



Title:	Deliverable D3.8.1 A-ERCS system specification	Document Version: 1.2
---------------	---	-------------------------------------

Project Number: 297239	Project Acronym: GEN6	Project Title: Governments ENabled with IPv6
--------------------------------------	-------------------------------------	--

Contractual Delivery Date: 31/12/2012	Actual Delivery Date: 03/01/2013	Deliverable Type* - Security**: R – CO
---	--	--

* Type: P - Prototype, R - Report, D - Demonstrator, O - Other

** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible and Editor/Author: Luka Koršič	Organization: ULFE	Contributing WP: WP3
--	----------------------------------	------------------------------------

Authors (organisations):

Mojca Volk (ULFE), Janez Sterle (ULFE), Luka Mali (ULFE), Dušan Mulac (ULFE), Jože Hanc (SECCSU), Matej Cerik (Water Science Institute), Jan Žorž (ULFE)

Abstract:

This deliverable summarizes the results of the design phase of the A-ERCS system. It comprises the overall A-ERCS system architecture and functional specifications as well as IPv6-related specifications of individual A-ERCS segments (A-ERCS Node, A-ERCS Node Extension, SECC segment, Backhaul Supported System). In addition, the document explains the upgraded and additionally implemented functionalities and features available in the A-ERCS system compared to functionalities and features of the existent ERCS system.

Keywords:

IPv6, Government, IPv6-enabled services, Emergency Response Systems, A-ERCS, Fire Department, Public Sector.

Revision History

The following table describes the main changes done in this document since its creation.

Revision	Date	Description	Author (Organization)
V0.1	18/9/2012	Document creation	Janez Sterle (ULFE)
V0.2	21/9/2012	Table of contents and initial inputs	Luka Koršič, Janez Sterle (ULFE)
V1.0	25/10/2012	First Draft	Luka Koršič (ULFE)
V1.1	21/12/2012	Document for internal review	Luka Koršič, Mojca Volk (ULFE)
V1.2	02/01/2013	Final Review	Emre Yuce (TUBITAK)

Disclaimer

The GEN6 project (number 261584) is co-funded by the European Commission under the ICT Policy Support Programme (PSP) as part of the Competitiveness and Innovation framework Programme (CIP). This document contains material that is the copyright of certain GEN6 partners and the EC, and that may be shared, reproduced or copied “as is”, following the Creative Commons “Attribution-Non Commercial-No Derivs 3.0 Unported (CC BY-NC-NC 3.0) licence. Consequently, you’re free to share (copy, distribute, transmit) this work, but you need to respect the attribution (respecting the project and authors names, organizations, logos and including the project web site URL “<http://www.gen6.eu>”), for non-commercial use only, and without any alteration, transformation or build upon this work.

The information herein does not necessarily express the opinion of the EC. The EC is not responsible for any use that might be made of data appearing herein. The GEN6 partners do not warrant that the information contained herein is capable of use, or that use of the information is free from risk, and so do not accept liability for loss or damage suffered by any person using this information.

Executive Summary

The focus of the A-ERCS pilot is to design, implement and demonstrate a communication system and services for a specific targeted stakeholder group, in our case an emergency response fire fighter unit during an on-site intervention. The aim is to demonstrate that state-of-the-art communication technologies and networks can facilitate an advanced emergency response communication system and provide professionalized data services by utilizing a carefully orchestrated combination of professional and commercial networks and relying on advanced features of the IPv6 technology.

This deliverable documents the first A-ERCS system architecture and technical specifications, which is part of an on-going work towards the A-ERCS pilot implementation and demonstration. In summary, it provides system design and technical specifications, focusing on architecture, addressing scheme, QoS and policy enforcement, security, routing, mobility, and services subsystem. Under each aspect, several different levels are addressed, that is, system level, node level, node extension level, strategic emergency control centre level, backhaul supported system, and device level. IPv6 functionalities and features supported in all A-ERCS segments are in the core of the A-ERCS system and services design.

To address usability, reliability and added value services in the context of emergency response environments, system and services design was completed in close collaboration with all technological stakeholders. Domain-specific aspects were addressed jointly with the SECCSU and OZRCO teams with a general tendency to provide realistic and usable system and services. Telekom Slovenije and ARNES provided valuable inputs regarding IPv6 aspects of the system and use of backhaul supported systems. In cooperation with Cisco, technology, networking and communication features in terms of IPv6 support were studied and first proof of concept implementations in laboratory environment were already completed by ULFE.

An additional objective, set out by ULFE for the A-ERCS system, is to make an effort towards delivering not only a proof of concept pilot for experimental use but a production A-ERCS system directly applicable into practice. For this purpose, first pilot implementations and testing have already started, with the results showing that today compact and integrated overlay communication solution such as the A-ERCS represents a technological challenge in the addressed emergency response domain. This even intensifies the importance and added value of the A-ERCS efforts, and is an additional motivator for the successful delivery and demonstration of the A-ERCS pilot.

Table of Contents

Table of Contents	5
Table Index.....	9
1 Introduction.....	12
1.1 A-ERCS pilot stakeholder ecosystem.....	13
1.2 A-ERCS system overview	15
1.3 A-ERCS specification methodology	20
2 Existent ERCS System Specification	22
2.1 ERCS environment	22
2.2 ERCS System Architecture.....	23
2.3 ERCS Service Subsystems	25
3 A-ERCS System Specification	27
3.1 A-ERCS System Architecture	27
3.1.1 Node Specification	29
3.1.2 Node Extension Specification	49
3.1.3 Strategic Emergency Control Center infrastructure specification.....	51
3.1.4 Backhaul Supported System.....	57
3.2 A-ERCS System Addressing Scheme	63
3.3 A-ERCS Backhaul Supported System Addressing Scheme requirements	63
3.4 A-ERCS System QoS and Policy Enforcement Design.....	64
3.4.1 Differentiated Services model.....	66
3.4.2 Node Level.....	67
3.4.3 Node Extension Level	67

3.4.4	Device Level.....	68
3.4.5	Strategic Emergency Control Center level	69
3.4.6	A-ERCS QoS and Policy Enforcement requirements for Backhaul Supported Systems.....	69
3.5	A-ERCS System Security Design.....	70
3.5.1	Control plane.....	70
3.5.2	Data plane	73
3.5.3	Management plane	77
3.5.4	User plane	79
3.5.5	A-ERCS Security Requirements for Backhaul Supported System	82
3.6	A-ERCS System Routing Design	83
3.6.1	Unicast routing.....	84
3.6.2	Multicast routing.....	94
3.6.3	A-ERCS Routing Design Requirements for Backhaul Supported System	99
3.7	A-ERCS System Mobility Design	99
3.7.1	Mobile IPv6	103
3.7.2	NEMO	104
3.7.3	Node level	104
3.7.4	Node Extension level	105
3.7.5	Device level	105
3.7.6	Strategic Emergency Control Center	106
3.7.7	A-ERCS Mobility Requirements for Backhaul Supported System.....	107
3.8	A-ERCS Service Subsystems Design	108
4	Conclusions.....	115

297239	GEN6	D 3.8.1: A-ERCS System Specification
--------	------	--------------------------------------

5 *References*.....129
6 *Appendix 1: Letters of support*.....132

Figure Index

<i>Figure 1-1: High-level A-ERCS system overview.....</i>	<i>17</i>
<i>Figure 1-2: High-level A-ERCS services overview.</i>	<i>18</i>
<i>Figure 2-1: The SECCSU vehicle where the A-ERCS system will be implemented.</i>	<i>22</i>
<i>Figure 2-2: Organization and chain of command for intervention procedures involving SECCSU.</i>	<i>23</i>
<i>Figure 2-3: High-level overview of existent ERCS system.....</i>	<i>24</i>
<i>Figure 2-4: The ERCS communication infrastructure available in the SECCSU vehicle.</i>	<i>25</i>
<i>Figure 3-1: A-ERCS system architecture.....</i>	<i>28</i>
<i>Figure 3-1: A-ERCS Node Architecture.</i>	<i>32</i>
<i>Figure 3-4: A-ERCS system DiffServ domain.</i>	<i>65</i>
<i>Figure 3-5: A-ERCS system IGP routing.</i>	<i>85</i>
<i>Figure 3-6: A-ERCS system IGP & EGP routing.</i>	<i>86</i>
<i>Figure 3-7: Mobile IPv6 in the A-ERCS system.</i>	<i>101</i>
<i>Figure 3-8: NEMO in the A-ERCS system.....</i>	<i>102</i>
<i>Figure 3-9: Organization and chain of command for intervention procedures involving SECCSU with A-ERCS overlay.</i>	<i>108</i>
<i>Figure 3-2: gen6.ltfe.org web portal for sensor applications.</i>	<i>114</i>

Table Index

Table 1-1: Requirements for A-ERCS services.	19
Table 2-1: ERCS capabilities and services overview.	26
Table 3-1: A-ERCS System Architecture – Node Specification – Core Router.	33
Table 3-2: A-ERCS System Architecture – Node Specification – Firewall.	37
Table 3-3: A-ERCS System Architecture – Node Specification – Router/AP.	39
Table 3-4: A-ERCS System Architecture – Node Specification – Server domain.	42
Table 3-5: A-ERCS System Architecture – Node Specification – System management domain.	44
Table 3-6: A-ERCS System Architecture – Node Specification – Photos, printers, faxes, scanners domain.	46
Table 3-7: A-ERCS System Architecture – Node Specification – User stations domain.	47
Table 3-8: A-ERCS System Architecture – Node Extension Specification – Mesh WiFi domain.	50
Table 3-9: A-ERCS System Architecture – Node Extension Specification – Sensor systems domain.	50
Table 3-10: A-ERCS System Architecture – Node Extension Specification – User stations domain.	51
Table 3-11: A-ERCS System Architecture – Node Extension Specification – DMR domain.	51
Table 3-12: A-ERCS System Architecture – Strategic Emergency Control Center Specification.	52
Table 3-13: A-ERCS System Architecture – Backhaul supported system.	58
Table 3-14: IPv6-based QoS requirements.	64
Table 3-15: A-ERCS node QoS requirements.	67
Table 3-16: A-ERCS node extension QoS requirements.	68
Table 3-17: A-ERCS device level QoS requirements.	69

Table 3-18: SECC QoS requirements.	69
Table 3-19: IPv6-based QoS requirements for backhaul supported systems.	70
Table 3-20: IPv6-based control plane security requirements.	71
Table 3-21: A-ERCS node control plane security requirements.	72
Table 3-22: A-ERCS node extension control plane security requirements.	72
Table 3-23: A-ERCS device level control plane security requirements.	73
Table 3-24: SECC control plane security requirements.	73
Table 3-25: IPv6-based data plane security requirements.	74
Table 3-26: A-ERCS node data plane security requirements.	75
Table 3-27: A-ERCS node extension data plane security requirements.	75
Table 3-28: A-ERCS node device level data plane security requirements.	76
Table 3-29: A-ERCS node data plane security requirements.	77
Table 3-30: IPv6-based management plane security requirements.	77
Table 3-31: A-ERCS node management plane security requirements.	78
Table 3-32: A-ERCS node extension management plane security requirements.	78
Table 3-33: A-ERCS node device level management plane security requirements.	79
Table 3-34: SECC management plane security requirements.	79
Table 3-35: IPv6-based user plane security requirements.	80
Table 3-36: A-ERCS node user plane security requirements.	81
Table 3-37: A-ERCS node user plane security requirements.	81
Table 3-38: A-ERCS node device level user plane security requirements.	82
Table 3-39: A-ERCS node user plane security requirements.	82

Table 3-40: IPv6-based security requirements for backhaul supported systems.	83
Table 3-41: IPv6-based unicast routing requirements.	84
Table 3-42: A-ERCS node unicast routing requirements.	90
Table 3-43: A-ERCS node extension unicast routing requirements.	91
Table 3-44: A-ERCS device level unicast routing requirements.	93
Table 3-45: SECC unicast routing requirements.	94
Table 3-46: IPv6-based multicast routing requirements.	94
Table 3-47: A-ERCS node multicast routing requirements.	97
Table 3-48: A-ERCS node extension multicast routing requirements.	98
Table 3-49: A-ERCS device level multicast routing requirements.	98
Table 3-50: SECC multicast routing requirements.	99
Table 3-51: IPv6-based routing requirements for backhaul supported systems.	99
Table 3-52: IPv6-based mobility requirements.	100
Table 3-53: A-ERCS node mobility requirements.	105
Table 3-54: A-ERCS node extension mobility requirements.	105
Table 3-55: A-ERCS device mobility requirements.	106
Table 3-56: SECC mobility requirements.	107
Table 3-57: IPv6-based mobility requirements for backhaul supported systems.	107
Table 3-58: A-ERCS services overview.	111

1 INTRODUCTION

The Slovenian pilot, Advanced Emergency Response Communication System (A-ERCS), represents a unique effort in terms of national IPv6 pilots in the GEN6 project by addressing IPv6 communication needs of a specific domain, that is, a fire fighter unit utilizing communications on field during an on-site intervention. Our vision is to contribute to further developments and adoption of advanced, reliable and highly convergent communication systems available for professional use in different emergency and catastrophic situations, and thus take the telecommunication services to the next level in serving for security and wellbeing of mankind. We would like to demonstrate that today a variety of powerful and efficient communication technologies exist that, if combined and orchestrated appropriately with advanced intelligent overlay solutions, can deliver reliable, resilient and autonomous communications able to serve and protect in extreme conditions where communication can represent a vital element of survival. Such solution is called Advanced Emergency Response Communication System (A-ERCS).

In particular, the A-ERCS pilot will demonstrate:

- a scalable and robust overlay system for data transport and rich multimedia service built across professional (e.g. DMR, TETRA, Satellite), commercial networks (e.g. UMTS/HSPA, LTE) and ruggedized commercial-of-the-shelf (COTS) systems (mesh Wi-Fi and ad-hoc WiMax),
- the ability of such a system to deliver seamless connectivity from targeted/affected areas across heterogeneous technologies and public networks, locally as well as on national and cross-border levels,
- capabilities of the IPv6 technology to assist in deployment of automatic network planning and deployment capabilities, vital to all A-ERCS systems,
- IPv6 support for advanced features, such as network, node and host auto configuration,
- the ability of such a system to assure secure and QoS-enabled transmission of data, voice and multimedia-rich services system by relying upon modern professional and commercial telecommunications networks and IPv6-based technologies and features.

This document represents the results of the second phase in the A-ERCS pilot activities, covering design and specification of the A-ERCS system. The work on the A-ERCS design and

specification took into account the general and domain-specific requirements resulting from the analysis completed in the first phase and documented in [1].

For better understanding of this document, the remainder of this section provides a brief overview of the ecosystem of involved partners and stakeholders, followed by a high-level A-ERCS architecture and services overview.

Section 2 explains in detail existent ERCS system specification and available services. The specifications cover all segments of interest to the A-ERCS system and services design, outlining also, the ERCS organizational structure and intervention procedures, characteristic for this specific end-user environment.

In section 3, A-ERCS system architecture and specifications are provided. The descriptions follow the architectural structure covering node level, node extension level, backhaul supported systems as well as SECC and device levels. It provides comparable specifications and clearly shows the upgraded and extended architecture and functional specifications of the A-ERCS system compared to existent ERCS infrastructure.

Section 4 concludes the document by discussing key findings and presents further steps and activities towards the A-ERCS pilot.

1.1 A-ERCS pilot stakeholder ecosystem

The targeted A-ERCS end-user group is very specific and in a very specific situation, that is, an emergency response fire fighter team requiring communication services during an on-site intervention. This in turn requires custom architecture design and system planning in order to deliver a compliant and useful solution. Therefore, in order to collect the specific requirements and expectations from first hand and integrate them appropriately into the A-ERCS system design and implementation, several external stakeholders are involved in the A-ERCS activities, as follows.

- **ULFE** as the official GEN6 partner and leader of the A-ERCS pilot, designing, specifying, implementing and demonstrating the A-ERCS system.
- **Municipality of Ljubljana (MOL), Department for Protection, Rescue and Civil Defence (OZRCO)**, covering pilot system requirements and pilot testing, as well as providing live emergency response environment and infrastructure.

The A-ERCS system design and specification is an on-going activity performed in close cooperation with the **Voluntary Fire Brigade (VFB)**, a civil protection service under the Public

Fire Fighter Service (PFFS) of the Municipality of Ljubljana (MOL), Department for Protection, Rescue and Civil Defence (OZRCO). More precisely, the A-ERCS node is designed for and will be deployed in a specialized vehicle in use by the Strategic Emergency Control Centre Support Unit (SECCSU) of the VFB. The major role of the SECCSU in the A-ERCS activities is to help in defining particular A-ERCS pilot requirements, implementation of the pilot A-ERCS unit in the SECCSU vehicle, and support with A-ERCS pilot demonstration and testing.

- **Water Science Institute**, preparing technical pilot system requirements and providing support for pilot testing.

On the application side of the A-ERCS pilot, the Water Science Institute provides valuable knowledge of the specific service requirements in the fire fighter domain, assists in identifying service-side A-ERCS pilot requirements, and defines service scenarios. Later on, this partner will help in A-ERCS pilot demonstration and testing.

- **Cisco System Slovenia & Global**, providing IPv6 networking equipment support.

Cisco Slovenia and Cisco Global is the core networking technology partner in the A-ERCS pilot contributing to the project with necessary networking equipment and assisting in the A-ERCS pilot deployment by providing appropriate technical support.

- **Telekom Slovenije, d.d.**, representing a commercial telecommunications operator and providing backhaul commercial mobile system and services support.

The largest Slovenian mobile operator represents the commercial networks domain in the A-ERCS. The operator is contributing to the project by making available for use commercial data communication services based on GSM/GPRS/UMTS/LTE/EPC technologies and providing network-side technical support throughout the A-ERCS deployment, testing and demonstration.

- **The Academic and Research Network of Slovenia (ARNES)** as a research and connectivity partner providing IPv4 and IPv6 services as well as support for pilot demonstrations.

ARNES holds an active role of an academic and research service provider in the A-ERCS pilot. They provide available services and support in the fixed networks and data centre services for the purpose of the A-ERCS pilot implementation, testing and evaluation (including free use of connectivity services, system and service configuration adjustments and technical support during the duration of the GEN6 project).

- **go6 Institute** in federating and consultancy role.

- **Ministry of Education, Science, Culture and Sport**, providing integration of the project in Slovenian government bodies.

Throughout the project, the go6 Institute is providing their support, federation and specialized consultancy services in the IPv6 domain, and the Ministry of Higher Education, Science and Technology will support the project by promoting the integration of the A-ERCS pilot in the Slovenian government.

1.2 A-ERCS system overview

This section introduces a high-level structure of the A-ERCS system.

Four preconditions were taken into account during system architecture planning:

1. all A-ERCS system segments are IPv6 enabled (as indicated also in Figure 1-1);
2. architecture and functionalities of existent ERCS system and services remain intact (explained further in Section 2), in an attempt to strictly follow the precondition defined by the SECCSU and OZRCO that the implementation of the A-ERCS pilot must not interrupt current SECCSU operation and service availability but is allowed only to complement and upgrade these while preserving intact reliability, availability and resilience of the current ERCS;
3. the system targets fulfilment of the defined A-ERCS system and services requirements, as specified in [1], with a specific focus on the delivery of the required services, as summarized in Table 1-1 and depicted in Figure 1-2;
4. further domain-specific requirements for operational service design of the A-ERCS system must match organizational structure of the emergency rescue intervention procedures, defined by the government bodies and followed in the SECCSU and OZRCO (specified in detail by the SECCSU and OZRCO teams, as explained in Section 2.1).

The A-ERCS is depicted in Figure 1-1. It comprises the following system segments (right to left):

- on-site infrastructure, termed **A-ERCS node extension**, comprising:
 - A-ERCS mobile devices for communication throughout the intervention among members of the on-site unit as well as with the Strategic Emergency Control Centre Support Unit (SECCSU);
 - sensor systems, such as water level sensors, earthquake monitoring system, heat sensors, etc., and on-site communication infrastructure, such as Mesh WiFi;

- communication infrastructure, located in the SECCSU vehicle, supporting intervention coordination and communication with the Strategic Emergency Control Centre (SECC) leading the entire operation; the core element of the A-ERCS system, an **A-ERCS node**, is implemented in the SECCSU vehicle;
- an **A-ERCS backhaul supported system**, constructed as a heterogeneous communication infrastructure comprising core network(s) and different professional and commercial networks and ruggedized COTS systems in the role of a (redundant) access infrastructure;
- and an **A-ERCS Strategic Emergency Control Centre (SECC)** located in distributed sites and responsible for the control and cross-communication of the entire operation on a national level (including cooperation and communication with other civil protection, rescue or military services) as well as cross-border connectivity.

The integrated segments together build a converged emergency response infrastructure, capable of providing operational assistance services for the on-site fire fighter unit and the SECCSU team, as well as surveillance of the on-site situation (more details are available in Section 3.7 and [1]). The targeted services are required to support the defined use case scenarios, delivering communication, multimedia and data services for intervention and situation surveillance purposes. A high-level overview of targeted services is presented in Figure 1-2 and in Table 1-1.

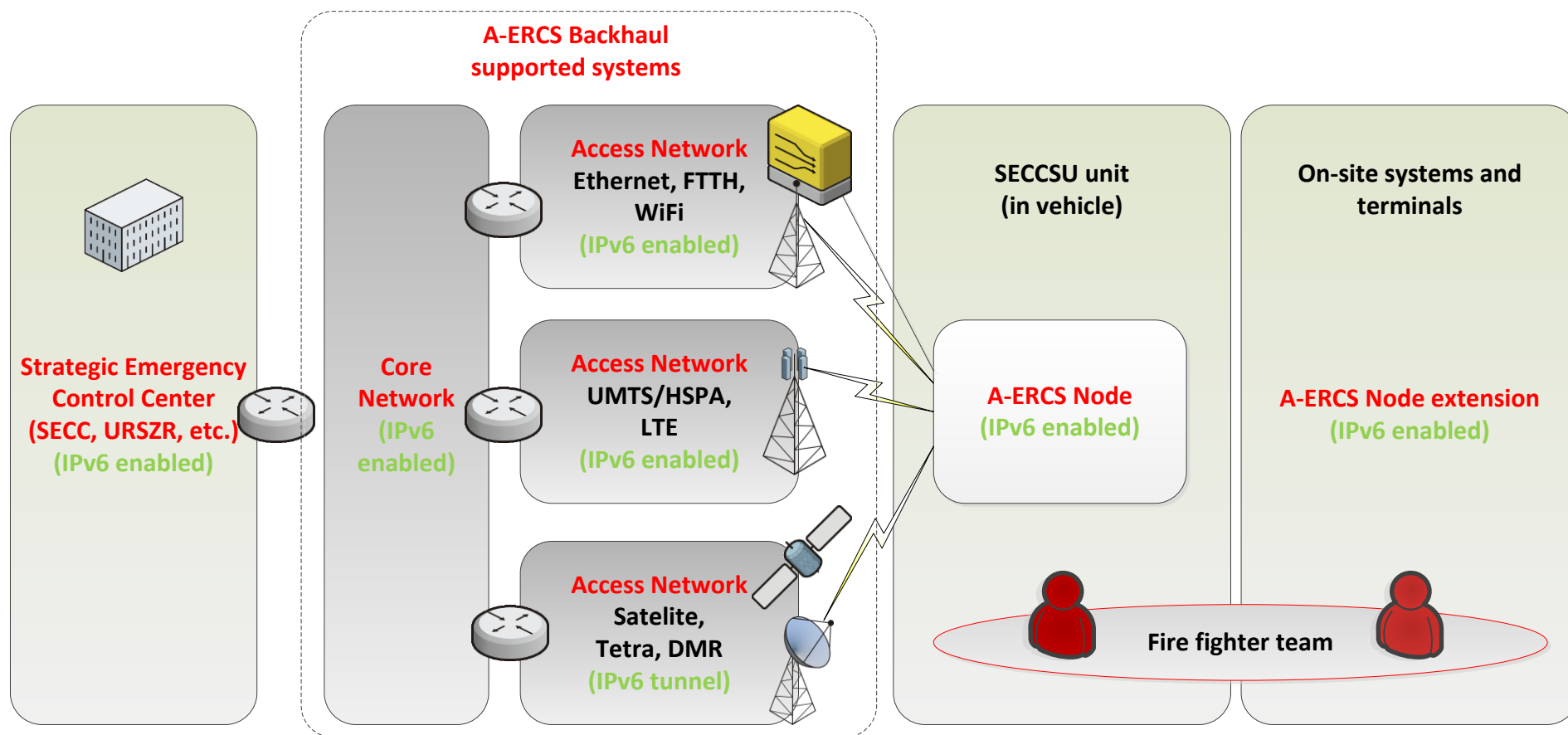


Figure 1-1: High-level A-ERCS system overview.

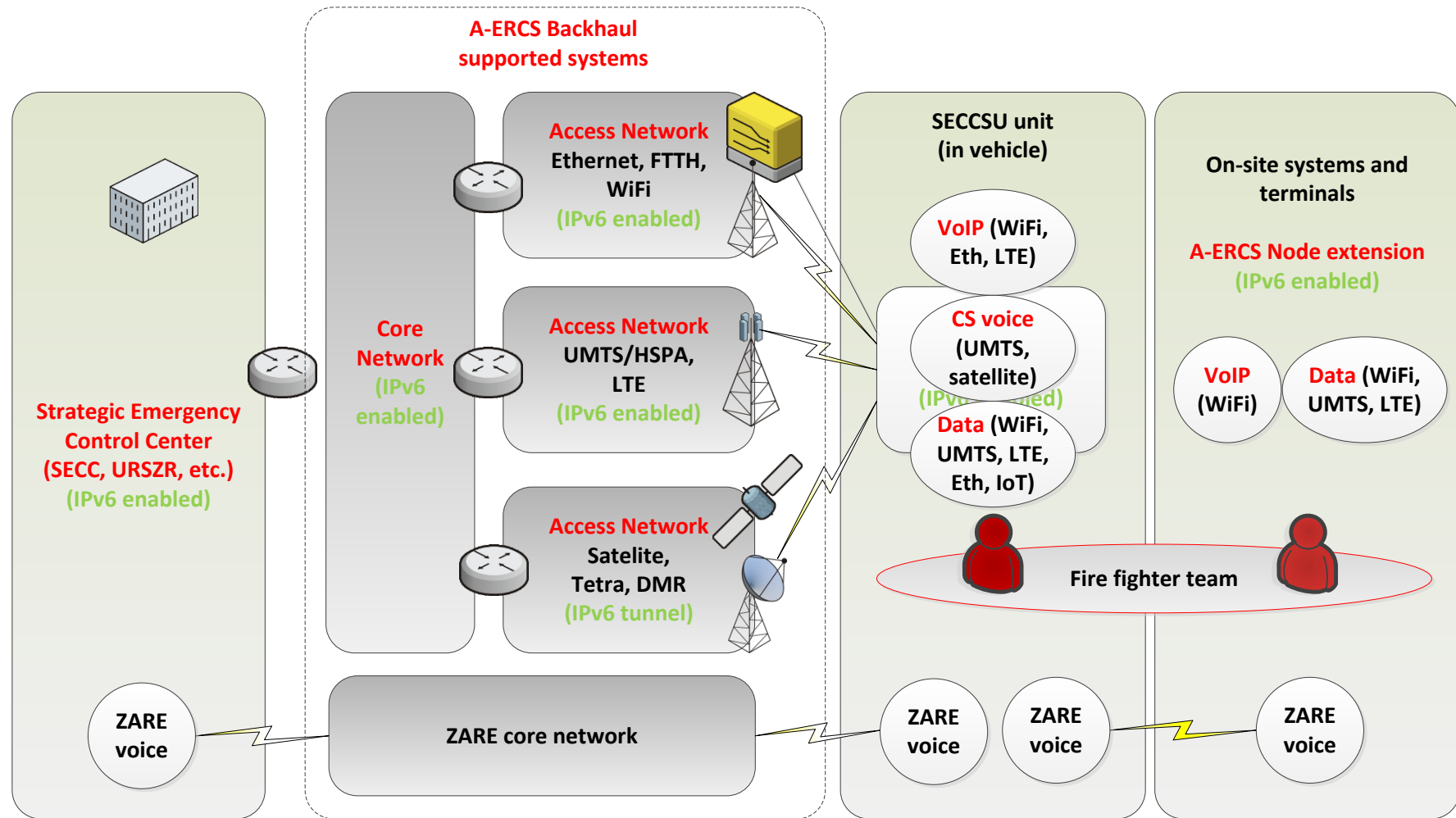


Figure 1-2: High-level A-ERCS services overview.

A-ERCS segment/capability	Requirement	Equipment requirements	Status
Requirements for voice services			
Fire fighter in operation	ZARE voice	Handheld radio	Existent
	VoIP over Mesh WiFi	WiFi terminal	Optional
SECCSU operator in operation	ZARE voice	Handheld radio	Existent
	CS voice over TETRA	TETRA terminal	Optional
	CS voice over satellite	Satellite terminal	Optional
	VoIP over LTE (prioritized)	LTE smartphone/softphone	Optional
	CS voice over UMTS	UMTS smartphone	Required
	VoIP over Ethernet/FTTH	Softphone of VoIP phone	Optional
	VoIP over Mesh WiFi	WiFi terminal	Optional
Requirements for data services			
Fire fighter team	Data via Mesh WiFi	WiFi	Optional
	Data via Local Mesh WiFi	WiFi	Required
	Data via UMTS/HSPA	UMTS/HSPA	Optional
	Data via LTE (prioritized)	LTE	Optional
SECCSU	Data from sensor systems via WiFi	Sensor system proprietary, WiFi	Optional
	Data via UMTS/HSPA	UMTS/HSPA	Required
	Data via LTE (prioritized)	LTE	Optional
	Data via Mesh WiFi	WiFi	Optional
	Data via Local Mesh WiFi	WiFi	Required
	Data via Ethernet/FTTH	Eth/FTTH	Optional
Requirements for messaging, video streaming and file transfer services			
Fire fighter team	Video streaming via UMTS/HSPA	UMTS/HSPA	Optional
	Video streaming via LTE	LTE	Optional
	Video streaming via Mesh WiFi	WiFi	Optional
	File transfer via UMTS/HSPA	UMTS/HSPA	Required
	File transfer via Mesh WiFi	WiFi	Optional
	File transfer via LTE	LTE	Optional
SECCSU	UMTS/HSPA messaging	UMTS/HSPA	Optional
	OTT messaging via Mesh WiFi	WiFi	Optional
	OTT messaging via LTE	LTE	Optional
	OTT messaging via Eth/FTTH	Eth/FTTH	Optional
	Video streaming via UMTS/HSPA	UMTS/HSPA	Optional
	Video streaming via LTE	WiFi	Optional
	Video streaming via UMTS/HSPA	LTE	Optional
	Video streaming via Eth/FTTH	Eth/FTTH	Optional
	File transfer via UMTS/HSPA	UMTS/HSPA	Required
	File transfer via Mesh WiFi	WiFi	Optional
	File transfer via LTE	LTE	Optional
	File transfer via Eth/FTTH	Eth/FTTH	Optional

Table 1-1: Requirements for A-ERCS services.

1.3 A-ERCS specification methodology

For the purpose of defining the A-ERCS system architecture and functional specifications, a versioning system will be used. This document represents version 1 of the A-ERCS system specification as a result of the first stage of an on-going effort in the activities A3.7.1 and A3.7.3 of the WP3 covering the A-ERCS pilot. In the following stages and activities, the architectural and functional specifications provided in this document will be further evolved and documented in the subsequent version. In summary, the contents of this document are subject to change, primarily due to the following facts:

- further evolvement of the A-ERCS architecture and specifications;
- availability of the commercial and professional backhaul support systems and/or their specific services, features and functionalities for the purposes of the A-ERCS pilot (availability of ZARE, UMTS/HSPA, LTE, satellite, TETRA, DMR, Eth/FTTH; availability of services supported on these systems, availability of prioritization, capacities and other configuration details in these systems and the respective services); in this respect, letters of support received from technology partners Telekom Slovenije, d.d., and OZRCO are attached in Section 7.
- availability of the networking equipment required for the implementation of the A-ERCS node (including feature lists and implementation details);
- availability of appropriate terminal and sensor equipment for the on-site fire fighter unit;
- any additional upcoming requirements and/or changes related to the intervention procedures organization of the SECCSU and OZRCO, affecting service requirements in general and definition of realistic service scenarios, compared to already defined service requirements and service scenarios in [1];
- further work on the IoT and sensor network support for the A-ERCS system, which is outside the GEN6 project but will be integrated into the overall A-ERCS ecosystem for its strategic importance.

In the remainder of this document, further details and explanations are provided to the above high-level structure of the envisioned A-ERCS system and services along with architectural, technological and functional specifications. The specifications are provided comparatively, first the specifications of the existent ERCS system are provided in Section 2, followed by the specifications of the targeted A-ERCS system in Section 3. The following A-ERCS aspects are

covered:

- system architecture,
- system addressing scheme,
- backhaul supported system addressing scheme requirements,
- system QoS and policy enforcement design,
- QoS and policy enforcement requirements for backhaul supported system,
- system security design,
- security requirements for backhaul supported system,
- system routing design,
- routing design requirements for backhaul supported system,
- system mobility design,
- mobility requirements for backhaul supported system, and
- service subsystem design.

Under each aspect, several different levels are addressed that correspond to the system segments defined in the high-level system overview, that is, system level, node level, node extension level, strategic emergency control centre level, backhaul supported system, device level, as applicable. Also, where necessary, the aspects are covered for different communication planes, that is, user plane, data plane, control plane and management plane.

Please note that for the backhaul supported systems only requirements per different aspects, segments, levels and planes can be defined. Implementation and configuration of these requirements is subject to their availability for the purposes of the A-ERCS pilot, provided by the A-ERCS stakeholders.

2 EXISTENT ERCS SYSTEM SPECIFICATION

In this chapter, specifications of the existent operational Emergency Response System (ERCS) are provided. First, an introduction is given outlining the ERCS environment, the SECCSU team as well as the domain-specific ERCS service organization. Next the existent ERCS system is specified following the defined A-ERCS specification methodology.

2.1 ERCS environment

The A-ERCS will be designed for and deployed in a specialized vehicle in use by the Strategic Emergency Control Centre Support Unit (SECCSU) of the VFB. Therefore, in this chapter further domain specifics are presented for better understanding of the remainder of this document.



Figure 2-1: The SECCSU vehicle where the A-ERCS system will be implemented.

The vehicle represents a mobile on-site command unit with a team of four operators responsible for on-site fire fighter intervention coordination on one side and communication with the Strategic Emergency Control Centre (SECC) on the other. In Figure 2-2 the organization and chain of command for intervention procedures involving SECCSU are presented. The intervention procedures define the ERCS system and services available to and used by the SECCSU and the on-site fire fighter units. For the presented organisation and chain of command the same preconditions apply as for the ERCS system, that is, during and after the implementation and demonstration of the A-ERCS system, the ERCS service organization must remain intact and fully operational.

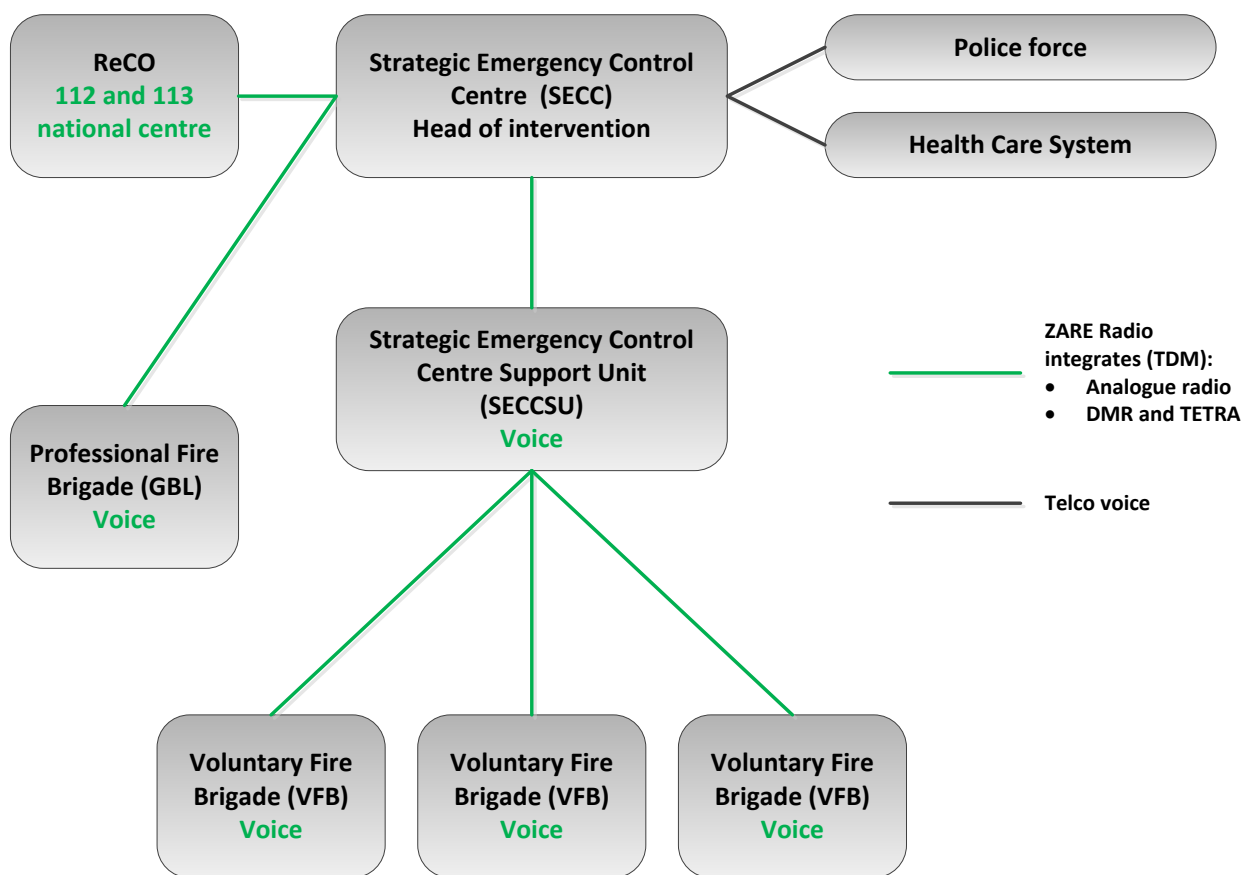


Figure 2-2: Organization and chain of command for intervention procedures involving SECCSU.

2.2 ERCS System Architecture

Today, the ERCS in use by the SECCSU is rather limited in its technologies, functionalities and

services. As depicted in Figure 2-3, the operating SECCSU team is equipped with a professional communication system ZARE currently supporting only narrowband voice services during an intervention (analogue/DMR-based professional mobile radio system for voice communications). The SECCSU team members and the on-site fire fighters use professional P2T radio terminals. Additionally, the vehicle is equipped with commercial Internet connectivity for situation surveillance purposes and in communication with the SECC (exchange of intervention reports, weather forecast updates, access to Internet), and for off-duty purposes. A local LAN/WiFi network is available inside the vehicle. For available data services, the SECCSU team members use their own personal terminal equipment, i.e., laptops. This is an additional domain-specific rationale, the principal reason is the fact that the team members are best familiar and skilled to use their own terminals (e.g., using a specially provided laptop is inefficient because the user is not always familiar with the operating system, file system organization, specific configurations, installed applications etc.).

Three operators of the SECCSU team communicate separately with three on-site fire fighter teams using ZARE to coordinate the intervention. The fourth operator, in charge of the entire operation coordination, communicates with the SECCSU team operators locally or using Internet access, and with the SECC contact, using ZARE for voice communication and Internet access for data exchange. In case one operator communicates with the on-site teams and with the SECC contact, separate ZARE terminals are used.

ZARE and Internet access systems are completely independent from one another and are not interconnected. **IPv6 is not available in any of the systems or system segments.**

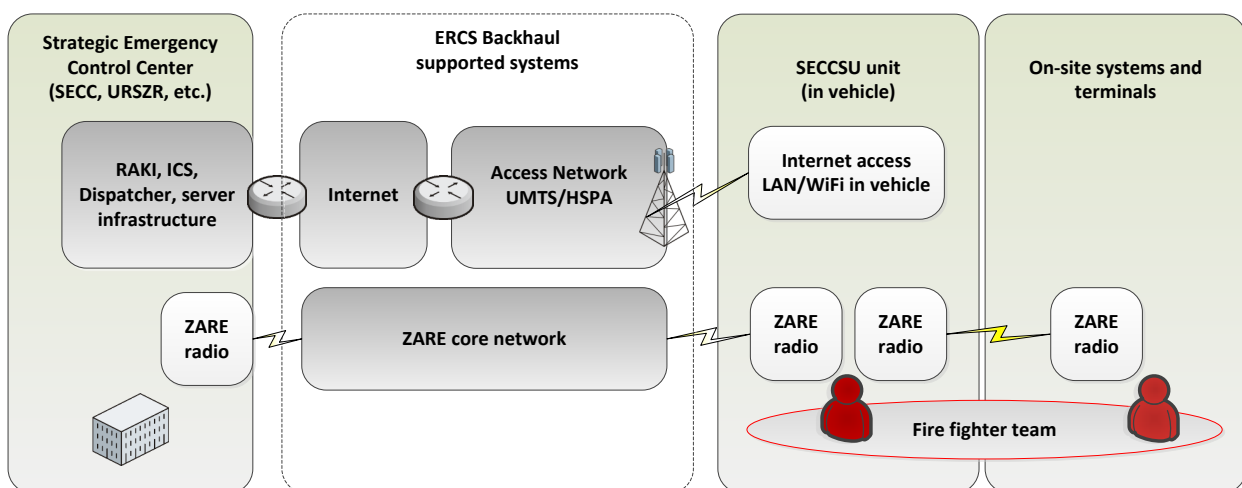


Figure 2-3: High-level overview of existent ERCS system.



Figure 2-4: The ERCS communication infrastructure available in the SECCSU vehicle.

2.3 ERCS Service Subsystems

Corresponding to the presented ERCS system architecture, two groups of services are available in the currently deployed and operational ERCS system.

TDM-based ZARE system provides voice and messaging service, available for separate communication between SECCSU and on-site team and between SECCSU and SECC. ZARE voice is the only official communication service available for the professional services in the current deployment of the ERCS. ZARE messaging is supported but not in use.

Internet access via UMTS/HSPA provides e-mail and file transfer services, available for communication between SECCSU and SECC. In addition, there are three IP-based services available in the SECC, which are also used to coordinate and manage a professional intervention but are not directly integrated with the ERCS:

- RAKI – intervention equipment registry, used by the Public Fire Fighter Service (JGS),

- ICS service – a communication and management tool for major interventions, and
- Dispatcher tool.

Summary of available services in the ERCS is provided in Table 3-58.

A-ERCS segment/capability	Elements/features/capabilities	Status
System capabilities		
A-ERCS node elements	ZARE	Existent, not part of the A-ERCS node
On-site systems	DMR radio	Existent
Backhaul supported systems	ZARE (DMR)	Existent
	UMTS/HSPA	Available
Supported services		
SECCSU operator in operation	ZARE voice	Existent
	ZARE messaging	Existent, not in use
	E-mail	Planned
	File transfer	Planned
Fire fighter team	ZARE voice	Existent
Other	RAKI (JGS equipment registry)	Existent, not integrated with the ERCS
	ICS (communications and management tool for major interventions)	Existent, not integrated with the ERCS
	Dispatcher tool	Existent, not integrated with the ERCS

Table 2-1: ERCS capabilities and services overview.

3 A-ERCS SYSTEM SPECIFICATION

In this section, architectural design and specification for the A-ERCS system and services are provided, following the specification methodology presented in Section 1.3.

3.1 A-ERCS System Architecture

A detailed A-ERCS system architecture is represented in Figure 3-1. As already explained in Section 1.2, it comprises the following segments:

- A-ERCS node, representing the core section of the solution,
- A-ERCS node extension, covering A-ERCS infrastructure and services available on site of the intervention,
- A-ERCS backhaul supported systems providing connectivity between the SECCSU and SECC as well as access to the Internet, and
- SECC infrastructure for global intervention coordination and management on a national and cross-border level.

In the following, all segments are represented and explained, followed by detailed specifications of individual segments, nodes and elements.

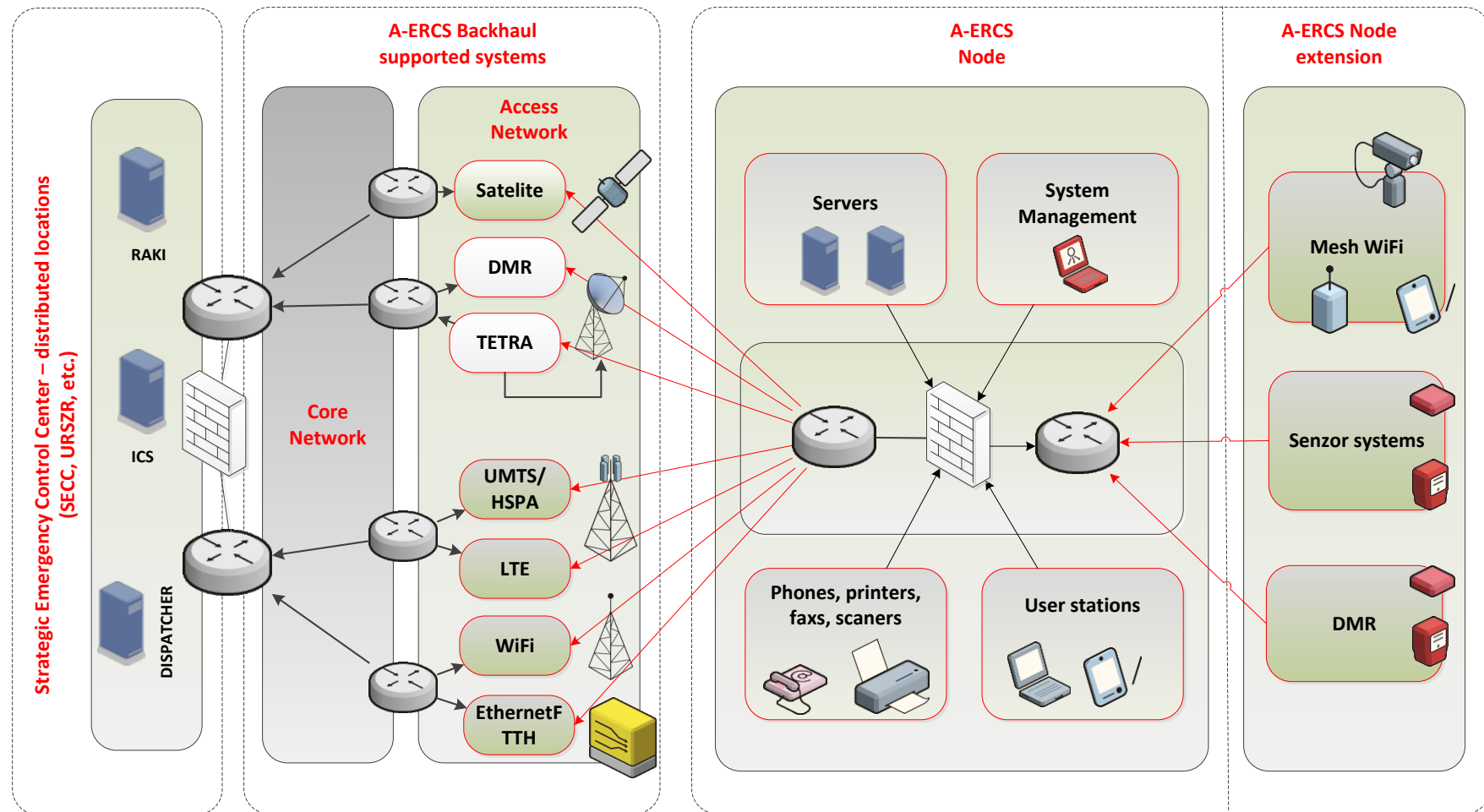


Figure 3-1: A-ERCS system architecture.

3.1.1 Node Specification

The core of the solution represents the A-ERCS node located in the SECCSU vehicle. Its role is to assist the SECCSU unit in communication with:

- the on-site nodes (also referred to as A-ERCS node extensions):
 - the fire fighter unit on site by utilizing DMR voice services, and data services (e.g., video transmission, image transmission, other data services) using local on-site WiFi mesh connectivity or available professional or commercial networks (e.g., ad-hoc microwave links, commercial WiFi infrastructure; especially in situations when the SECCSU is not located directly on site),
 - sensor system(s) deployed on site (e.g., avalanche conditions measurement system, hydro sensors etc.), and
- the SECC infrastructure, such as dispatch centres, Integrated Communication Systems (ICS), inventory database (RAKI), etc., via available professional (TETRA, satellite, DMR) or commercial (UMTS/HSPA, LTE, commercial WiFi, xDSL, FTTH, Ethernet) networks or ruggedized COTS systems (microwave links); the utilization of these networks is subject to their availability and a corresponding service prioritization as defined by the A-ERCS node.

The principal role of the A-ERCS node is to provide intelligence that is able to automatically and transparently set up, configure and sustain connectivity with and between the available networks and systems at all times during the intervention, taking into account the fact that during the intervention one or several systems might cease or fail to operate. For example, in the case of a major natural catastrophe, such as an earthquake, the A-ERCS system will try to set up connectivity between the SECCSU and the SECC via an available UMTS/HSPA network. If the UMTS network fails during and after aftershock, the A-ERCS node would instantly and seamlessly re-establish the connectivity via a satellite network or an ad-hoc WiFi/WiMAX backhaul system that was set up subsequently.

Furthermore, based on currently available connectivity, the A-ERCS node must prioritize services according to the currently available transmission capacities. For example, voice services will have priority one, followed by messaging as priority two, and video/image transfer as priority three. Actual availability of these services will be subject to available networks and the respective capacities. In case of an intervention due to a massive traffic accident, the A-

ERCS node will establish voice and messaging services between the SECCSU and SECC via the ZARE system, and video/image transfer via a commercial network UMTS/HSPA. However, in case of an earthquake, the majority of commercial systems will probably fail. In this case, the A-ERCS node would establish voice and messaging service via a TETRA system, while video/image transfer service would no longer be available due to lack of capacities unless a dedicated microwave link (e.g., ad-hoc WiFi) is set up between the SECCSU and the SECC. After an aftershock and outage of the TETRA system and the microwave link, voice services would be re-established via a satellite system while other services would no longer be available.

An important aspect of the A-ERCS node operation is its ability to respond to current circumstances and to set up and configure communication services automatically and with minimum delay. This accounts for highly reliable communications and is achieved through a set of advanced self-configuration and self-organization features. Also, the A-ERCS system itself needs to provide reliable and resilient operation, requiring further self-configuration and self-healing features.

Also incorporated in the A-ERCS node will be local applications (such as a push application to deliver fire routes and 3D building plans to the fire fighter's device, a fire fighter body temperature monitoring application, or an accountant application) and databases (for example local fire route and 3D building plans database, intervention inventory and contact lists), and a management system.

The described A-ERCS node features require a corresponding hardware infrastructure. Core components are a router and a firewall, a server as well as terminal equipment (user devices, monitors, printers and faxes etc.). Further functional details are described in the following sections.

The high-level A-ERCS node architecture is represented in **Fehler! Verweisquelle konnte nicht gefunden werden..** It comprises two separate levels, based on core and access elements. These elements can be implemented as physical or logical components of the system.

The two core elements of the A-ERCS node are a **Core Router** and a **Core Firewall**. Also, the following elements are part of the A-ERCS node:

- Router A/P,
- Server domain,
- System management domain,

297239	GEN6	D 3.8.1: A-ERCS system specification
--------	------	--------------------------------------

- SECCSU equipment (phones, printers, faxes, scanners) domain, and
- User stations domain.

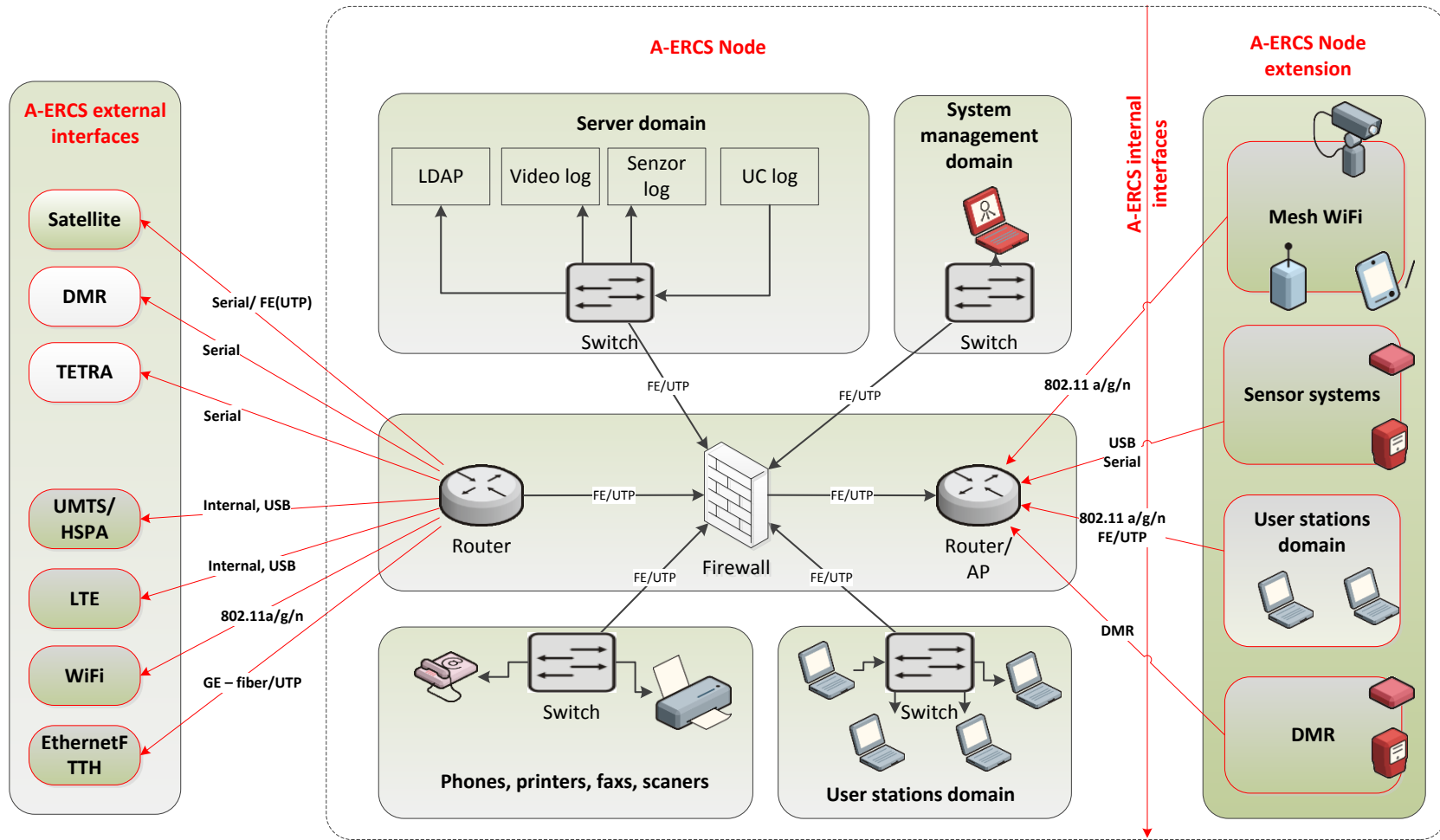


Figure 3-2: A-ERCS Node Architecture.

3.1.1.1 Core Router

The core router provides the following functionalities:

- various physical and logical interfaces for interconnection to professional and commercial communication systems (UMTS/HSPA/LTE, serial, optical and electrical Ethernet),
- mobility and tunnelling endpoint (GTP, PPP, PPPoE, GRE, PMIPv6/GRE, etc.),
- edge policing and QoS functionality (service prioritization, policing/shaping, marking, priority queuing, etc.),
- static and dynamic unicast and multicast routing.

Network Element	Interfaces	Purpose	Status
Core Router	2x Fast Ethernet (UTP)	to Firewall	Required
		to Satellite	Optional ¹
	2x Gigabit Ethernet (SFP/UTP)	to Ethernet	Optional
		to FTTH	Optional
	3x Serial	to Satellite	Optional ²
		to DMR/analogue radio (ZARE)	Required
		to TETRA	Optional
	1x Wireless 802.11 a/g/n	WiFi client	Required
	2x USB	UMTS/HSPA USB modem	Optional ³
		LTE USB modem	Optional ⁴
	Internal UMTS/HSPA modem	to UMTS/HSPA network	Required
	Internal LTE modem	to LTE network	Required

Table 3-1: A-ERCS System Architecture – Node Specification – Core Router.

¹ Required if connection to Satellite not available via serial interface

² Required if connection to satellite not available via Fast Ethernet interface

³ Required if internal UMTS/HSPA modem not available

⁴ Required if internal LTE modem not available

High-level requirements on the Core Router:

- Internet Protocols: IPv4, IPv6
- Logical interfaces based on VLAN ID
- IP over Ethernet (IPoE)
 - IPv4 over Ethernet
 - IPv6 over Ethernet
 - IPv4/IPv6 over Ethernet
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
 - DHCPv6 client/server – “Stateless”
 - DHCPv6 relay
- Unicast Routing:
 - Static
 - RIPng
 - OSPFv3
 - OSPFv3 extensions
 - Multiple OSPFv3 instances
 - Policy-based routing
 - MP-BGP
- Multicast Routing: PIM-SM, PIM-SSM
- Multicast Signalling: MLDv1, MLDv2
- Packet Filtering based on:
 - VLAN ID
 - CoS, Traffic Class, DSCP, FlowLabel
 - MAC Source/Destination Address
 - IPv6 Source/Destination Address
 - IPv6 Multicast Scope Option
 - UDP/TCP port
- QoS:
 - DiffServ model
 - DSCP Service Classes on L2-L4
 - Output/Input Policing and shaping

- Marking DSCP, Traffic Class FlowLabel, CoS, VLAN ID
 - Prioritisation and scheduling (FIFO, PQ, WRR, LLQ)
- RADIUS:
 - Client
 - Server
- DNS:
 - Client
- Mobility:
 - Protocols:
 - Mobile IPv6
 - DSMIPv6
 - PMIPv6/GRE
 - NEMO
 - Roles:
 - Home Agent (HA)
 - Mobile IPv6, DSMIPv6
 - NEMO client
 - Mobility Access Gateway (MAG)
 - PDP context:
 - IPv4
 - IPv6
 - IPv4 and IPv6
 - EPS bearer:
 - IPv4
 - IPv6
 - IPv4 and IPv6
- Tunnels:
 - GRE
 - IPv6overIPv4
 - 6rd
 - PPP over serial
 - LCP
 - IPCP
 - PAP/CHAP

- PPPv6 over serial
 - LCP
 - IPCPv6
 - PAP/CHAP
 - DHCPv6 over serial
- PPP over Ethernet (PPPoE)
 - IPv4 over PPPoE
 - IPv6 over PPPoE
 - IPv4/IPv6 over PPPoE
- Address & Protocol Translation:
 - IPv4 NAT/PAT
 - NAT64 (DNS64)
- VPN:
 - IPsec Site-to-Site
- Wireless
 - 802.11 a/g/n
 - client mode
 - WPA/WPA2
 - 802.1x
 - RADIUS support
- OAM:
 - Different levels of management access
 - Logging: SNMP, SYSLOG
 - Device management:
 - CLI: local, TELNET, SSHv2
 - HTTP/HTTPS
 - SNMPv2/v3
 - Integration with 3rd party management systems

3.1.1.2 Core Firewall

The Core Firewall provides the following functionalities:

- central security endpoint for user and service flow control, stateless and statefull filtering, QoS enforcement,

- central network service endpoint (AAA, 802.1X, DHCP, unicast and multicast routing),
- entry point for user and service domain interconnect based on Ethernet interfaces.
- The access level of the A-ERCS node relies on the core firewall that provides the central interconnect point for user, service and management domains:
- server domain hosts network (DNS, LDAP, radius) and application servers (video log, sensor data log, etc.),
- user domain hosts fixed and wireless user terminals,
- system management domain.

Network Element	Interfaces	Purpose	Status
Firewall	5x Fast Ethernet (UTP)	to Core Router	Required
		to Router/AP	Required
		to Server domain	Required
		to System management domain	Required
		to Others domain	Required
		to User stations domain	Required

Table 3-2: A-ERCS System Architecture – Node Specification – Firewall.

High-level requirements on the Firewall:

- Internet Protocols: IPv4, IPv6
- Logical interfaces based on VLAN ID
- IP over Ethernet (IPoE)
 - IPv4 over Ethernet
 - IPv6 over Ethernet
 - IPv4/IPv6 over Ethernet
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC

- DHCPv6 client/server – “stateless”
- DHCPv6 relay
- Unicast Routing:
 - Static
 - RIPng
 - OSPFv3
 - OSPFv3 extensions
 - Multiple OSPFv3 instances
 - Policy-based routing
- Multicast Routing: PIM-SM, PIM-SSM
- Multicast Signalling: MLDv1, MLDv2
- Packet Filtering based on:
 - VLAN ID
 - CoS, Traffic Class, DSCP, FlowLabel
 - MAC Source/Destination Address
 - IPv6 Source/Destination Address
 - IPv6 Multicast Scope Option
 - UDP/TCP port
- QoS:
 - DiffServ model
 - DSCP Service Classes on L2-L4
 - Output/Input Policing and shaping
 - Marking DSCP, Traffic Class FlowLabel, CoS, VLAN ID
 - Prioritisation and scheduling (FIFO, PQ, WRR, LLQ)
- RADIUS:
 - Client
 - Server
 - Proxy
- Address Translation
 - IPv4 NAT/PAT
- Security:
 - Stateful packet filtering (L3-L7)
 - Application layer filtering (L5-L7)
 - IDS/IPS

- ALG:
 - FTP
 - SIP
- VPN:
 - IPsec Site-to-Site
- OAM:
 - Different levels of management access
 - Logging: SNMP, SYSLOG
 - Device management:
 - CLI: local, TELNET, SSHv2
 - HTTP/HTTPS
 - SNMPv2/v3
 - Integration with 3rd party management systems

3.1.1.3 Router/AP

Network Element	Interfaces	Purpose	Status
Router/AP	2x Fast Ethernet (UTP)	to Firewall	Required
		to User stations domain	Required
	2x Wireless 802.11 a/g/n	WiFi Access Point	Required
		WiFi Mesh client	Required
	2x Serial	to Sensor systems	Optional
		do DMR/analogue radio (ZARE)	Required
	1x USB	to Sensor systems	Optional

Table 3-3: A-ERCS System Architecture – Node Specification – Router/AP.

High-level requirements on the Router/AP:

- Internet Protocols: IPv4, IPv6
- Logical interfaces based on VLAN ID
- IP over Ethernet (IPoE)
 - IPv4 over Ethernet

- IPv6 over Ethernet
- IPv4/IPv6 over Ethernet
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
 - DHCPv6 client/server – “Stateless”
 - DHCPv6 relay
- Unicast Routing:
 - Static
 - RIPng
 - OSPFv3
 - OSPFv3 extensions
 - Multiple OSPFv3 instances
 - Policy-based routing
- Multicast Routing: PIM-SM, PIM-SSM
- Multicast Signalling: MLDv1, MLDv2
- Packet Filtering based on:
 - VLAN ID
 - CoS, Traffic Class, DSCP, FlowLabel
 - MAC Source/Destination Address
 - IPv6 Source/Destination Address
 - IPv6 Multicast Scope Option
 - UDP/TCP port
- QoS:
 - DiffServ model
 - DSCP Service Classes on L2-L4
 - Output/Input Policing and shaping
 - Marking DSCP, Traffic Class, FlowLabel, CoS, VLAN ID
 - Prioritisation and scheduling (FIFO, PQ, WRR, LLQ)
- RADIUS:
 - Client
 - Proxy
- Mobility:

- Protocols:
 - Mobile IPv6
 - DSMIPv6
 - NEMO
- Roles:
 - Mobile IPv6 client
 - DSMIPv6 client
 - NEMO client
- Tunnels:
 - PPP over serial
 - LCP
 - IPCP
 - PAP/CHAP
 - PPPv6 over serial
 - LCP
 - IPCPv6
 - PAP/CHAP
 - DHCPv6 over serial
- Wireless
 - 802.11 a/g/n
 - access point mode
 - client mode
 - mesh client mode
 - WPA/WPA2
 - 802.1x
 - RADIUS support (client)
- OAM:
 - Different levels of management access
 - Logging: SNMP, SYSLOG
 - Device management:
 - CLI: local, TELNET, SSHv2
 - HTTP/HTTPS
 - SNMPv2/v3
 - Integration with 3rd party management systems

3.1.1.4 Server domain

Network Element	Interfaces	Purpose	Status
RAKI Server ⁵	IPv4/IPv6 over Ethernet	Inventory database	Required
ICS Server ⁶	IPv4/IPv6 over Ethernet	Integrated Communication System (ICS)	Optional
DISPATCH Server ⁷	IPv4/IPv6 over Ethernet	Dispatch Service	Optional
L2/L3 switch	N x Fast Ethernet	Network aggregation	Required

Table 3-4: A-ERCS System Architecture – Node Specification – Server domain.

High-level requirements on the L2/L3 switch:

- Internet Protocols: IPv4, IPv6
- Logical interfaces based on VLAN ID
- IP over Ethernet (IPoE)
 - IPv4 over Ethernet
 - IPv6 over Ethernet
 - IPv4/IPv6 over Ethernet
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
- Multicast Signalling: MLDv1, MLDv2
- MLD snooping/proxy
- Packet Filtering based on:
 - VLAN ID
 - CoS, Traffic Class, DSCP, FlowLabel
 - IPv6 Source/Destination Address

⁵ Local copy of the server

⁶ Local copy of the server

⁷ Local copy of the server

- IPv6 Multicast Scope Option
- UDP/TCP port
- QoS:
 - DiffServ model
 - DSCP Service Classes on L2-L4
 - Output/Input Policing and shaping
 - Marking DSCP, Traffic Class FlowLabel, CoS, VLAN ID
 - Prioritisation and scheduling (FIFO, PQ, WRR, LLQ)
- RADIUS
 - Client
- Security:
 - 802.1x
 - Authenticator
- OAM:
 - Different levels of management access
 - Logging: SNMP, SYSLOG
 - Device management:
 - CLI: local, TELNET, SSHv2
 - HTTP/HTTPS
 - SNMPv2/v3
 - Integration with 3rd party management systems

3.1.1.5 System management domain

Network Element	Interfaces	Purpose	Status
RADIUS Server ⁸	IPv4/IPv6 over Ethernet	AAA services	Required
DHCPv4 Server	IPv4 over Ethernet	Dynamic IPv4 addresses	Required
DHCPv6 Server	IPv6 over Ethernet	Dynamic IPv6 addresses – “Stateful”	Optional

⁸ May be provisioned on a virtual server

Network Element	Interfaces	Purpose	Status
	IPv6 over Ethernet	Dynamic IPv6 addresses – “Stateless”	Required
DNS Server ⁹	IPv4 and IPv6 over Ethernet	DNS server for IPv4 (A)	Required
	IPv6 over Ethernet	DNS server for IPv6 (AAAA)	Required
DNS64 Server ¹⁰	IPv6 over Ethernet	DNS64 server for IPv-only devices	Optional
DC ¹¹	IPv4/IPv6 over Ethernet	Domain controller	Optional
Logging server ¹²	IPv4/IPv6 over Ethernet	Video logging	Required
		Sensor logging	Required
		UC logging	Required
		SYSLOG	Optional
SYSLOG server ¹³	IPv4/IPv6 over Ethernet	SYSLOG logging	Required
SNMP server ¹⁴	IPv4/IPv6 over Ethernet	SNMP management	Required
L2/L3 Switch	24x FastEthernet	Network Aggregation	Required

Table 3-5: A-ERCS System Architecture – Node Specification – System management domain.

High-level requirements on the L2/L3 switch:

- Internet Protocols: IPv4, IPv6
- Logical interfaces based on VLAN ID
- IP over Ethernet (IPoE)
 - IPv4 over Ethernet
 - IPv6 over Ethernet

⁹ May be provisioned on a virtual server

¹⁰ May be provisioned on a virtual server

¹¹ May be provisioned on a virtual server

¹² May be provisioned on a virtual server

¹³ May be provisioned on a virtual server

¹⁴ May be provisioned on a virtual server

- IPv4/IPv6 over Ethernet
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
- Multicast Signalling: MLDv1, MLDv2
- MLD snooping/proxy
- Packet Filtering based on:
 - VLAN ID
 - CoS, Traffic Class, DSCP, FlowLabel
 - IPv6 Source/Destination Address
 - IPv6 Multicast Scope Option
 - UDP/TCP port
- QoS:
 - DiffServ model
 - DSCP Service Classes on L2-L4
 - Output/Input Policing and shaping
 - Marking DSCP, Traffic Class FlowLabel, CoS, VLAN ID
 - Prioritisation and scheduling (FIFO, PQ, WRR, LLQ)
- RADIUS
 - Client
- Security:
 - 802.1x
 - Authenticator
- OAM:
 - Different levels of management access
 - Logging: SNMP, SYSLOG
 - Device management:
 - CLI: local, TELNET, SSHv2
 - HTTP/HTTPS
 - SNMPv2/v3
 - Integration with 3rd party management systems

3.1.1.6 SECCSU equipment (phones, printers, faxes, scanners) domain

Network Element	Interfaces	Purpose	Status
IP Phone	IPv4/IPv6 over Ethernet	VoIP	Optional
Printer ¹⁵	IPv4/IPv6 over Ethernet	Document printing	Required
Fax ¹⁶	IPv4/IPv6 over Ethernet	Document faxing	Optional
Scanner ¹⁷	IPv4/IPv6 over Ethernet	Document scanning	Optional
L2/L3 Switch	24x FastEthernet	Network Aggregation	Required

Table 3-6: A-ERCS System Architecture – Node Specification – Photos, printers, faxes, scanners domain.

High-level requirements on the L2/L3 switch:

- Internet Protocols: IPv4, IPv6
- Logical interfaces based on VLAN ID
- IP over Ethernet (IPoE)
 - IPv4 over Ethernet
 - IPv6 over Ethernet
 - IPv4/IPv6 over Ethernet
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
- Multicast Signalling: MLDv1, MLDv2
- MLD snooping/proxy
- Packet Filtering based on:
 - VLAN ID
 - CoS, Traffic Class, DSCP, FlowLabel
 - IPv6 Source/Destination Address

¹⁵ Printer, Fax and Scanner may exist as an all-in-one box

¹⁶ Printer, Fax and Scanner may exist as an all-in-one box

¹⁷ Printer, Fax and Scanner may exist as an all-in-one box

- IPv6 Multicast Scope Option
- UDP/TCP port
- QoS:
 - DiffServ model
 - DSCP Service Classes on L2-L4
 - Output/Input Policing and shaping
 - Marking DSCP, Traffic Class FlowLabel, CoS, VLAN ID
 - Prioritisation and scheduling (FIFO, PQ, WRR, LLQ)
- RADIUS
 - Client
- Security:
 - 802.1x
 - Authenticator
- OAM:
 - Different levels of management access
 - Logging: SNMP, SYSLOG
 - Device management:
 - CLI: local, TELNET, SSHv2
 - HTTP/HTTPS
 - SNMPv2/v3
 - Integration with 3rd party management systems

3.1.1.7 User stations domain

Network Element	Interfaces	Purpose	Status
Workstation	IPv4/IPv6 over Ethernet	User workstation	Optional
Laptop	IPv4/IPv6 over Ethernet	User laptop	Required
L2/L3 Switch	24x FastEthernet	Network Aggregation	Required

Table 3-7: A-ERCS System Architecture – Node Specification – User stations domain.

High-level requirements on the L2/L3 switch:

- Internet Protocols: IPv4, IPv6

- Logical interfaces based on VLAN ID
- IP over Ethernet (IPoE)
 - IPv4 over Ethernet
 - IPv6 over Ethernet
 - IPv4/IPv6 over Ethernet
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
- Multicast Signalling: MLDv1, MLDv2
- MLD snooping/proxy
- Packet Filtering based on:
 - VLAN ID
 - CoS, Traffic Class, DSCP, FlowLabel
 - IPv6 Source/Destination Address
 - IPv6 Multicast Scope Option
 - UDP/TCP port
- QoS:
 - DiffServ model
 - DSCP Service Classes on L2-L4
 - Output/Input Policing and shaping
 - Marking DSCP, Traffic Class FlowLabel, CoS, VLAN ID
 - Prioritisation and scheduling (FIFO, PQ, WRR, LLQ)
- RADIUS
 - Client
- Security:
 - 802.1x
 - Authenticator
- OAM:
 - Different levels of management access
 - Logging: SNMP, SYSLOG
 - Device management:
 - CLI: local, TELNET, SSHv2
 - HTTP/HTTPS

- SNMPv2/v3
 - Integration with 3rd party management systems

3.1.2 Node Extension Specification

A-ERCS Node Extension is a segment of the A-ERCS infrastructure, deployed on-site where the fire fighter units are in operation (either VFB or Public Fire Fighter Service JGS). In the A-ERCS context it is positioned as an extension to the infrastructure deployed in the SECCSU vehicle. Its role is to provide services utilizing DMR voice services, and data services (e.g., video transmission, image transmission, other data services) using local on-site WiFi mesh connectivity or available professional or commercial networks (e.g., ad-hoc microwave links, commercial WiFi infrastructure; especially in situations when the SECCSU is not located directly on site).

In general, the implementation and operational features of the A-ERCS node extension for communication services must follow the requirements and features of the A-ERCS node. Two systems/technologies are planned, ZARE for voice communication and local Mesh WiFi for data communication.

Part of the A-ERCS node extension is also sensor systems. To support local SECCSU applications as well as to allow application in other parts and units of the emergency response system as a whole, implementation of sensor infrastructure is planned. Available data and content of the applications are subject to deployed sensors and probes, and user interfaces available (e.g., web portal, native application, OTT application, push messaging service, etc.). For A-ERCS pilot purposes, a centralized web portal has already been experimentally designed and implemented as explained in Section 3.7.

Additional requirements and limitation in this segment apply to terminal equipment that the on-site fire fighter units can use. In several cases, the equipment must be ruggedized, specifically designed and assembled for the harsh operational conditions. According to the specified use case scenarios and the planned local SECCSU applications, two groups of terminal equipment are planned:

- professional ruggedized terminal equipment for use on the intervention site, resistant to humidity/moist, high temperatures, unsanitary conditions, impacts and vibrations etc.; ZARE P2T radio and ruggedized tablets are such examples;
- commercial of the shelf equipment for use in the vehicles, camps, command centres etc., such as laptops, tablets, smartphones etc.

As a result, the following domains are identified for the Node Extension segment:

- Mesh WiFi domain,
- Sensor systems domain, covering implementation and deployment of sensors and providing sensor data service via Mesh WiFi domain,
- User stations domain, and
- DMR domain.

The identified domains are specified in the following.

3.1.2.1 Mesh WiFi domain

Network Element	Interfaces	Purpose	Status
Mesh WiFi AP	Wireless 802.11 a/g/n	WiFi Mesh client	Required
	Wireless 802.11 a/g/n	WiFi access point	Required
IP Video camera	IPv4/IPv6 over Wireless 802.11 a/g/n	Video logging, streaming	Optional
PDA	IPv4/IPv6 over Wireless 802.11 a/g/n	Firefighter user equipment	Optional
Smartphone	IPv4/IPv6 over Wireless 802.11 a/g/n	Firefighter user equipment	Optional
Tablet computer	IPv4/IPv6 over Wireless 802.11 a/g/n	Firefighter user equipment	Optional

Table 3-8: A-ERCS System Architecture – Node Extension Specification – Mesh WiFi domain.

3.1.2.2 Sensor systems domain

Network Element	Interfaces	Purpose	Status
Sensor	USB	Sensor	Optional
Sensor	Serial	Sensor	Optional

Table 3-9: A-ERCS System Architecture – Node Extension Specification – Sensor systems domain.

3.1.2.3 User stations domain

Network Element	Interfaces	Purpose	Status
Laptop	IPv4/IPv6 over Wireless 802.11 a/g/n	User laptop	Required
IP Video camera	IPv4/IPv6 over Wireless 802.11 a/g/n	Video logging, streaming	Optional
PDA	IPv4/IPv6 over Wireless 802.11 a/g/n	Firefighter user equipment	Optional
Smartphone	IPv4/IPv6 over Wireless 802.11 a/g/n	Firefighter user equipment	Optional
Tablet computer	IPv4/IPv6 over Wireless 802.11 a/g/n	Firefighter user equipment	Optional

Table 3-10: A-ERCS System Architecture – Node Extension Specification – User stations domain.

3.1.2.4 DMR domain

Network Element	Interfaces	Purpose	Status
DMR terminal	Wireless (DMR)	User handheld DMR station	Required

Table 3-11: A-ERCS System Architecture – Node Extension Specification – DMR domain.

3.1.3 Strategic Emergency Control Center infrastructure specification

In terms of communications infrastructure, the SECC represents the backend part of the A-ERCS infrastructure that is in direct communication with the A-ERCS node via the backhaul supported systems. Its role is twofold:

- to assure voice communication with the SECCSU team member in charge of this operational connectivity during an intervention according to the specified intervention procedures, and
- to provide (selected, adjusted or limited) access to and connectivity with add-on intervention services, that is, dispatcher, RAKI inventory and ICS tool.

To provide connectivity towards the SECCSU via the backhaul supported systems, a SECC router, SECC firewall and SECC L2/L3 switch are required.

In the following, detailed specifications of the presented segments, elements and nodes are provided.

Network Element	Interfaces	Purpose	Status
RAKI Server	IPv4/IPv6 over Ethernet	Inventory database	Required
ICS Server	IPv4/IPv6 over Ethernet	Integrated Communication System (ICS)	Optional
DISPATCH Server	IPv4/IPv6 over Ethernet	Dispatch Service	Optional
Router	Gigabit Ethernet	to Backhaul supported systems	Optional
	Fast Ethernet	to Backhaul supported systems	Required
Firewall	Fast Ethernet	to Routers	Required
L2/L3 switch	Nx Fast Ethernet	Network aggregation	Required

Table 3-12: A-ERCS System Architecture – Strategic Emergency Control Center Specification.

High-level requirements on the **SECC Router**:

- Internet Protocols: IPv4, IPv6
- Logical interfaces based on VLAN ID
- IP over Ethernet (IPoE)
 - IPv4 over Ethernet
 - IPv6 over Ethernet
 - IPv4/IPv6 over Ethernet
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
 - DHCPv6 client/server – “Stateless”
 - DHCPv6 relay
- Unicast Routing:
 - Static

- RIPng
- OSPFv3
 - OSPFv3 extensions
 - Multiple OSPFv3 instances
 - Policy-based routing
- MP-BGP
- Multicast Routing: PIM-SM, PIM-SSM
- Multicast Signalling: MLDv1, MLDv2
- Packet Filtering based on:
 - VLAN ID
 - CoS, Traffic Class, DSCP, FlowLabel
 - MAC Source/Destination Address
 - IPv6 Source/Destination Address
 - IPv6 Multicast Scope Option
 - UDP/TCP port
- QoS:
 - DiffServ model
 - DSCP Service Classes on L2-L4
 - Output/Input Policing and shaping
 - Marking DSCP, Traffic Class FlowLabel, CoS, VLAN ID
 - Prioritisation and scheduling (FIFO, PQ, WRR, LLQ)
- Mobility:
 - Protocols:
 - Mobile IPv6
 - DSMIPv6
 - PMIPv6/GRE
 - NEMO
 - Roles:
 - Home Agent (HA)
 - Local Mobility Anchor (LMA)
- Tunnels:
 - GRE
 - 6rd
 - PPP over Ethernet (PPPoE)

- IPv4 over PPPoE
 - IPv6 over PPPoE
 - IPv4/IPv6 over PPPoE
- Address Translation
 - IPv4 NAT/PAT
- VPN:
 - IPsec Site-to-Site
- OAM:
 - Different levels of management access
 - Logging: SNMP, SYSLOG
 - Device management:
 - CLI: local, TELNET, SSHv2
 - HTTP/HTTPS
 - SNMPv2/v3
 - Integration with 3rd party management systems

High-level requirements on the **SECC Firewall**:

- Internet Protocols: IPv4, IPv6
- Logical interfaces based on VLAN ID
- IP over Ethernet (IPoE)
 - IPv4 over Ethernet
 - IPv6 over Ethernet
 - IPv4/IPv6 over Ethernet
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
 - DHCPv6 client/server – “stateless”
 - DHCPv6 relay
- Unicast Routing:
 - Static
 - RIPng
 - OSPFv3

- OSPFv3 extensions
 - Multiple OSPFv3 instances
 - Policy-based routing
- Multicast Routing: PIM-SM, PIM-SSM
- Multicast Signalling: MLDv1, MLDv2
- Packet Filtering based on:
 - VLAN ID
 - CoS, Traffic Class, DSCP, FlowLabel
 - MAC Source/Destination Address
 - IPv6 Source/Destination Address
 - IPv6 Multicast Scope Option
 - UDP/TCP port
- QoS:
 - DiffServ model
 - DSCP Service Classes on L2-L4
 - Output/Input Policing and shaping
 - Marking DSCP, Traffic Class FlowLabel, CoS, VLAN ID
 - Prioritisation and scheduling (FIFO, PQ, WRR, LLQ)
- Address Translation
 - IPv4 NAT/PAT
- Security:
 - Stateful packet filtering (L3-L7)
 - Application layer filtering (L5-L7)
 - IDS/IPS
 - ALG:
 - FTP
 - SIP
- VPN:
 - IPsec Site-to-Site
- OAM:
 - Different levels of management access
 - Logging: SNMP, SYSLOG
 - Device management:
 - CLI: local, TELNET, SSHv2

- HTTP/HTTPS
- SNMPv2/v3
- Integration with 3rd party management systems

High-level requirements on the **L2/L3 switch**:

- Internet Protocols: IPv4, IPv6
- Logical interfaces based on VLAN ID
- IP over Ethernet (IPoE)
 - IPv4 over Ethernet
 - IPv6 over Ethernet
 - IPv4/IPv6 over Ethernet
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
 - DHCPv6 relay
- Multicast Signalling: MLDv1, MLDv2
- MLD snooping/proxy
- Packet Filtering based on:
 - VLAN ID
 - CoS, Traffic Class, DSCP, FlowLabel
 - IPv6 Source/Destination Address
 - IPv6 Multicast Scope Option
 - UDP/TCP port
- QoS:
 - DiffServ model
 - DSCP Service Classes on L2-L4
 - Output/Input Policing and shaping
 - Marking DSCP, Traffic Class FlowLabel, CoS, VLAN ID
 - Prioritisation and scheduling (FIFO, PQ, WRR, LLQ)
- RADIUS
 - Client
- Security:

- 802.1x
 - Authenticator
- OAM:
 - Different levels of management access
 - Logging: SNMP, SYSLOG
 - Device management:
 - CLI: local, TELNET, SSHv2
 - HTTP/HTTPS
 - SNMPv2/v3
 - Integration with 3rd party management systems

3.1.4 Backhaul Supported System

This segment represents a heterogeneous infrastructure comprising existent and newly deployed professional, commercial and alternative networks able to provide data connectivity based on IPv6. Its role is to provide transparent data transport infrastructure used by the A-ERCS node for connectivity between the SECCSU and the SECC as well as for access to Internet. The A-ERCS node will be in charge of prioritization and establishment of connectivity via available systems based on the defined use case scenarios, as explained earlier.

On the side of professional systems, today, ZARE system is in use on a national level for civil protection and rescue services in Slovenia [4]. Built with Professional Mobile Radio (PMR) technologies it assures high reliability and coverage. However, current network capabilities are limited to up to 9.6 Kbit/s with no direct support for IPv6 data transfer. Currently, only voice communications and low bitrate file transfer are supported. Bearing in mind that the system is narrowband, it does not correspond to the requirements of an advanced modern ERCS system. Therefore, within the A-ERCS system, additional professional backhaul systems are planned for use, that is satellite systems. Further details are available in [1].

Regarding commercial backhaul systems, these are not used for civil protection or fire fighter purposes for the time being. It is the plan for the A-ERCS system to bring commercial networks into the overall A-ERCS infrastructure, more specifically UMTS/HSPA and LTE networks. Currently, Mobitel, Si.mobil and Tušmobil are the three major Slovenian mobile operators with their own network infrastructure. All operators support UMTS and HSPA+ radio network technologies, providing bandwidth capabilities up to 21 Mbit/s. Mobitel and Tušmobil networks also supports IPv6 PDP context setup. Further details are available in [1].

The third backhaul option for the A-ERCS system, also not in use for the time being for the purposes of fire fighting or civil protection in general, are alternative ad-hoc and other ruggedized COTS systems. Backhaul WiMAX and mesh WiFi systems provides an alternative to professional and commercial communication solutions, specifically in unusual or even critical conditions. An important advantage of such systems is the ability for an ad-hoc setup as well as a variety of advanced features for instant network setup, configuration and operation (such as plug-and-play capabilities, self-organizing and mesh capabilities). Further details are available in [1].

Network Segment	Interfaces	Purpose	Status
Commercial mobile network	UMTS/HSPA	to SECCSU Core router	Required
	LTE	to SECCSU Core router	Optional
Professional network	TETRA	to SECCSU Core router	Optional
	DMR/analogue radio (ZARE)	to SECCSU Core router	Required
	Satellite	to SECCSU Core router	Optional
Alternative network	FTTH	to SECCSU Core router	Optional
	Ethernet	to SECCSU Core router	Optional
	WiFi	to SECCSU Core router	Required
	xDSL	to SECCSU Core router	Required

Table 3-13: A-ERCS System Architecture – Backhaul supported system.

High-level requirements of the **UMTS/HSPA network segment**:

- Internet Protocols: IPv4, IPv6
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC (RA mode)
 - DHCPv6 server
 - DHCPv6-PD
 - DNSv6 server
- No Packet Filtering
- QoS:

- DiffServ model
- 4 Service Classes
- SLA Assurance
- Mobility:
 - Roles:
 - GGSN, SGSN
 - PDP context:
 - IPv4
 - IPv6
 - IPv4 and IPv6
- No IPv4 NAT/PAT
- APN:
 - Public APN
 - Private APN
 - Extended User Authentication (RADIUS support)
 - QoS support

High-level requirements of the **LTE network segment**:

- Internet Protocols: IPv4, IPv6
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC (RA mode)
 - DHCPv6 server
 - DHCPv6-PD
 - DNSv6 server
- No Packet Filtering
- QoS:
 - DiffServ model
 - 4 Service Classes
 - SLA Assurance
- Mobility:
 - Roles:
 - P-GW, S-GW, MME

- EPS bearer:
 - IPv4
 - IPv6
 - IPv4 and IPv6
- No IPv4 NAT/PAT
- APN:
 - Public APN
 - Private APN
 - Extended User Authentication (RADIUS support)
 - QoS support

High-level requirements of the **WiFi network segment**:

- Internet Protocols: IPv4, IPv6
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
 - DHCPv6 server
 - DHCPv6-PD
 - DNSv6 server
- IP over Ethernet (IPoE)
 - IPv4 over Ethernet
 - IPv6 over Ethernet
 - IPv4/IPv6 over Ethernet
- Wireless
 - 802.11 a/g/n
 - access point mode
 - WPA/WPA2
 - 802.1x
 - RADIUS support (client)
- No Packet Filtering
- NO IPv4 NAT/PAT

High-level requirements of the **Ethernet/FTTH network segment**:

- Internet Protocols: IPv4, IPv6
- IP over Ethernet (IPoE)
 - BNG functionality
 - IPv4 over Ethernet
 - IPv6 over Ethernet
 - IPv4/IPv6 over Ethernet
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
 - DHCPv6 server
 - DHCPv6-PD
 - DNSv6 server
- No Packet Filtering
- No IPv4 NAT/PAT

High-level requirements of the **xDSL network segment**:

- Internet Protocols: IPv4, IPv6
- PPP over Ethernet (PPPoE)
 - BRAS functionality
 - IPv4 over PPPoE
 - IPv6 over PPPoE
 - IPv4/IPv6 over PPPoE
- IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
 - DHCPv6 server
 - DHCPv6-PD
 - DNSv6 server
- No Packet Filtering
- No IPv4 NAT/PAT

High-level requirements of the **TETRA segment**:

- Serial interface
 - PPP over serial
 - LCP
 - IPCP
 - PAP/CHAP
 - PPPv6 over serial
 - LCP
 - IPCPv6
 - PAP/CHAP
 - DHCPv6 over serial
- No Packet Filtering
- QoS:
 - 4 Service Classes

High-level requirements of the **DMR segment**:

- Serial interface
 - PPP over serial
 - LCP
 - IPCP
 - PAP/CHAP
 - PPPv6 over serial
 - LCP
 - IPCPv6
 - PAP/CHAP
 - DHCPv6 over serial
- No Packet Filtering
- QoS:
 - 4 Service Classes

High-level requirements of the **Satellite segment**:

- Serial interface
 - PPP over serial

- LCP
 - IPCP
 - PAP/CHAP
- PPPv6 over serial
 - LCP
 - IPCPv6
 - PAP/CHAP
 - DHCPv6 over serial
- Fast Ethernet interface
 - Internet Protocols: IPv4, IPv6
 - IP over Ethernet (IPoE)
 - IPv4 over Ethernet
 - IPv6 over Ethernet
 - IPv4/IPv6 over Ethernet
 - IPv6 Addressing:
 - Link-local addresses
 - Global addresses
 - SLAAC
 - DHCPv6 server
 - DHCPv6-PD
 - DNSv6 server
- No Packet Filtering
- No IPv4 NAT/PAT

3.2 A-ERCS System Addressing Scheme

A-ERCS System Addressing Scheme will be covered in the upcoming stages of the A-ERCS system specification and planning. Addressing scheme will be specified for Node Level, Node Extension level, and Strategic Emergency Control Center Level.

3.2.1 A-ERCS Backhaul Supported System Addressing Scheme requirements

A-ERCS Backhaul Supported System Addressing Scheme requirements will be covered in the upcoming stages of the A-ERCS system specification and planning. Addressing scheme will be

specified for Node Level, Device Level, and Strategic Emergency Control Center Level.

3.3 A-ERCS System QoS and Policy Enforcement Design

In this chapter, A-ERCS system QoS and Policy Enforcement design is analysed and described in detail. QoS in A-ERCS system will rely on Differentiated Services (DiffServ) model [23] that provides end-to-end control and data plane QoS assurance. It is required on all segments of the A-ERCS system.

In the following, the detailed features are described, and in further chapters the requirements on each of the A-ERCS segments are specified.

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based QoS requirements			
A-ERCS node	Differentiated Services model		Required
A-ERCS node extension	Differentiated Services model		Required
Strategic Emergency Control Center	Differentiated Services model		Required

Table 3-14: IPv6-based QoS requirements.

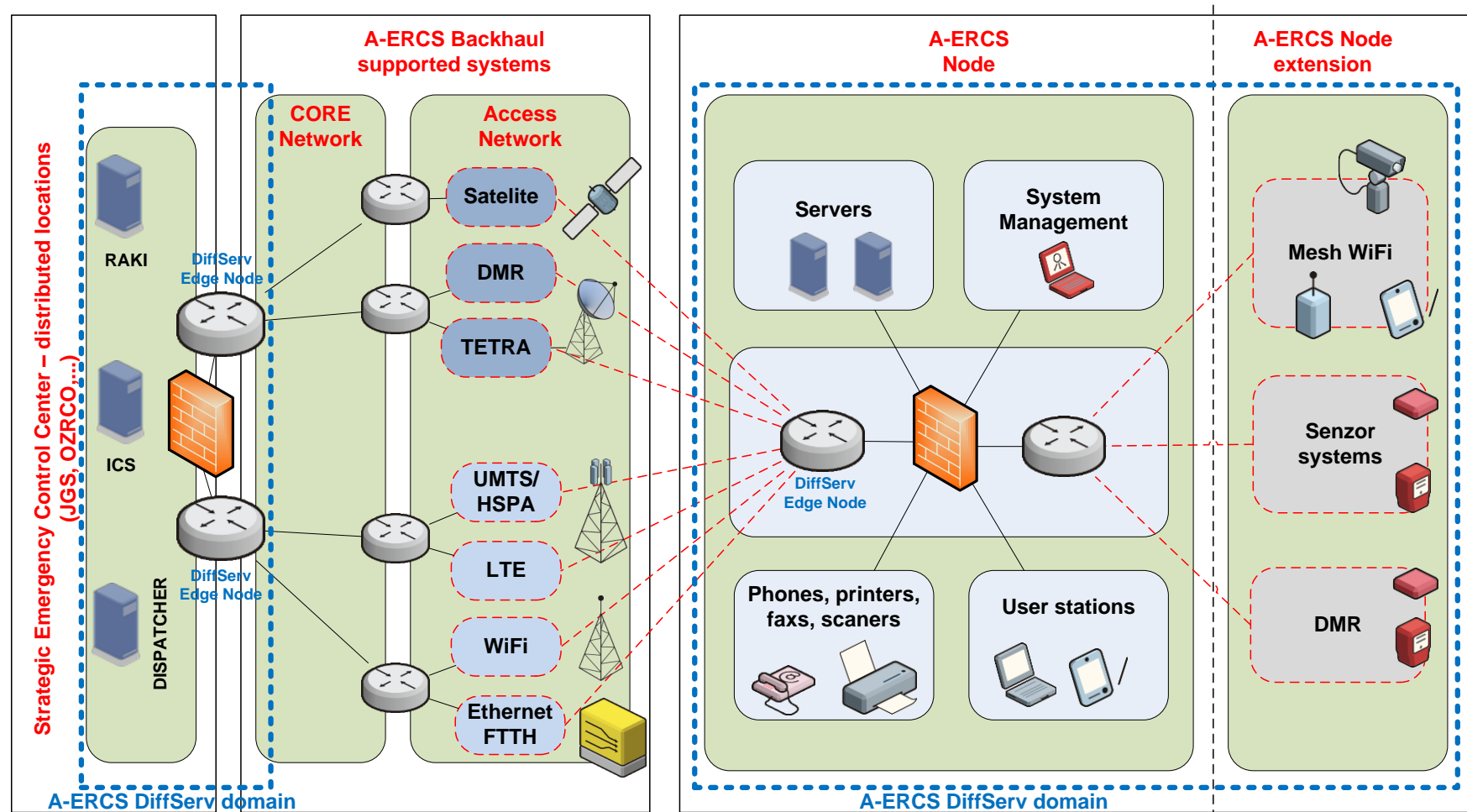


Figure 3-3: A-ERCS system DiffServ domain.

3.3.1 Differentiated Services model

Differentiated Services (DiffServ) model defines DiffServ domain that enables an end-to-end QoS assurance mechanism based on QoS information present in Traffic Class or Flow Label field in IPv6 packets.

From the DiffServ model point of view, the Traffic Class field represents DS field consisting of DS codepoint (DSCP) with length of 6 bits, and 2 unused bits reserved for explicit congestion notification. The DSCP field therefore enables 64 service classes, dependent on the value present in the DSCP field. Flow Label field is 20 bits long which means 2^{20} service classes.

The QoS operation consists of several steps:

- Packet classification,
- Packet marking and/or remarking,
- Traffic policing,
- Traffic shaping,
- Packet queuing.

Packet classification is intended to categorize IPv6 packets into multiple service classes with different priority levels. Classification uses some kind of traffic descriptor (e.g. IPv6 addresses, MAC addresses, VLAN ID etc.) to classify IPv6 packets. With packet marking, devices can write service class information in a DSCP field and classification can be performed solely on the basis of DSCP value. If there is a need to change already defined DSCP value that can be done with packet remarking. Traffic shaping and policing are performed at the edge of DiffServ domain in order to ensure that all traffic entering the DiffServ domain complies with the QoS rules.

The DiffServ architecture defines DiffServ edge and core nodes. DiffServ edge nodes do intelligent QoS-related functions such as packet classification, packet marking/remarking, traffic policing and shaping, and furthermore forward IPv6 packets into the DiffServ domain. DiffServ core nodes are basically only forwarding IPv6 packets according to specified Per-Hop Behaviour (PHB) which refers to queueing, policing and shaping, all according to the configured rules.

From the A-ERCS system perspective, the DiffServ edge nodes will be core routers at SECC and

core router within A-ERCS node. Optionally, the DiffServ edge node could also be Router/AP within A-ERCS node. Even though it is hardly possible, DiffServ core nodes would mainly need to be implemented in A-ERCS backhaul supported systems.

Since hierarchical QoS provides option to manage QoS at different levels, for example physical and logical interface, it could prove useful in A-ERCS system. Also, the QoS L2/L3 interworking function is required because it provides mapping between Ethernet Class of Service field and IPv6 Traffic Class field.

For management purposes of DiffServ devices and interfaces in A-ERCS system, the DiffServ Management Information Base (MIB) is required and is to be used with Simple Network Management Protocol (SNMP) for remote monitoring and troubleshooting of QoS.

3.3.2 Node Level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node QoS requirements			
DiffServ model	Diffserv model	Traffic Class	Required
		Flow Label	Optional
	Packet classification		Required
	Packet marking		Required
	Packet remarking		Required
	Traffic policing		Required
	Traffic shaping		Required
	Packet queueing		Required
	Hierarchical QoS		Required
	QoS IWF L2/L3 (Traffic Class/CoS)		Required
	MIB		Required

Table 3-15: A-ERCS node QoS requirements.

3.3.3 Node Extension Level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node extension QoS requirements			
DiffServ model	Diffserv model	Traffic Class	Required
		Flow Label	Optional
	Packet classification		Optional

A-ERCS segment/capability	Requirement	Details	Status
	Packet marking		Optional
	Packet remarking		Optional
	Traffic policing		Optional
	Traffic shaping		Optional
	Packet queueing		Optional
	Hierarchical QoS		Optional
	QoS IWF L2/L3 (Traffic Class/CoS)		Required
	MIB		Required

Table 3-16: A-ERCS node extension QoS requirements.

3.3.4 Device Level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node Core router QoS requirements			
DiffServ model	Diffserv model	Traffic Class	Required
		Flow Label	Optional
	Packet classification		Required
	Packet marking		Required
	Packet remarking		Required
	Traffic policing		Required
	Traffic shaping		Required
	Packet queueing		Required
	Hierarchical QoS		Required
	QoS IWF L2/L3 (Traffic Class/CoS)		Required
	MIB		Required
A-ERCS node Firewall QoS requirements			
DiffServ model	Diffserv model	Traffic Class	Required
		Flow Label	Optional
	Packet classification		Required
	Packet marking		Required
	Packet remarking		Required
	Traffic policing		Required
	Traffic shaping		Required
	Packet queueing		Required
	Hierarchical QoS		Optional
	QoS IWF L2/L3 (Traffic Class/CoS)		Required
	MIB		Required
A-ERCS node Router/AP QoS requirements			
DiffServ model	Diffserv model	Traffic Class	Required

A-ERCS segment/capability	Requirement	Details	Status
		Flow Label	Optional
	Packet classification		Required
	Packet marking		Required
	Packet remarking		Required
	Traffic policing		Required
	Traffic shaping		Required
	Packet queueing		Required
	Hierarchical QoS		Optional
	QoS IWF L2/L3 (Traffic Class/CoS)		Required
	MIB		Required

Table 3-17: A-ERCS device level QoS requirements.

3.3.5 Strategic Emergency Control Center level

A-ERCS segment/capability	Requirement	Details	Status
SECC QoS requirements			
DiffServ model	Diffserv model	Traffic Class	Required
		Flow Label	Optional
	Packet classification		Required
	Packet marking		Required
	Packet remarking		Required
	Traffic policing		Required
	Traffic shaping		Required
	Packet queueing		Required
	Hierarchical QoS		Optional
	QoS IWF L2/L3 (Traffic Class/CoS)		Required
	MIB		Required

Table 3-18: SECC QoS requirements.

3.3.6 A-ERCS QoS and Policy Enforcement requirements for Backhaul Supported Systems

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based QoS requirements for Backhaul Supported Systems			
UMTS/HSPA	Differentiated Services model	4 Service Classes	Optional
		SLA assurance	Optional

A-ERCS segment/capability	Requirement	Details	Status
LTE	Differentiated Services model	4 Service Classes	Optional
		SLA assurance	Optional
WiFi	Differentiated Services model	No packet remarking	Optional
Ethernet/FTTH	Differentiated Services model	No packet remarking	Optional
xDSL	Differentiated Services model	No packet remarking	Optional
TETRA	Differentiated Services model	4 Service Classes	Optional
DMR	Differentiated Services model	4 Service Classes	Optional
Satellite	Differentiated Services model	No packet remarking	Optional

Table 3-19: IPv6-based QoS requirements for backhaul supported systems.

3.4 A-ERCS System Security Design

In this chapter, A-ERCS system security design is analysed and described in details. Security functions in the A-ERCS are divided between control plane, data plane, management plane and user plane.

In the following, the detailed features are described, and in further chapters, the requirements on each of the A-ERCS segments are specified.

3.4.1 Control plane

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based control plane security requirements			
A-ERCS node	Secure Routing	OSPFv3	Optional
		MP-BGP	Optional
	Secure Mobility	Mobile IPv6	Required
		NEMO	Required
A-ERCS node extension	Secure Routing	OSPFv3	Optional
		MP-BGP	Optional
	Secure Mobility	Mobile IPv6	Required
		NEMO	Optional
Strategic Emergency Control	Secure Routing	OSPFv3	Optional

A-ERCS segment/capability	Requirement	Details	Status
Center		MP-BGP	Optional
	Secure Mobility	Mobile IPv6	Required
		NEMO	Required

Table 3-20: IPv6-based control plane security requirements.

3.4.1.1 Secure routing

To ensure that no false routing information is distributed among routers in A-ERCS system, some routing security mechanisms are required.

In OSPFv3, IPsec Authentication Header (AH) [9] and IPsec Encapsulating Security Payload (ESP) [10] should be used to provide integrity, authentication and/or confidentiality [8]. For authentication only, IPsec AH or IPsec ESP can be used. If encryption is needed, IPsec ESP should be used.

For ensuring security with MP-BGP, the TCP Authentication Option (TCP AO) [11] should be used. The TCP Authentication Option specifies stronger Message Authentication Codes (MACs) than previously defined TCP MD5-based protection of BGP sessions [12]. Main purpose of TCP AO is the authentication of TCP segments, particularly the protection of BGP data that can be affected if BGP sessions would run over spoofed TCP segments.

3.4.1.2 Secure mobility

In A-ERCS system, mobility is provided with Mobile IPv6 and NEMO with both of them using signalling messages to dynamically establish tunnels.

Signalling messages in Mobile IPv6 can be protected (authenticated) with IPsec [13] or with Binding Authorization Data [35]. Binding messages (Update, Acknowledgement) between home Agent and mobile nodes must be protected with IPsec while the use Binding Authorization Data is mandatory when mobile node is sending Binding Updates directly to correspondent node.

As in Mobile IPv6, NEMO also requires that all signalling messages between mobile nodes and Home Agent must also be authenticated with IPsec.

3.4.1.3 Node level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node control plane security requirements			
Secure routing	OSPFv3	IPsec AH	Optional
		IPsec ESP	Optional
	MP-BGP	TCP AO	Optional
Secure mobility	Mobile IPv6	IPsec ESP	Required
		Binding Authorization Data	Optional
	NEMO	IPsec ESP	Required

Table 3-21: A-ERCS node control plane security requirements.

3.4.1.4 Node extension level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node extension control plane security requirements			
Secure routing	OSPFv3	IPsec AH	Optional
		IPsec ESP	Optional
	MP-BGP	TCP AO	Optional
Secure mobility	Mobile IPv6	IPsec ESP	Required
		Binding Authorization Data	Required
	NEMO	IPsec ESP	Required

Table 3-22: A-ERCS node extension control plane security requirements.

3.4.1.5 Device level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node Core router control plane security requirements			
Secure routing	OSPFv3	IPsec AH	Optional
		IPsec ESP	Optional
	MP-BGP	TCP AO	Required
Secure mobility	Mobile IPv6	IPsec ESP	Required
		Binding Authorization Data	Optional
	NEMO	IPsec ESP	Required

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node Firewall control plane security requirements			
Secure routing	OSPFv3	IPsec AH	Not required
		IPsec ESP	Not required
	MP-BGP	TCP AO	Not required
Secure mobility	Mobile IPv6	IPsec ESP	Not required
		Binding Authorization Data	Not required
	NEMO	IPsec ESP	Not required
A-ERCS node Router/AP control plane security requirements			
Secure routing	OSPFv3	IPsec AH	Optional
		IPsec ESP	Optional
	MP-BGP	TCP AO	Optional
Secure mobility	Mobile IPv6	IPsec ESP	Required
		Binding Authorization Data	Optional
	NEMO	IPsec ESP	Optional

Table 3-23: A-ERCS device level control plane security requirements.

3.4.1.6 Strategic Emergency Control Center

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based control plane requirements			
Secure routing	OSPFv3	IPsec AH	Optional
		IPsec ESP	Optional
	MP-BGP	TCP AO	Required
Secure mobility	Mobile IPv6	IPsec ESP	Required
		Binding Authorization Data	Optional
	NEMO	IPsec ESP	Required

Table 3-24: SECC control plane security requirements.

3.4.2 Data plane

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based data plane security requirements			
A-ERCS node	Native IPv6 data channel security	IPsec	Required
		SSL/TLS	Required
	Tunnelled IPv6 data channel security	IPsec	Required
	IPv6 Access control	Access Lists	Required
A-ERCS node extension	Native IPv6 data channel security	IPsec	Required
		SSL/TLS	Required
	Tunnelled IPv6 data channel security	IPsec	Required
	IPv6 Access control	Access Lists	Optional
Strategic Emergency Control Center	Native IPv6 data channel security	IPsec	Required
		SSL/TLS	Required
	Tunnelled IPv6 data channel security	IPsec	Required
	IPv6 Access control	Access Lists	Required

Table 3-25: IPv6-based data plane security requirements.

3.4.2.1 Native IPv6 data channel security

To enable secure data forwarding over native IPv6 networks within A-ERCS system, security mechanisms should be enabled, particularly IPsec and SSL/TLS. If using IPsec AH, data integrity and authentication is provided. Additionally, if data confidentiality is required, IPsec ESP which provides encryption should be used.

To ensure data confidentiality without the use of IPsec ESP, SSL/TLS [14] [15] mechanism can be used. SSL is a widely implemented protocol and represents the basis for TLS. It supports encryption and operates at top of the TCP, providing higher layer data encryption. SSL was never officially standardized in the IETF, however, TLS is an IETF standards track protocol that is based on SSL. It is expected that in A-ERCS system SSL/TLS mechanisms will be used to provide secure web-based services.

3.4.2.2 Tunnelled IPv6 data channel security

Data plane security requirements in A-ERCS system exist also if IPv6 traffic is forwarded via tunnels (e.g. Mobile IP, NEMO). As mentioned before, to ensure data integrity, authentication and confidentiality, IPsec AH or IPsec ESP will be used. Also, for web-based services that run over tunnels, SSL/TLS mechanisms can be used to ensure privacy.

3.4.2.3 IPv6 Access control

Some kind of access control mechanism is needed in A-ERCS system to prevent certain data traffic to be forwarded across devices and/or networks. For data plane IPv6 traffic, Access Control Lists (ACL) can be used to permit or deny certain type of traffic. ACLs can typically control inbound and outbound traffic and can operate on either unicast or multicast IPv6 traffic.

3.4.2.4 Node level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node data plane security requirements			
Native IPv6 data channel security	IPsec	AH	Required
		ESP	Required
	SSL/TLS		Required
Tunnelled IPv6 data channel security	IPsec	AH	Required
		ESP	Required
	SSL/TLS		Required
IPv6 Access control	Access Lists	Unicast	Required
		Multicast	Required

Table 3-26: A-ERCS node data plane security requirements.

3.4.2.5 Node extension level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node extension data plane security requirements			
Native IPv6 data channel security	IPsec	AH	Required
		ESP	Required
	SSL/TLS		Required
Tunnelled IPv6 data channel security	IPsec	AH	Required
		ESP	Required
	SSL/TLS		Required
IPv6 Access control	Access Lists	Unicast	Optional
		Multicast	Optional

Table 3-27: A-ERCS node extension data plane security requirements.

3.4.2.6 Device level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node Core router data plane security requirements			
Native IPv6 data channel security	IPsec	AH	Required
		ESP	Required
	SSL/TLS		Required
Tunnelled IPv6 data channel security	IPsec	AH	Required
		ESP	Required
	SSL/TLS		Required
IPv6 Access control	Access Lists	Unicast	Required
		Multicast	Required
A-ERCS node Firewall data plane security requirements			
Native IPv6 data channel security	IPsec	AH	Required
		ESP	Required
	SSL/TLS		Required
Tunnelled IPv6 data channel security	IPsec	AH	Not required
		ESP	Not required
	SSL/TLS		Not required
IPv6 Access control	Access Lists	Unicast	Required
		Multicast	Required
A-ERCS node Router/AP data plane security requirements			
Native IPv6 data channel security	IPsec	AH	Required
		ESP	Required
	SSL/TLS		Required
Tunnelled IPv6 data channel security	IPsec	AH	Required
		ESP	Required
	SSL/TLS		Required
IPv6 Access control	Access Lists	Unicast	Required
		Multicast	Required

Table 3-28: A-ERCS node device level data plane security requirements.

3.4.2.7 Strategic Emergency Control Center level

A-ERCS segment/capability	Requirement	Details	Status
SECC data plane security requirements			
Native IPv6 data channel security	IPsec	AH	Required
		ESP	Required
	SSL/TLS		Required

A-ERCS segment/capability	Requirement	Details	Status
Tunnelled IPv6 data channel security	IPsec	AH	Required
		ESP	Required
	SSL/TLS		Required
IPv6 Access control	Access Lists	Unicast	Required
		Multicast	Required

Table 3-29: A-ERCS node data plane security requirements.

3.4.3 Management plane

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based management plane security requirements			
A-ERCS node	Secure remote shell access	SSH	Required
	Secure remote monitoring & management	SNMPv3	Required
	Secure web access	HTTPS	Required
A-ERCS node extension	Secure remote shell access	SSH	Required
	Secure remote monitoring & management	SNMPv3	Required
	Secure web access	HTTPS	Required
Strategic Emergency Control Center	Secure remote shell access	SSH	Required
	Secure remote monitoring & management	SNMPv3	Required
	Secure web access	HTTPS	Required

Table 3-30: IPv6-based management plane security requirements.

3.4.3.1 Secure remote shell access

For remote shell access (e.g. remote access to router command line interface) in A-ERCS system, the SSH [16] transport layer protocol will be used. It is widely adopted in various network environments and typically runs on top of TCP providing encryption, server authentication and integrity protection.

3.4.3.2 Secure remote monitoring & management

Centralized remote monitoring and management of devices in the A-ERCS system is very important as it provides characteristics of the whole system. In IPv6-based network environments such as the A-ERCS system, the Simple Network Management Protocol Version 3 (SNMPv3) [17] can be used to ensure such a capability.

SNMPv3 is typically supported on most of the network equipment (routers, switches, servers, workstations...). The SNMPv3 protocol includes the following components: managed device, agent and Network Management System (NMS). Agent is the software that runs on a managed device which also has a local Management Information Base (MIB) that describes the structure of the management data on a device. The SNMPv3 can be used to only query the MIB or it can also write in the MIB and by doing that the device can be remotely configured.

3.4.3.3 Secure web access

Many network equipment devices nowadays provide web-based graphical user interface (GUI) for monitoring and administration of devices. As basic Hypertext Transfer Protocol (HTTP) doesn't provide any security mechanisms, HTTPS [18] should be used for remote administration of devices in A-ERCS system. HTTPS is basically HTTP transported over SSL, thus ensuring confidentiality of web-based data.

3.4.3.4 Node level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node management plane security requirements			
Secure remote shell access	SSH		Required
Secure remote monitoring & management	SNMPv3		Required
Secure web management access	HTTPS		Required

Table 3-31: A-ERCS node management plane security requirements.

3.4.3.5 Node extension level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node extension management plane security requirements			
Secure remote shell access	SSH		Required
Secure remote monitoring & management	SNMPv3		Required
Secure web management access	HTTPS		Required

Table 3-32: A-ERCS node extension management plane security requirements.

3.4.3.6 Device level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node Core router management plane security requirements			
Secure remote shell access	SSH		Required
Secure remote monitoring & management	SNMPv3		Required
Secure web management access	HTTPS		Required
A-ERCS node Firewall management plane security requirements			
Secure remote shell access	SSH		Required
Secure remote monitoring & management	SNMPv3		Required
Secure web management access	HTTPS		Required
A-ERCS node Router/AP management plane security requirements			
Secure remote shell access	SSH		Required
Secure remote monitoring & management	SNMPv3		Required
Secure web management access	HTTPS		Required

Table 3-33: A-ERCS node device level management plane security requirements.

3.4.3.7 Strategic Emergency Control Center level

A-ERCS segment/capability	Requirement	Details	Status
SECC management plane security requirements			
Secure remote shell access	SSH		Required
Secure remote monitoring & management	SNMPv3		Required
Secure web management access	HTTPS		Required

Table 3-34: SECC management plane security requirements.

3.4.4 User plane

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based user plane security requirements			
A-ERCS node	User authentication & authorization	RADIUS	Required
		LDAP	Required
		802.1x	Required
A-ERCS node extension	User authentication & authorization	RADIUS	Required
		LDAP	Required
		802.1x	Required
Strategic Emergency Control Center	User authentication & authorization	RADIUS	Required
		LDAP	Required
		802.1x	Required

Table 3-35: IPv6-based user plane security requirements.

3.4.4.1 User authentication & authorization

User authentication refers to the procedure where user's identity is authenticated on the basis of passwords, digital certificates etc. Additionally, user authorization is used to permit or deny already authenticated user to perform an activity or a certain set of actions. User authentication and authorization is typically implemented as a part of centralized AAA (Authentication, Authorization and Accounting) system that is based on RADIUS protocol (Remote Authentication Dial In User Service) [19].

For AAA services in A-ERCS system, the centralized RADIUS server will be used and will include a database containing all authentication and authorization parameters for users/services. In order to communicate with the RADIUS server, RADIUS client functionality should be implemented on devices that require AAA services.

Additionally, users and/or services can be listed in a directory (e.g. Windows Active Directory) and LDAP [20] (Lightweight Directory Access Protocol) protocol should be used to access and maintain directory information. If Directory services (i.e. LDAP server) would be implemented in A-ERCS system, the LDAP client functionality will be required on certain devices.

To provide port-based network access control on Ethernet switches or WiFi Access Points, the IEEE 802.1x [21] mechanism should be used in A-ERCS system. End device supporting 802.1x uses EAP (Extensible Authentication Protocol) to transport user authentication parameters towards 802.1x authenticator (e.g. Ethernet switch or WiFi Access Point), followed by RADIUS protocol which transports EAP messages towards the authentication server (i.e. RADIUS server). End device does not get network access until the user is successfully authenticated via EAP and

RADIUS.

3.4.4.2 Node level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node user plane security requirements			
User authentication & authorization	RADIUS	Client	Required
		Server	Required
		Proxy	Optional
	LDAP	Client	Required
		Server	Required
	802.1x	Client	Required
		Authenticator	Required

Table 3-36: A-ERCS node user plane security requirements.

3.4.4.3 Node extension level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node extension user plane security requirements			
User authentication & authorization	RADIUS	Client	Required
		Server	Not required
		Proxy	Not required
	LDAP	Client	Required
		Server	Not required
	802.1x	Client	Required
		Authenticator	Optional

Table 3-37: A-ERCS node user plane security requirements.

3.4.4.4 Device level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node Core router user plane security requirements			
User authentication &	RADIUS	Client	Required

A-ERCS segment/capability	Requirement	Details	Status
authorization		Server	Optional
		Proxy	Optional
	LDAP	Client	Required
		Server	Not required
	802.1x	Client	Optional
		Authenticator	Optional
A-ERCS node Firewall user plane security requirements			
User authentication & authorization	RADIUS	Client	Required
		Server	Optional
		Proxy	Optional
	LDAP	Client	Required
		Server	Not required
	802.1x	Client	Optional
		Authenticator	Optional
		A-ERCS node Router/AP user plane security requirements	
User authentication & authorization	RADIUS	Client	Required
		Server	Optional
		Proxy	Optional
	LDAP	Client	Required
		Server	Not required
	802.1x	Client	Optional
		Authenticator	Required

Table 3-38: A-ERCS node device level user plane security requirements.

3.4.4.5 Strategic Emergency Control Center level

A-ERCS segment/capability	Requirement	Details	Status
SECC user plane security requirements			
User authentication & authorization	RADIUS	Client	Required
		Server	Optional
		Proxy	Optional
	LDAP	Client	Required
		Server	Optional
		Client	Optional
	802.1x	Authenticator	Optional

Table 3-39: A-ERCS node user plane security requirements.

3.4.5 A-ERCS Security Requirements for Backhaul Supported System

In this chapter, requirements for A-ERCS Security in the Backhaul Supported Systems are specified.

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based Security requirements for Backhaul Supported Systems			
UMTS/HSPA	No IPv6 packet filtering	UDP port 500, 4500	Required
		TCP port 443	Required
LTE	No IPv6 packet filtering	UDP port 500, 4500	Required
		TCP port 443	Required
WiFi	No IPv6 packet filtering	UDP port 500, 4500	Required
		TCP port 443	Required
Ethernet/FTTH	No IPv6 packet filtering	UDP port 500, 4500	Required
		TCP port 443	Required
xDSL	No IPv6 packet filtering	UDP port 500, 4500	Required
		TCP port 443	Required
TETRA	No IPv6 packet filtering	UDP port 500, 4500	Required
		TCP port 443	Required
DMR	No IPv6 packet filtering	UDP port 500, 4500	Required
		TCP port 443	Required
Satellite	No IPv6 packet filtering	UDP port 500, 4500	Required
		TCP port 443	Required

Table 3-40: IPv6-based security requirements for backhaul supported systems.

3.5 A-ERCS System Routing Design

In this chapter the A-ERCS system routing design is analysed and described in details. As stated in previous document [7], static or dynamic IPv6 unicast and multicast routing techniques can be used. Routing capabilities are required on the A-ERCS node, A-ERCS node extension and on core routers at SECC.

In the following, the detailed features are described, and in further chapters, the requirements on each of the A-ERCS segments are specified.

3.5.1 Unicast routing

Static IPv6 unicast routing is a basic requirement on all segments of the A-ERCS system. Dynamic IPv6 unicast routing protocols are also required, mainly OSPFv3 and also MP-BGP.

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based unicast routing requirements			
A-ERCS node	Static routing		Required
	Dynamic routing	RIPng	Optional
		IS-IS for IPv6	Optional
		OSPFv3	Required
		MP-BGP	Optional
A-ERCS node extension	Static routing		Required
	Dynamic routing	RIPng	Optional
		IS-IS for IPv6	Optional
		OSPFv3	Optional
		MP-BGP	Not required
Strategic Emergency Control Center	Static routing		Required
	Dynamic routing	RIPng	Optional
		IS-IS for IPv6	Optional
		OSPFv3	Required
		MP-BGP	Required

Table 3-41: IPv6-based unicast routing requirements.

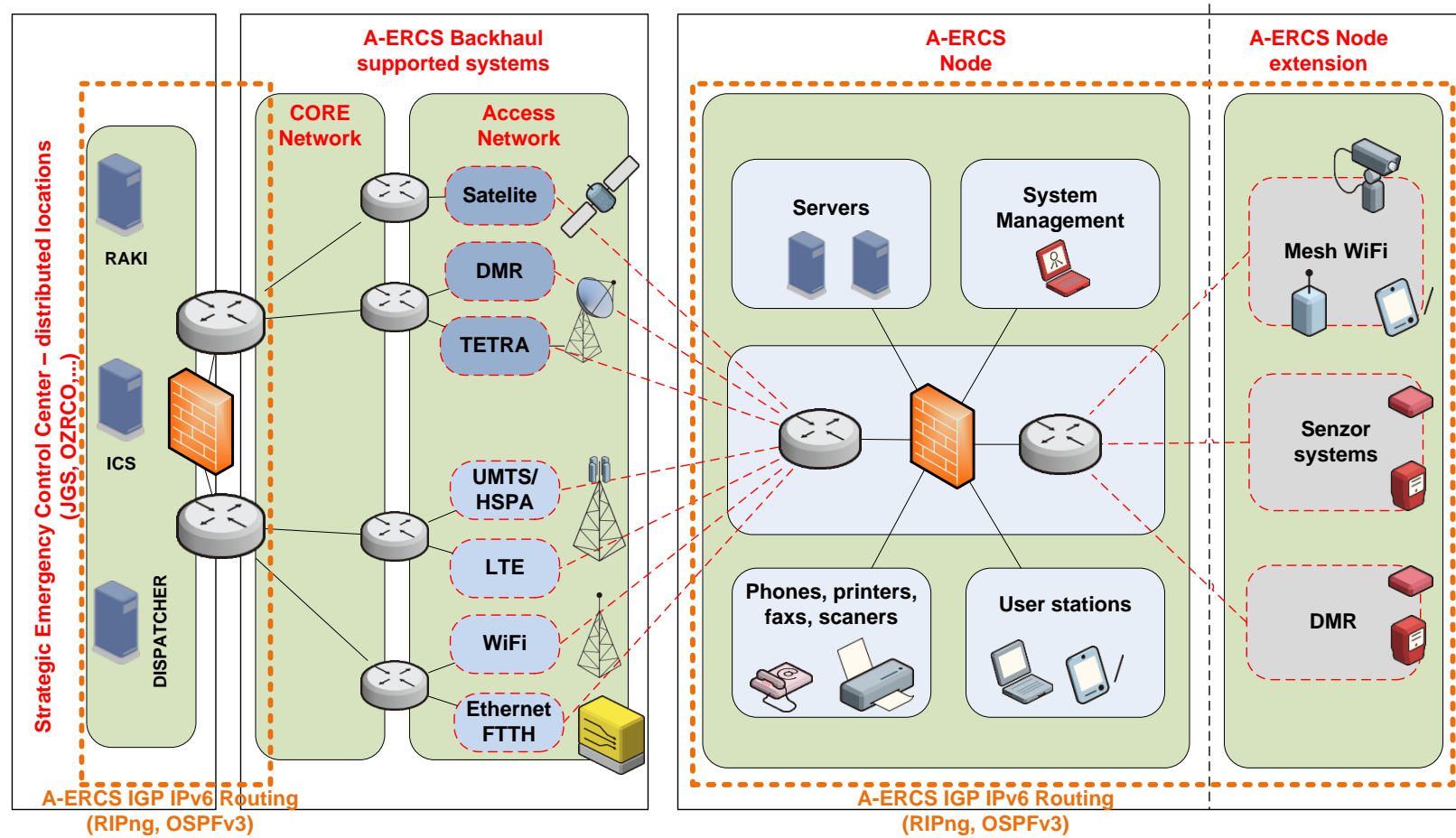


Figure 3-4: A-ERCS system IGP routing.

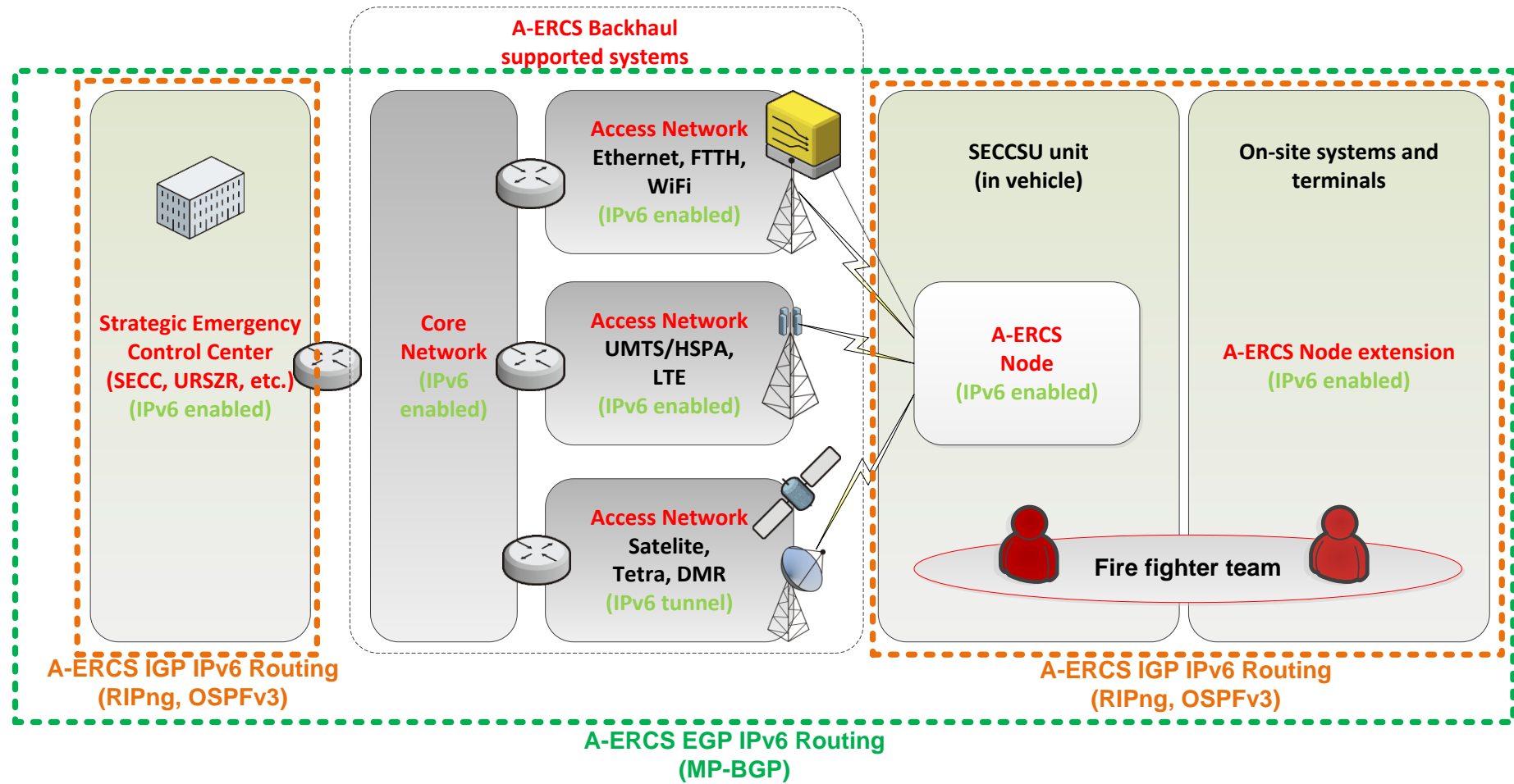


Figure 3-5: A-ERCS system IGP & EGP routing.

3.5.1.1 Static routing

For basic routing purposes (i.e. default routes) in the A-ERCS system, static routing can be used. For advanced unicast routing features, OSPFv3 and MP-BGP protocols are required.

3.5.1.2 OSPFv3

As a link-state routing protocol, OSPFv3 [22] is designed to operate in complex network systems such as A-ERCS system. It runs directly on top of IPv6 and is therefore appropriate choice to use in an all-IPv6 network system.

To ensure that no rouge and/or invalid OSPFv3 routers participate in OSPFv3 Link State Advertisements (LSA) exchange, the OSPFv3 authentication should be used. Encryption can also be used to prevent unwanted listening. For authentication and encryption OSPFv3 relies on IPv6's Authentication Header (AH) and Encapsulating Security Payload (ESP).

The separation of different OSPFv3 domains can be achieved with multiple OSPFv3 processes running on the same device. Additionally, to support Address Families feature, multiple OSPFv3 instances per interface is also required.

Although OSPFv3 is an IPv6 unicast routing protocol it also supports advertising other address families such as unicast IPv4 [23]. This OSPFv3 functionality can be used to simplify routing in dual-stack network environments such as A-ERCS system and also, router workload is reduced.

In a complex mobile network system with a fast changing topology such as A-ERCS, there is always a need to reduce the number of LSAs exchanged to ensure efficient routing and forwarding of IPv6 packets. This can be achieved with dynamic fast convergence features of OSPFv3, mainly with LSA and SPF throttling feature that provide a mechanism to slow down LSAs and delay SPF calculations during times on network instability. Additionally, even faster OSPFv3 convergence can be achieved with SPF and LSA rate-limiting. For very fast failure detection, the Bidirectional Forwarding Detection (BFD) can be used. BFD is designed to provide fast failure detection times regardless of the media type or topology and can work with link-local or global IPv6 unicast addresses.

In OSPFv3, when there are multiple intra-AS paths available, OSPFv3 External Path Preference Option can be used to help routers decide which of the paths should be preferred over others.

Another useful feature is OSPFv3 Graceful Restart [24] that provides a mechanism to restart

control plane of an OSPFv3 router with minimal impact on forwarding plane. If a Graceful Restart feature would be used, it is important that all neighbour devices are aware of a graceful restart.

The A-ERCS system, being a mobile ad-hoc network that requires robust and efficient IPv6 traffic forwarding, would also find useful OSPFv3 MANET extensions [25] which improve routing efficiency and reduce overhead traffic in mobile ad-hoc environments. These extensions include:

- Coupling OSPFv3 with Radio Aware Routing radios that provide real-time characteristics of an interface and thus support dynamic interface cost.
- Minimizing OSPFv3 packet sizes.
- Minimizing the number of OSPFv3 packet transmissions by caching LSAs.
- Selective peering to reduce the number of redundant full adjacencies.

For management purposes of elements in A-ERCS system, the OSPFv3 Management Information Base (MIB) is required and is to be used with Simple Network Management Protocol (SNMP) for remote monitoring and troubleshooting of OSPFv3 on devices.

In a closed and well-controlled network system such as A-ERCS the policy-based routing feature is desirable. Policy-based routing allows defining policies for routing and forwarding of packets that meet certain criteria. Typically, IPv6 packets are checked if they match certain rule (e.g. source IPv6 address, DSCP field, flowlabel) and if matched, the packets are forwarded according to corresponding rule (i.e. forward packets to specific next hop gateway or output interface).

3.5.1.3 MP-BGP

MP-BGP protocol [27] can act as an Interior Gateway Protocol or as an Exterior Gateway Protocol for routing of IPv6. Typically, it is used as an EGP.

Since it is very unlikely that A-ERCS node or node extension would act as an autonomous system (AS), MP-BGP is not required on A-ERCS node or node extension. However, it is expected that the entire A-ERCS system would act as an AS and therefore MP-BGP should be used for routing between other autonomous systems.

To ensure that only certain routes are announced or redistributed into another routing protocol, MP-BGP supports prefix filter feature.

If multiple external routes are available, the MG-BGP protocol support multipath feature that enables load sharing between these routes.

Since the A-ERCS system is basically a closed network environment, it requires constant and stable primary uplink and a few more backup uplinks that ensure high availability. Even so, during emergency and disaster situations it can occurs that primary and more backup uplinks are not available. To avoid the loss of connectivity, the BGP best External feature enables advertising the most preferred router among those received from the external BGP neighbour as a backup route. Typically, if MP-BGP multipath is enabled the Best External feature will not be available.

To achieve shorter convergence times within fast-responsive A-ERCS system, MP-BGP supports some Convergence Optimization techniques such as BGP Next-Hop Tracking that provides next hop changes to be rapidly reported to the BGP routing process, or using BFD to enable fast failure detection on primary and backup uplinks.

At times, the restart or even shutdown of MP-BGP routers is required. After the shutdown, routers are temporarily unreachable and consequently certain routes are not available. To minimize packet loss during MP-BGP convergence, the BGP provides the Graceful Shutdown mechanism [28] that enables signalling to other routers that MP-BGP session will shutdown and furthermore, alternative paths are propagated to neighbour routers within A-ERCS system.

For management purposes of elements in A-ERCS system, the MP-BGP MIB is required and is to be used with the SNMP protocol for remote monitoring and troubleshooting of MP-BGP devices.

Policy-based routing for MP-BGP would also be beneficial since it allows certain policies to affect MP-BGP routing decisions. Usually it can be used to control traffic flow direction, to change to next hop address or to change the way the traffic is sent to a neighbour router.

3.5.1.4 Node level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node unicast routing requirements			
Static routing	Static routing		Required
OSPFv3	OSPFv3		Required
	OSPFv3 Authentication with IPsec		Required
	OSPFv3 Encryption with IPsec		Optional

A-ERCS segment/capability	Requirement	Details	Status
	OSPFv3 Address Families	IPv4	Optional
		IPv6	Required
	OSPFv3 BFD		Optional
	OSPFv3 External Path Preference		Optional
	OSPFv3 Fast Convergence		Optional
	OSPFv3 Graceful Restart		Optional
	Multiple OSPFv3 processes per device		Required
	Multiple OSPFv3 instances per interface		Required
	OSPFv3 MANET Extensions		Optional
	OSPFv3 Dynamic Interface Cost Support		Optional
	OSPFv3 MIB		Optional
	OSPFv3 Policy-based routing	Source-based	Optional
		QoS-based	Optional
		Load sharing	Optional
MP-BGP	MP-BGP		Optional
	MP-BGP Prefix Filter		Optional
	MP-BGP Multipath Support		Optional
	MP-BGP Best External		Optional
	MP-BGP Convergence Optimization		Optional
	MP-BGP BFD		Optional
	MP-BGP Graceful Shutdown		Optional
	MP-BGP MIB		Optional
	MP-BGP Policy-based routing		Optional

Table 3-42: A-ERCS node unicast routing requirements.

3.5.1.5 Node Extension level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node extension unicast routing requirements			
Static routing	Static routing		Required
OSPFv3	OSPFv3		Required
	OSPFv3 Authentication with IPsec		Required
	OSPFv3 Encryption with IPsec		Optional
	OSPFv3 Address Families	IPv4	Optional
		IPv6	Required
	OSPFv3 BFD		Optional
	OSPFv3 External Path Preference		Optional
	OSPFv3 Fast Convergence		Optional
	OSPFv3 Graceful Restart		Optional

A-ERCS segment/capability	Requirement	Details	Status
	Multiple OSPFv3 processes per device		Required
	Multiple OSPFv3 instances per interface		Required
	OSPFv3 MANET Extensions		Optional
	OSPFv3 Dynamic Interface Cost Support		Optional
	OSPFv3 MIB		Optional
	OSPFv3 Policy-based routing	Source-based	Optional
		QoS-based	Optional
		Load sharing	Optional
MP-BGP	MP-BGP		Optional
	MP-BGP Prefix Filter		Optional
	MP-BGP Multipath Support		Optional
	MP-BGP Best External		Optional
	MP-BGP Convergence Optimization		Optional
	MP-BGP BFD		Optional
	MP-BGP Graceful Shutdown		Optional
	MP-BGP MIB		Optional
	MP-BGP Policy-based routing		Optional

Table 3-43: A-ERCS node extension unicast routing requirements.

3.5.1.6 Device level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node Core router unicast routing requirements			
Static routing	Static routing		Required
OSPFv3	OSPFv3		Required
	OSPFv3 Authentication with IPsec		Required
	OSPFv3 Encryption with IPsec		Optional
	OSPFv3 Address Families	IPv4	Optional
		IPv6	Required
	OSPFv3 BFD		Optional
	OSPFv3 External Path Preference		Optional
	OSPFv3 Fast Convergence		Optional
	OSPFv3 Graceful Restart		Optional
	Multiple OSPFv3 processes per device		Required
	Multiple OSPFv3 instances per interface		Required
	OSPFv3 MANET Extensions		Optional
	OSPFv3 Dynamic Interface Cost Support		Optional
	OSPFv3 MIB		Optional
	OSPFv3 Policy-based routing	Source-based	Optional

A-ERCS segment/capability	Requirement	Details	Status
		QoS-based	Optional
		Load sharing	Optional
MP-BGP	MP-BGP		Optional
	MP-BGP Prefix Filter		Optional
	MP-BGP Multipath Support		Optional
	MP-BGP Best External		Optional
	MP-BGP Convergence Optimization		Optional
	MP-BGP BFD		Optional
	MP-BGP Graceful Shutdown		Optional
	MP-BGP MIB		Optional
	MP-BGP Policy-based routing		Optional
A-ERCS node Firewall unicast routing requirements			
Static routing	Static routing		Required
OSPFv3	OSPFv3		Required
	OSPFv3 Authentication with IPsec		Required
	OSPFv3 Encryption with IPsec		Optional
	OSPFv3 Address Families	IPv4	Optional
		IPv6	Required
	OSPFv3 BFD		Optional
	OSPFv3 External Path Preference		Optional
	OSPFv3 Fast Convergence		Optional
	OSPFv3 Graceful Restart		Optional
	Multiple OSPFv3 processes per device		Required
	Multiple OSPFv3 instances per interface		Required
	OSPFv3 MANET Extensions		Optional
	OSPFv3 Dynamic Interface Cost Support		Optional
	OSPFv3 MIB		Optional
	OSPFv3 Policy-based routing	Source-based	Optional
		QoS-based	Optional
		Load sharing	Optional
A-ERCS node Router/AP unicast routing requirements			
Static routing	Static routing		Required
OSPFv3	OSPFv3		Required
	OSPFv3 Authentication with IPsec		Required
	OSPFv3 Encryption with IPsec		Optional
	OSPFv3 Address Families	IPv4	Optional
		IPv6	Required
	OSPFv3 BFD		Optional
	OSPFv3 External Path Preference		Optional
	OSPFv3 Fast Convergence		Optional
	OSPFv3 Graceful Restart		Optional
Multiple OSPFv3 processes per device		Required	

A-ERCS segment/capability	Requirement	Details	Status
	Multiple OSPFv3 instances per interface		Required
	OSPFv3 MANET Extensions		Optional
	OSPFv3 Dynamic Interface Cost Support		Optional
	OSPFv3 MIB		Optional
	OSPFv3 Policy-based routing	Source-based	Optional
		QoS-based	Optional
		Load sharing	Optional

Table 3-44: A-ERCS device level unicast routing requirements.

3.5.1.7 Strategic Emergency Control Center

A-ERCS segment/capability	Requirement	Details	Status
SECC unicast routing requirements			
Static routing	Static routing		Required
OSPFv3	OSPFv3		Required
	OSPFv3 Authentication with IPsec		Required
	OSPFv3 Encryption with IPsec		Optional
	OSPFv3 Address Families	IPv4	Optional
		IPv6	Required
	OSPFv3 BFD		Optional
	OSPFv3 External Path Preference		Optional
	OSPFv3 Fast Convergence		Optional
	OSPFv3 Graceful Restart		Optional
	Multiple OSPFv3 processes per device		Required
	Multiple OSPFv3 instances per interface		Required
	OSPFv3 MANET Extensions		Optional
	OSPFv3 Dynamic Interface Cost Support		Optional
	OSPFv3 MIB		Optional
	OSPFv3 Policy-based routing	Source-based	Optional
		QoS-based	Optional
		Load sharing	Optional
MP-BGP	MP-BGP		Required
	MP-BGP Prefix Filter		Required
	MP-BGP Multipath Support		Required
	MP-BGP Best External		Optional
	MP-BGP Convergence Optimization		Optional
	MP-BGP BFD		Optional
	MP-BGP Graceful Shutdown		Optional
	MP-BGP MIB		Required

A-ERCS segment/capability	Requirement	Details	Status
	MP-BGP Policy-based routing		Required

Table 3-45: SECC unicast routing requirements.

3.5.2 Multicast routing

Static IPv6 multicast routing is required by all segments of the A-ERCS system. Additionally, dynamic multicast routing protocols are required, namely Protocol Independent Multicast Sparse Mode (PIM-SM) and Protocol Independent Multicast Source Specific Multicast (PIM-SSM).

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based multicast routing requirements			
A-ERCS node	Static routing		Required
	Dynamic routing	PIM-SM	Required
		PIM-SSM	Required
A-ERCS node extension	Static routing		Required
	Dynamic routing	PIM-SM	Required
		PIM-SSM	Required
Strategic Emergency Control Center	Static routing		Required
	Dynamic routing	PIM-SM	Required
		PIM-SSM	Required

Table 3-46: IPv6-based multicast routing requirements.

3.5.2.1 Static routing

For basic multicast routing in the A-ERCS system, static multicast routes can be used. In IPv6 multicast, dynamic protocols PIM-SM and PIM-SSM can be used independently or both at the same time.

3.5.2.2 PIM-SM

PIM-SM protocol [28] is a multicast routing protocol that uses its own multicast routing table which is separated from unicast routing tables regardless of the unicast routing protocol used. However, PIM-SM protocol uses information present in unicast routing tables to enable Reverse Path Forwarding (RPF) that ensures the forwarding of multicast packets is loop-free.

PIM-SM can operate on a source or more often on a shared tree which is used for distributing multicast data flows and it requires a rendezvous point (RP) within its architecture. Basically, the RP represents the root node of a PIM-SM shared tree and is responsible for forwarding of IPv6 packets towards listeners within multicast groups. With PIM-SM, any of the members of the multicast group can begin transmitting multicast traffic to other members of the group (*, G).

The RP also maintains database of multicast groups and receives PIM Join messages to keep track of PIM-SM nodes with active listeners within multicast group. Typically, the multicast traffic is sent from multicast source towards the RP and is encapsulated in unicast PIM Register messages. The RP then decapsulates unicast-encapsulated multicast traffic and forwards it natively over the multicast tree to the multicast listeners.

The location of the RP within the A-ERCS system is dependent on where is the source of multicast traffic. If the multicast source is somewhere within the A-ERCS node and/or the A-ERCS node extension, the RP would be on core router of the A-ERCS node. If the multicast source is at SECC then the RP would be on core routers at SECC.

In order to prevent that no unwanted multicast source can start sending unicast-encapsulated multicast traffic towards RP, the PIM-SM provides filtering of PIM Register messages.

RP configuration can be set manually on the actual RP node and also on the other PIM nodes within PIM-SM architecture. In IPv6, PIM-SM supports embedded RP functionality [30] that allows other devices to learn information about RP from multicast group destination address in IPv6 packets instead of manual configuration of RP on all nodes.

For management purposes of the elements in A-ERCS system, the PIM-SM MIB is required and is to be used with the SNMP protocol for remote monitoring and troubleshooting of PIM-SM devices.

3.5.2.3 PIM-SSM

PIM-SSM mechanism [31] is based on a subset of the PIM-SM protocol with strict restrictions. With PIM-SM, the multicast traffic from all multicast sources is sent towards multicast listeners within certain multicast group while with PIM-SSM, the multicast traffic is forwarded to multicast listeners only from those multicast sources that the listeners have explicitly joined.

With PIM-SSM, the multicast source of certain multicast group is always known in advance and

therefore multicast trees are efficiently build directly from source. This means that PIM-SSM does not rely on RP and shared multicast trees like PIM-SM, instead it builds separate source multicast tree for each combination of source address and multicast group (S, G).

For management purposes of the elements in A-ERCS system, the PIM-SSM MIB is required and is to be used with the SNMP protocol for remote monitoring and troubleshooting of PIM-SSM devices.

3.5.2.4 Multicast signalling

Multicast signalling is required by members of the multicast group to notify other members of that group that they wish to receive multicast traffic for that certain multicast group. Additionally, multicast routers also use multicast signalling to discover if there are active listeners in a certain multicast group. For multicast signalling in IPv6, the Multicast Listener Discovery (MLD) protocol was developed. MLD messages are included in the ICMPv6 protocol.

3.5.2.4.1 MLDv1

MLD protocol version 1 [32] is based on the Internet Group Membership Protocol (IGMP) version 2 which is used for multicast signalling in IPv4. It enables multicast routers to discover if there are any nodes wishing to join certain multicast group and consequently receive multicast traffic for that group.

Typically, the multicast router acts as a MLD Querier and periodically sends out MLD queries to discover the presence of multicast listeners. When a host or MLD listener receives such a query, it responds with the MLD report. The multicast listener also sends out MLD report messages when it wants to join certain multicast group without receiving MLD query first. If a multicast listener desires to leave certain multicast group, it sends out MLD Done message.

In A-ERCS system, MLDv1 can be used with PIM-SM and MLD listeners will be end hosts or devices. The role of MLD Querier could be provisioned either on core routers at SECC, A-ERCS node Core router or Router/AP.

3.5.2.4.2 MLDv2

MLD protocol version 2 [33] [34] is based on the Internet Group Membership Protocol version 3 (IGMPv3) and is designed to be interoperable with MLDv1. In contrast to MLDv1, MLDv2 allows multicast listeners to specify from which multicast source or sources they would like to receive

multicast traffic (i.e. source-specific multicast). Another difference is that MLDv2 does not use MLD Done messages but instead relies only on timers.

MLDv2 in combination with PIM-SSM will be used to enable source-specific multicast in A-ERCS system. MLD queriers could be core routers at SECC or routers within A-ERCS node, while MLD listeners will be end hosts or devices.

3.5.2.5 Node level

A-ERCS segment/capability	Requirement	Details	Status
SECC multicast routing requirements			
Static routing	Static routing		Required
PIM-SM	PIM-SM		Required
	Rendezvous Point (RP)		Required
	PIM Embedded RP Support		Optional
	PIM Register message filtering		Optional
	Multicast signalling	MLDv1	Required
		MLDv2	Required
PIM-SSM	PIM-SSM		Required
	Multicast signalling	MLDv1	Not required
		MLDv2	Required

Table 3-47: A-ERCS node multicast routing requirements.

3.5.2.6 Node extension level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node extension multicast routing requirements			
Static routing	Static routing		Optional
PIM-SM	PIM-SM		Optional
	Rendezvous Point (RP)		Optional
	PIM Embedded RP Support		Optional
	PIM Register message filtering		Optional
	Multicast signalling	MLDv1	Required
		MLDv2	Required
PIM-SSM	PIM-SSM		Optional
	Multicast signalling	MLDv1	Not required
		MLDv2	Required

Table 3-48: A-ERCS node extension multicast routing requirements.

3.5.2.7 Device level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node Core router multicast routing requirements			
Static routing	Static routing		Required
PIM-SM	PIM-SM		Required
	Rendezvous Point (RP)		Required
	PIM Embedded RP Support		Optional
	PIM Register message filtering		Optional
	Multicast signalling	MLDv1	Required
		MLDv2	Required
PIM-SSM	PIM-SSM		Required
	Multicast signalling	MLDv1	Not required
		MLDv2	Required
A-ERCS node Firewall multicast routing requirements			
Static routing	Static routing		Required
PIM-SM	PIM-SM		Required
	Rendezvous Point (RP)		Optional
	PIM Embedded RP Support		Optional
	PIM Register message filtering		Optional
	Multicast signalling	MLDv1	Required
		MLDv2	Required
PIM-SSM	PIM-SSM		Required
	Multicast signalling	MLDv1	Not required
		MLDv2	Required
A-ERCS node Router/AP multicast routing requirements			
Static routing	Static routing		Required
PIM-SM	PIM-SM		Required
	Rendezvous Point (RP)		Optional
	PIM Embedded RP Support		Optional
	PIM Register message filtering		Optional
	Multicast signalling	MLDv1	Required
		MLDv2	Required
PIM-SSM	PIM-SSM		Required
	Multicast signalling	MLDv1	Not required
		MLDv2	Required

Table 3-49: A-ERCS device level multicast routing requirements.

3.5.2.8 Strategic Emergency Control Center

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node extension multicast routing requirements			
Static routing	Static routing		Required
PIM-SM	PIM-SM		Required
	Rendezvous Point (RP)		Required
	PIM Embedded RP Support		Optional
	PIM Register message filtering		Optional
	Multicast signalling	MLDv1	Required
		MLDv2	Required
PIM-SSM	PIM-SSM		Optional
	Multicast signalling	MLDv1	Not required
		MLDv2	Required

Table 3-50: SECC multicast routing requirements.

3.5.3 A-ERCS Routing Design Requirements for Backhaul Supported System

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based routing requirements for Backhaul Supported Systems			
UMTS/HSPA	No routing requirements		TBD
LTE	No routing requirements		TBD
WiFi	No routing requirements		TBD
Ethernet/FTTH	No routing requirements		TBD
xDSL	No routing requirements		TBD
TETRA	No routing requirements		TBD
DMR	No routing requirements		TBD
Satellite	No routing requirements		TBD

Table 3-51: IPv6-based routing requirements for backhaul supported systems.

3.6 A-ERCS System Mobility Design

In this chapter the A-ERCS system mobility design is analysed and described in details. In IPv6, mobility can be either user- or system/network-initiated, depending on where lies the intelligence required to ensure IPv6 connectivity. Mobility capabilities are required on the A-ERCS node, A-ERCS node extension and on core routers at SECC.

In the following, the detailed features are described, and in further chapters, the requirements on each of the A-ERCS segments are specified.

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based mobility requirements			
A-ERCS node	User-initiated	Mobile IPv6	Optional
		DSMIPv6	Optional
	System/network-initiated	PMIPv6	Optional
		NEMO	Required
A-ERCS node extension	User-initiated	Mobile IPv6	Optional
		DSMIPv6	Optional
	System/network-initiated	PMIPv6	Optional
		NEMO	Optional
Strategic Emergency Control Center	User-initiated	Mobile IPv6	Optional
		DSMIPv6	Optional
	System/network-initiated	PMIPv6	Optional
		NEMO	Required

Table 3-52: IPv6-based mobility requirements.

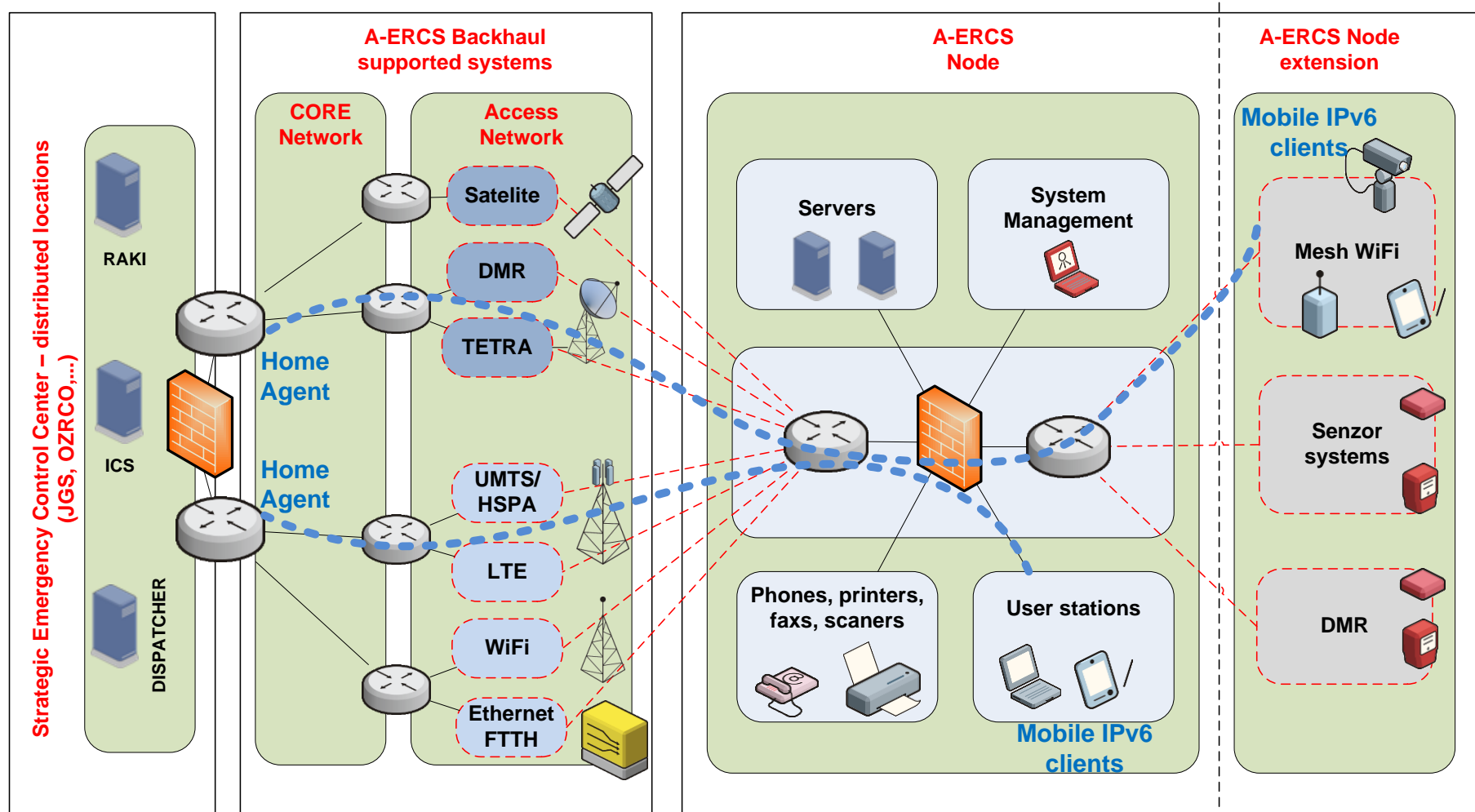


Figure 3-6: Mobile IPv6 in the A-ERCS system.

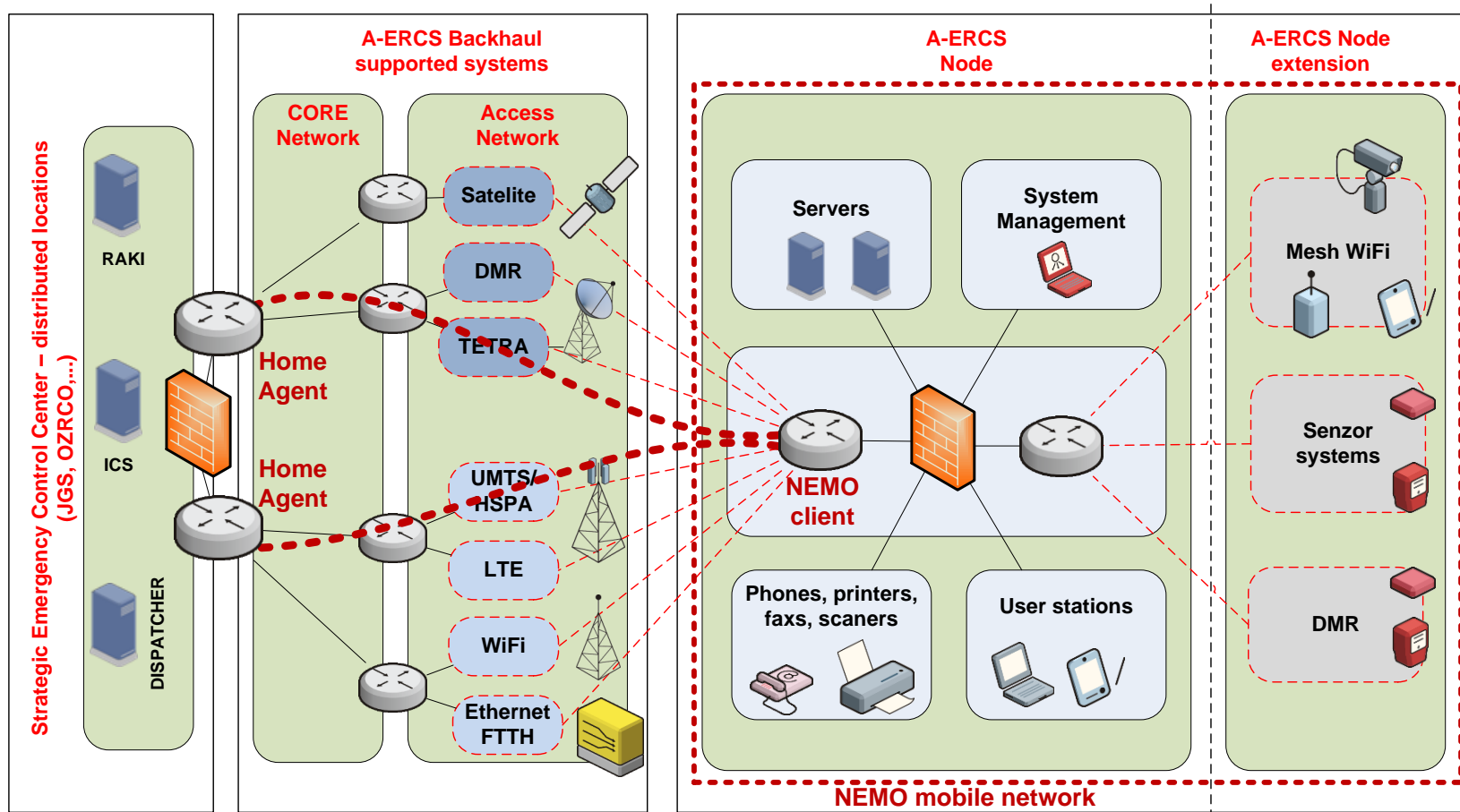


Figure 3-7: NEMO in the A-ERCS system.

3.6.1 Mobile IPv6

Mobile IPv6 [35] is a user-initiated mobility mechanism that allows mobile nodes to hold to their IPv6 home address and remain reachable even in foreign IPv6 networks. To achieve this kind of mobility, the client application on a mobile node must provide the necessary intelligence.

The essential element within the Mobile IPv6 architecture is Home Agent which is located in a home network of a mobile node and is responsible for registration of care-of addresses that are sent via “Binding Update” messages from mobile nodes in foreign networks. Home Agent also takes care of tunnelling IPv6 packets to and from mobile nodes.

With A-ERCS node and/or A-ERCS node extension being mobile nodes, the Mobile Pv6 Home Agent functionality is required on core routers at SECC. Optionally, the Home Agent functionality can also be enabled on routers in the A-ERCS node.

A correspondent node is node that wants to communicate with a mobile node and its home IPv6 address. If all the traffic is forwarded through Home Agent (i.e. bidirectional tunnelling) then no Mobile IPv6 support is required on correspondent node. To achieve that packets from correspondent node are forwarded directly to mobile node, the correspondent node must support mobile node binding registration. From the A-ERCS system perspective, the Correspondent node support is not required although it could prove useful to avoid bidirectional tunnelling and instead use route optimization.

Security features in Mobile IPv6 include the use of IPsec and the Binding Authorization Data option within IPv6 mobility extension header. IPsec can be used for authentication and encryption of signalling and data traffic between mobile nodes and Home Agent. If IPsec is not available, the Binding Authorization Data should be used for authentication of signalling messages between mobile nodes and Home Agent. The preferred option for A-ERCS system should be IPsec if it is available on all the other elements of A-ERCS system. If not, the binding Authorization Data option should be used.

Mobile IPv6 supports Dynamic Home Agent Address Discovery for mobile nodes that do not know the appropriate address of the Home Agent. This functionality could be useful in cases of multiple (redundant) Home Agents in home network. The mechanism is based on ICMPv6 messages being sent to the Mobile IPv6 Home Agents anycast address. Since the A-ERCS system must be highly reliable, multiple Home Agents are possible and therefore Dynamic Home Agent

Address Discovery is very desirable.

For management purposes of elements in A-ERCS system, the Mobile IPv6 MIB is required and is to be used with the SNMP protocol for remote monitoring and troubleshooting of Mobile IPv6 devices.

3.6.2 NEMO

Network Mobility [36] is a system/network initiated mobility mechanism derived from Mobile IPv6. Unlike Mobile IPv6, which provides the mobility of IPv6 mobile hosts, NEMO supports the mobility of whole IPv6 networks. This allows every node (end host) in the mobile IPv6 network behind the mobile router to be reachable on the same address at all times regardless of their location in the IPv6 internet. Network mobility is enabled with the NEMO basic support protocol that runs between a Home Agent and a mobile router.

A NEMO Home Agent is basically a Mobile IPv6 Home Agent with extensions to support network mobility. These extensions include mobile network prefix registration that allows NEMO Home Agent to differentiate between mobile networks belonging to different mobile routers. From the A-ERCS system perspective, the NEMO Home Agent functionality is required on core routers at SECC and NEMO mobile router functionality is required on A-ERCS node and/or A-ERCS node extension. With NEMO selected as a mobility mechanism, the core router within A-ERCS node provides mobility to all the elements within the A-ERCS node and/or A-ERCS node extension, while with Mobile IPv6, each network element that desires to be mobile has to support Mobile IPv6 functionality.

In contrast to Mobile IPv6 where correspondent and mobile node can communicate directly, NEMO requires that all traffic between the nodes in the mobile network and correspondent node passes through the NEMO Home Agent.

IPsec is used for authentication of all signalling messages between the mobile router and the home agent. In A-ERCS system that means IPsec between NEMO Home Agent on core router at SECC and NEMO mobile routers on A-ERCS nodes and/or A-ERCS node extensions.

For management purposes of elements in A-ERCS system, the NEMO MIB is required and is to be used with the SNMP protocol for remote monitoring and troubleshooting of NEMO devices.

3.6.3 Node level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node mobility requirements			
Mobile IPv6	Home Agent		Optional ¹⁸
	Mobile Node		Required
	Correspondent node support		Optional
	Authentication	IPsec	Required
		Binding Auth.	Required
	Dynamic Home Agent Address Discovery		Required
NEMO	MIB		Required
	Home Agent		Not required
	Mobile Router		Required
	Authentication - IPsec		Required
	MIB		Required

Table 3-53: A-ERCS node mobility requirements.

3.6.4 Node Extension level

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node extension mobility requirements			
Mobile IPv6	Home Agent		Not required
	Mobile Node		Required
	Correspondent node support		Optional
	Authentication	IPsec	Required
		Binding Auth.	Required
	Dynamic Home Agent Address Discovery		Required
NEMO	MIB		Required
	Home Agent		Not required
	Mobile Router		Required
	Authentication - IPsec		Required
	MIB		Required

Table 3-54: A-ERCS node extension mobility requirements.

3.6.5 Device level

¹⁸ Home Agent functionality may also be required on an A-ERCS node

A-ERCS segment/capability	Requirement	Details	Status
A-ERCS node Core router mobility requirements			
Mobile IPv6	Home Agent		Required
	Mobile Node		Optional
	Correspondent node support		Optional
	Authentication	IPsec	Required
		Binding Auth.	Required
	Dynamic Home Agent Address Discovery		Optional
NEMO	MIB		Required
	Home Agent		Not required
	Mobile Router		Required
	Authentication - IPsec		Required
A-ERCS node Firewall mobility requirements			
Mobile IPv6	Home Agent		Not required
	Mobile Node		Not required
	Correspondent node support		Not required
	Authentication	IPsec	Not required
		Binding Auth.	Not required
	Dynamic Home Agent Address Discovery		Not required
NEMO	MIB		Not required
	Home Agent		Not required
	Mobile Router		Not required
	Authentication - IPsec		Not required
A-ERCS node router/AP mobility requirements			
Mobile IPv6	Home Agent		Not required
	Mobile Node		Optional
	Correspondent node support		Optional
	Authentication	IPsec	Optional
		Binding Auth.	Optional
	Dynamic Home Agent Address Discovery		Optional
NEMO	MIB		Optional
	Home Agent		Not required
	Mobile Router		Optional
	Authentication - IPsec		Optional
NEMO	MIB		Optional

Table 3-55: A-ERCS device mobility requirements.

3.6.6 Strategic Emergency Control Center

A-ERCS segment/capability	Requirement	Details	Status
SECC mobility requirements			
Mobile IPv6	Home Agent		Required
	Mobile Node		Not required
	Correspondent node support		Optional
	Authentication	IPsec	Required
		Binding Auth.	Required
	Dynamic Home Agent Address Discovery		Required
NEMO	MIB		Required
	Home Agent		Required
	Mobile Router		Not required
	Authentication		Required
	MIB		Required

Table 3-56: SECC mobility requirements.

3.6.7 A-ERCS Mobility Requirements for Backhaul Supported System

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based mobility requirements for Backhaul Supported Systems			
UMTS/HSPA	PDP context	IPv4	Required
		IPv6	Required
		IPv4 and IPv6	Required
LTE	EPS bearer	IPv4	Required
		IPv6	Required
		IPv4 and IPv6	Required
WiFi	No mobility requirements		TBD
Ethernet/FTTH	No mobility requirements		TBD
xDSL	No mobility requirements		TBD
TETRA	No mobility requirements		TBD
DMR	No mobility requirements		TBD
Satellite	No mobility requirements		TBD

Table 3-57: IPv6-based mobility requirements for backhaul supported systems.

3.7 A-ERCS Service Subsystems Design

In this chapter, A-ERCS services subsystem design is described. The design and specification follow the A-ERCS service requirements specified in [1], upgrading the portfolio of the ERCS services specified in Section 2.3. The role of the A-ERCS system in this respect is to act as an overlay solution capable of providing new and additional communication services transparently to already existent ERCS services. Accordingly, the new communication channels are added to the ERCS organization as depicted in Figure 3-8 (please note that the original ERCS organization and chain of command remain unchanged).

As summarized in Table 3-58, the following A-ERCS services are part of this A-ERCS subsystem.

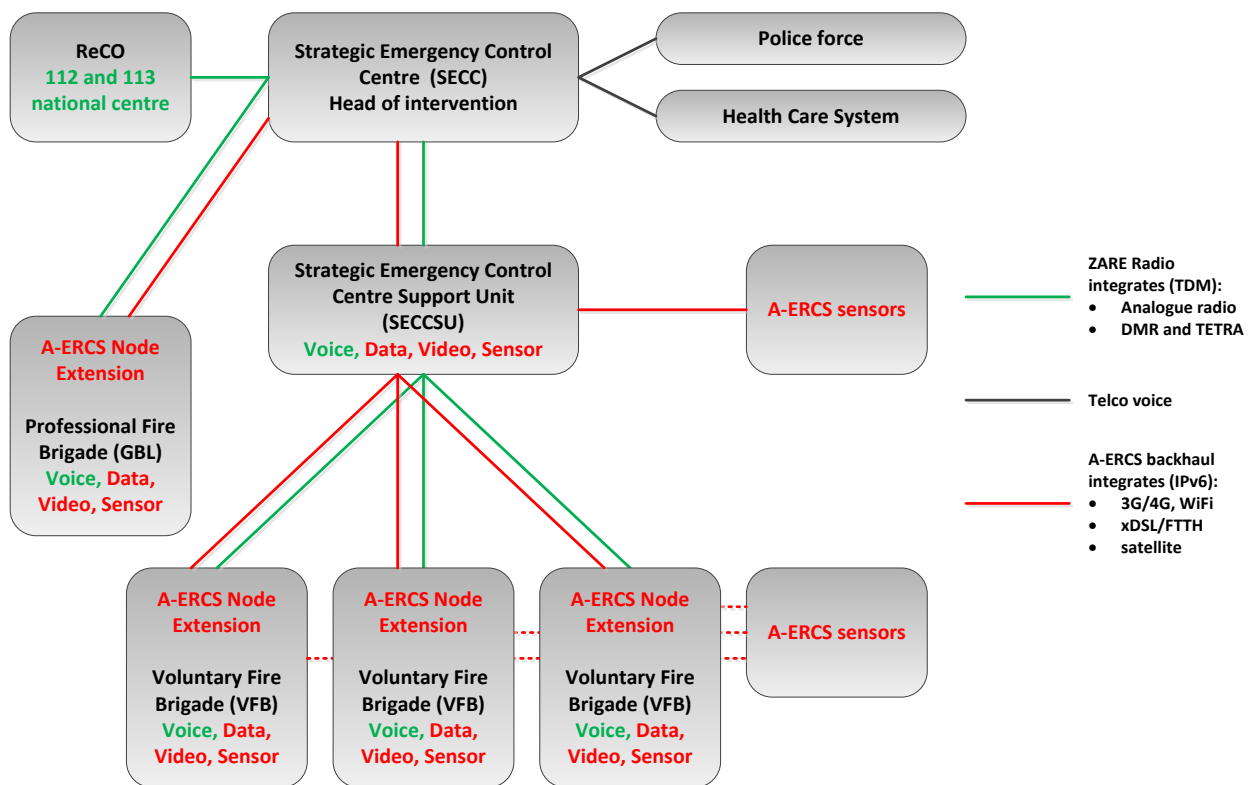


Figure 3-8: Organization and chain of command for intervention procedures involving SECCSU with A-ERCS overlay.

Subsystem for voice services

ZARE voice services, already available in the ERCS, will be supported in the A-ERCS as a standalone service utilizing existent ZARE system and terminal equipment. According to

availability, options for integration of ZARE voice service with the overlay A-ERCS solution will be considered and implemented.

ZARE messaging service is supported in the currently deployed ZARE system but not used within the intervention procedures. The decision for including this service into the A-ERCS service portfolio is again subject to availability of the ZARE system for integration purposes as well as the actual need for such a service in the A-ERCS, which will be decided jointly with OZRCO and SECCSU experts at A-ERCS pilot planning stage.

Based on the overlay A-ERCS system, IP-based voice service will be supported, for communication between the SECCSU and the on-site fire fighter units, and between the SECCSU and the SECC.

Subsystem for data services

In this subsystem, data-based A-ERCS services will be supported, including (but not limited to) messaging service, video streaming service, data transfer, e-mail service and file transfer. All listed services will be available to the SECCSU team. Availability of data services to SECC and on-site fire fighter units is subject to domain-specific strategy and will be decided in the pilot planning stage.

Subsystem for sensors

This is a specialized subsystem, primarily not planned for the A-ERCS in the GEN6 project but added later on due to its strategic importance and value-added differentiation. It covers services based on sensors and the respective sensor data. For example, today during an intervention the on-site fire fighter unit monitors the avalanche situation manually (that is, by observing the level and progression of the problematic terrain). When using the A-ERCS system, a set of avalanche monitoring sensors and an IoT backend system, the fire fighters could have an automatic avalanche alarm system, delivering a message for any important/critical change in the situation.

In the scope of the A-ERCS system, data transmission service is needed to deliver the information, while the sensor service requires a sensor deployment on-site and a backend IoT-based system. There are many deployment options for such a service, concerning:

- the use case scenario; examples interesting for the SECCSU and on-site fire fighters are avalanche monitoring, water level/flooding monitoring, environment monitoring (air quality, noise, pollution, temperature, light etc.), and fire fighter safety control;

- the deployed sensor system on-site; the choice of sensors is subject to the use case scenario, availability of sensor types, cost, ad-hoc or permanent deployment, required mobility of sensors etc.;
- the back-end IoT system providing sensor data aggregation, storage, analysis and visualization, either in real time or as a big data service;
- the end-user interface and type of sensor service; concrete deployment is again subject to use case scenario as well as to domain-specific requirements and limitations, especially taking into consideration an intervention principle that each specific unit and operator must receive only critical information and in a format that corresponds to their communication capabilities (for example, a fire fighter needs water flooding information; a useful service would be an automatic voice call of message delivering current water level every 10 minutes to a ruggedized smartphone terminal; web portal available on a laptop is not an appropriate form in this situation); examples of sensor services are:
 - an automated voice call based alarming service for on-site fire fighters via VoIP service,
 - an automated messaging alarming service for on-site fire fighters via data-based messaging service,
 - a web portal with sensor data statistics and visualizations available via smartphones, laptops and tablets for the SECCSU unit.

For A-ERCS pilot purposes, a centralized web portal has already been experimentally designed and implemented (gen6.ltfe.org), as shown on Figure 3-9. It offers data aggregation, statistical analyses and visualizations for the following sensors under test:

- environment sensors including butane gas sensors, humidity sensors and temperature sensors, used to monitor the environment in the proximity of a fire fighter in order to assure safe and healthy conditions;
- water level sensor and water temperature sensors as an example of a specialized sensor network implementation for on-site conditions monitoring; and
- environment noise sensors, that can be used for personal environment monitoring as well as for crowds monitoring and situation/conditions monitoring.

Subsystem for management

This subsystem covers primarily internal SECCSU services, required for efficient on-site intervention coordination and reporting. For the time being, no integrated ERCS services are

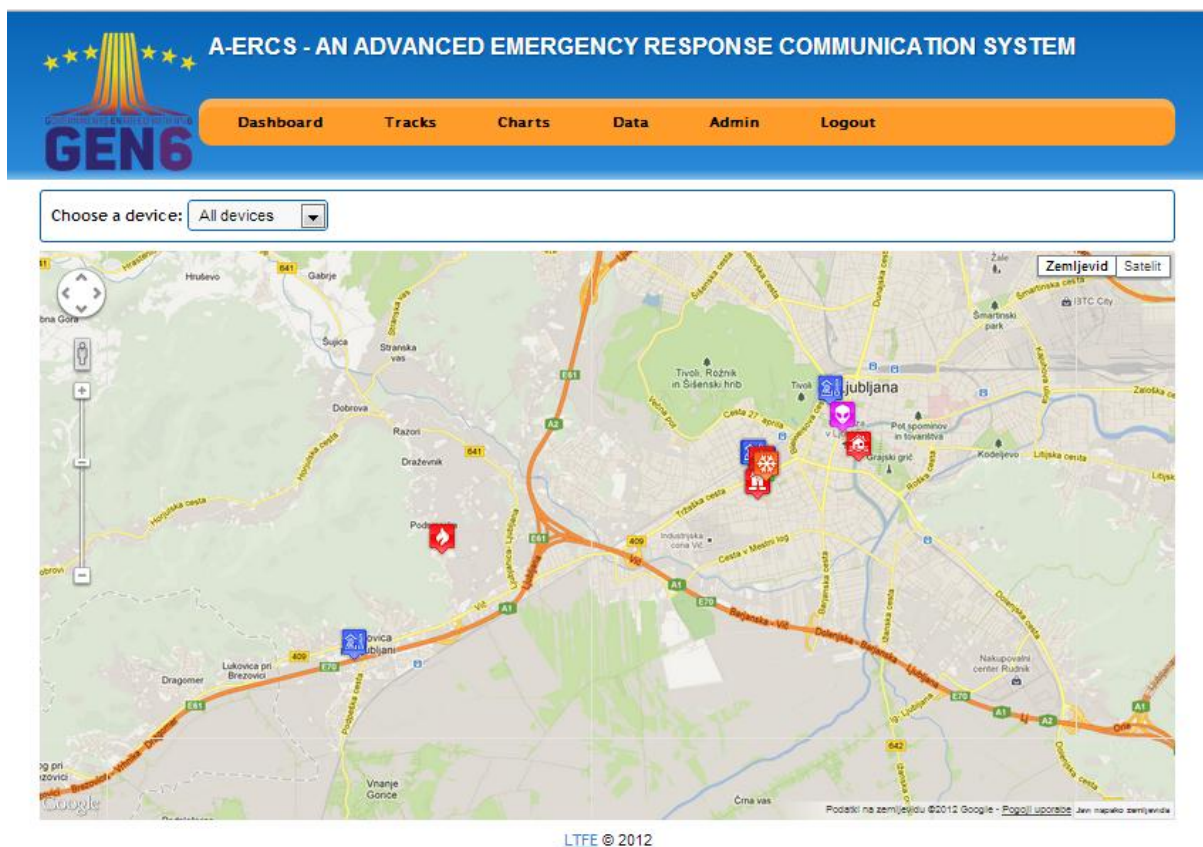
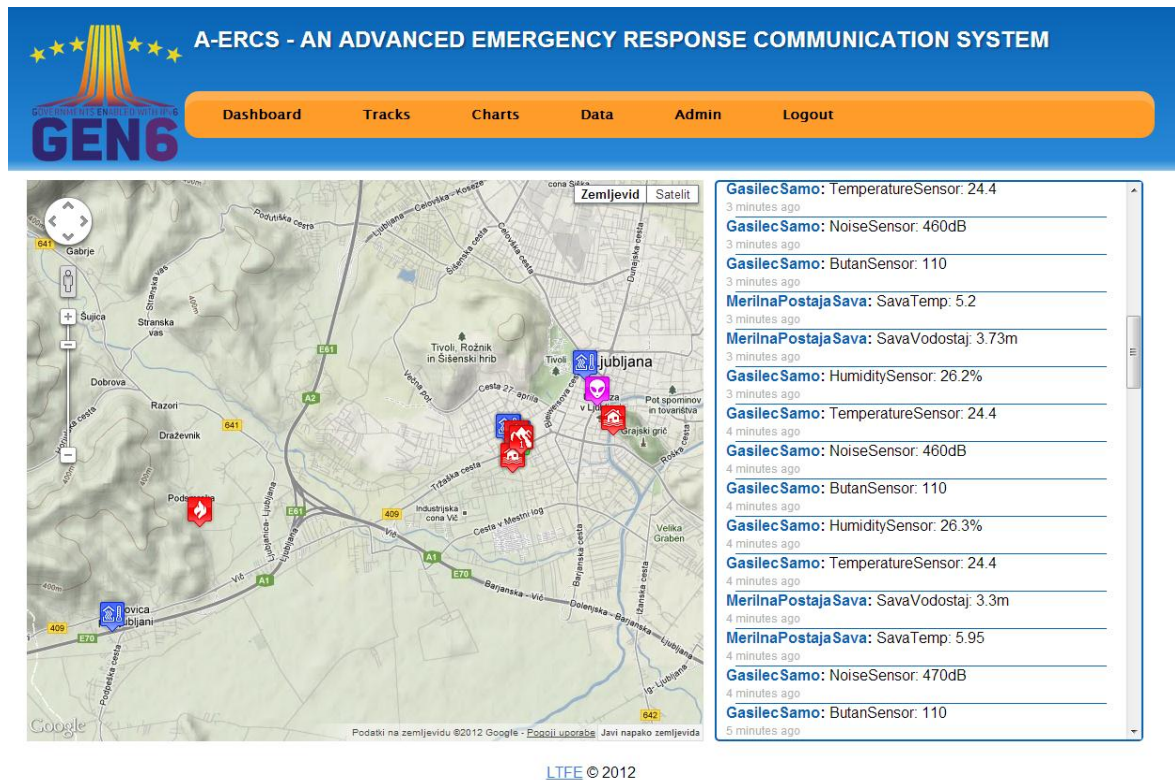
available for this purpose. The A-ERCS will provide for such data-based services, for example inventory, operation reporting service etc. Concrete choice of services and their design are subject to further use case scenario planning in tight cooperation with the SECCSU team.

Also, an additional data services group included in this subsystem are services based on the SECC infrastructure. For the time being, ERCS supports RAKI, dispatcher tool and ICS services, which are available to the SECC. In the upcoming stages, options for integration of these services into the A-ERCS system and their availability to the SECCSU will be considered.

A-ERCS segment/capability	Elements/features/capabilities	Status
Supported services		
SECCSU operator in operation	ZARE voice	Existent
	ZARE messaging	Existent, not in use
	VoIP	Planned
	Messaging	Planned
	Video streaming	Planned
	Data transfer	Planned
	E-mail	Planned
	File transfer	Planned
	Transfer of sensor data	Planned
	Other (applications, data sharing, etc.)	Planned
Fire fighter team	ZARE voice	Existent
	VoIP	Planned
	Video streaming	Planned
	Data transfer	Planned
Other	RAKI (JGS equipment registry)	Existent, not integrated with the ERCS
	ICS (communications and management tool for major interventions)	Existent, not integrated with the ERCS
	Dispatcher tool	Existent, not integrated with the ERCS
	Management services	Planned

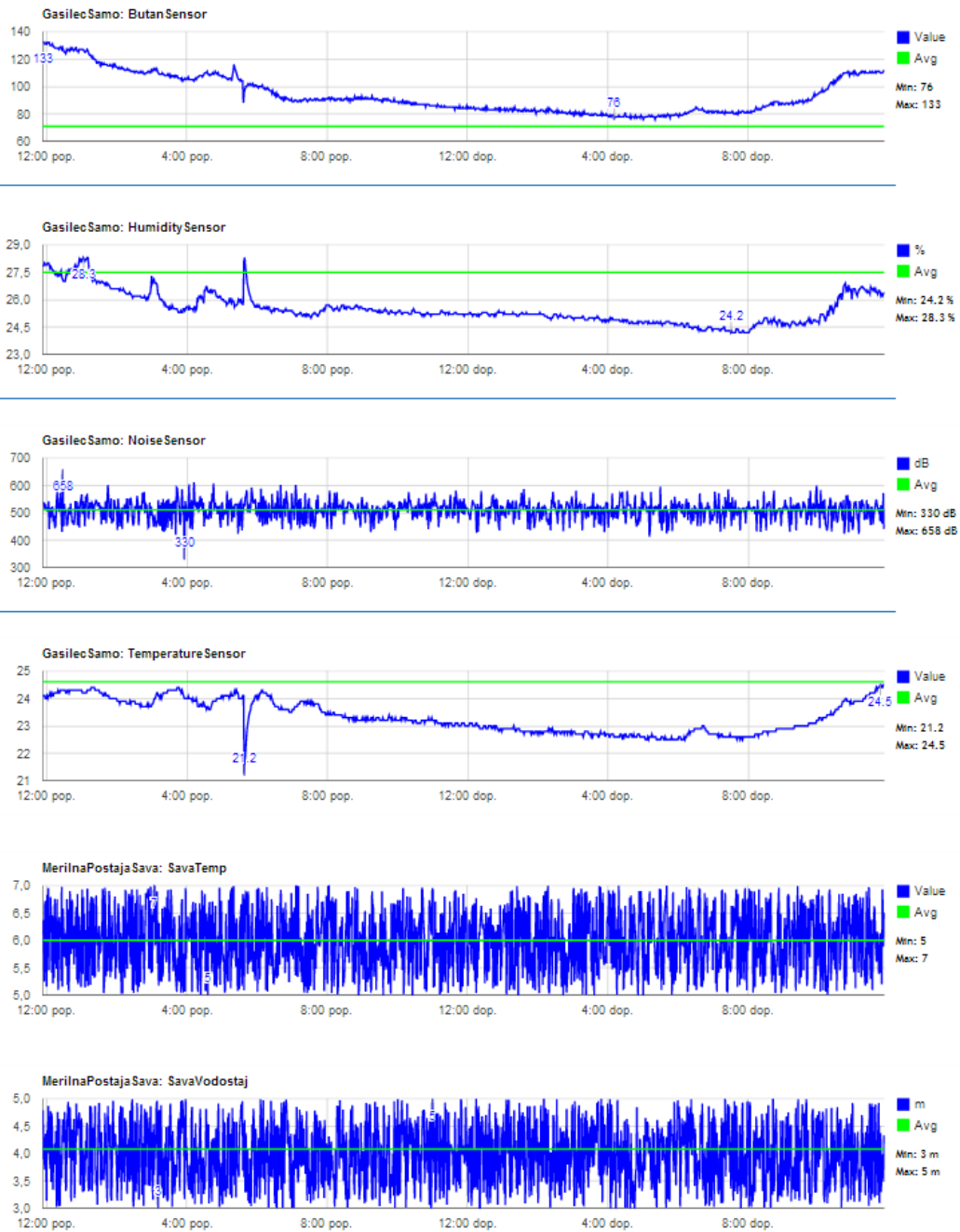
Table 3-58: A-ERCS services overview.


Further use case scenarios and service specifications will be completed in the upcoming system and services design and specification stages as well as during A-ERCS pilot planning.





Choose a device:





A-ERCS - AN ADVANCED EMERGENCY RESPONSE COMMUNICATION SYSTEM

[Dashboard](#)
[Tracks](#)
[Charts](#)
[Data](#)
[Admin](#)
[Logout](#)

Choose a device: All devices

ID	Device name	Sensor name	Sensor type	Sensor value	Sensor timestamp	Server timestamp
602252	GasilecSamo	HumiditySensor	Humidity	26.3		1355914428
602251	GasilecSamo	TemperatureSensor	Temperature	24.5		1355914418
602250	GasilecSamo	NoiseSensor	Noise	581		1355914408
602249	GasilecSamo	ButanSensor	Butan	112		1355914398
602248	GasilecSamo	HumiditySensor	Humidity	26.3		1355914388
602247	MerilnaPostajaSava	SavaTemp	temperatura	6.5		1355914388
602246	MerilnaPostajaSava	SavaVodostaj	vodostaj	4.33		1355914388
602245	GasilecSamo	TemperatureSensor	Temperature	24.5		1355914378
602244	GasilecSamo	NoiseSensor	Noise	453		1355914368
602243	GasilecSamo	ButanSensor	Butan	112		1355914358
602242	GasilecSamo	HumiditySensor	Humidity	26.4		1355914348
602241	GasilecSamo	TemperatureSensor	Temperature	24.5		1355914337
602240	MerilnaPostajaSava	SavaTemp	temperatura	5.89		1355914327
602239	MerilnaPostajaSava	SavaVodostaj	vodostaj	3.49		1355914327
602238	GasilecSamo	NoiseSensor	Noise	441		1355914327
602237	GasilecSamo	ButanSensor	Butan	111		1355914317
602236	GasilecSamo	HumiditySensor	Humidity	26.3		1355914307
602235	GasilecSamo	TemperatureSensor	Temperature	24.5		1355914297
602234	GasilecSamo	NoiseSensor	Noise	479		1355914287
602233	GasilecSamo	ButanSensor	Butan	110		1355914277
602232	MerilnaPostajaSava	SavaVodostaj	vodostaj	3.99		1355914268
602231	MerilnaPostajaSava	SavaTemp	temperatura	6.58		1355914268
602230	GasilecSamo	HumiditySensor	Humidity	26.3		1355914267
602229	GasilecSamo	TemperatureSensor	Temperature	24.5		1355914256
602228	GasilecSamo	NoiseSensor	Noise	572		1355914246
602227	GasilecSamo	ButanSensor	Butan	110		1355914236
602226	GasilecSamo	HumiditySensor	Humidity	26.2		1355914226
602225	GasilecSamo	TemperatureSensor	Temperature	24.4		1355914216
602224	MerilnaPostajaSava	SavaVodostaj	vodostaj	3.92		1355914208
602223	MerilnaPostajaSava	SavaTemp	temperatura	6.93		1355914208
602222	GasilecSamo	NoiseSensor	Noise	595		1355914206
602221	GasilecSamo	ButanSensor	Butan	109		1355914196
602220	GasilecSamo	HumiditySensor	Humidity	26.2		1355914186
602219	GasilecSamo	TemperatureSensor	Temperature	24.4		1355914176
602218	GasilecSamo	NoiseSensor	Noise	460		1355914166
602217	GasilecSamo	ButanSensor	Butan	110		1355914155
602216	MerilnaPostajaSava	SavaTemp	temperatura	5.2		1355914147
602215	MerilnaPostajaSava	SavaVodostaj	vodostaj	3.73		1355914147
602214	GasilecSamo	HumiditySensor	Humidity	26.2		1355914145
602213	GasilecSamo	TemperatureSensor	Temperature	24.4		1355914135
602212	GasilecSamo	NoiseSensor	Noise	460		1355914125
602211	GasilecSamo	ButanSensor	Butan	110		1355914115
602210	GasilecSamo	HumiditySensor	Humidity	26.3		1355914105

Figure 3-9: gen6.lfe.org web portal for sensor applications.

4 PILOTING AND TESTING A-ERCS ENVIRONMENT

The A-ERCS objective is not only to deliver an experimental proof of concept but an actual production A-ERCS system directly applicable into practice. This, in addition to following the domain-specific design and implementation guidelines, requires a compact and ruggedized system implementation with integrated modules for transparent backhaul connectivity. For this purpose, first pilot implementations and testing have already started as a preparation phase for the upcoming A-ERCS implementation and demonstration.

4.1 A-ERCS pilot testing environment

Figure 4-1 represents a pre-testing environment set up in the Laboratory for telecommunications. It is based on a QoE system developed by ULFE for QoS and QoE measurements of IP-based data services via fixed and mobile systems using the global Internet infrastructure. The A-ERCS system interconnected via the available fixed and mobile backhaul supported system towards the Internet will represent the System Under Test (SUT).



Figure 4-1: A-ERCS SUT – pre-testing environment.

Using the QoE system, the A-ERCS pilot will be tested using the following KPIs.

- SUT response time
 - PING RTT [ms]
 - WEB download time [ms]
 - DNS response time [ms]
- SUT service speed
 - WEB speed [Kbit/s]
 - Download Speed [Kbit/s]
 - Upload Speed [Kbit/s]
- SUT service availability
 - DNS service availability [%]
 - PING response Availability [%]
 - WEB service availability [%]

In addition, initial QoE measurements of the available backhaul supported systems have already been completed following the above methodology. In the following, reference results for 4 QoE clients connected to different backhaul supported systems on fixed locations (ULFE, go6 Lab) completed in the period July – October 2012 are shown.

Figure 4-2 summarizes reference QoE measurements for global Internet services based on IPv4 and IPv6. In the following, Figure 4-3 to Figure 4-7 show dashboards of QoE measurement results for fixed backhaul supported systems, considered for use in the A-ERCS pilot implementation and demonstration.

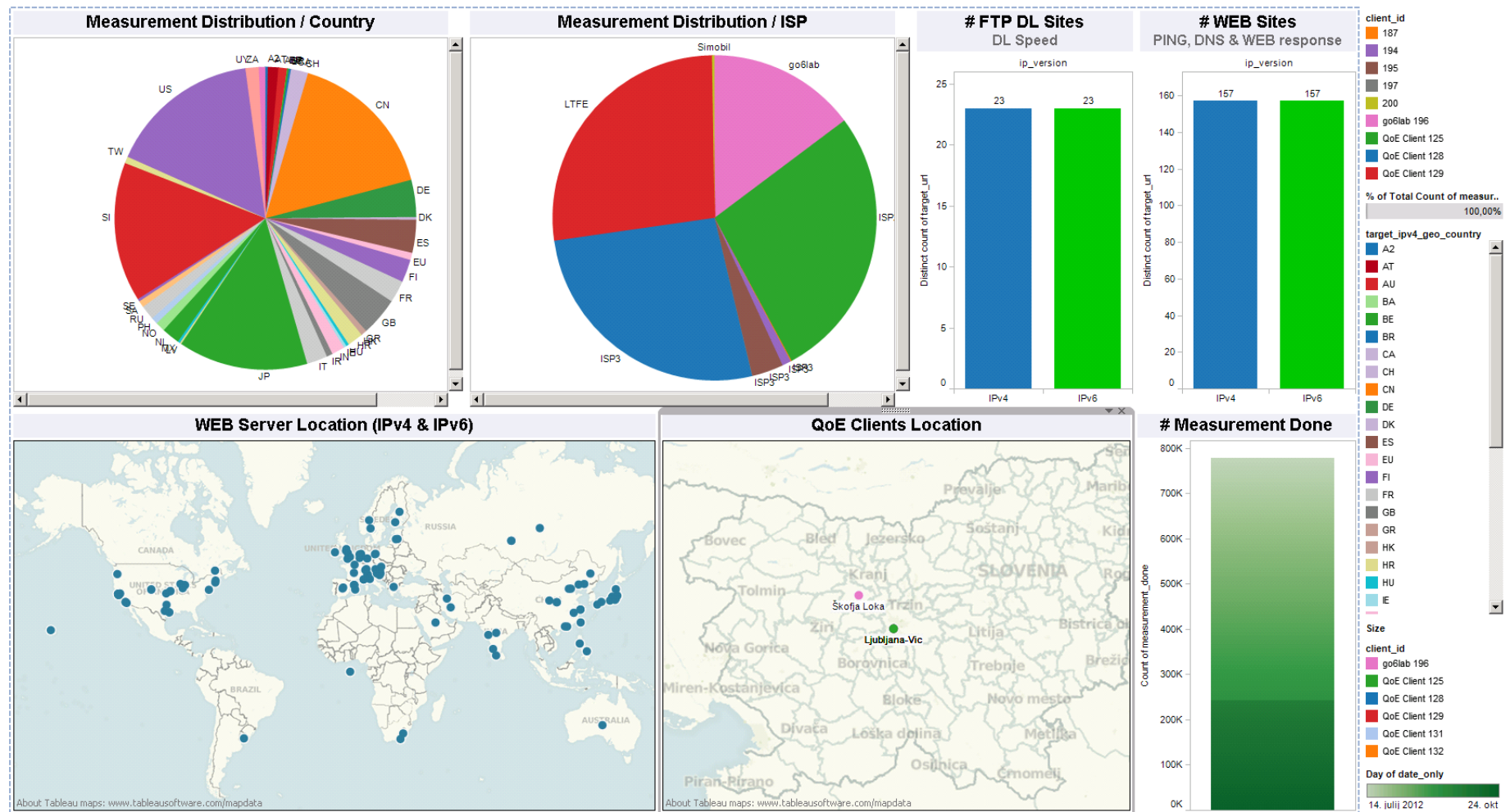


Figure 4-2: Reference QoE measurements for global Internet – general statistics.

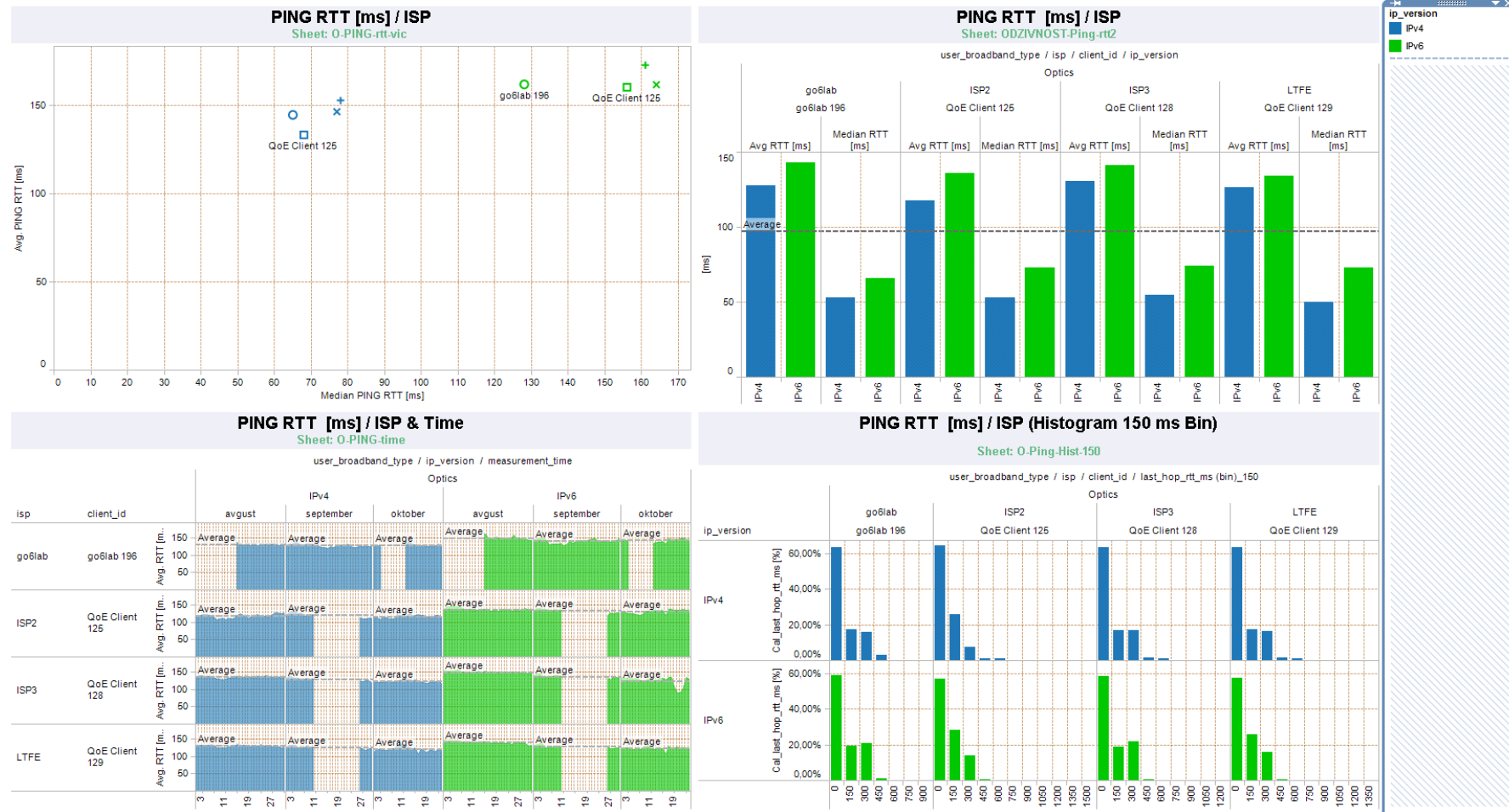


Figure 4-3: Dashboard of results for PING RTT measurements of global Internet services.

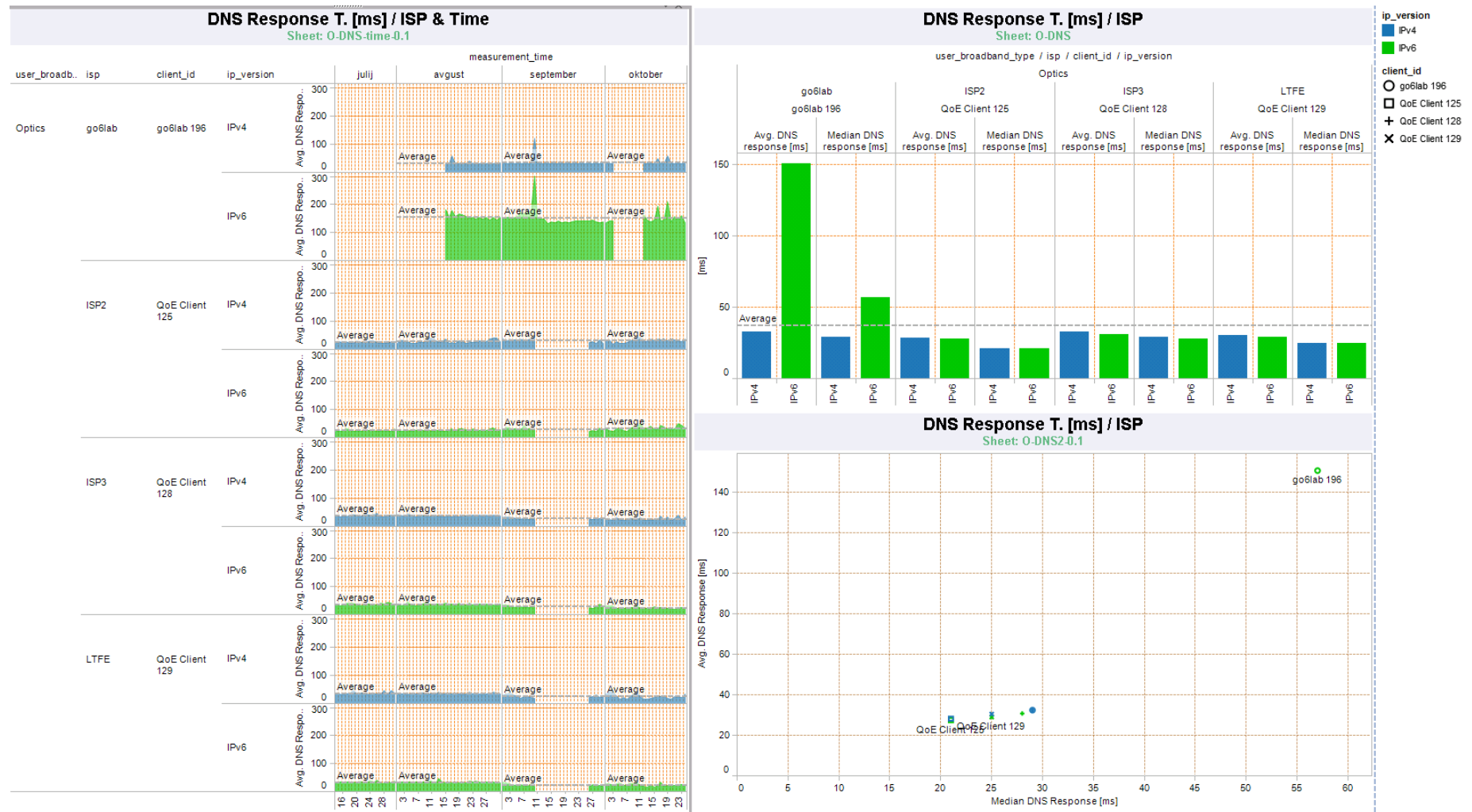


Figure 4-4: Dashboard of results for DNS measurements of global Internet services.



Figure 4-5: Dashboard of results for WEB response time measurements of global Internet services.

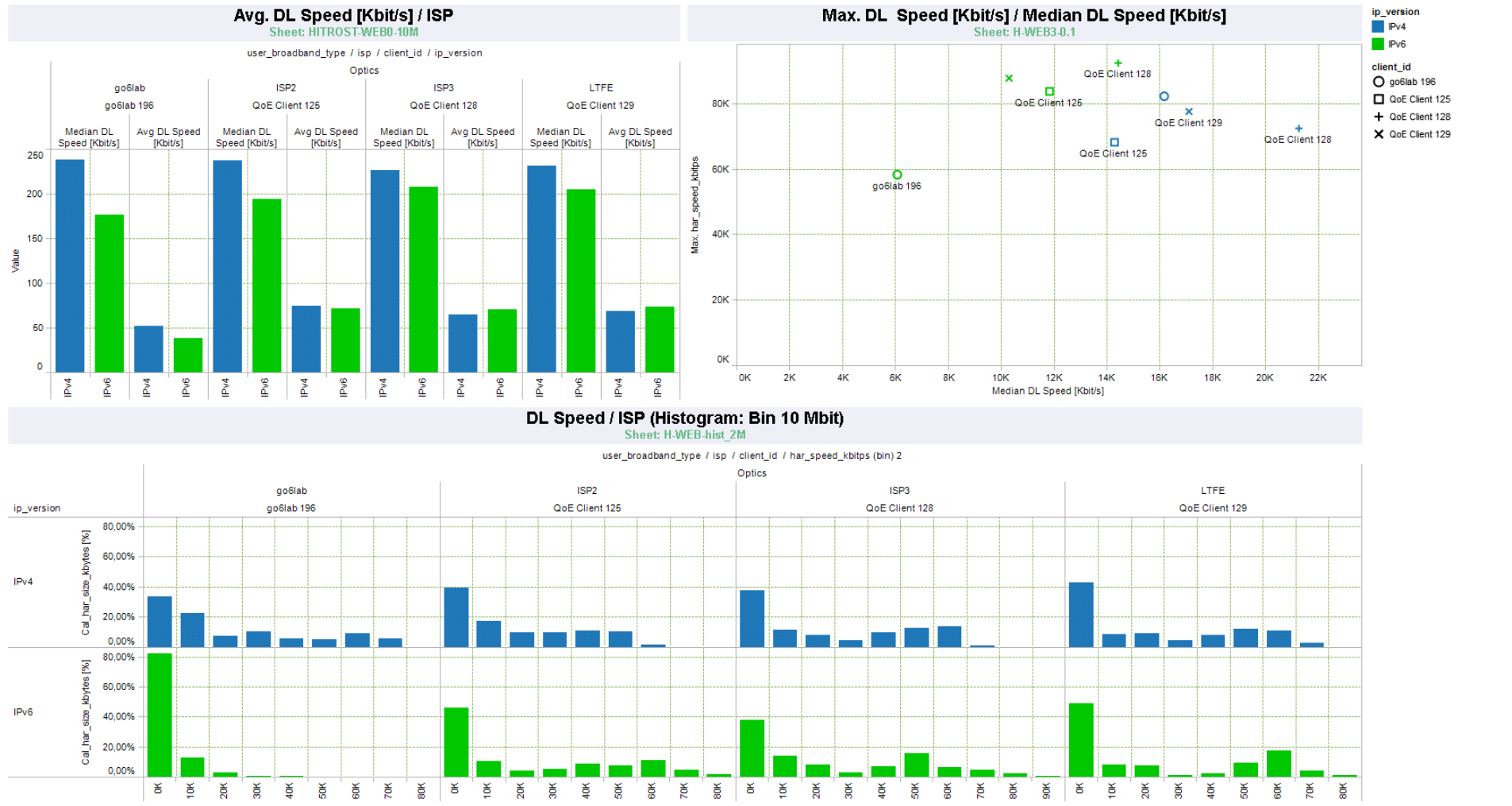


Figure 4-6: Dashboard of results for DL speed measurements of global Internet services.

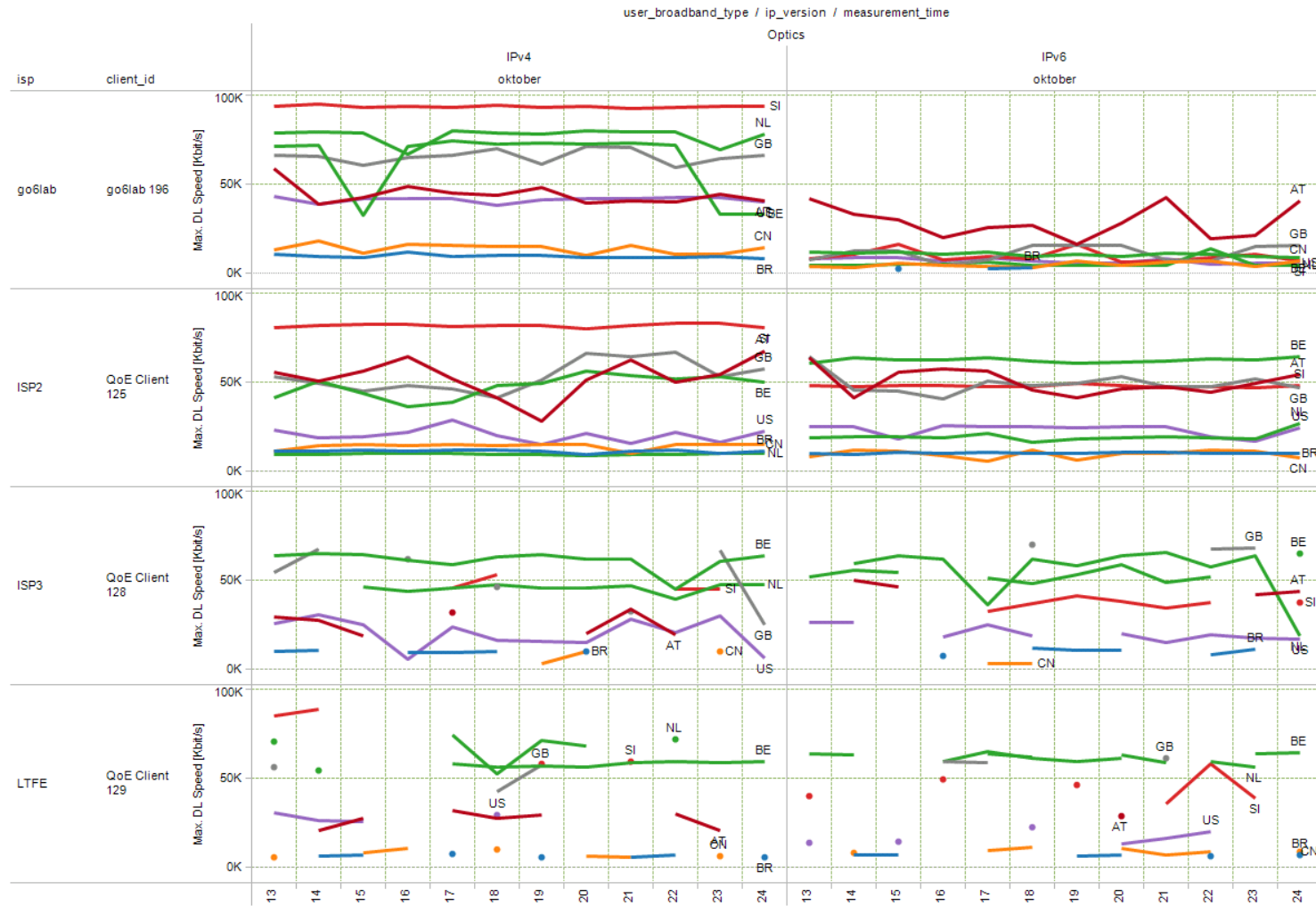


Figure 4-7: Dashboard of results for Max DL speed measurements of global Internet services.

For mobile backhaul supported systems measurements, the presented QoE measurements system was additionally extended with GPS probe, which enables measurement tagging per QoE client with location data. Next, QoE measurement using three mobile probes were completed. The deployed QoE system is displayed in Figure 4-8. The measurements were completed on a highway between Ljubljana and Kranj, Slovenia, at an approximate speed of 130 km/h. Some selected snapshots of the results are shown on Figure 4-9 and Figure 4-10.



Figure 4-8: Upgraded mobile QoE measurement system deployed in a civil vehicle, showing the GPS probe (above), three QoE probes for parallel measurements of three competitive HSPA mobile networks (below left), and DC/AC power supply transformation for the QoE probes (below right) .

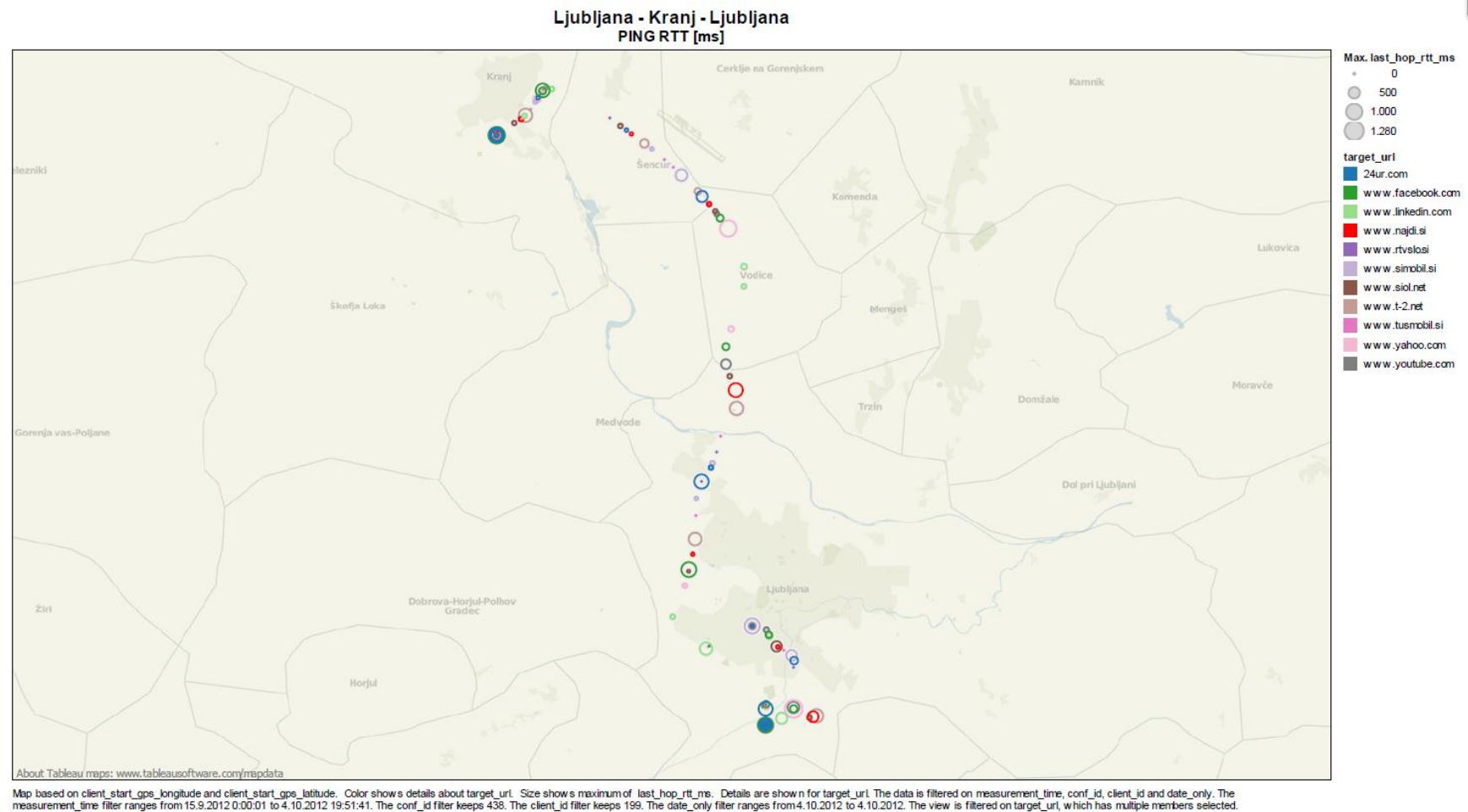


Figure 4-9: PING RTT [ms] tagged with GPS coordinates.

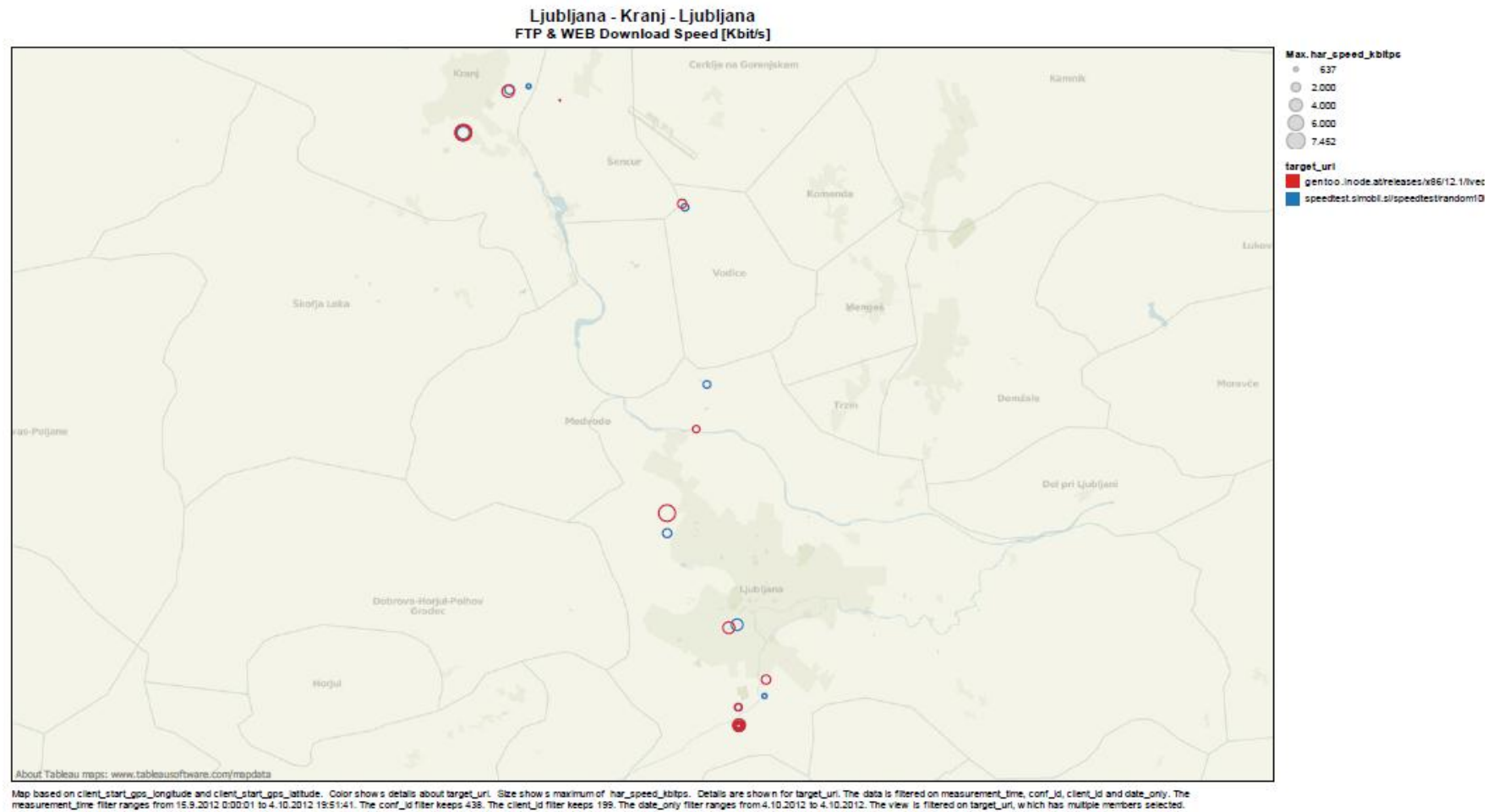


Figure 4-10: Results for FTP and Web DL speed [Kbit/s] measurement tagged with GPS coordinates.

The above pre-testing results show two important findings.

IPv4 and IPv6 technologies in the fixed backhaul supported systems are mature according to the initial QoE measurement results. However, there is a complex challenge of providing a solution integrating fixed and mobile backhaul supported systems with IPv6 in a compact integrated node. Identifying this upcoming challenge, efforts are currently dedicated to resolving the network equipment availability with integrated 3G/4G, WiFi, serial and Ethernet interfaces, in cooperation with the committed technology partners. In the long run, the solution to this challenge is the use of LTE as the mobile node and the backhaul supported system, which supports IPv6 by default.

In conclusion, the above findings only intensify the importance and added value of the A-ERCS efforts in terms of technological challenges and market potential, and are an additional motivator for the successful delivery and demonstration of the A-ERCS pilot.

5 CONCLUSIONS

The Slovenian pilot, Advanced Emergency Response Communication System (A-ERCS), represents a unique effort in terms of national IPv6 pilots in this project by addressing IPv6 communication needs of a specific domain, that is, a fire fighter unit utilizing communications on field during an intervention.

Following the A-ERCS system and services requirements, this deliverable represents the results of the second stage towards the A-ERCS pilot establishment and demonstration, documenting A-ERCS system architecture and technical specifications. In summary, it provides system design and technical specifications, focusing on architecture, addressing scheme, QoS and policy enforcement, security, routing, mobility, and services subsystem. Under each aspect, several different levels are addressed, that is, system level, node level, node extension level, strategic emergency control centre level, backhaul supported system, and device level. IPv6 functionalities and features supported in all A-ERCS segments was the core aspect of the design and specifications.

Usability, reliability and added value services in the context of emergency response interventions is one of the core aspects and a guiding topic of the A-ERCS. Therefore, A-ERCS system and services design was completed in close collaboration with all technological stakeholders. Domain-specific aspects were addressed jointly with the SECCSU and OZRCS teams with a general tendency to provide realistic and usable system and services. Existent ERCS infrastructure, and intervention services organization and chain of command were studied, followed by A-ERCS design as an overlay system. This will allow in further for a transparent A-ERCS infrastructure implementation without any disturbances or outages in the existent operational ERCS system and services, as specifically required by the OZRCS. Telekom Slovenije and ARNES provided valuable inputs regarding IPv6 aspects of the system and use of backhaul supported systems. In cooperation with Cisco, technology, networking and communication features in terms of IPv6 support were studied and first proof of concept implementations in laboratory environments were already completed by ULFE.

This specification is a result of on-going work towards A-ERCS pilot establishment and demonstration. In the upcoming stages of the A-ERCS efforts, the presented specifications will be further evolved and specified jointly with the A-ERCS pilot planning activities.

An additional objective, set out by ULFE for the A-ERCS system is to make an effort towards

297239	GEN6	D 3.8.1: A-ERCS system specification
--------	------	--------------------------------------

delivering not only a proof of concept pilot for experimental use but a production A-ERCS system directly applicable into practice. This, in addition to following the above mentioned domain-specific design and implementation guidelines, requires a compact and ruggedized system implementation with integrated modules for transparent backhaul connectivity. For this purpose, an initial test environment has been set up as a preparation stage for the A-ERCS pilot implementation. The results show two important findings, namely, the maturity of the backhaul technologies IPv4 and IPv6 on one side, and a complex challenge of providing a compact and integrated solution for the addressed specific domain on the other side. This together even intensifies the importance and added value of the A-ERCS efforts in terms of technological challenges and market potential, and is an additional motivator for the successful delivery and demonstration of the A-ERCS pilot.

6 REFERENCES

[1]	Requirements analysis for A-ERCS, GEN6, ULFE, Deliverable D3.4, 27/4/2012, http://www.gen6.eu/docs/deliverables/GEN6_PU_D3_4_v1_4.pdf .
[2]	Post and Electronic Communications Agency of the Republic of Slovenia , A report of the development of electronic communication market for Q1 2011 (Poročilo o razvoju trga elektronskih komunikacij za prvo četrtletje 2011) http://www.apek.si/datoteke/File/2011/telekomunikacije/Poro%C4%8Dilo_Q1_2011.pdf
[3]	IPv6 Address Prefix Reserved for Documentation, http://tools.ietf.org/html/rfc3849
[4]	Republic of Slovenia, Ministry of Defence, Administration for civil protection and relief, telecommunications system: ZARE communication system; http://www.sos112.si/eng/page.php?src=pr12.htm
[5]	IETF RFC 2080, "RIPng for IPv6"; http://datatracker.ietf.org/doc/rfc2080/
[6]	IETF RFC 5308, "Routing IPv6 with IS-IS"; http://datatracker.ietf.org/doc/rfc5308/
[7]	GEN6, ULFE, Requirement Analysis for A-ERCS; http://www.gen6.eu/docs/deliverables/GEN6_PU_D3_4_v1_4.pdf
[8]	IETF RFC 4552, "Authentication/Confidentiality for OSPFv3"; http://datatracker.ietf.org/doc/rfc4552/
[9]	IETF RFC 4302, "IP Authentication Header"; http://datatracker.ietf.org/doc/rfc4302/
[10]	IETF RFC 4303, "IP Encapsulating Security Payload (ESP)"; http://datatracker.ietf.org/doc/rfc4303/
[11]	IETF RFC 5925, "The TCP Authentication Option"; http://datatracker.ietf.org/doc/rfc5925/
[12]	IETF RFC 2385, "Protection of BGP Sessions via the TCP MD5 Signature Option"; http://datatracker.ietf.org/doc/rfc2385/
[13]	IETF RFC 3776, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents"; http://datatracker.ietf.org/doc/rfc3776/
[14]	IETF RFC 6101, "The Secure Sockets Layer (SSL) Protocol Version 3.0"; http://datatracker.ietf.org/doc/rfc6101/
[15]	IETF RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2"; http://datatracker.ietf.org/doc/rfc5246/
[16]	IETF RFC 4253, "The Secure Shell (SSH) Transport Layer Protocol"; http://datatracker.ietf.org/doc/rfc4253/

[17]	IETF RFC 3411, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks"; http://datatracker.ietf.org/doc/rfc3411/
[18]	IETF RFC 2818, "HTTP Over TLS"; http://datatracker.ietf.org/doc/rfc2818/
[19]	IETF RFC 2865, "Remote Authentication Dial In User Service (RADIUS)"; http://datatracker.ietf.org/doc/rfc2865/
[20]	IETF RFC 4511, "Lightweight Directory Access Protocol (LDAP): The Protocol"; http://datatracker.ietf.org/doc/rfc4511/
[21]	IEEE 802.1X-2010, "Port-based Network Access Control"; http://www.ieee802.org/1/pages/802.1x-2010.html
[22]	IETF RFC 5340, "OSPF for IPv6"; http://datatracker.ietf.org/doc/rfc5340/
[23]	IETF RFC 5838, "Support of Address Families in OSPFv3"; http://datatracker.ietf.org/doc/rfc5838/
[24]	IETF RFC 5187, "OSPFv3 Graceful Restart"; http://datatracker.ietf.org/doc/rfc5187/
[25]	IETF RFC 5820, "Extensions to OSPF to Support Mobile Ad Hoc Networking"; http://datatracker.ietf.org/doc/rfc5820/
[26]	IETF RFC 4271, "A Border Gateway Protocol 4 (BGP-4)"; http://datatracker.ietf.org/doc/rfc4271/
[27]	IETF RFC 4760, "Multiprotocol Extensions for BGP-4"; http://datatracker.ietf.org/doc/rfc4760/
[28]	IETF RFC 6198, "Requirements for the Graceful Shutdown of BGP Sessions"; http://datatracker.ietf.org/doc/rfc6198/
[29]	IETF RFC 4601, "Protocol Independent Multicast – Sparse Mode (PIM-SM) Protocol Specification"; http://datatracker.ietf.org/doc/rfc4601/
[30]	IETF RFC 3956, "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address"; http://datatracker.ietf.org/doc/rfc3956/
[31]	IETF RFC 4607, "Source-Specific Multicast for IP"; http://datatracker.ietf.org/doc/rfc4607/
[32]	IETF RFC 2710, "Multicast Listener Discovery (MLD) for IPv6"; http://datatracker.ietf.org/doc/rfc2710/
[33]	IETF RFC 3710, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6"; http://datatracker.ietf.org/doc/rfc3810/
[34]	IETF RFC 4604, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast"; http://datatracker.ietf.org/doc/rfc4604/

[35]	IETF RFC 6275, "Mobility Support in IPv6"; http://datatracker.ietf.org/doc/rfc6275/
[36]	IETF RFC 3963, "Network Mobility (NEMO) Basic Support Protocol"; http://datatracker.ietf.org/doc/rfc3963/
[37]	IETF RFC 2475, "An Architecture for Differentiated Services"; http://datatracker.ietf.org/doc/rfc2475/
[38]	IETF RFC 3344, "IP Mobility Support for IPv4, Revised"; http://datatracker.ietf.org/doc/rfc5944/
[39]	IETF RFC 5213, "Proxy Mobile IPv6"; http://datatracker.ietf.org/doc/rfc5213/
[40]	IETF RFC 5555, "Mobile IPv6 Support for Dual Stack Hosts and Routers"; http://datatracker.ietf.org/doc/rfc5555/
[41]	IETF RFC 4862, "IPv6 Stateless Address Autoconfiguration"; http://datatracker.ietf.org/doc/rfc4862/
[42]	RFC 3315, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"; http://datatracker.ietf.org/doc/rfc3315/
[43]	RFC 3736, "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6"; http://datatracker.ietf.org/doc/rfc3736/

7 APPENDIX 1: LETTERS OF SUPPORT



Mestna občina
Ljubljana
Mestna uprava

Oddelek za
zaščito, reševanje
in civilno obrambo

Zamkova 3
1000 Ljubljana
telefon: 01 306 43 30
faks: 01 306 43 47
glavna.pisarna@ljubljana.si
www.ljubljana.si

Number: 843-38/2012-1
Date: 5.10.2012

SUBJECT: LETTER OF INTENT

Governments ENabled with IPv6 (GEN6, CIP-ICT-PSP-2011-297239)

This is to confirm that **The City of Ljubljana, Disaster Management Department** officially expresses interest in implementation and results of the Slovenian pilot Advanced Emergency Response Communications System (A-ERCS), representing a part of the European project Governments ENabled with IPv6 (GEN6, CIP-ICT-PSP-2011-297239) and under responsibility of the University of Ljubljana, Faculty of Electrical Engineering, Laboratory for telecommunications.

The City of Ljubljana, Disaster Management Department is involved in one projects in the field of emergency response systems and disaster relief, that is ANDROID (ANDROID is an Erasmus academic network that aims to promote co-operation and innovation among European Higher Education to increase society's resilience to disasters of human and natural origin. The network's teaching and research is concerned with what resilience is, what it means to society, and how societies might achieve greater resilience in the face of increasing threats from natural and human induced hazards. The network will create a European approach that will help us understand the attributes that enable physical, socio-cultural, politico-economic and natural systems to adapt, by resistance or changing, in order to reach and maintain an acceptable level of functioning. The network will also raise awareness and promote a common understanding among stakeholders of the importance of disaster resilience education and the essential role of European HEIs in improving society's ability to increase disaster resilience), the experience and knowledge of which are related to the research domain addressed with the A-ERCS system, therefore representing opportunity for knowledge transfer as well as continuation to achieve joint contributions in the domain.

The City of Ljubljana, Disaster Management Department will support University of Ljubljana, Faculty of Electrical Engineering, Laboratory for Telecommunications throughout the implementation of the project GEN6 in advisory, technical and demonstrational capacities as an expert on technical, operational and interoperability issues in civilian crisis management. It will offer their expertise and actively participate in project planning and implementation, providing domain-specific inputs, advice and assessment for emergency response systems as well as support and active participation in demonstration and promotion activities with their technical staff and infrastructure.

We remain at your disposal for any information you may require.

Sincerely,



Head of the Disaster management Department of the City of Ljubljana


Robert KUS, M.Sc.
Head of the Disaster management Department of the City of Ljubljana

TelekomSlovenije

University of Ljubljana
Faculty of Electrical Engineering
Laboratory for telecommunications
Tržaška c. 25
1000 Ljubljana
Slovenia

Ljubljana, 4.11.2012

LETTER OF SUPPORT

We would like to express our interest and full support for execution and delivery of the results of the Slovenian pilot Advanced Emergency Response Communications System (A-ERCS), representing a part of the European project Governments ENabled with IPv6 (GEN6, CIP-ICT-PSP-2011-297239) and under responsibility of University of Ljubljana, Faculty of Electrical Engineering, Laboratory for telecommunications.

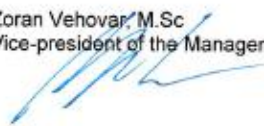
Communications solutions for professional environments using latest networking technologies and advanced mobile and wireless architectures is a strategic focus of Telekom Slovenije, d.d., and is included in corporate and research objectives in the forthcoming period. Implementations and piloting of IPv6-based technologies and converged communication services with IoT enhancements in emergency response environments are of increasing importance and therefore of our long-term interest.

Therefore, we confirm to participate in the external non-beneficiary stakeholder group of the Slovenian pilot A-ERCS of the GEN6 project, holding an active role of a wireless telco operator and service provider. We will make available to the Slovenian A-ERCS team services and support in the LTE/HSPA/UMTS and fixed networks for the purpose of the A-ERCS pilot implementation, testing and evaluation (including free use of connectivity services, system and service configuration adjustments and technical support during the duration of the GEN6 project).

We are looking forward to cooperating with you.

Yours sincerely,

Zoran Vehovar, M.Sc.
Vice-president of the Management board



TelekomSlovenije
d.d.




Telekom Slovenije, d.d., Cigaletova 15, 1000 Ljubljana, phone: +386 1 234 10 00, www.telekom.si