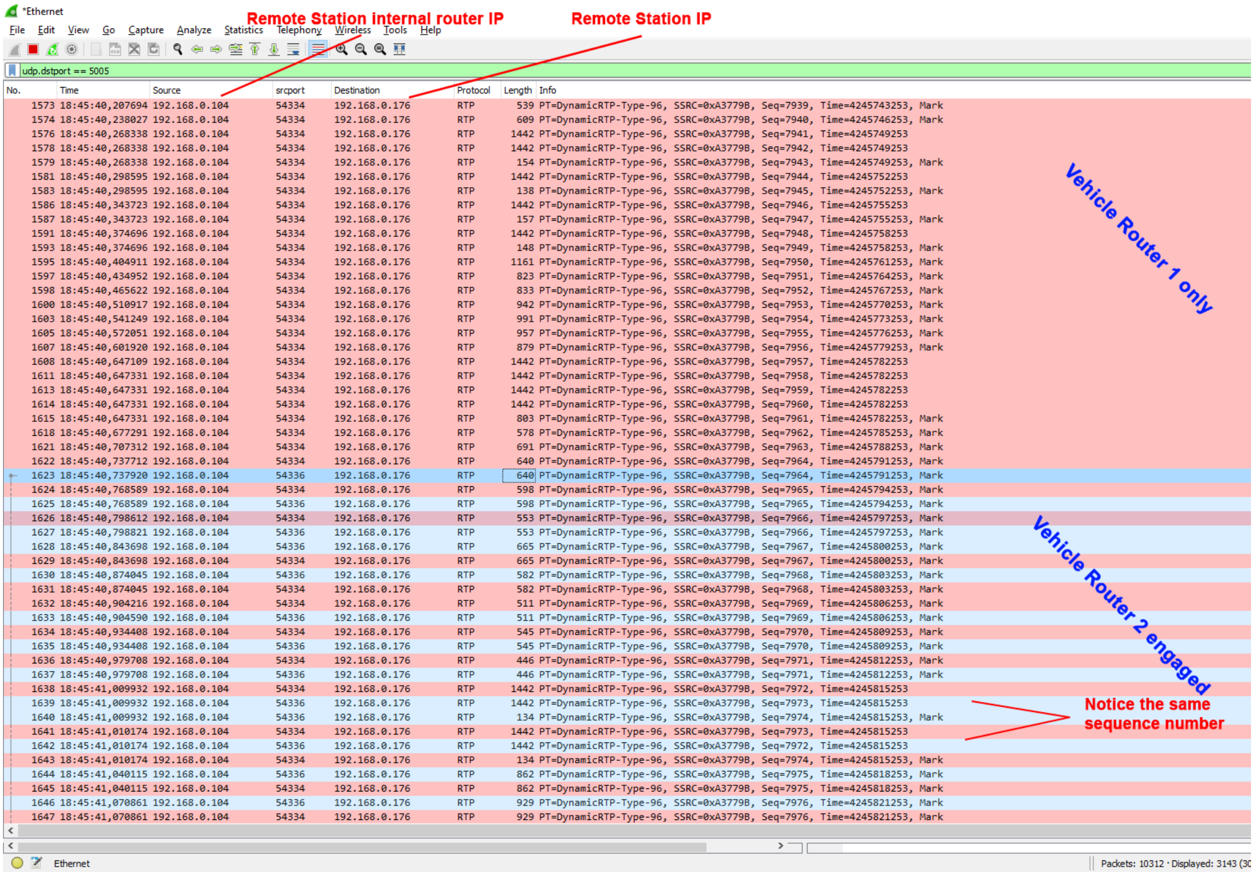
5.2.Network monitoring

The routing system can be also viewed and verified by network monitoring. Both vehicle and remote station can be monitored to assert the correctness of the network setup and multi-SIM redundancy. One powerful tool for monitoring this complex network activity is Wireshark.

Wireshark is a widely used open-source network protocol analyzer that allows users to capture and inspect data packets travelling across a computer network in real-time. It provides detailed information about network traffic, making it a valuable tool for diagnosing network issues, ensuring network security and monitoring data flow. By intercepting and inspecting the data packets as they leave the vehicle's computer, engineers can confirm that data packets are taking the intended routes and reaching their destinations.

5.2.1. Remote station side

When viewing the network data flow from the side of the Remote Station, it is expected that there are multiple observable channels of data transmission for the same application port. In the following image we will examine a transition, when the vehicle software engages dual-SIM mode.

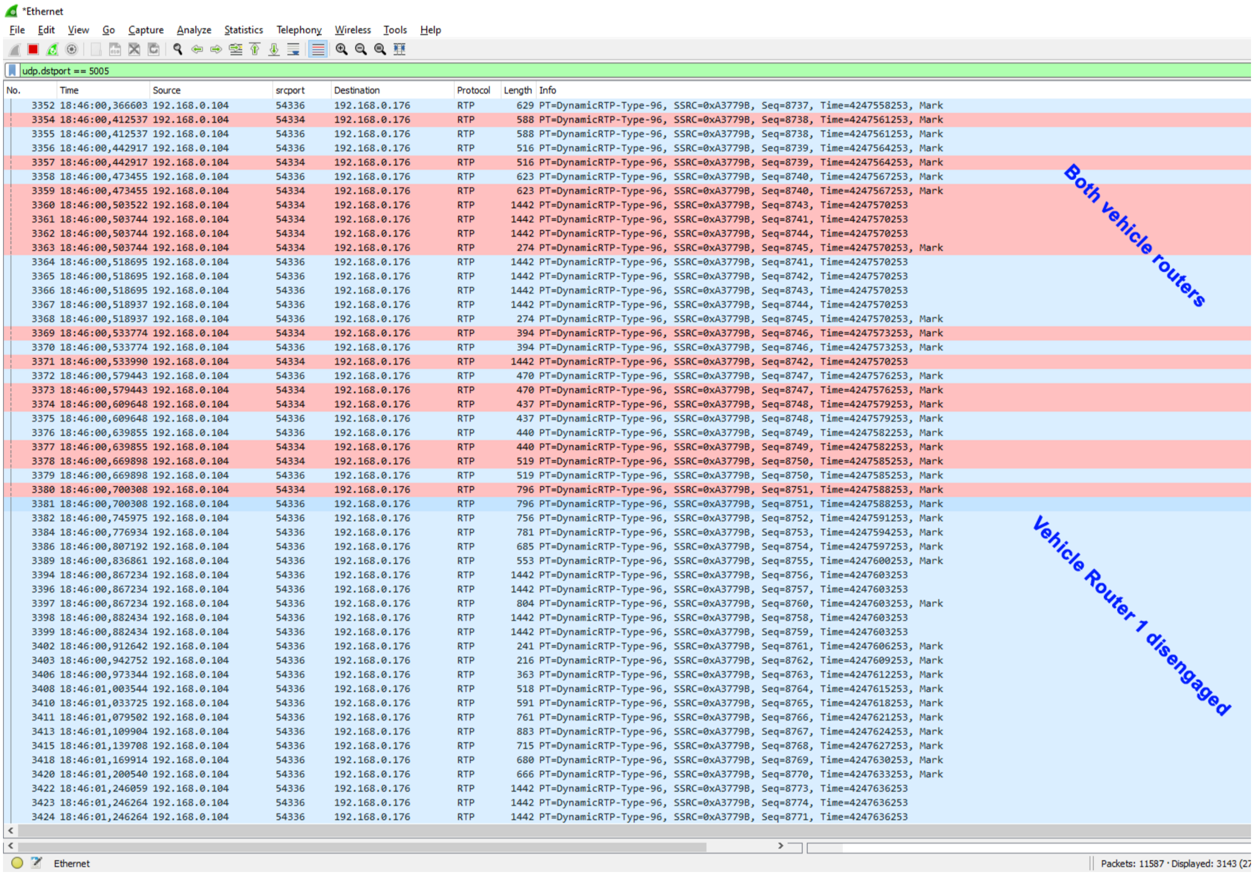

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Remote Station internal router IP
Remote Station IP
Vehicle Router 1 only
Vehicle Router 2 engaged
Notice the same sequence number
Ethernet
Packets: 10312 · Displayed: 3143 (3(

```
udp.dstport == 5005

No.  Time            Source        srcport  Destination   Protocol Length Info
1573 18:45:40,207694 192.168.0.104  54334   192.168.0.176  RTP      539 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7939, Time=4245743253, Mark
1574 18:45:40,238027 192.168.0.104  54334   192.168.0.176  RTP      609 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7940, Time=4245746253, Mark
1576 18:45:40,268338 192.168.0.104  54334   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7941, Time=4245749253
1578 18:45:40,268338 192.168.0.104  54334   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7942, Time=4245749253
1579 18:45:40,268338 192.168.0.104  54334   192.168.0.176  RTP      154 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7943, Time=4245749253, Mark
1581 18:45:40,298595 192.168.0.104  54334   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7944, Time=4245752253
1583 18:45:40,298595 192.168.0.104  54334   192.168.0.176  RTP      138 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7945, Time=4245752253, Mark
1586 18:45:40,343723 192.168.0.104  54334   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7946, Time=4245755253
1587 18:45:40,343723 192.168.0.104  54334   192.168.0.176  RTP      157 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7947, Time=4245755253, Mark
1591 18:45:40,374696 192.168.0.104  54334   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7948, Time=4245758253
1593 18:45:40,374696 192.168.0.104  54334   192.168.0.176  RTP      148 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7949, Time=4245758253, Mark
1595 18:45:40,404911 192.168.0.104  54334   192.168.0.176  RTP     1161 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7950, Time=4245761253, Mark
1597 18:45:40,434952 192.168.0.104  54334   192.168.0.176  RTP      823 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7951, Time=4245764253, Mark
1598 18:45:40,465622 192.168.0.104  54334   192.168.0.176  RTP      833 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7952, Time=4245767253, Mark
1600 18:45:40,510917 192.168.0.104  54334   192.168.0.176  RTP      942 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7953, Time=4245770253, Mark
1603 18:45:40,541249 192.168.0.104  54334   192.168.0.176  RTP      991 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7954, Time=4245773253, Mark
1605 18:45:40,572051 192.168.0.104  54334   192.168.0.176  RTP      957 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7955, Time=4245776253, Mark
1607 18:45:40,601920 192.168.0.104  54334   192.168.0.176  RTP      879 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7956, Time=4245779253, Mark
1608 18:45:40,647109 192.168.0.104  54334   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7957, Time=4245782253
1611 18:45:40,647331 192.168.0.104  54334   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7958, Time=4245782253
1613 18:45:40,647331 192.168.0.104  54334   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7959, Time=4245782253
1614 18:45:40,647331 192.168.0.104  54334   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7960, Time=4245782253
1615 18:45:40,647331 192.168.0.104  54334   192.168.0.176  RTP      803 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7961, Time=4245782253, Mark
1618 18:45:40,677291 192.168.0.104  54334   192.168.0.176  RTP      578 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7962, Time=4245785253, Mark
1621 18:45:40,707312 192.168.0.104  54334   192.168.0.176  RTP      691 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7963, Time=4245788253, Mark
1622 18:45:40,737712 192.168.0.104  54334   192.168.0.176  RTP      640 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7964, Time=4245791253, Mark
1623 18:45:40,737920 192.168.0.104  54336   192.168.0.176  RTP      640 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7964, Time=4245791253, Mark
1624 18:45:40,768589 192.168.0.104  54334   192.168.0.176  RTP      598 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7965, Time=4245794253, Mark
1625 18:45:40,768589 192.168.0.104  54336   192.168.0.176  RTP      598 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7965, Time=4245794253, Mark
1626 18:45:40,798612 192.168.0.104  54334   192.168.0.176  RTP      553 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7966, Time=4245797253, Mark
1627 18:45:40,798821 192.168.0.104  54336   192.168.0.176  RTP      553 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7966, Time=4245797253, Mark
1628 18:45:40,843698 192.168.0.104  54336   192.168.0.176  RTP      665 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7967, Time=4245800253, Mark
1629 18:45:40,843698 192.168.0.104  54334   192.168.0.176  RTP      665 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7967, Time=4245800253, Mark
1630 18:45:40,874045 192.168.0.104  54336   192.168.0.176  RTP      582 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7968, Time=4245803253, Mark
1631 18:45:40,874045 192.168.0.104  54334   192.168.0.176  RTP      582 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7968, Time=4245803253, Mark
1632 18:45:40,904216 192.168.0.104  54334   192.168.0.176  RTP      511 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7969, Time=4245806253, Mark
1633 18:45:40,904590 192.168.0.104  54336   192.168.0.176  RTP      511 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7969, Time=4245806253, Mark
1634 18:45:40,934408 192.168.0.104  54334   192.168.0.176  RTP      545 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7970, Time=4245809253, Mark
1635 18:45:40,934408 192.168.0.104  54336   192.168.0.176  RTP      545 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7970, Time=4245809253, Mark
1636 18:45:40,979708 192.168.0.104  54334   192.168.0.176  RTP      446 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7971, Time=4245812253, Mark
1637 18:45:40,979708 192.168.0.104  54336   192.168.0.176  RTP      446 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7971, Time=4245812253, Mark
1638 18:45:41,009932 192.168.0.104  54334   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7972, Time=4245815253
1639 18:45:41,009932 192.168.0.104  54336   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7973, Time=4245815253
1640 18:45:41,009932 192.168.0.104  54336   192.168.0.176  RTP      134 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7974, Time=4245815253, Mark
1641 18:45:41,010174 192.168.0.104  54334   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7973, Time=4245815253
1642 18:45:41,010174 192.168.0.104  54336   192.168.0.176  RTP     1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7972, Time=4245815253
1643 18:45:41,010174 192.168.0.104  54334   192.168.0.176  RTP      134 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7974, Time=4245815253, Mark
1644 18:45:41,040115 192.168.0.104  54336   192.168.0.176  RTP      862 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7975, Time=4245818253, Mark
1645 18:45:41,040115 192.168.0.104  54334   192.168.0.176  RTP      862 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7975, Time=4245818253, Mark
1646 18:45:41,070861 192.168.0.104  54336   192.168.0.176  RTP      929 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7976, Time=4245821253, Mark
1647 18:45:41,070861 192.168.0.104  54334   192.168.0.176  RTP      929 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=7976, Time=4245821253, Mark
```

*Figure 21: Wireshark on remote station - rou*ter 2 engage event

The image displays a camera stream that uses the RTP protocol and the UDP port 5005 as the destination. Wireshark can color-code the data based on different criteria. In this case, we used the UDP protocol as the criterion, which assigns a distinct color to each combination of source and destination IP addresses and UDP ports.

The image shows a clear contrast between the first and the second half. The first half is red, indicating that only one router is sending the data. The second half has blue stripes, meaning that both routers are active and providing redundancy for higher reliability. The stripes are formed unevenly as the different paths taken by the routers have different latency. The next image then displays how the stream responsibility is handed over solely to the second router, which completes the cross-border scenario.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Both vehicle routers
Vehicle Router 1 disengaged
Ethernet

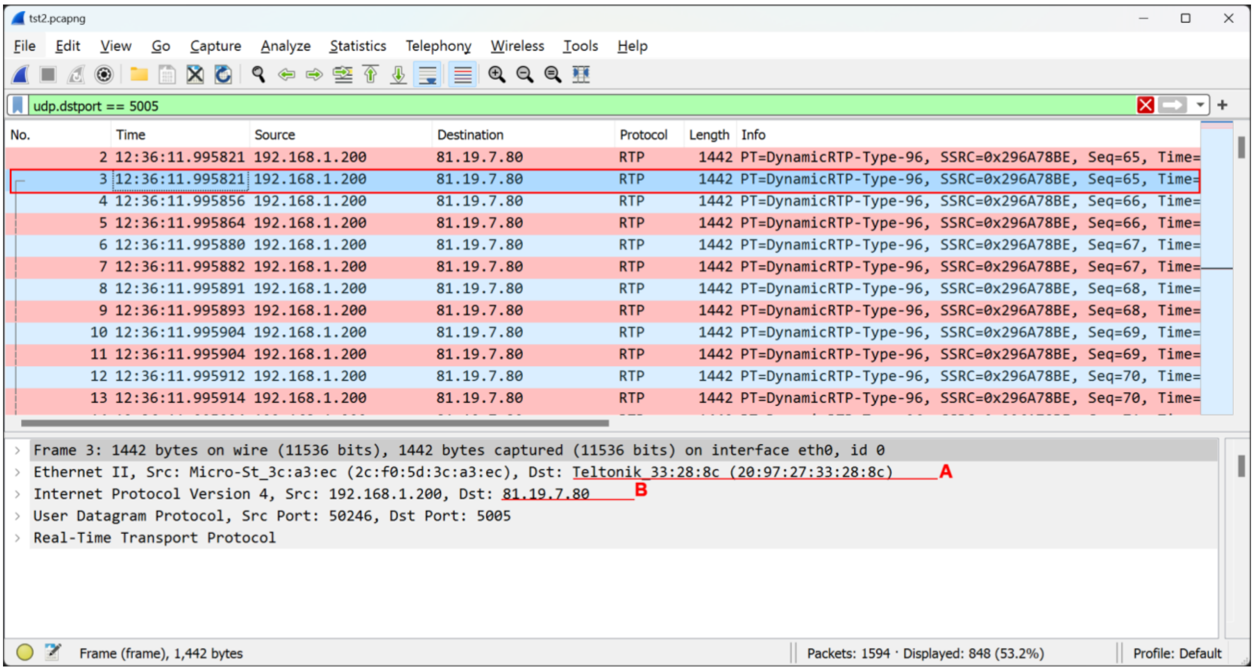
```
udp.dstport == 5005

No.   Time            Source        srcport  Destination    Protocol  Length  Info
3352 18:46:00,366603 192.168.0.104  54336    192.168.0.176  RTP        629 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8737, Time=4247558253, Mark
3354 18:46:00,412537 192.168.0.104  54334    192.168.0.176  RTP        588 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8738, Time=4247561253, Mark
3355 18:46:00,412537 192.168.0.104  54336    192.168.0.176  RTP        588 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8738, Time=4247561253, Mark
3356 18:46:00,442917 192.168.0.104  54336    192.168.0.176  RTP        516 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8739, Time=4247564253, Mark
3357 18:46:00,442917 192.168.0.104  54334    192.168.0.176  RTP        516 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8739, Time=4247564253, Mark
3358 18:46:00,473455 192.168.0.104  54336    192.168.0.176  RTP        623 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8740, Time=4247567253, Mark
3359 18:46:00,473455 192.168.0.104  54334    192.168.0.176  RTP        623 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8740, Time=4247567253, Mark
3360 18:46:00,503522 192.168.0.104  54334    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8743, Time=4247570253
3361 18:46:00,503744 192.168.0.104  54334    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8741, Time=4247570253
3362 18:46:00,503744 192.168.0.104  54334    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8744, Time=4247570253
3363 18:46:00,503744 192.168.0.104  54334    192.168.0.176  RTP        274 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8745, Time=4247570253, Mark
3364 18:46:00,518695 192.168.0.104  54336    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8741, Time=4247570253
3365 18:46:00,518695 192.168.0.104  54336    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8742, Time=4247570253
3366 18:46:00,518695 192.168.0.104  54336    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8743, Time=4247570253
3367 18:46:00,518937 192.168.0.104  54336    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8744, Time=4247570253
3368 18:46:00,518937 192.168.0.104  54336    192.168.0.176  RTP        274 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8745, Time=4247570253, Mark
3369 18:46:00,533774 192.168.0.104  54334    192.168.0.176  RTP        394 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8746, Time=4247573253, Mark
3370 18:46:00,533774 192.168.0.104  54336    192.168.0.176  RTP        394 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8746, Time=4247573253, Mark
3371 18:46:00,533990 192.168.0.104  54334    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8742, Time=4247570253
3372 18:46:00,579443 192.168.0.104  54336    192.168.0.176  RTP        470 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8747, Time=4247576253, Mark
3373 18:46:00,579443 192.168.0.104  54334    192.168.0.176  RTP        470 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8747, Time=4247576253, Mark
3374 18:46:00,609648 192.168.0.104  54334    192.168.0.176  RTP        437 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8748, Time=4247579253, Mark
3375 18:46:00,609648 192.168.0.104  54336    192.168.0.176  RTP        437 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8748, Time=4247579253, Mark
3376 18:46:00,639855 192.168.0.104  54336    192.168.0.176  RTP        440 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8749, Time=4247582253, Mark
3377 18:46:00,639855 192.168.0.104  54334    192.168.0.176  RTP        440 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8749, Time=4247582253, Mark
3378 18:46:00,669898 192.168.0.104  54334    192.168.0.176  RTP        519 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8750, Time=4247585253, Mark
3379 18:46:00,669898 192.168.0.104  54336    192.168.0.176  RTP        519 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8750, Time=4247585253, Mark
3380 18:46:00,700308 192.168.0.104  54334    192.168.0.176  RTP        796 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8751, Time=4247588253, Mark
3381 18:46:00,700308 192.168.0.104  54336    192.168.0.176  RTP        796 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8751, Time=4247588253, Mark
3382 18:46:00,745975 192.168.0.104  54336    192.168.0.176  RTP        756 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8752, Time=4247591253, Mark
3384 18:46:00,776934 192.168.0.104  54336    192.168.0.176  RTP        781 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8753, Time=4247594253, Mark
3386 18:46:00,807192 192.168.0.104  54336    192.168.0.176  RTP        685 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8754, Time=4247597253, Mark
3389 18:46:00,836861 192.168.0.104  54336    192.168.0.176  RTP        553 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8755, Time=4247600253, Mark
3394 18:46:00,867234 192.168.0.104  54336    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8756, Time=4247603253
3396 18:46:00,867234 192.168.0.104  54336    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8757, Time=4247603253
3397 18:46:00,867234 192.168.0.104  54336    192.168.0.176  RTP        804 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8760, Time=4247603253, Mark
3398 18:46:00,882434 192.168.0.104  54336    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8758, Time=4247603253
3399 18:46:00,882434 192.168.0.104  54336    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8759, Time=4247603253
3402 18:46:00,912642 192.168.0.104  54336    192.168.0.176  RTP        241 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8761, Time=4247606253, Mark
3403 18:46:00,942752 192.168.0.104  54336    192.168.0.176  RTP        216 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8762, Time=4247609253, Mark
3406 18:46:00,973344 192.168.0.104  54336    192.168.0.176  RTP        363 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8763, Time=4247612253, Mark
3408 18:46:01,003544 192.168.0.104  54336    192.168.0.176  RTP        518 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8764, Time=4247615253, Mark
3410 18:46:01,033725 192.168.0.104  54336    192.168.0.176  RTP        591 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8765, Time=4247618253, Mark
3411 18:46:01,079502 192.168.0.104  54336    192.168.0.176  RTP        761 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8766, Time=4247621253, Mark
3413 18:46:01,109904 192.168.0.104  54336    192.168.0.176  RTP        883 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8767, Time=4247624253, Mark
3415 18:46:01,139708 192.168.0.104  54336    192.168.0.176  RTP        715 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8768, Time=4247627253, Mark
3418 18:46:01,169914 192.168.0.104  54336    192.168.0.176  RTP        680 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8769, Time=4247630253, Mark
3420 18:46:01,200540 192.168.0.104  54336    192.168.0.176  RTP        666 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8770, Time=4247633253, Mark
3422 18:46:01,246059 192.168.0.104  54336    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8773, Time=4247636253
3423 18:46:01,246264 192.168.0.104  54336    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8774, Time=4247636253
3424 18:46:01,246264 192.168.0.104  54336    192.168.0.176  RTP       1442 PT=DynamicRTP-Type-96, SSRC=0xA3779B, Seq=8771, Time=4247636253

Packets: 11587 · Displayed: 3143 (27
```

Figure 22: Wireshark on remote station - router 1 disengage event

The IP address of the remote station in the internal network does not change throughout the data exchange. Neither does the source IP address, which usually represents the last router IP address in the path. This is because the router performs network address translation (NAT) and alters the original source of the data. The only field that varies is the source port.

The logged data shows that the same sequence numbers (Seq) are received twice, which means that the datagrams are duplicated. However, with NAT, we cannot tell if the datagrams come from two different router paths or from one path that sends them twice. The only way to know that is to look at the data flow from the edge router. Therefore, from the Remote Station side, we can only check if the redundancy is enabled, but not if it works properly.

On the other hand it is possible to verify the solution by logging the data on the vehicle side. Using the wireshark again, we can check that the datagrams are being sent to a correct router. The behavior is displayed on the images below.



udp.dstport == 5005

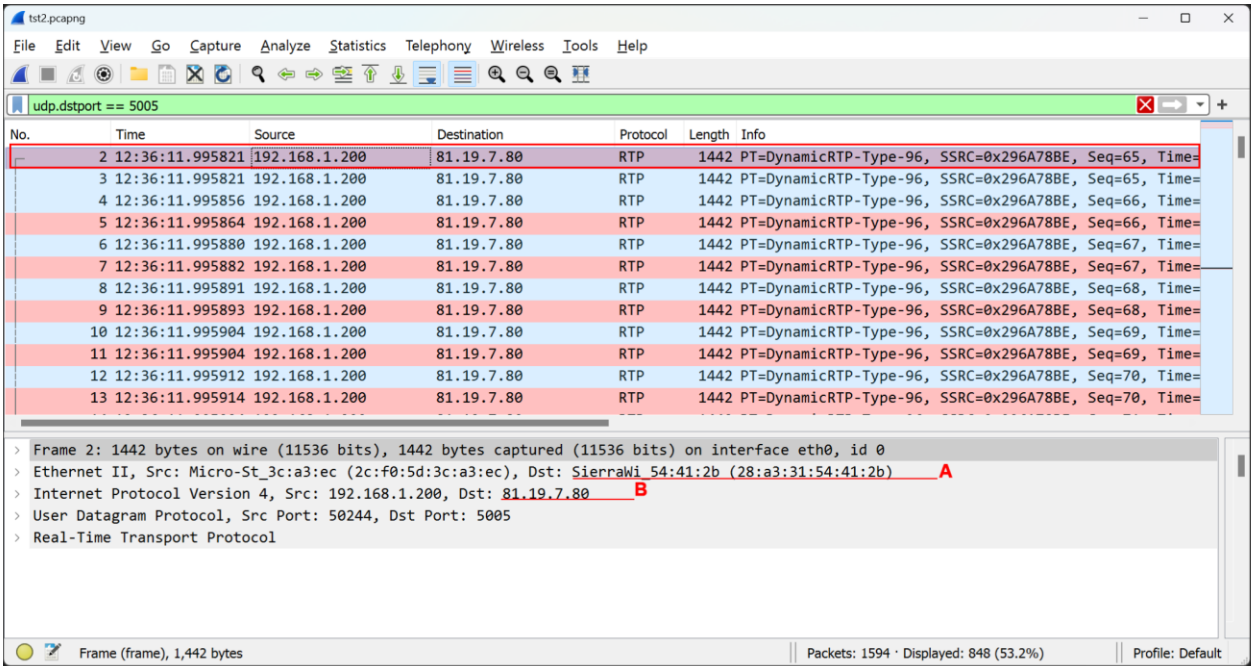
```
No.  Time            Source         Destination  Protocol Length Info
   2 12:36:11.995821 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=65, Time=
   3 12:36:11.995821 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=65, Time=
   4 12:36:11.995856 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=66, Time=
   5 12:36:11.995864 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=66, Time=
   6 12:36:11.995880 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=67, Time=
   7 12:36:11.995882 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=67, Time=
   8 12:36:11.995891 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=68, Time=
   9 12:36:11.995893 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=68, Time=
  10 12:36:11.995904 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=69, Time=
  11 12:36:11.995904 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=69, Time=
  12 12:36:11.995912 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=70, Time=
  13 12:36:11.995914 192.168.1.200  81.19.7.80   RTP      1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=70, Time=
```

```
> Frame 3: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits) on interface eth0, id 0
> Ethernet II, Src: Micro-St_3c:a3:ec (2c:f0:5d:3c:a3:ec), Dst: Teltonik_33:28:8c (20:97:27:33:28:8c)
> Internet Protocol Version 4, Src: 192.168.1.200, Dst: 81.19.7.80
> User Datagram Protocol, Src Port: 50246, Dst Port: 5005
> Real-Time Transport Protocol
```

Frame (frame), 1,442 bytes | Packets: 1594 · Displayed: 848 (53.2%) | Profile: Default

Figure 23: Wireshark on vehicle - router 1

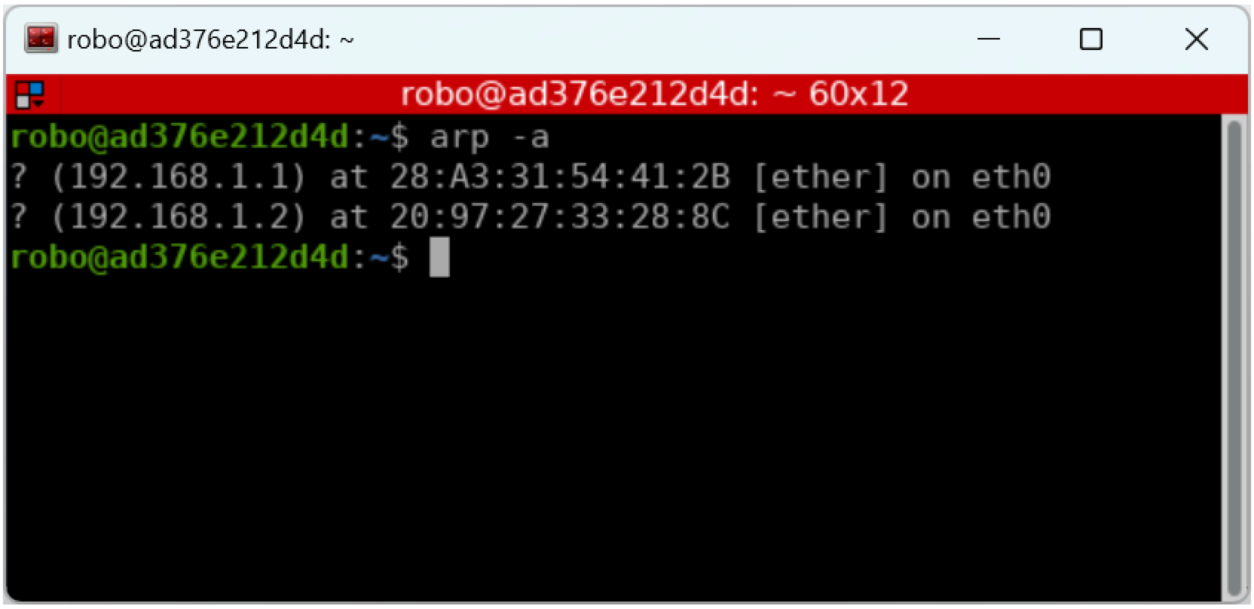
The image above displays the data that was logged and saved by the vehicle’s master computing unit. This unit is connected to a network that has two routers: Teltonika RUTX50 and Sierra Wireless Airlink XR90. These routers can be identified by their MAC addresses, which are shown at marker **A** in the image. The master computing unit has an IP address of 192.168.1.200, which is the source of the data packets. The remote station that receives the data has an IP address of 81.19.7.80, which is shown at marker **B** in the image. To be more exact, it is an IP of the edge router that will forward the data to the remote station. To send the data to the right router, the master computing unit needs to know the router’s MAC address. This is done by using the ARP protocol, which is a method of finding the MAC addresses of devices on a network. After the master computing unit obtains the MAC address of the router, it can forward the data packets to the router, which then routes them to the remote station.


tst2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
A
B

```
udp.dstport == 5005

No.  Time             Source         Destination  Protocol  Length Info
   2 12:36:11.995821 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=65, Time=
   3 12:36:11.995821 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=65, Time=
   4 12:36:11.995856 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=66, Time=
   5 12:36:11.995864 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=66, Time=
   6 12:36:11.995880 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=67, Time=
   7 12:36:11.995882 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=67, Time=
   8 12:36:11.995891 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=68, Time=
   9 12:36:11.995893 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=68, Time=
  10 12:36:11.995904 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=69, Time=
  11 12:36:11.995904 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=69, Time=
  12 12:36:11.995912 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=70, Time=
  13 12:36:11.995914 192.168.1.200  81.19.7.80   RTP       1442 PT=DynamicRTP-Type-96, SSRC=0x296A78BE, Seq=70, Time=

> Frame 2: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits) on interface eth0, id 0
> Ethernet II, Src: Micro-St_3c:a3:ec (2c:f0:5d:3c:a3:ec), Dst: SierraWi_54:41:2b (28:a3:31:54:41:2b)
> Internet Protocol Version 4, Src: 192.168.1.200, Dst: 81.19.7.80
> User Datagram Protocol, Src Port: 50244, Dst Port: 5005
> Real-Time Transport Protocol

Frame (frame), 1,442 bytes          Packets: 1594 · Displayed: 848 (53.2%)          Profile: Default
```

Figure 24: Wireshark on vehicle - router 2

Therefore, when looking at the logged data, technician can check the destination MAC address of the datagram or packet and distinguish which router path is actually taken. Both images above have a red selection rectangle showing which packet detail is being displayed. By examining the destination fields of the IP header and the physical layer, it is evident that the datagrams are sent to the appropriate routers for routing. The image below shows the ARP cache with the IP to MAC mapping, which reveals the actual IP addresses and MAC addresses of the routers.



```
robo@ad376e212d4d:~$ arp -a
? (192.168.1.1) at 28:A3:31:54:41:2B [ether] on eth0
? (192.168.1.2) at 20:97:27:33:28:8C [ether] on eth0
robo@ad376e212d4d:~$
```

Figure 25: ARP cache

6. TEST RESULTS

The software-based cross-border solution described in the provided testing scenarios is not only feasible but also highly verifiable through the use of Wireshark and conventional network monitoring methods. The three testing scenarios detailed - GPS-driven scenario, manual hardware management, and SIMs with disabled roaming - all demonstrate the adaptability and reliability of the system when users transition between different mobile networks, replicating real-world border-crossing situations.

The GPS-driven scenario leverages GPS technology to seamlessly switch between SIM cards based on the user's proximity to the border. This approach allows for virtual border testing, ensuring a smooth handover and optimized data transmission. Meanwhile, the manual hardware management scenario simulates border crossing by manually disconnecting and reconnecting routers, which effectively tests the system's ability to switch between SIM cards during border transitions.

The third scenario, using SIM cards with disabled roaming capabilities, tests the system's response to the limitations imposed by SIM card settings. This scenario adds an additional layer of realism, as it simulates conditions where routers are restricted from connecting to foreign networks.

Wireshark, a widely-used network protocol analyzer, plays a crucial role in verifying the system's performance and redundancy. By capturing and inspecting data packets in real-time, it offers a transparent view of the network's activity, allowing engineers to confirm that data packets are following the intended routes and reaching their destinations. From both the remote station and vehicle sides, Wireshark can confirm the proper functioning of the system.

Furthermore, using a standard teleoperation setup as part of this network-oriented research actually allowed Roboauto to not only verify with Wireshark that the video packets are being sent via the different networks as intended, but also that from a use case point of view, that this solution resulted in a seamlessly continued operation when crossing both virtual and real borders. No disruptions in the video streams displayed on the different monitors of the teleoperation driving station were observed during the tests.

In summary, the combination of these testing scenarios and the use of Wireshark as a network monitoring tool and the actual Roboauto teleoperation solution as a use case validation tool demonstrates that the software-based dual-sim cross-border solution is not only possible but also verifiable through conventional means.

7. CONCLUSIONS

In summary, this research delves into the challenges and solutions in leveraging 5G for cross-border teleoperation. Collaboration among Mobile Network Operators (MNOs) is crucial, exemplified by projects like 5G-MOBIX, 5G-CARMEN, 5GCroCo, and 5G-Blueprint. The practical multi-SIM/multi-modem solution, irrespective of vendors and User Equipment (UE), stands out for its effectiveness in enhancing connection stability.

The executive summary underscores the importance of network stability in the growing teleoperation market. Safety implications of network interruptions are highlighted, emphasizing the adaptability of the multi-SIM solution to current and future market needs.

The introduction sets the context for stable connections in remote vehicle operation, distinguishing between intra-PLMN inter-gNB and inter-PLMN handovers, paving the way for the exploration of the multi-SIM solution.

The analysis of cross-border scenarios reveals challenges and introduces UE-based and network-based measures. Despite shortcomings in failover dual SIM routers, innovative solutions, like the central prediction function from the 5G-Mobix project, emerge.

Roboauto’s 5G communication redundancy solution advances reliable vehicle connectivity. The MultiUDP protocol, RoboProto layer, and iptables based routing driver provide software-based solution for reliable and secure teleoperation. The cross-border solution demonstrates robustness and versatility, validated through realistic simulations and testing scenarios, showcasing adaptability and scalability.

Testing has affirmed feasibility and verifiability through Wireshark, conventional monitoring tools and the actual teleoperation use case. Three testing scenarios validate the system's response, adaptability, and reliability.

In conclusion, this research addresses 5G challenges with practical solutions. Collaboration among MNOs, the multi-SIM approach, and advancements in communication channel redundancy contribute to a comprehensive understanding. This research contributes to the practical application of 5G in critical sectors, ensuring uninterrupted connectivity for cross-border teleoperation.

REFERENCES

[1] PR Newswire, 'Global Teleoperation of Automated Vehicles Market Report 2022', June 2022 [Online]. Available: https://www.prnewswire.com/news-releases/global-teleoperation-of-automated-vehicles-market-report-2022-market-to-surpass-530-million-by-2028-with-the-market-opening-up-by-2024-301574036.html

[2] 5G-Mobix, 'D3.7 Final Report on Development, Integration and Roll-out', April 2022 [Online]. Available: https://www.5g-mobix.com/assets/files/5G-MOBIX-D3.7_Final-report-on-development-integration-and-roll-out_V1.0.pdf

[3] Techplayon, '5G NR Measurement – Serving Cell and Neighbor Cell', January 2020 [Online]. Available: https://www.techplayon.com/5g-nr-measurement-serving-cell-and-neighbor-cell/

[4] Techplayon, '5G NR Measurement Events', February 2020 [Online]. Available: https://www.techplayon.com/5g-nr-measurement-events/