Title: **Deliverable D3.4** **Requirement Analysis for A-ERCS**	**Document Version:** 1.4

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

Contractual Delivery Date: 30/04/2012	**Actual Delivery Date:** 05/05/2012	**Deliverable Type* - Security**:** R – PU

* 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: Janez Sterle	**Organization:** ULFE	**Contributing WP:** WP3

Authors (organisations):

Mojca Volk (ULFE), Jan Žorž (ULFE), Luka Koršič (ULFE), Luka Mali (ULFE), Dušan Mulac (ULFE), Jože Hanc (SECCSU), Matej Cerk (Water Science Institute).

Abstract:

This deliverable summarizes the requirements and guidelines identified for the establishment of the A-ERCS pilot. The analysis captures state of the art regarding the technologies and solutions in the field of A-ERCS systems, current status of the systems that are subject to implementation and upgrades in the A-ERCS pilot, and architectural, functional, technological and service requirements for the pilot implementation and operation.

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	27/2/2012	Document creation	Janez Sterle (ULFE)
v0.2	14/3/2012	Table of contents and initial inputs	Janez Sterle (ULFE)
v1.0	2/3/2012	First Draft	Mojca Volk (ULFE)
v1.1	20/4/2012	Document for internal review	Mojca Volk (ULFE)
v1.2	23/04/2012	Internal Review	Onur BEKTAŞ (ULAKBİM)
v1.3	24/04/2012	Final corrections	Mojca Volk (ULFE)
v1.4	04/05/2012	Final Review	Jordi Palet (Consulintel)

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 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.

A major phase in designing and implementing such a pilot is the requirements analysis study. This deliverable includes identification and analysis of aspects relevant to IPv6 introduction in the A-ERCS pilot with clear definition and planning of possible services, as well as initial guidelines and analyses for A-ERCS pilot planning, design and specification.

In summary, in-depth system requirements are specified. A high-level A-ERCS architecture is presented followed by requirement analysis of the following segments: local and backhaul connectivity, self-x functionalities, automatic network planning and deployment, routing and mobility, and seamless connectivity. Also, service requirements analysis is included, covering the following aspects: general A-ERCS service requirements, specification of target service scenarios, reuse of existent services, and aspects of urgency, security, reliability and QoS. Specific attention is given to service planning and prioritization as required by the specified service scenarios.

One of the main goals of the A-ERCS activities is to provide added value and usable services for civil protection and fire fighting purposes. Therefore, to prepare realistic A-ERCS requirements analysis, proprietary fire fighter unit requirements were taken into consideration. Domain specific requirements are studied in-depth along with an analysis of current systems and services available to the fire fighter unit, representing the basis for the implementation of the A-ERCS pilot.

The requirements study was completed in close collaboration of all involved internal and external stakeholders, foremost in close cooperation with the Strategic Emergency Control Centre Support Unit (SECCSU), with an attempt to gather realistic requirements that will serve as the core input into the A-ERCS system and services design and planning.

Table of Contents

Figure Index

Table Index

1. INTRODUCTION

An Advanced Emergency Response Communication System (A-ERCS) represents a vision of convergent, reliable and smart communication system designed specifically for professional use in emergency situations. Such examples are interventions and rescue missions, where different civil protection units vitally rely on communication during an on-site operation, for instance fire fighter units, medical rescue teams, military armed forces, police units etc.

Today, civil protection services are reluctant to use the latest communication technologies for the reasons of extremely high communication reliability, priority and robustness requirements throughout the operation. These requirements are in the sense of instant service operation (e.g. continuous voice communication without interruptions and downtime) and robustness of the communication system in the event of major catastrophes (e.g. operational communication system after a major earthquake or flooding). In the face of such stringent preconditions, so far only professional solutions have been able to provide appropriate capabilities and features while disregarding commercial networks, primarily for the following reasons.

1. Professional systems are specifically designed to provide autonomous and highly reliable communication services in extreme conditions; the downside, however, is the fact that such systems are typically based on well-established and proven technologies such as analogue/DMR radio and TETRA with rather low transmission rates, which represents a major bottleneck when envisioning advanced communication services. Also, technologically unfamiliar systems are typically proprietary silos systems with minimal or no interconnectivity support.

2. Commercial communication systems are designed for reliable operation in normal conditions and under normal load. In extreme conditions, such as massive natural catastrophes (for instance earthquakes, tsunamis etc.) or other huge events when people tend to use services massively (e.g. a massive traffic accident in an urban area), the commercial communication systems cannot be relied upon due to overload, failures or outages.

3. User prioritization requires appropriate techniques and mechanisms implemented in the network as well as an appropriate business scheme. So far, the majority of commercial communication systems have not supported data communication prioritization for data services either for technical or business reasons. With the adoption of modern mobile communication technologies, service prioritization for data transmission has become easily facilitated (e.g. by appropriate EPS bearer class definitions in the LTE/EPC network). However, appropriate service and user profiling and prioritization schemes are yet to be adopted, requiring detailed specifications of

normal and critical operation scenarios.

4. In extreme conditions and when an intervention is underway, professional users require instant service operation without the need for any kind of manual system or service setup or configuration. In the face of this requirement, professional services can be provided in a single professional system (typically silos) that is carefully designed and preconfigured to be able to deliver the required service operation in extreme conditions and by utilizing an extremely reliable and ruggedized communication path to assure high availability (e.g., a professional satellite system able to survive major earthquake catastrophe). An alternative option, however, is a heterogeneous system with high availability features assured through utilization of a variety of communication channels, together able to survive the extreme conditions (e.g., a combined TETRA and satellite system); in this case, automated intelligence is required to assist in appropriate communication channel/system selection and configuration. For the time being, such systems are rare, remain strictly in the professional domain and do not combine professional and commercial networks to provide connectivity.

The focus of the A-ERCS pilot activities is to design, implement and demonstrate a communication system that provides different communication services for a fire fighter unit during an on-site intervention. The aim of our efforts 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.

1.1 Vision

Our vision, driving the A-ERCS efforts, 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.

The aim of the A-ERCS pilot is to clearly demonstrate the state-of-the-art IPv6-enabled features in emergency response environments. More specifically, the A-ERCS pilot will demonstrate:

- A scalable and robust overlay system for data transport and rich multimedia service built across both professional (e.g. DMR, TETRA, Satellite) and 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, and self-organization and self-healing characteristics.
- 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.

A major phase in designing and implementing such a pilot is the requirements analysis study. This deliverable includes identification and analysis of aspects relevant to IPv6 introduction in the A-ERCS pilot with clear definition and planning of possible services and available networks. To do so, domain specific requirements are studied in-depth along with an analysis of current systems and services available to the fire fighter unit that represent the basis for the implementation of the A-ERCS pilot.

For better understanding of this document, first a general overview of the envisioned A-ERCS system is briefly represented in the following chapter. Next, emergency response communication system and services requirements are studied in-depth, focusing on various IPv6-related aspects that are of relevance when designing a reliable, resilient and multimedia-rich communication system. Characteristics of the available live pilot field environment are analysed to identify all major preconditions relevant to pilot design and deployment. Specific attention is given to proprietary requirements of the target user group and the targeted environment defining the communication conditions, that is, a fire fighter unit communicating during an on-site intervention in the case of a major catastrophe. In conclusion, key findings are drawn that represent the basis for the A-ERCS system design and definition of communication services scenarios tailored to bring added value to the fire fighter unit.

1.2 General A-ERCS system and services overview

1.2.1 The A-ERCS pilot ecosystem

Throughout this project, several external stakeholders will be involved in activities related to the design, deployment and demonstration of the A-ERCS pilot aside and in cooperation with the official partner ULFE.

All A-ERCS activities will be performed in close collaboration and for the purposes of use 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 (URSZR). More precisely, the A-ERCS node will be designed for and deployed in a specialized vehicle in use by the **Strategic Emergency Control Centre Support Unit (SECCSU)** of the VFB. 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. The operating SECCSU team is equipped with a professional communication system ZARE currently supporting only narrowband voice services during the intervention (analogue/DMR-based professional mobile radio system for voice communications). Additionally, the vehicle is equipped with Internet connectivity for situation surveillance purposes (exchange of intervention reports, weather forecast updates and water flow level information). The major role of the SECCSU in the A-ERCS activities will be to help in defining particular A-ERCS pilot requirements, implementation of the pilot A-ERCS unit in the SECCSU vehicle, and A-ERCS pilot demonstration and testing.

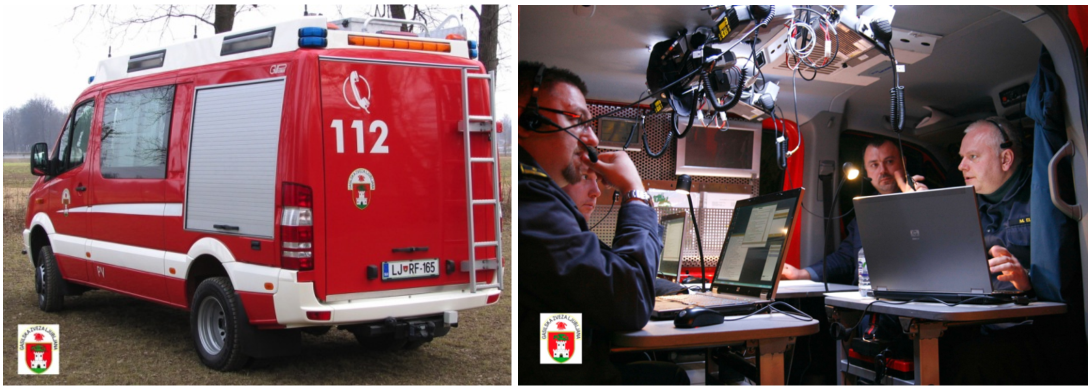


Figure 1-1: Strategic Emergency Control Centre Support Unit SECCSU vehicle

On the application side of the A-ERCS pilot, the project activities will be carried out in collaboration with the Water Science Institute that will provide valuable knowledge of the specific service requirements in the fire fighter domain, assist in identifying service-side A-ERCS pilot requirements, defining service scenarios and perform A-ERCS pilot demonstration and testing.

In order to deploy the A-ERCS system pilot, and more specifically to successfully implement the A-ERCS node in the SECCSU vehicle using professional networking equipment, Cisco Slovenia will be contributing to the project as an external technology partner providing the necessary networking equipment and assisting in the A-ERCS pilot deployment by providing appropriate technical support.

To deploy the A-ERCS pilot operating over both professional and commercial communication systems, two additional external stakeholders will be involved in the project activities. Eion Wireless will be a technology partner for the local and backhaul wireless backhaul domain, specializing in WiFi, WiMAX and microwave technologies, and will be providing wireless solution support throughout the A-ERCS system design, implementation and testing. Another technology partner will be a Slovenian mobile operator representing the commercial networks domain. The operator will contribute 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.

Throughout the project, the go6 Institute will offer 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.

1.2.2 The A-ERCS system description

A high-level structure of the A-ERCS system is depicted in Figure 1-2. As depicted, the aim of the A-ERCS system is to integrate the following separate domains into a unified and converged emergency response infrastructure (bottom to top):

- An on-site fire fighter unit using an **A-ERCS mobile device** for communication throughout the intervention among members of the on-site unit as well as with the Strategic Emergency Control Centre Support Unit (SECCSU).
- The SECCSU unit located in a specialized vehicle, responsible for 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.
- An A-ERCS Strategic Emergency Control Centre 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.

As indicated, all A-ERCS system segments are IPv6 enabled.

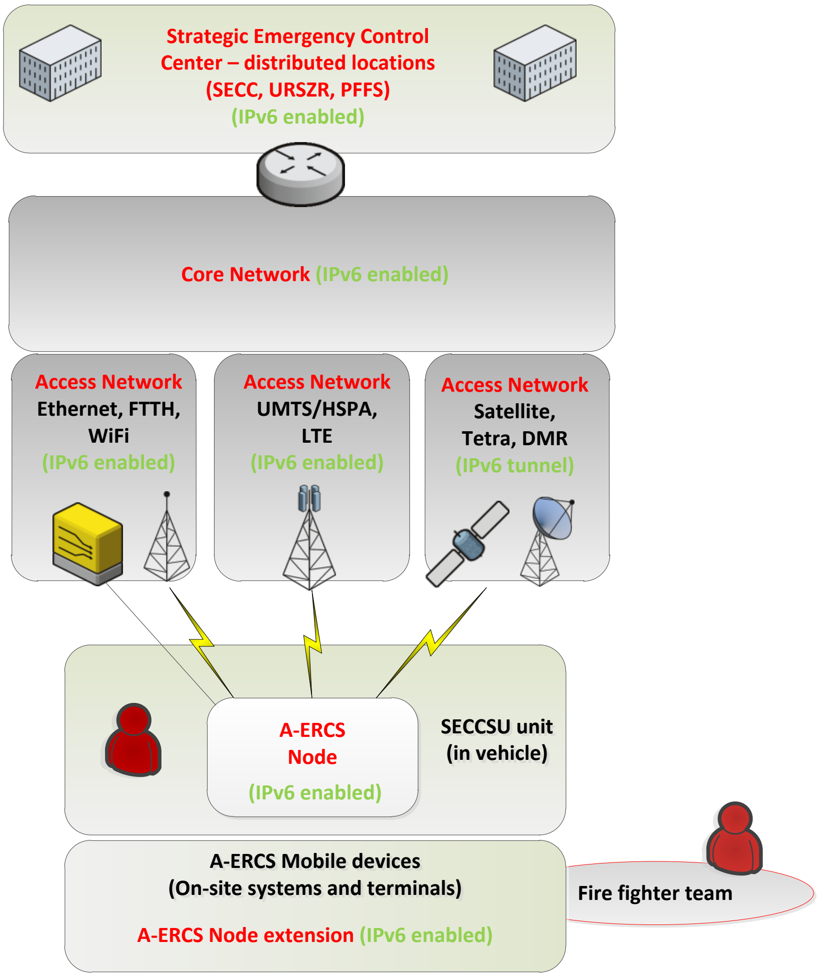


Figure 1-2: High-level A-ERCS system overview

1.2.3 A-ERCS node

A more detailed A-ERCS system architecture is represented in Figure 1-3. The core of the solution represents the A-ERCS node located in the SECCSU vehicle. Its role is to assist the SECCSU unit to communicate 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.).
- 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.

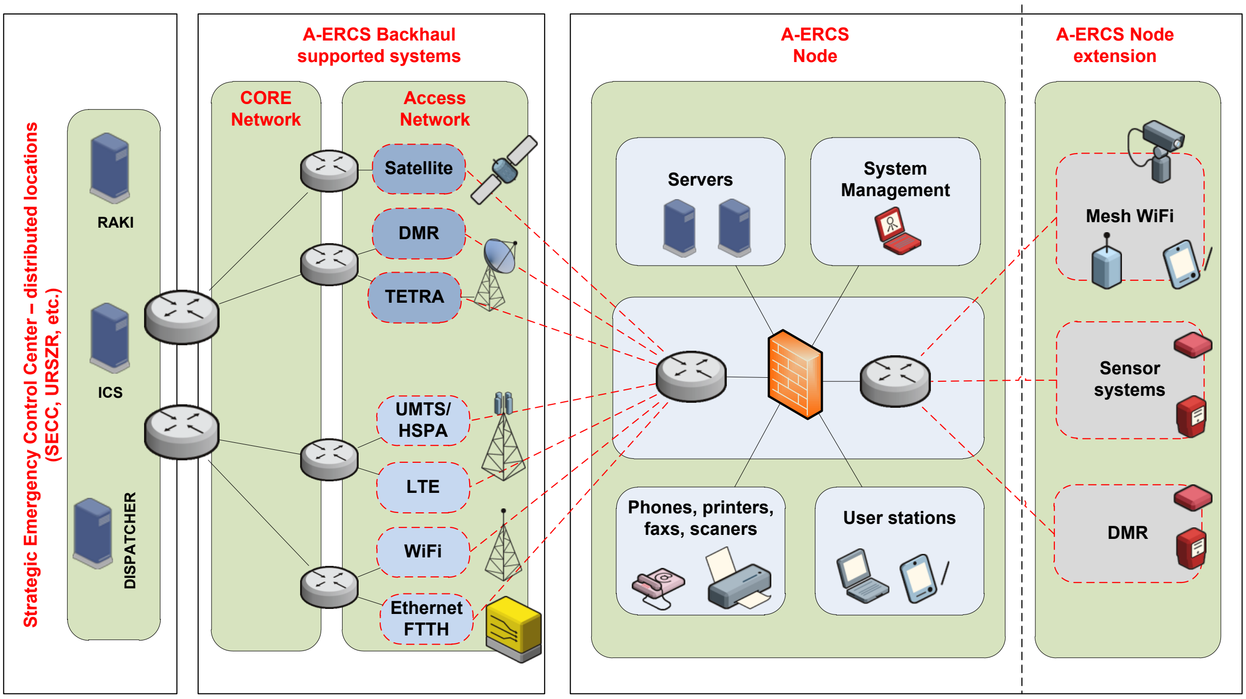


Figure 1-3: A-ERCS system architecture

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 briefly described in the following sections.

1.2.3.1 A-ERCS Node Architecture

The high-level A-ERCS node architecture is represented in Figure 1-4. 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. 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.

The Core Firewall provides the following functionalities:

- Central security endpoint for user and service flow control, stateless and stateful 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.

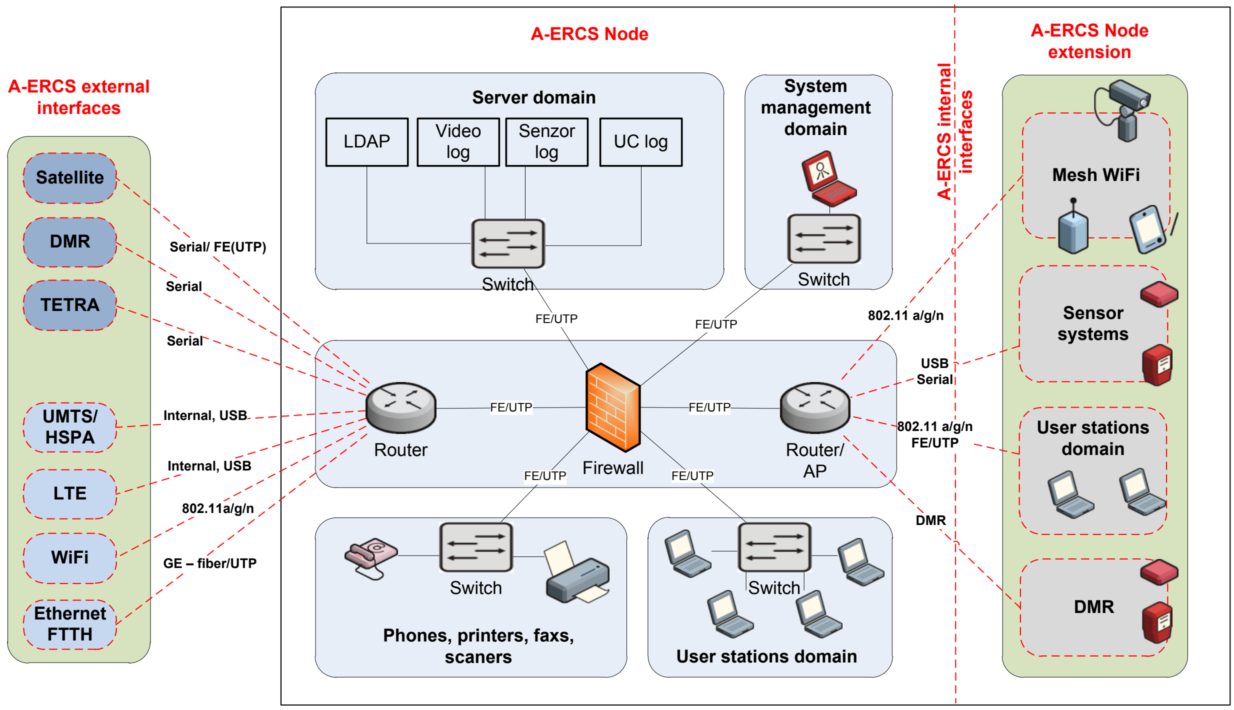


Figure 1-4: A-ERCS node architecture

1.2.4 Backhaul capabilities

The A-ERCS system will support three types of backhaul network connectivity, that is, through professional and commercial communication networks as well as alternative ad-hoc setup communication systems.

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 chapter 4.1.

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 support IPv6 PDP context setup. Further details are available in chapter 4.2.

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 chapter 4.3.

2. A-ERCS System Requirements Analysis

2.1 Basic requirements for A-ERCS node functionalities

Based on the brief A-ERCS system and A-ERCS node descriptions provided in chapter 1.2, basic A-ERCS system, service and node requirements are collected in this chapter. From the IPv6 viewpoint, the requirements are subject to the implementation of the Core Router and Core Firewall of the A-ERCS node as well as use of available networks for connectivity purposes. However, some other general requirements are also outlined that represent a vital step in defining the A-ERCS pilot as a whole.

2.1.1 General A-ERCS pilot requirements

General A-ERCS pilot requirements summarize the key elements of the A-ERCS system that the pilot is required to introduce into the existent live pilot field environment. The analysis focuses on IPv6 aspects bearing in mind that for the time being no IPv6 capabilities are enabled in the environment.

A-ERCS segment/capability	Requirement	Status
A-ERCS system segments introduced into the live pilot field environment		
Local segment		
On-site segment (A-ERCS node extensions)	ZARE radio	Existent
	A-ERCS Mobile Device (based on analogue/ZARE radio)	Required
	Sensor systems	Optional
	Other (local on-site WiFi, video camera systems, etc.)	Required
SECCSU vehicle (A-ERCS node)	ZARE system	Existent
	Core Router	Required
	Core Firewall	Required
	User stations domain	Required
	Other (phones, printers, faxes, scanners)	Required
	Server domain	Required
	System management domain	Required
Backhaul access network domain		
Commercial mobile networks	UMTS/HSPA	Required
	LTE	Optional
Professional networks	TETRA	Optional
	ZARE system	Existent
	Satellite	Optional
Alternative networks	Ethernet	Optional
	FTTH	Optional
	WiFi	Required
	xDSL	Required
Backhaul core network domain		

SECC	Dispatch centre	Optional
	Integrated Communication System (ICS)	Optional
	Inventory database (RAKI)	Existent

Table 2-1: A-ERCS system segments introduced into the live pilot field environment

A-ERCS segment/capability	Requirement	Status
A-ERCS services introduced into the live pilot field environment		
Local segment		
On-site segment (A-ERCS node extensions to A-ERCS node)	ZARE voice	Existent
	Digital voice	Required
	ZARE messaging	Optional
	Messaging	Required
	Video streaming	Optional
	Data transfer	Required
	Sensor data transfer	Optional
SECCSU vehicle (A-ERCS node to SECC)	ZARE voice	Existent
	ZARE messaging	Optional
	Digital voice	Required
	Messaging	required
	Video streaming	Optional
	Data transfer	Required
	E-mail	Optional
	File transfer	Optional
	Other (applications, data sharing, etc.)	Optional

Table 2-2: A-ERCS services introduced into the live pilot field environment

A-ERCS segment/capability	Requirement	Status
A-ERCS pilot segments with required IPv6 support (IPv6-enabled)		
Local segment		
On-site segment (A-ERCS node extensions)	A-ERCS Mobile Device	Required
	Sensor systems	Optional
	Other (local on-site WiFi, video camera systems, etc.)	Required
SECCSU vehicle (A-ERCS node)	Core Router	Required
	Core Firewall	Required
	User stations domain	Required
	Other (phones, printers, faxes, scanners)	Required
	Server domain	Required
	System management domain	Required
Backhaul access network domain		
Commercial mobile networks	UMTS/HSPA	Required
	LTE	Optional
Professional networks	TETRA	Optional
	DMR	Required
	Satellite	Optional
Alternative networks	Ethernet	Optional

	FTTH	Optional
	WiFi	Required
	xDSL	Required
Backhaul core network domain		
SECC	Dispatch centre	Optional
	Integrated Communication System (ICS)	Optional
	Inventory database (RAKI)	Required

Table 2-3: A-ERCS pilot segments with required IPv6 support (IPv6-enabled)

2.1.2 Requirements for Core Router functionalities

Note that requirements summarized in this chapter are defined into detail in latter chapters of this document.

A-ERCS segment/capability	Requirement	Status
Core Router functionalities		
Dynamic unicast and multicast routing support	Internal Unicast forwarding and routing based on OSPFv3and RIP-ng routing protocols	Required
	External unicast forwarding and routing based on MP-BGP	Required
	Multicast forwarding and routing based on SSM model (PIM-SM, PIM-SSM)	Required
	Multicast signalization for endpoint and intermediate devices based on MLDv1 and MLDv2	Required
Packet filtering based on L2, L3 and L4 protocol information	e.g. VLAN ID, CoS, DSCP, FlowLabel, source/destination IPv6 address, transport protocol filters for UDP and TCP etc.	Required
Policing rules and QoS functionalities based on DiffServ model	Packet classification in DSCP service classes, based on L2, L3 and L4 information	Required
	Policing and shaping in input and output interface direction	Required
	Packet marking in DSCP field, COS and VLAN ID field	Required
	Packet prioritisation and scheduling (e.g. FIFO, PQ, WRR, LLQ queuing models)	Required
Mobility and Tunnel endpoint support	LMA, MAG and HA functionality	Required
	GTP protocol termination	Required
	PPP over serial termination	Required
	PPPoE termination	Required
	PMIP/GRE termination	Required
SLAAC and DHCPv6 support	RA mode	Required
	DHCPv6 relay mode	Required

Table 2-4: Requirements for Core Router functionalities of the A-ERCS node

2.2 Analysis of Local (ad-hoc) and backhaul connectivity principles

The purpose of the A-ERCS system is to provide twofold connectivity:

- Between the fire fighter unit performing the intervention and the SECCSU.
- Between SECCSU and SECC.

As a result, the A-ERCS node is required to provide:

- On-site (local) connectivity between the A-ERCS node in the SECCSU vehicle and the devices used on site (ref. Figure 1-4) using the following technologies:
    - mesh WiFi (802.11a/g/n) for data connectivity to devices (video cameras, PDAs, tablets, etc.) and user station domain,
    - USB serial for connectivity with sensor systems,
    - DMR and analogue radio;
- Backhaul connectivity to provide connectivity between SECCSU and SECC or when the SECCSU is not located on site also between SECCSU and devices used on site, using the following technologies:
    - satellite,
    - DMR and analogue radio,
    - TETRA,
    - UMTS/HSPA,
    - LTE,
    - WiFi,
    - Ethernet
    - FTTH,
    - xDSL.

In this chapter, high-level local and backhaul connectivity principles are defined, followed by more detailed requirements specifications and definitions in the following chapters, separately for commercial, professional and alternative ruggedized COTS networks.

A-ERCS segment/capability	**Requirement**	**Status**
A-ERCS node connectivity (interface) requirements		
Backhaul connectivity technologies		Required
Professional networks	Satellite (serial/FE(UPT)	Optional
	DMR and analogue radio (serial)	Required
	TETRA (serial)	Optional
Commercial networks	UMTS/HSPA (internal, USB)	Required
	LTE (internal, USB)	Optional

	WiFi (802.11a/g/n)	Required
	Ethernet/FTTH (GE-fiber/UTP)	Optional
On-site connectivity technologies		Required
Mesh WiFi network	WiFi (802.11a/g/n)	Required
Sensor systems	USB serial connectivity	Optional
User station domain	WiFi (802.11a/g/n), FE/UPT	Required
DMR users	DMR and analogue radio (serial)	Required

Table 2-5: A-ERCS node connectivity requirements

2.2.1 Requirements for on-site and backhaul network capabilities

A-ERCS segment/capability	Requirement	Status
Backhaul network capabilities		
Backhaul over professional networks (DMR, analogue radio, TETRA, satellite or other)	IPv6 and IPv4 transport over tunnelling mechanisms (PPP, GRE, …)	Required
Backhaul over commercial networks (UMTS/HSPA, LTE, WiFi)	Native IPv6 (IPv6 PDP context)	Required
	IPv4 (IPv4 PDP context)	Required
	Dual stack support (IPv4 and IPv6 PDP context)	Required
Backhaul over xDSL/FTTH	Native IPv6 (IPv6 over PPPoE, IPv6 over Ethernet)	Required
	IPv4 (IPv4 over PPPoE, IPv4 over Ethernet)	Required
	Dual stack support (IPv6/IPv4 over PPPoE, IPv6/IPv4 over Ethernet)	Required

Table 2-6: Requirements for backhaul network capabilities

A-ERCS segment/capability	Requirement	Status
On-site network capabilities		
DMR and analogue radio	Serial	Required
WiFi Mesh	Native IPv6 (IPv6 over Ethernet)	Optional
	IPv4 (IPv4 over Ethernet)	Optional
	Dual stack support (IPv6/IPv4 over Ethernet)	Optional
Sensor systems	TBD	Optional

Table 2-7: Requirements for on-site network capabilities

2.3 Analysis of Self-organizing, self-healing and auto-configuration network features

An important set of features planned for the A-ERCS pilot is to assure self-organizing, self-healing and auto-configuration network features. The principal role of these is to provide as automated A-ERCS operations as possible and herewith provide valuable services for use during interventions. In essence, the A-ERCS node relies on these features when assuring the intelligence that allows for seamless communication as well as recovery and setup scenarios in case one or several of the currently used networks or services fail due to the extreme conditions, throughout which the A-ERCS system is expected to operate. Aside the intelligence incorporated in algorithms and configurations of the A-ERCS node, the features are achieved using IPv6 technology. Also, IPv6-based features are required elsewhere in the A-ERCS system where IPv6 technology is utilized.

2.3.1 IPv6 Auto configuration

IPv6 auto-configuration capabilities include the following mechanisms:

- Generation of automatic link-local addresses.
- Stateless Address Auto-configuration (SLAAC).
- Dynamic Host Configuration Protocol Version 6 (DHCPv6).
- Logical interfaces on router.

Every IPv6 node has the ability to automatically configure its IPv6 addresses. The link-local IPv6 address is automatically configured based on MAC address of the physical interface, and Duplicate Address Detection (DAD) takes place to ensure that IPv6 address is unique on local link and/or network. Any IPv6 node with an active network interface generates and configures its link-local IPv6 address for that interface, therefore, there can be multiple IPv6 link-local addresses on IPv6 node (as many as the number of active interfaces present).

Global IPv6 addresses on a node are provisioned via Stateless Address Auto-configuration (SLAAC) mechanism that requires no manual configuration on an end device, mobile node or router. It is standardized by IETF with RFC4862 [11]. The SLAAC mechanism on an IPv6 node uses IPv6 network prefix advertised by routers and the node's MAC address to generate globally unique IPv6 address. Additionally, a well-known pseudo-random function such as Message Digest 5 (MD5) can be used instead of the MAC address for the generation of globally unique IPv6 addresses.

Dynamic Host Configuration Protocol Version 6 (DHCPv6) can work in two modes: stateful and stateless. Stateful DHCPv6 protocol (defined with [12]) works in a very similar way as DHCPv4, which means all configuration parameters needed by a node to configure its IPv6 address, subnet mask and gateway, are provided within DHCPv6 messages. Also, there exists a stateless version of DHCPv6 (defined with RFC3736 [13]), in case of which it is assumed that nodes use SLAAC mechanism to generate its IPv6 addresses, and rely on stateless DHCPv6 information to acquire additional configuration parameters such as DNSv6 server address.

Mobile device can use the aforementioned capabilities to automatically configure its IPv6 network configuration parameters. The best practice scenario would be to generate its link-local IPv6 address, use SLAAC to configure its IPv6 globally unique address and use stateless DHCPv6 server to acquire DNSv6 server address.

Routers also generate and configure link-local addresses on all its IPv6-enabled logical or physical interfaces. Global addresses are typically configured manually, except on IPv6 internet uplinks where SLAAC functionality can also be used if provided by IPv6 Internet service providers.

From the local IPv6 network perspective, router (e.g. the Core Router in the A-ERCS node) sends out Router Advertisement messages to advertise its IPv6 prefix, MTU and MAC address. These parameters are used by SLAAC on mobile devices (e.g., mobile devices in the A-ERCS node extension). Router can also act as a DHCPv6 server or relay. Typically, it would act as a stateless DHCPv6 server in the combination with SLAAC capabilities.

To ensure reliable IPv6 tunnelling functions, logical interfaces on routers can be used. Since the logical interface is not susceptible to physical network outages, its IPv6 address is always reachable and is therefore recommended to use it as a tunnel endpoint.

If OSPFv3 would be used as a routing protocol, the IPv6 router uses its automatically generated link-local addresses as a source address for OSPFv3 packets. Hereby the routers learn link-local address of other routers connected to its interfaces and can use these addresses as next-hop addresses for IPv6 routing. If OSPFv3 operates on a logical interface, the global address is used on this interface.

A-ERCS segment/capability	Requirement	Details	Status
IPv6 Auto configuration requirements			
A-ERCS node	Link-local addresses	TBD	Required
	Global addresses	TBD	Required
	Stateless Address Autoconfiguration	TBD	Required
	DHCPv6	stateful	Optional
Core routers	Link-local addresses	TBD	Required
	Global addresses	TBD	Required
	Stateless Address Autoconfiguration	TBD	Optional
	DHCPv6	stateful	Optional
		stateless	Optional
		relay	Optional

Table 2-8: IPv6 Auto configuration requirements

2.3.2 IPv6 Self-healing network features

IPv6 by itself doesn’t support any self-healing features; therefore it depends on self-healing features of dynamic routing and mobility protocols used in the IPv6 network.

OSPFv3 routing protocol and its extensions for mobile networks (currently in draft phase within the IETF) offer the greatest number of self-healing features of all dynamic protocols used in IPv6. Self-healing features of OSPFv3 include:

- OSPFv3 compliance with Radio Aware Routing (RAR) to provide faster convergence with fine tuning of Radio-Aware link metrics (metrics can be tuned based on current and maximum bandwidth, resources, latency, hysteresis etc.).
- Minimized OSPFv3 packet size.
- Caching of LSAs to minimize the number of OSPFv3 packet exchange.
- Reduction of flooding of LSAs.
- Selective peering, which is used to reduce redundant full adjacencies of an OSPFv3 node, also the number of routing updates is reduced.

One of the possible features of OSPFv3 is also the support for multiple protocol instances on a link with the use of an “Instance ID” parameter contained in an OSPFv3 packet. This allows configuration and routing of multiple prefixes separately one from another on a single link (e.g. multi-homed router in an A-ERCS node).

In case of multiple uplink Internet service providers, a router, through prefix delegation, can acquire multiple different prefixes. Prefixes can then be advertised to mobile nodes based on the locally configured priority of these prefixes.

If using mobility protocols (e.g. Mobile IPv6, PMIPv6, DSMIPv6) some smart policing can be used to ensure self-healing functions. On mobile nodes, policy routing can be used to route certain IPv6 packets independently from other IPv6 packets regardless of the configured default route. For example, IPv6 node can have two tunnels established and policy routing defines which packets are sent through which tunnel. In case where desired path through IPv6 network is known, source routing in combination with policy routing can also be used to provide some self-healing features.

A-ERCS segment/capability	Requirement	Details	Status
Requirements for IPv6 Self-healing network features			
A-ERCS node	OSPFv3	TBD	Required
	OSPFv3 extensions	TBD	Required
	Multiple OSPFv3 instances	TBD	Required
	Priority based prefix delegation	TBD	Optional
	Source routing	TBD	Optional
	Policy routing	TBD	Required

Table 2-9: Requirements for IPv6 Self-healing network features

2.3.3 Integrating IPv6 and WiFi auto-configuration and self-organization

Another aspect of auto-configuration and self-healing features provisioning are capabilities supported in wireless ad-hoc networks, such as the planned Mesh WiFi of the A-ERCS system. These features need to be appropriately integrated with the IPv6 auto-configuration and self-organizing features in order to assure joint benefits of both sets of capabilities. In this chapter, a brief overview of ad-hoc wireless auto-configuration and self-organizing features is given. Detailed requirements, specifications and integration plans are subject to further efforts towards the A-ERCS pilot when network equipment feature list is available and further implementation details are known.

Wireless ad-hoc networks are self-healing and self-configurable, making them fast to deploy and more reliable. Connectivity to global communication system (GCS) is provided by proprietary radio or commercial wireless networks such as a cellular network.

Real time applications, such as voice and video, relay on Quality of Service (QoS) mechanisms, used in ad-hoc networks. User and device authentication and communication channel protection (encryption and integrity) is provided in the network by the proprietary crypto modules.

The following are the key ad-hoc network properties, relevant to the above aspects:

- Nodes are connected wirelessly and the network supports fast deployment.
- Two nodes in wireless line of sight auto connect using the ad-hoc principle.
- Network topology is mesh and nodes are equivalent to each other.
- There is no single point of failure in an ad-hoc network so the network is more reliable.
- An ad-hoc network is based on multi-hop principle of relying data.

2.4 Analysis of automatic network/system planning and deployment concepts and approaches

This chapter summarizes the principal aspects of automatic network/system planning and deployment concepts for the different segments, planned in the A-ERCS system.

2.4.1 Professional systems (analogue radio, DMR and TETRA)

In general, professional systems represent closed/separated network service domains, built as silos. Service planning, setup and provisioning is fully under control of dedicated professional centre. Network policy and service usage is defined by hosted organizations (URSZR for DMR radio, Police department for TETRA system), which means that the end users have no or limited influence on service and network policy.

In the A-ERCS system, professional network services will be mainly used for classical voice communications. DMR and analogue radio can be configured in two modes:

- Network mode – enables interconnect capabilities between a mobile terminal and the network.
- Direct mode – enables direct service interconnect between two mobile terminals.

Professional systems also support data transfer with low bit rates (system speed is limited to 9.6 Kbit/s). The use of data transfer services of the professional networks in the A-ERCS system is subject to the decisions of involved operators to enable data transfer service. If available, the system capabilities will be used in the A-ECRS system for:

- L1 point-to-point backhaul connectivity.
- L1 point-to-point on site connectivity.

A-ERCS segment/capability	Requirement	Status
A-ERCS node connectivity (interface) requirements for backhaul connectivity technologies		
Professional networks	DHCPv6 over serial interface support	Required
	PPPv6 over serial interface support	Required

Table 2-10: A-ERCS node connectivity (interface) requirements for backhaul connectivity

2.4.2 Commercial mobile communication networks

Commercial mobile networks can be classified as open systems with well-defined services and interfaces for end users and network interconnect. A commercial mobile service provider typically provides two types of data services:

- Internet connection service, where service planning, setup and provisioning is solely under control of the mobile operator.
- Mobile VPN connection service where service planning, setup and provisioning are shared between the mobile operator and a customer. Customer provisioning system holds a vital role in user/terminal authentication and authorization processes.

Selection between the provided mobile services is dynamic and is based on APN name concept.

2.4.2.1 Internet connection service

Internet connection service can provide fixed or dynamic IPv6 and/or IPv4 address allocation from Internet service provider address space. The end-point user terminals are auto-configured based on network mechanisms, such as GTP tunnelling and SLAAC/DHCPv6 protocols for IPv6 network parameters assignment and DHCP/PPP mechanisms for IPv4 network parameters assignment. The network mechanism enables dynamic provisioning of user terminals with IPv6 and/or IPv4 address delegation, DNS server address and other network parameters needed for Internet connection setup.

The main benefit of the Internet connection service is service mobility. The mobile operator can provide the same globally unique IP address (IPv6 and/or IPv4) every time a mobile terminal connects to the operator's network. Mobile terminals or end point systems (e.g. router) are always accessible on the same network ID, represented by their IP address.

2.4.2.2 Mobile VPN connection service

Mobile VPN connection service enables virtualization of mobile network resources for private communication. The main benefit of mobile VPN connection service, beside privacy, is the ability of providing IPv6 and/or IPv4 address allocation from the customer address space. VPN service is therefore under the policy and control of customer provisioning system.

User terminal configuration is based on extensions of service provider's network mechanisms enabled by GGSN/P-GW gateway (e.g. GTP tunnelling and SLAAC/DHCPv6 protocols for IPv6 network parameters assignment and DHCPv4/PPP mechanisms for IPv4 network parameters assignment) with external data plane tunnelling mechanisms (e.g. IPSec, GRE, MPLS VPN) and control plane protocols (e.g. Radius protocol). External tunnelling and Radius control enables secure and flexible connectivity with targeted customer network domain, provisioned by the customer.

Connectivity of the mobile terminal and other end point systems (e.g. Core Router in the A-ERCS node) to the mobile VPN network is under control of the customer provisioning system.

A-ERCS segment/capability	Requirement	Status
Backhaul connectivity technologies on the A-ERCS node		
Commercial networks interconnect	DHCPv6 over IPv6 PDP context	Required
	DHCPv6 and DHCPv4 over dual stack PDP context	Optional
	SLAAC over IPv6 PDP context	Required
	PPP over IPv4 PDP context	Optional

Table 2-11: Backhaul connectivity technologies on the A-ERCS node

A-ERCS segment/capability	Requirement	Status
Requirements for core and backhaul connectivity technologies		
GGSN mobile operator node	DHCPv6 over IPSec	Optional
	DHCPv4 over IPSec	Optional
	Radius over IPSec	Required
	IPSec LAN-to-LAN tunnel	Required
	Radius to GTP tunnel IWF	Required

A-ERCS segment/capability	Requirement	Status
	DHCPv4 to GTP tunnel IWF	Optional
	DHCPv6 to GTP tunnel IWF	Optional
	DHCPv6 over IPv6 PDP context	Optional
	DHCPv4 over IPv4 PDP context	Optional
	SLAAC over IPv6 PDP context	Required
	PPPv4v6 over PPP PDP context	Optional
	Fix IPv6 and or IPv4 address assignment	Required
	Dynamic IPv6 and or IPv4 address assignment	Required
VPN Customer gateway and provisioning system	DHCPv6 over IPSec Relay	Optional
	DHCPv4 over IPSec Relay	Optional
	Radius over IPSec	Required
	IPSec LAN-to-LAN tunnel	Required
	Radius server	Required
	Fix IPv6 and or IPv4 address assignment	Required
	Dynamic IPv6 and or IPv4 address assignment	Required

Table 2-12: Requirements for core and backhaul connectivity technologies

2.5 Analysis of routing and mobility in IP-based systems (technologies and techniques for seamless user and network mobility - DSMIPv6, PMIPv6, SYSTEM/USER INITIATED)

In this chapter an analysis of basic routing and mobility principles in IPv6-based system is represented briefly. The topics are of relevance to the entire A-ERCS systems, as it will be IP-based. More specifically, the Core Router of the A-ERCS node will play the principal role for the provisioning of IP-based routing and mobility.

2.5.1 IPv6 routing

Routing in IPv6 is basically the same as in IPv4, with minimal modifications and extensions that are required by IPv6. IPv6 routing can be previsioned statically or dynamically with any of the following dynamic routing protocols for IPv6:

- RIPng.
- IS-IS for IPv6.
- OSPFv3.
- MP-BGP.

In the following, different routing options are represented in more detail.

2.5.1.1 Static routing

Static routing in IPv6 is identical to static routing in IPv4. However, there can be a slight difference in usage and/or equipment configuration as required by different network equipment vendors.

2.5.1.2 RIPng

RIPng (Routing Information Protocol Next Generation) is defined by the IETF with RFC2080 [4] and is the simplest of all IPv6 routing protocols. It is based on RIPv2 and was designed to work as an Interior Gateway Protocol (IGP) in small- to medium-sized networks, and is therefore not suitable for complex environments.

It is a distance vector protocol with a working scope of 15 hops. RIPng uses Split Horizon mechanism to avoid problems caused by including routes in updates sent to the router from which they were learned. It also supports Split Horizon with Poison Reverse, which is a technique that does include such routes in routing updates, but sets their metrics to infinity.

RIPng is an UDP-based protocol that uses UDP port 512 on top of the IPv6 for sending and receiving routing updates. For RIPng updates it uses the multicast group IPv6 address. It supports sending out routing table entries that are basically IPv6 prefixes in local routing table, also it provides the ability to specify the next hop IPv6 address for prefixes specified in a routing table entries.

2.5.1.3 IS-IS for IPv6

IS-IS for IPv6 (Intermediate System to Intermediate System for IPv6) is a routing protocol originally defined by the ISO and also published by the IETF in the RFC5308 [5]. It was intended to be an intra-domain routing protocol for Connectionless Network Service (CLNS) traffic. IS-IS for IPv6 is not a lot different from IS-IS for IPv4, and as in IPv4, it is an appropriate choice for large and complex networks.

IS-IS for IPv6 is a link-state protocol, which means that every node independently builds a database of network topology based on the received routing updates called List State Protocol (LSP) Data Units. LSPs contain routing information in the form of a typed variable-length data (TLVs). Every node then independently calculates next best paths to every possible destination in the network. These calculated best paths then form local routing tables.

Its main advantage is that it doesn't use IPv6 for transporting LSPs and it can run directly on top of Layer 2 as a native network layer protocol.

For IPv6 specifics, two new TLVs were defined in the IS-IS for IPv6, namely "IPv6 Reachability" and "IPv6 interface". The "IPv6 Reachability" prefix basically contains information about a network prefix while the "IPv6 Interface Address" TLV can contain link-local or non-link-local IPv6 addresses.

2.5.1.4 OSPFv3

OSPFv3 (Open Shortest Path First Version 3) or OSPF for IPv6 is defined by IETF with RFC5340 [6]. It is based on OSPFv2 with enhancements and extensions as required by the IPv6. Similar to IS-IS for IPv6, it is link-state protocol designed to operate in large and complex network environments, however in certain cases IS-IS for IPv6 can be even more effective.

The basic mechanisms of OSPF used in IPv4, including routing information flooding, Designated Router (DR) election, area support and Shortest Path First (SPF) calculations, remain unchanged. However, some modifications were required and the most noticeable of them would be the ability to handle increased address size of the IPv6. Some of the other such enhancements are the following:

- Addressing semantics have been removed from OSPF packets and the basic Link State Advertisements (LSAs).
- Multiple addresses and instances per interface (use of link-local address).
- New LSA have been created to carry IPv6 addresses and prefixes.
- OSPF now runs on a per-link basis rather than on a per-subnet basis.
- Flooding scope for LSAs has been generalized.
- Authentication has been removed from the OSPF protocol and instead relies on IPv6 Authentication Header (AH) and Encapsulation Security Payload (ESP).

All optional capabilities used with OSPF for IPv4 (e.g. circuit support, Not-So-Stubby-Areas) are also supported.

While IS-IS for IPv6 runs directly on top of Layer 2, OSPF for IPv6 uses IPv6 for transporting messages. However, it does not use TCP or UDP, but is instead encapsulated directly in IPv6 datagrams with protocol number 89. The OSPFv3 messages also contain checksum fields that provide error detection and correction functions.

2.5.1.5 MP-BGP

MP-BGP (Multiprotocol Extensions for BGP-4) is defined by IETF in RFC4760 [7] and specifies extensions to the BGP-4 protocol defined in RFC4271. These extensions made BGP-4 available for other network layer protocols, such as IPv6 or MPLS.

Even though it can be used as an IGP, MP-BGP is mostly used by ISPs as an Exterior Gateway Protocol (EGP) to establish routing between one another and is therefore one of the most important protocols of the Internet. It can also be used for signalling and transporting routes for VPNs.

MP-BGP for IPv6 basically supports the same features and functionality as BGP-4 for IPv4. IPv6 extensions for MP-BGP include support for an IPv6 address family, network layer reachability information (NLRI) and next hop attributes that use IPv6 addresses. To achieve this, these extensions also introduced two new attributes, namely "Multiprotocol Reachable NLRI" and "Multiprotocol Unreachable NLRI". The first one is used to carry the set of reachable destinations together with the next hop information to be used for forwarding to these directions. The "Multiprotocol Unreachable NLRI" is used to carry the set of unreachable destinations.

MP-BGP neighbours establish TCP sessions on port 179, which is used for MP-BGP exchange of routing information.

A-ERCS segment/capability	Requirement	Details	Status
IPv6-based routing requirements			
A-ERCS node	Static routing	TBD	Required
	Dynamic routing	RIPng	Optional
		IS-IS for IPv6	Optional
		OSPFv3	Required
		MP-BGP	Optional
Core routers	Static routing	TBD	Required
	Dynamic routing	RIPng	Optional
		IS-IS for IPv6	Optional
		OSPFv3	Required
		MP-BGP	Required

Table 2-13: IPv6-based routing requirements

2.5.2 Mobility

Mobility in IPv6 allows a host device to be identified by a single permanent IPv6 address even if the device moves from one IPv6 network to another. Mobility in IPv6 is also independent of the type of physical network; therefore mobility from fixed to mobile or wireless system can easily be achieved.

In IPv6, mobility can be user- or system/network-initiated. User-initiated mobility relies on user equipment having the intelligence to ensure IPv6 connectivity while being outside of a home network. On the other hand, system/network-mobility is achieved by using ISPs network equipment capabilities without mobile node involvement.

There are some standardized protocols that focus on mobility aspects in IPv6:

- Mobile IPv6 (MIPv6).
- Proxy Mobile IPv6 (PMIPv6).

- Mobile IPv6 Support for Dual Stack Hosts and Routers (DSMIPv6).

2.5.2.1 Mobile IPv6

Mobile IPv6 (MIPv6) is based on Mobile IPv4 and is defined by the IETF in RFC3344 [8]. It is a user-initiated mobility technique that requires client application on a mobile node (i.e. the node moving from one network to another). That allows the mobile node to be reachable by its home address (i.e. IPv6 address in a home network) disregarding its current location.

While the mobile node is in a home network, packets destined to its home IPv6 address are routed to the mobile node's home network using standard routing mechanisms. When a mobile node leaves its home network and starts connecting via a foreign network, it gets a care-of address. A care-of address is an IPv6 address that has the subnet prefix associated with a foreign network. It is typically provisioned automatically using IPv6 stateless auto-configuration or DHCPv6.

The care-of address must then be signalled from a mobile node to the home agent. Home agent is a router on a home network and it registers the mobile node's care-of address with a mobile node's home address. This association between a mobile node's home address and a care-of address is known as a "binding" for the mobile node.

The mobile node sends its care-of address in a "Binding Update" message, the home agent replies with a "Binding Acknowledgement" message.

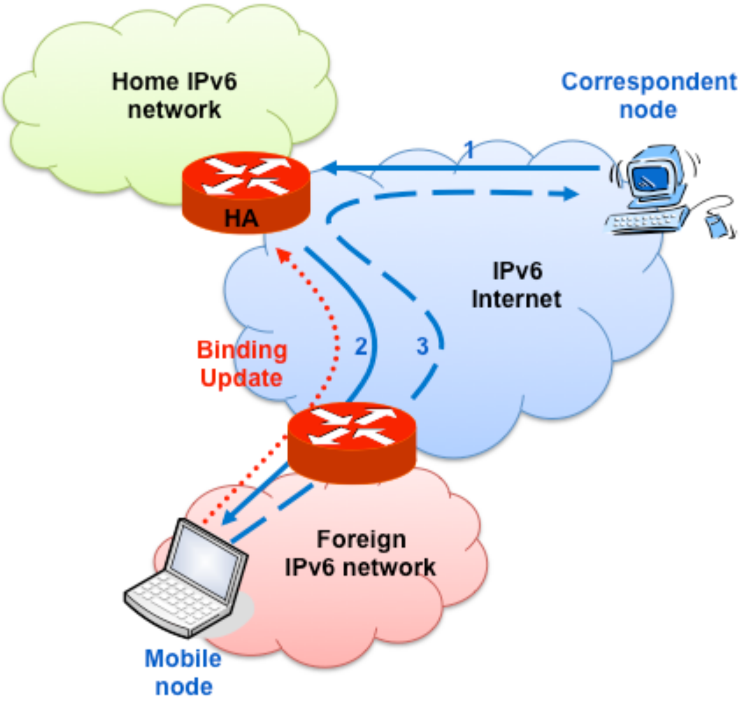


Figure 2-1: Mobile IPv6 – bidirectional tunnelling

Any node that wants to communicate with a mobile node is called a correspondent node.

When a correspondent node sends out packets destined to mobile node’s home address, the packets are routed to the home agent and then tunnelled using IPv6 encapsulation to the mobile node’s care-of address. Packets to the correspondent node are tunnelled from the mobile node to the home agent (i.e. reverse tunnelling) and then routed normally from the home network to the correspondent node. The whole procedure is called bidirectional tunnelling and does not require Mobile IPv6 support on a correspondent node.

If a correspondent node supports mobile node binding registration, the mobile node can provide its care-of address not only to home agent but also to correspondent node. This allows the use of “route optimization” functionality in Mobile IPv6. When a correspondent node wants to communicate with a mobile node, the binding registration occurs on a correspondent node and a “return routability” test is performed to verify the binding cache entry. Packets from the correspondent node can then be routed directly to the care-of address of the mobile node. Routing packets directly provides the most efficient way of communication between the correspondent node and the mobile node. Also, the impact of temporary failures of the home agent is reduced.

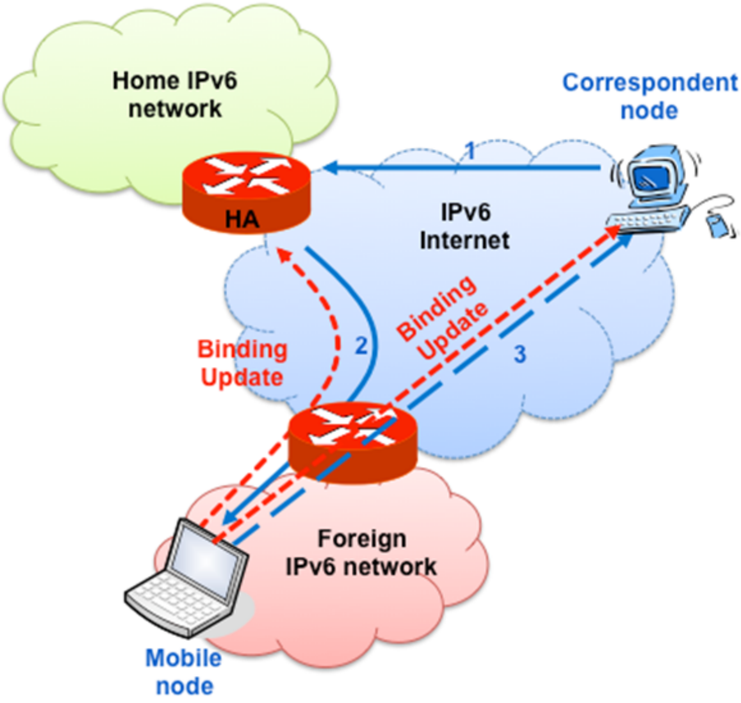


Figure 2-2: Mobile IPv6 – route optimization

When using “route optimization”, the packets from the correspondent node are destined to the care-of address of the mobile node and an IPv6 routing header is used to carry the home address of the mobile node. Packets from the mobile node carry its home address in IPv6 “Home Address” destination option.

Mobile IPv6 supports multiple home agents and also a dynamic home agent discovery that allows the mobile node to automatically find a home agent.

2.5.2.2 Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6) is defined by the IETF in RFC5213 [9] and in contrast to Mobile IPv6 does not require mobile node participation as it provides network-based mobility. With the network-based mobility there is no exchange of signalization messages directly between mobile node and the home agent. A proxy mobility agent is used instead and it provides mobility management on behalf of the mobile node that is visiting the network.

The main elements in PMIPv6 architecture are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The Local Mobility Anchor is used for maintaining the mobile node's reachability state and provides connection to the home network of a mobile node. The Mobile Access Gateway performs the mobility management on behalf of a mobile node, and is present in a foreign network, which the mobile node is currently visiting. The MAG detects when the mobile node accesses the foreign network and initiates binding registration to the LMA. There can be multiple LMAs in PMIPv6 domain, each responsible for a different group of mobile nodes.

When a mobile node enters a PMIPv6-enabled network it must first be authorized for network-based mobility service. If the authorization is successful the mobile node will then acquire an IPv6 address and be able to move anywhere in that PMIPv6 domain.

The MAG tracks mobile node movement and sends Proxy Binding Update messages about the current location of the mobile node to the LMA. The LMA responds with Proxy Binding Acknowledgement messages including the mobile node's home network prefix. The LMA also builds the Binding Cache for maintaining mobile node reachability state. The bidirectional tunnel is then established between the LMA and the MAG. The mobility access gateway now starts acting as a router in a home network by sending out Router Advertisements advertising mobile node's home prefix.

Any node on the Internet wanting to communicate with the mobile node sends out packets destined to home address of the mobile node. These packets are intercepted by the LMA that encapsulates and forwards them to the MAG through the bidirectional tunnel. The MAG then removes the other header and forwards original packets to the mobile node. If a correspondent node is currently connected to the same MAG as the mobile node, the packets from the correspondent node to the mobile node can be routed directly through the MAG. The procedures are the same for packets travelling in reverse direction.

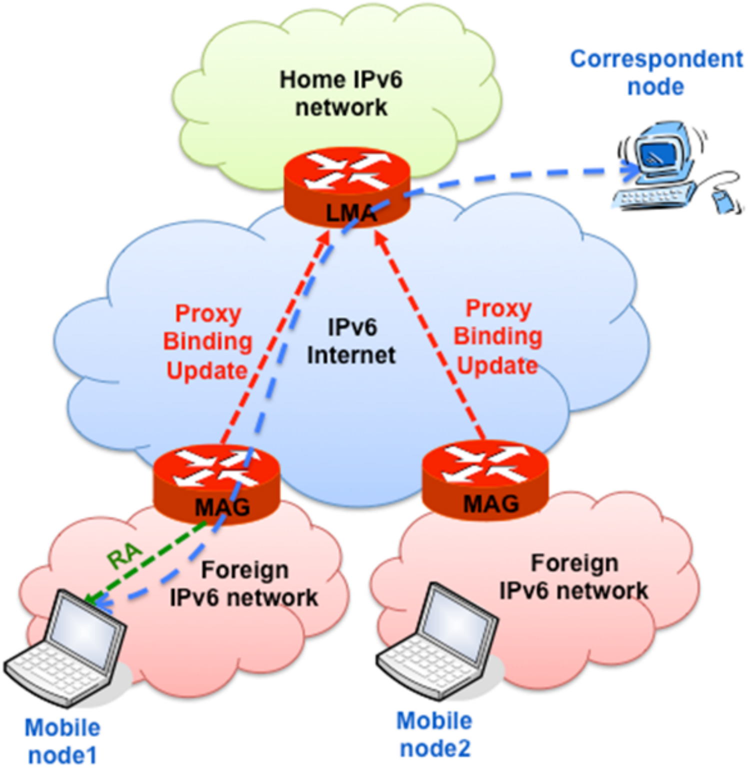


Figure 2-3: Proxy Mobile IPv6

If a mobile node leaves the network, this is signalled by MAG to the LMA that will remove the binding and routing state for the mobile node. The LMA will then wait for certain amount of time to receive a Proxy Binding Update from a new MAG. When the new MAG detects mobile node, it updates the LMA and starts sending out router advertisements. If a Proxy Binding Update is not received, the LMA deletes the binding cache entry.

2.5.2.3 DSMIPv6

Mobile IPv6 Support for Dual Stack Hosts and Routers (DSMIPv6) is a user-initiated mobility technique and is defined by the IETF in RFC5555 [10]. It provides extensions to Mobile IPv6 by supporting the registration of IPv4 addresses and prefixes. It also enables transport of both IPv4 and IPv6 traffic over the tunnels to the home agent, allowing the mobile node to move from IPv4 to IPv6 network or the other way around. DSMIPv6 requires that the mobile nodes and the home agents are dual stacked and support IPv4 and IPv6 care-of-addresses. Dual stack mobile node uses only Mobile IPv6 functionality to manage mobility, even though it can transport IPv4 or IPv6 packets.

As in Mobile IPv6, the mobile node in a foreign network must signal its care-of address to its home agent. If a mobile node is dual-stacked, it has an IPv4 and an IPv6 address, so the home agent must create binding cache entry for each address. The home IPv4 address and care-of IPv4 addresses are included in IPv6 mobility header.

If a foreign network supports IPv6, the mobile node configures globally unique IPv6 address and sends binding update to the IPv6 address of a home agent. The home agent then creates binding entries for IPv6 home address and optional for IPv4 address separately. Both bindings are associated with the mobile node's IPv6 care-of address, therefore any packet destined for IPv4 or IPv6 home address will be intercepted by home agent, which will tunnel them in IPv6 packets to the mobile node. Actually, there are two tunnels established, one for IPv4-in-IPv6 encapsulation and the other one for IPv6-in-IPv6 encapsulation.

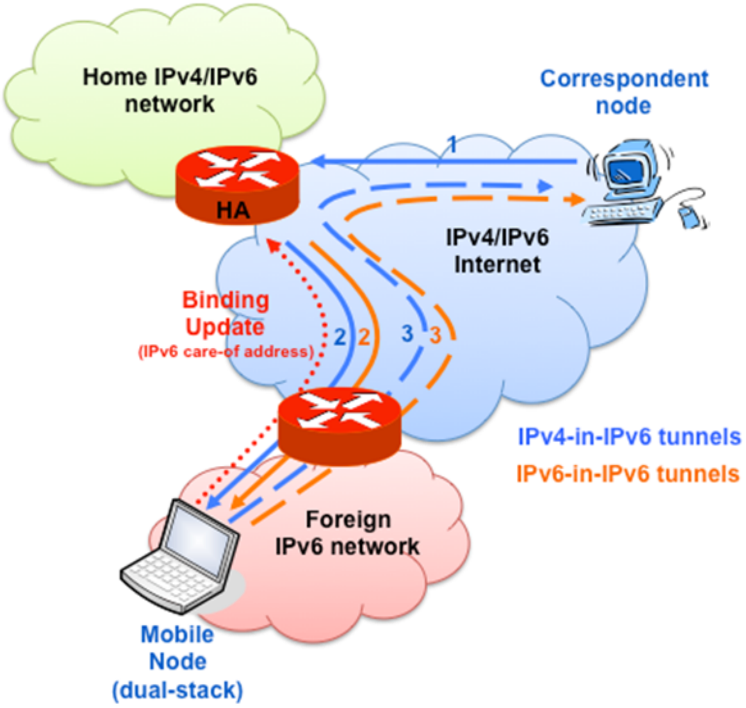


Figure 2-4: DSMIPv6 – IPv6 enabled foreign network

If the mobile node visits a foreign network that only supports IPv4, the mobile node has to tunnel IPv6 packets containing the binding update message to the IPv4 address of the home agent. The binding update contains mobile node's IPv4 care-of address. The home agent then creates binding cache entries for IPv4 and IPv6 home address. Two tunnels are than established, one for IPv6-in-IPv4 and the other one for IPv4-in-IPv4 traffic. If there is a NAT device between the mobile node and the home agent, the NAT traversal mechanism can be used. To traverse the NAT device, IPv6 packets are encapsulated in UDP on top of IPv4. For DSMIPv6 NAT traversal the UDP allocated port number is 4191.

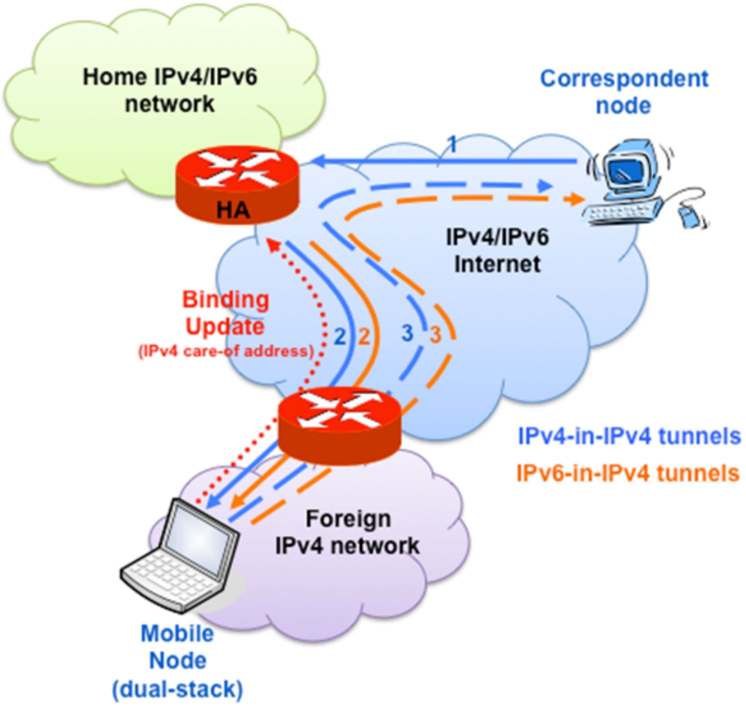


Figure 2-5: DSMIPv6 – IPv4-only foreign network

Since DSMIPv6 is an extension to Mobile IPv6, route optimization functionality can also be used if a foreign network is IPv6 capable and the correspondent node also supports Mobile IPv6. Route optimization is not possible when visiting a foreign network with IPv4-only capabilities and also for all IPv4 traffic.

A-ERCS segment/capability	Requirement	Status
IPv6-based mobility requirements		
A-ERCS node	Mobile IPv6	Required[1]
	PMIPv6	Required
	DSMIPv6	Required[2]
Core routers	Mobile IPv6	Required
	PMIPv6	Required
	DSMIPv6	Required

Table 2-14: IPv6-based mobility requirements

2.6 Analysis of seamless backhaul connectivity into available core networks

For seamless backhaul connectivity it is required to have the IP connectivity between the A-ERCS node and core routers of the backhaul infrastructure towards the SECC. This is already provided if using one of the commercially available networks such as UMTS/HSPA, LTE, WiFi, Ethernet or FTTH. This also applies when using dedicated systems like satellite, DMR or TETRA;

[1] *Home Agent functionality may also be required on an A-ERCS node*

[2] *Home Agent functionality may also be required on an A-ERCS node*

these, however, normally don't provide IP connectivity, therefore some modifications and enhancements are required to ensure IP capability.

If assumed that IP connectivity is provided within all available backhaul network segments then IPv6 mobility mechanisms can be used to ensure seamless backhaul connectivity between those segments. As mentioned before, IPv6 mobility mechanisms can be divided into user-initiated mobility (Mobile IPv6, DSMIPv6) and network/system mobility (PMIPv6) (ref. chapter 2.5 for further details).

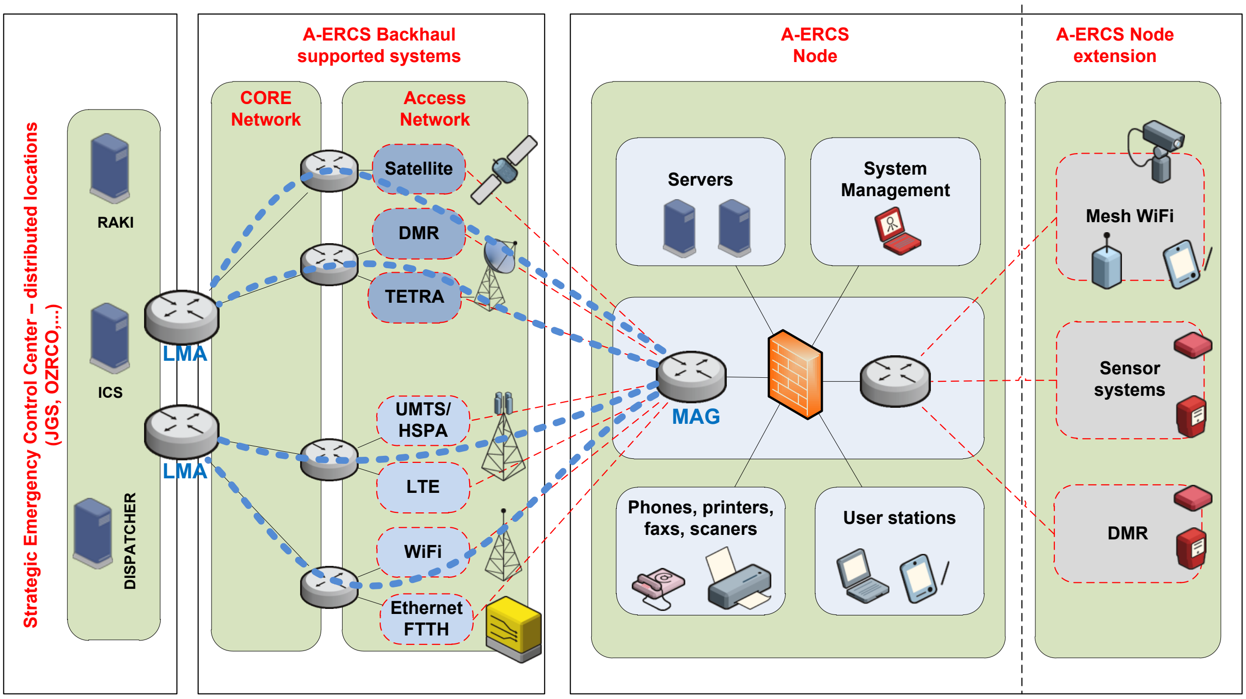


Figure 2-6: Seamless backhaul connectivity – network/system mobility

For network/system mobility, the recommended mechanism is PMIPv6 that enables seamless backhaul mobility between different network segments without mobile node participation. The problem with PMIPv6 is that it currently doesn't provide the capability to work over IPv4-only network. On the other hand, PMIPv6 is the only possible solution to work with all kinds of IPv6 mobile nodes since it doesn't require client applications on mobile devices. With PMIPv6, the LMA functionality is required on the core router in the backhaul core network towards the SECC and MAG functionality on the A-ERCS node as shown in Figure 2-6.

In case of user-initiated mobility mechanisms, Home Agent functionality is required on the core router in the backhaul core network towards the SECC, representing Home Network in terms of IPv6 mobility. If all network segments support IPv6 then Mobile IPv6 can be selected to ensure cross-network mobility. For IPv4-only network segments, the only appropriate solution is DSMIPv6 that can work over IPv4 or IPv6 network segments.

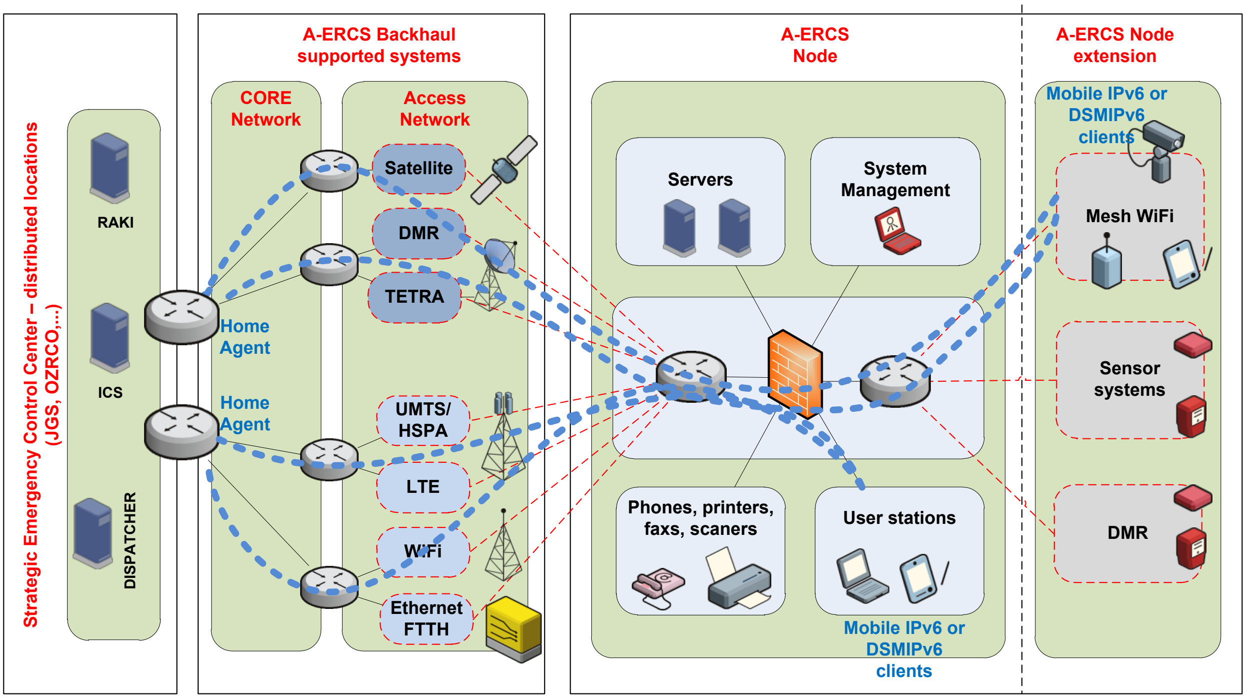


Figure 2-7: Seamless backhaul connectivity – user-initiated mobility

A-ERCS segment/capability	Requirement	Equipment requirements	Status
Seamless backhaul connectivity requirements			
A-ERCS node	Mobile IPv6	Mobile IPv6 client	Required[3]
	PMIPv6	MAG	Required
	DSMIPv6	DSMIPv6 client	Required[4]
Core routers	Mobile IPv6	Mobile IPv6 Home Agent	Required
	PMIPv6	LMA	Required
	DSMIPv6	DSMIPv6 Home Agent	Required

Table 2-15: Seamless backhaul connectivity requirements

[3] *Home Agent functionality may also be required on an A-ERCS node*

[4] *Home Agent functionality may also be required on an A-ERCS node*

3. ERCS Service Requirements Analysis

3.1 General A-ERCS service requirements

As already briefly explained in chapter 1.2, for the time being, ERCS system in use for fire fighter purposes by the SECCSU is limited and utilizes only a dedicated ZARE system, a PMR system that bases on analogue radio and DMR technologies. For professional use, only narrowband voice services are used, which is not in line with A-ERCS concepts and visions. Bearing this in mind, the proposed A-ERCS pilot will greatly extend the portfolio of available services to the fire fighter unit in action as well as to the SECCSU and SECC units controlling and organizing the intervention.

An important precondition clearly defined by the SECCSU unit and by the civil protection services of the MOL as a whole is 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. Therefore, existent system and services portfolio represents the starting grounds, based on which A-ERCS system, services and service scenarios can be planned and designed.

Another aspect that greatly affects the planning and design of A-ERCS services are the specific fire fighter unit requirements, induced by the SECCSU and the entire civil protection service organization of the SECC and MOL. These are explained in more detail in chapter 5 but taken into consideration throughout the analyses and requirements specifications in this section.

General A-ERCS service requirements	Status
Implementation of the A-ERCS pilot must not interrupt operation of existent ERCS system and services	Required
Implementation of the A-ERCS pilot must not decrease availability of existent ERCS system and services	Required
Implementation of the A-ERCS pilot must not affect resilience of existent ERCS system and services	Required
Support for analogue/DMR voice services via ZARE system	Existent, Required
Support for digital voice services	Required
Support for messaging services via ZARE system	Optional
Support for messaging services	Required
Support for data transfer services	Required
Support for video streaming services	Optional
Support for file transfer services	Optional
Support for email services	Optional
Support for sensor transfer services	Optional

Table 3-1: General A-ERCS service requirements

3.2 Specification of target services scenarios and individual services for on-site operational assistance, and for situation surveillance

Bearing in mind the specifics and the extreme conditions under which the A-ERCS services must operate, clear and in-depth specification of target service scenarios is a vital step in establishing an A-ERCS system. In doing so, we have identified the following preconditions and preliminary points, based on which service scenarios and services are discussed in more detail in the remainder of this section.

- The purpose of the A-ERCS services is threefold:
    - To provide operational assistance to the fire fighter unit on site during and intervention (operation):
        - for communication between members of the fire fighter unit on site (e.g., voice communication between the firemen),
        - for communication between the fire fighter unit and the SECCSU (e.g., voice communication between a fireman and an SECCSU operator),
        - for delivery of application/contents to the members of the fire fighter unit (e.g., push of 3D building plans to a PDA in a vehicle);
    - To provide operational assistance to the SECCSU unit:
        - for communication between the fire fighter unit and the SECCSU (e.g., voice communication between a fireman and an SECCSU operator),
        - for communication between the SECCSU and the SECC (e.g., message services between an SECCSU operator and a decision maker of the SECC),
        - for delivery of application/contents to the members of the SECCSU (e.g., push of 3D building plans to a PDA in a vehicle);
    - For surveillance of the on-site situation (e.g., real time sensor data monitoring and collection for later analyses, for example video stream and avalanche sensor measurements).
- The delivery of the services to the SECCSU unit and to the on-site fire fighter unit is subject to predefined organizational procedures; further details are available in chapter 5.1.
- The planning of the A-ERCS services must take into consideration the conditions, procedures and situations, under which the involved persons are communicating. As is true for any ERCS services, these must be efficient and assistive rather than complex and time consuming. This is specifically important when designing various complementary services, such as access to inventories, push notifications and multimedia-rich messaging, as well as when designing the appropriate user interfaces. Even though

these are not the aspects of this A-ERCS pilot, such requirements and preconditions are also considered when specifying service scenarios and individual services.

- Another precondition for service and service scenario definition is the availability and usability of terminal equipment on site. Again, even though this is not the focus of this A-ERCS pilot, some prerequisites and preconditions are considered when planning service scenarios and services. Obviously, fire fighter terminal equipment must be professional in two aspects:
    - In order to sustain the extreme conditions under which the services are consumed; typically ruggedized equipment is used (water resistant, resilient, portable, with lighted display etc.).
    - In order to correspond to the situation in which the service is consumed; advanced user interface features such as hands-free commands, speaker voice, graphical representations, sound alarms etc. can serve usefully to the fireman in action.

Based on the above, Table 3-2 summarizes the required A-ERCS services for two types of users during an on-site intervention:

- A fire fighter.
- A SECCSU operator.

A-ERCS segment/capability	Requirement	Status
Required A-ERCS services for different users of the A-ERCS system		
Fire fighter in operation	ZARE voice	Existent
	Voice over IP (VoIP)	Optional
	Video streaming	Optional
	Data transfer	Required
SECCSU operator in operation	ZARE voice	Existent
	ZARE messaging	Optional
	VoIP	Optional
	Messaging	required
	Video streaming	Optional
	Data transfer	Required
	E-mail	Optional
	File transfer	Optional
	Sensor data transfer	Optional
	Other (applications, data sharing, etc.)	Required

Table 3-2: Required A-ERCS services for different users of the A-ERCS system

The services listed in Table 3-2 can be further categorized from two aspects:

- Importance (priority) of the service; actual prioritization is subject to definition of the service scenarios and the design of the A-ERCS systems; further details are available in chapter 3.4; on a high level, two groups can be identified:

  - Critical: service is of high priority and represents a critical communication tool for a successful intervention; voice and data connectivity (for critical data transfer) services are of this type.
  - Background: services that can assist in the intervention but are not critical to its success; for example data transfer for inventory updates in a centralized database.

- Aim (purpose) of the service; we have defined two classes:
  - Operational assistance, which is a class of services that assist in execution and completion of an intervention, either in real time or afterwards; examples of such services are on-site voice communications or messaging between the SECCSU and SECC units.
  - Situation surveillance, representing a class of services that serve for monitoring of the on-site situation either for better intervention control and use of operational assistance services (e.g., monitoring of avalanche sensors, resulting in appropriate actions) or for later use (e.g., file transmission service for inventory update and accounting data collection).

Aside the above, services can be further categorized from many important aspects, such as QoS and security requirements, interactivity, multimedia intensity, real time characteristics, etc. These aspects are addressed in chapter 3.4.

3.2.1 Targeted service scenarios

The targeted service scenarios for the A-ERCS pilot are planned generically to correspond to the specific requirements of the SECCSU operations (as explained in chapter 5). The scenarios cover the usage of A-ERCS services throughout an on-going intervention and are limited to one SECCSU unit operations responsible for intervention coordination, comprising:

- Communication with the SECC.
- Communication with three fire fighter teams on site.
- Internal control and management of the intervention.

Two generic scenarios are planned, as follows.

3.2.1.1 Operational assistance scenarios

When an intervention is undergoing, a SECCSU unit is set up, comprising four operators. Three operators are responsible for intervention coordination, each coordinating one fire fighter team (a group of fire fighters in a unit) or the next lower level of intervention coordination pyramid (in case of a massive catastrophe a pyramid system is established with several SECC units on different levels of command). The fourth operator, called the controller, is in charge of coordinating the other three operators and for communication with the SECC. Use of available services is explained in order of their importance.

3.2.1.1.1 Voice service scenario

Each operator communicates with the members of the fire fighter team using ZARE voice service. At the same time, members of the fire fighter team also communicate among each other using the ZARE voice service. For both cases, an alternative option is to use VoIP services via (local) Mesh WiFi network (but not in critical conditions), either for local communication or for communication between remote units (if Mesh WiFi established for the purpose of the intervention).

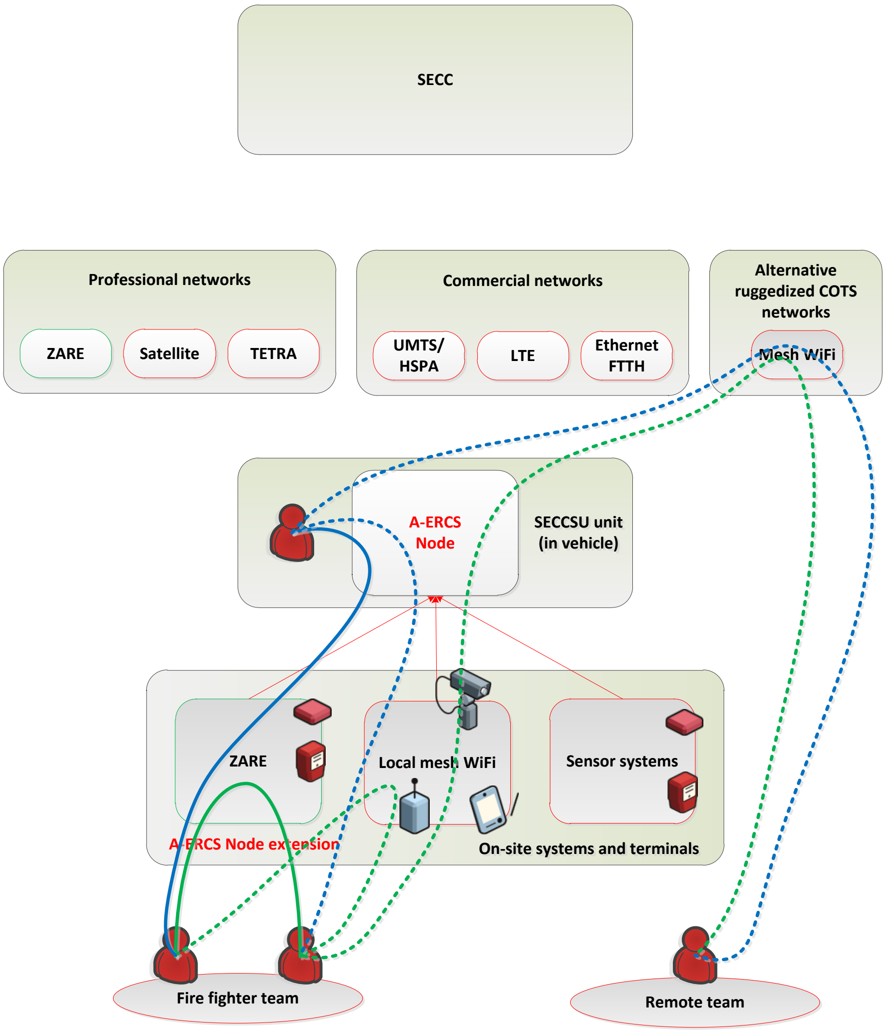


Figure 3-1: Voice services among fire fighter team members and between SECCSU operator and team members (local and remote)

The SECCSU controlling operator communicates with the SECC using ZARE voice services.

If appropriate for the given situation, in this case professional or commercial systems can be used instead of ZARE (subject to further directives and availability for the A-ERCS pilot), that is:

- Circuit-switched voice via TETRA, or via a satellite system.
- Circuit-switched voice via UMTS or VoIP via LTE.
- VoIP via Ethernet/FTTH (for communication between SECCSU and SECC, only if available).
- VoIP via Mesh WiFi (if Mesh WiFi network established).

The role of the A-ERCS node is to sustain a voice communication according to availability of the above networks. If any of the networks currently in use fails, an alternative network must be selected for voice service. If no professional or commercial network is available, voice communication is automatically re-established via ZARE system. The decision logic is defined with the intelligence and priorities in the A-ERCS node.

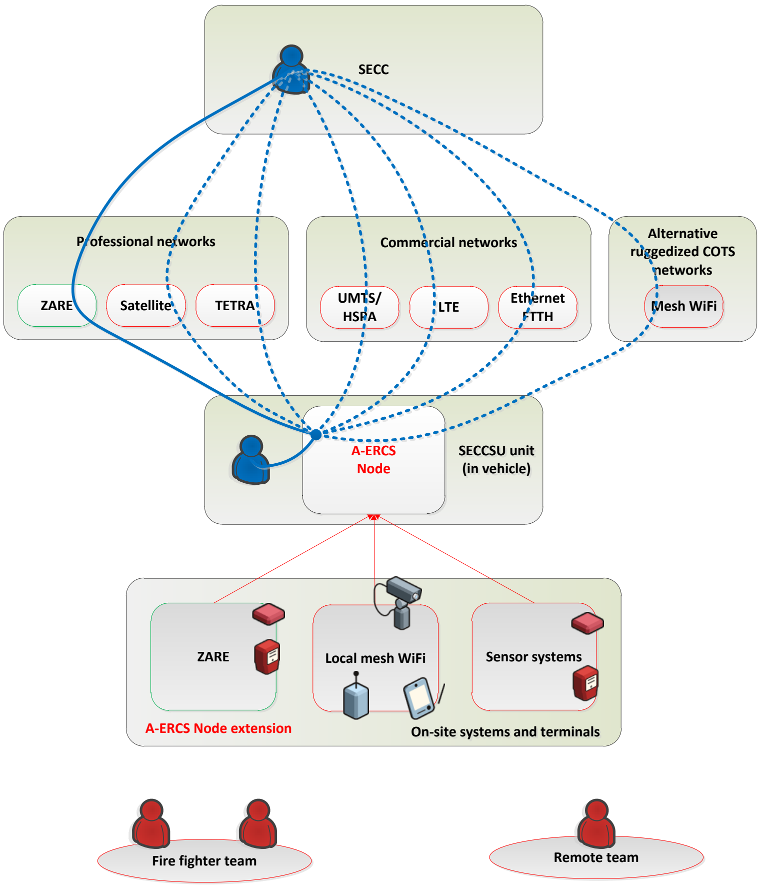


Figure 3-2: Voice services between SECCSU controlling operator and SECC

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

Table 3-3: Requirements for voice services

3.2.1.1.2 Data service scenario

According to needs, the members of the fire fighter team and SECCSU can use also data services, either in downlink or uplink. Data service is available via one of the following networks:

- A Mesh WiFi network set up on site (local mesh WiFi, for direct data communication between the SECCSU and the fire fighter unit) or in a region (Mesh WiFi, for direct data communication between the SECCSU and the fire fighter unit, for communication between distributed units and SECCSU, and for communication between SECCSU and SECC).
- A commercial network (LTE, UMTS/HSPA), if resources are available for data services while providing voice services.

For example, when a fire fighter team is going into action, fire rescue plans and 3D building models are delivered to a handheld terminal (e.g., a PDA or a smartphone) via LTE/UMTS while driving on site (pull data service). In another example a fire fighter is accessing applications for sensor monitoring, inventory access etc. while in operation on site (pull data service via ad-hoc WiFi). In the third example, a fire fighter uses push data service to transfer an on-site image to the SECCSU for further instructions, for example current level of spilled toxic fluids (using either ad-hoc WiFi network or LTE).

The SECCSU operators controlling the fire fighter teams can use push data services to deliver different data contents to the fire fighter team members, e.g. delivery of 3D building plans while on site via a local ad-hoc WiFi network. Also, the SECCSU controller uses push data services to deliver contents to the SECC, for instance sending images received from the on-site fire fighters in the SECC for further instructions. The SECCSU operators can use also pull data services, for example to access on-site sensors and read sensor measurements (e.g., body temperature measured with sensors installed in fire fighter clothing). A general request from the SECCSU and the SECC is to establish an on-going data connectivity service (preferably as a shared data network) to access a variety of web applications that are planned for the near future.

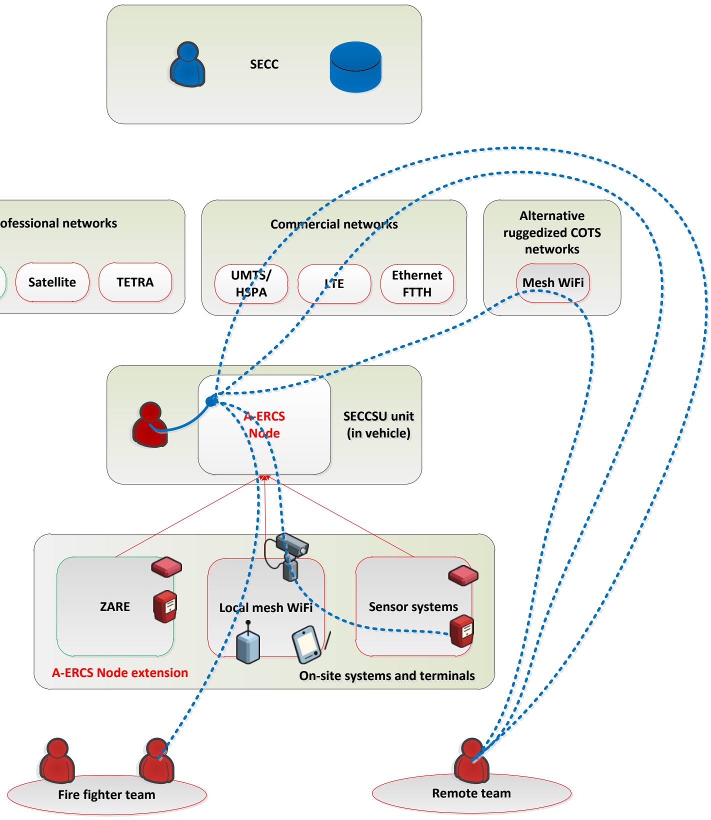


Figure 3-3: Data services between SECCSU operator and local or remote fire fighter team members

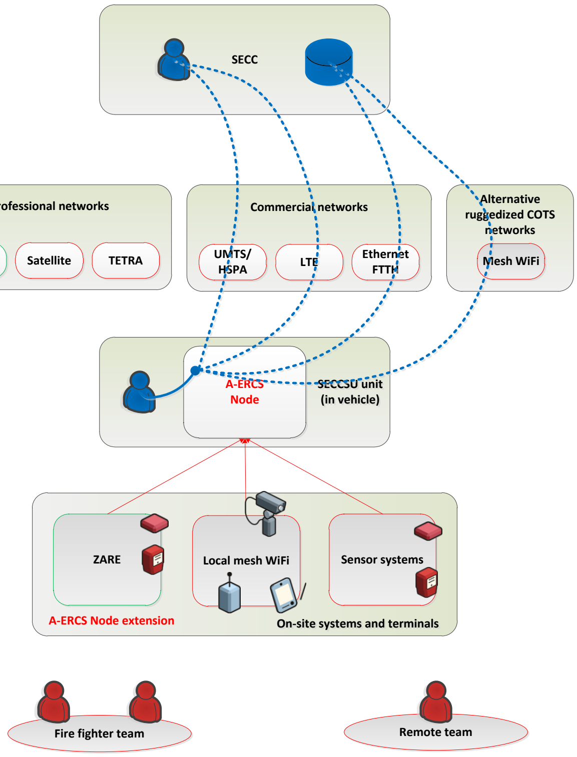


Figure 3-4: Data services between SECCSU controlling operator and SECC

A-ERCS segment/capability	Requirement	Equipment requirements	Status
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

Table 3-4: Requirements for data services

3.2.1.1.3 Messaging service scenario

Throughout the intervention, the SECCSU controlling operator can use messaging service to communicate with the SECC. For the time being, ZARE system supports messaging service but is not in use during intervention. Therefore, during this scenario, the SECCSU controlling operator and the SECC can communicate using messaging service that is available in UMTS/HSPA, and as an optional alternative messaging service provided over the top (OTT) using data transfer service (refer to data services section for further details).

3.2.1.1.4 Video streaming service scenario

Similar to sensor data services and messaging, the SECCSU operators and the fire fighter team members can use video streaming service scenarios by utilizing available data transfer services (refer to data services section for further details). An example of video streaming service use is real-time surveillance of the on-site situation and conditions in the SECC, or video camera feed capture and storage for later analyses and reporting (after the intervention is finished, situation surveillance service). Another example is delivery of streamed video to a PDA of a fire fighter during an intervention if the intervention site is very large. Video streaming service is carried out using data services, but is interpreted as a separate service due to high bandwidth requirements and requirements for additional features on the terminal devices.

3.2.1.1.5 File transfer service scenario

Similar to the above, the SECCSU operators and the fire fighter team members can use file transfer service scenarios by utilizing available data transfer services (refer to data services section for further details). Examples of usage are transfer of files containing fire escape routes, equipment instructions and manuals etc. file transfer service relies on data transfer service but is treated separately due to low packet loss requirements.

A-ERCS segment/capability	Requirement	Equipment requirements	Status
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 3-5: Requirements for messaging, video streaming and file transfer services

3.2.1.2 Situation surveillance scenarios

Throughout intervention, a variety of additional services can be used that serve either for efficient decision making and use of operational assistance services or for late purposes. This group actually represents data services – there is a variety of cases where data transfer services are required for situation surveillance, for example access to the Internet for additional information, access to databases to acquire fire route maps, as well as for any type of service that requires data transfer between remote sites (e.g., sensor data transfer, video streaming, file transfer, etc.; as explained in the following). The key differentiation of this group of data services from operational assistance data services is the priority assigned to the communication. Technically speaking the same networks are utilized for their provisioning as explained in chapter 3.2.1.1.2.

The following is the list of situation surveillance services along with some use case examples.

- Sensor data transfer service – for situation surveillance purposes, sensor data transfer services are used to gather data from the sensors on site and its storage in appropriate databases for later analyses. In the E-ERCS system, data services via Mesh WiFi, xDSL, Ethernet, FTTH, UMTS/HSPA or LTE are utilized.
- Video streaming service – for situation surveillance purposes, video streaming services are used to record on site situations and its storage in appropriate databases for later

analyses. In the E-ERCS system, data services via Mesh WiFi, xDSL, Ethernet, FTTH, UMTS/HSPA or LTE are utilized.

- E-mail – this is a basic support service, intended for support communication between the SECCSU controlling operator and the SECC (e.g., for inventory list updates, financial information transfers, etc.). In the E-ERCS system, data services via Mesh WiFi, xDSL, Ethernet, FTTH, UMTS/HSPA or LTE are utilized.
- File transfer service – this is another basic support service, intended for reliable file transfer, such as updated inventories, accounting files etc. In the E-ERCS system, data services via Mesh WiFi, xDSL, Ethernet, FTTH, UMTS/HSPA or LTE are utilized.
- Other – a variety of other applications can also be used to increase the efficiency of situational surveillance, such as document sharing tools, video conference systems for decision makers, accountant programmes etc. these services are either local or require data transfer services between remote sites. A general request from the SECCSU and the SECC is to establish an on-going data connectivity service (preferably as a shared data network) to access a variety of web applications that are planned for the near future. One such example that is planned and considered of a high-priority service is access to an intervention task management database.

When analysing the service requirements, this group of service is listed only for the SECCSU unit even though the fire fighters may use a selection of services as well (ref. Table 3-2). This is due to the following facts:

- The application is actually delivered using data transfer service.
- The situation surveillance services are designed foremost for use for the SECCSU operators and for SECC as a complementary set of tools aside the operational assistance services.
- A selection of situational surveillance services can be made available to the fire fighters as well as they can deliver critical or vital information, but this decision is subject to current situation and criticality of each individual intervention as well as to the availability of appropriate terminal equipment on site (e.g., in case of massive fire, PDAs are not useful due to smoke and heat).

3.3 Analysis of challenges, issues and approaches to re-use, upgrade and enhance existent services (transition viewpoint)

The A-ERCS pilot will be designed for and implemented in the operational SECCSU infrastructure. Therefore, when planning the design and implementation, the following preconditions and starting points must be considered:

- 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.

- Existent ERCS system is based on legacy technologies, that is, the ZARE system built as a PMR.
- Currently, during an intervention, only analogue voice service is available for use.
- No IPv6 technologies are available in the existent ERCS infrastructure.

Therefore, from the IPv6 viewpoint no transition challenges in the existent ERCS are identified aside from the requirement of the URSZR that ZARE system must operate without disturbances and modifications. Integration aspects for the ZARE system into the A-ERCS system is subject to further availability of the ZARE system for the purposes of this project, capability analyses and decision making.

On the side of the re-use of services in the professional and commercial networks, the plan is to utilize available services without major changes and modifications. Specific IPv6 –related network configuration requirements are already addressed in previous chapters while service operation itself remains unchanged. However, there is one exception, that is, services in the LTE network (in case of its availability for the purposes of the A-ERCS pilot). In this case, we wish to demonstrate prioritized LTE service usage for the A-ERCS purposes, which required appropriate user/service prioritization using dedicated EPS bearers or user-based policing in the EPC core (MME, HSS, S-GW and P-GW), supported and configured by the LTE operator. For the time being, plans are in process to include an LTE network into the A-ERCS pilot. However, no active implementation is available at the moment at the operator that has shown interest to cooperate in the A-ERCS pilot. Therefore, further planning of LTE service usage and the appropriate requirements specification are subject to availability of the LTE implementation.

3.4 Service classification – priority, urgency, security requirements, quality requirements, multimedia intensity and resource requirements, real-time characteristics

Based on the specified target service scenarios, presented in chapter 0, the following groups of operational assistance services are planned to be supported in the A-ERCS system:

- Voice.
- Messaging.
- Data transfer (including access to shared web applications, sensor data transfer, file transfer, video streaming and other services – e-mail, desktop applications, access to Internet, etc.).

For these services, priorities must be defined and implemented in the intelligence of the A-ERCS node for the purpose of automated network selection and service provisioning as planned in the A-ERCS system. The priorities must be defined for the type of service, the technology/network and content.

Table 3-6 summarizes services that are considered for support in the A-ERCS system while Table 3-7 defines service priorities per service group, technology/network and content transmitted. Service priorities are defined for the A-ERCS system as a whole and apply to both SECCSU operators and fire fighters (where applicable).

A-ERCS segment/capability	Requirement	Status
Service requirements		
Fire fighter in operation	ZARE voice	Existent
	VoIP over Mesh WiFi	Optional
	Data via Mesh WiFi	Optional
	Data via UMTS/HSPA	Optional
	Data via LTE (prioritized)	Optional
	Video streaming via UMTS/HSPA	Optional
	Video streaming via LTE	Optional
	Video streaming via Mesh WiFi	Optional
	File transfer via UMTS/HSPA	Optional
	File transfer via Mesh WiFi	Optional
	File transfer via LTE	Optional
SECCSU operator in operation	ZARE voice	Existent
	CS voice over satellite	Optional
	VoIP over LTE (prioritized)	Optional
	CS over UMTS	Optional
	VoIP over Ethernet/FTTH	Optional
	VoIP over Mesh WiFi	Optional
	Data via UMTS/HSPA	Required
	Data via LTE (prioritized)	Optional
	Data via Mesh WiFi	Optional
	Data via Ethernet/FTTH	Optional
	ZARE messaging	Optional[5]
	UMTS/HSPA messaging	Optional
	OTT messaging via Mesh WiFi	Optional
	OTT messaging via LTE	Optional
	OTT messaging via Eth/FTTH	Optional
	Video streaming via UMTS/HSPA	Optional
	Video streaming via LTE	Optional
	Video streaming via Eth/FTTH	Optional
	File transfer via UMTS/HSPA	Optional
	File transfer via Mesh WiFi	Optional
	File transfer via LTE	Optional

[5] *Supported in the ZARE system but not in use for professional purposes.*

	File transfer via Eth/FTTH	Optional

Table 3-6: Service requirements

A-ERCS segment/capability	Requirement			
Service priorities				
Service type	**Content**	**Priority**	**Technology/network**	**Order of selection**
Voice	Voice	1	ZARE	1 (1.1)
			VoIP over LTE (prioritized)	2 (1.2)
			CS over UMTS	3 (1.3)
			CS voice over satellite	4 (1.4)
			VoIP over Mesh WiFi	5 (1.5)
			VoIP over Ethernet/FTTH	6 (1.6)
Messaging	Message	2	ZARE messaging	1 (2.1)
			UMTS/HSPA messaging	2 (2.2)
			OTT messaging via LTE	3 (2.3)
			OTT messaging via Mesh WiFi	4 (2.4)
			OTT messaging via Eth/FTTH	5 (2.5)
Data transfer	Access to shared web applications	3	Data via LTE (prioritized)	1 (3.1)
			Data via Mesh WiFi	2 (3.2)
			Data via UMTS/HSPA	3 (3.3.)
			Data via Ethernet/FTTH	4 (3.4)
	Image transfer	4	Data via LTE (prioritized)	1 (4.1)
			Data via Mesh WiFi	2 (4.2)
			Data via UMTS/HSPA	3 (4.3)
			Data via Ethernet/FTTH	4 (4.4)
	File transfer	5	Data via LTE (prioritized)	1 (5.1)
			Data via Mesh WiFi	2 (5.2)
			Data via UMTS/HSPA	3 (5.3)
			Data via Ethernet/FTTH	4 (5.4)
	Sensor data transfer	6	Data via LTE (prioritized)	1 (6.1)
			Data via Mesh WiFi	2 (6.2)
			Data via UMTS/HSPA	3 (6.3)
	Video streaming	7	Data via LTE (prioritized)	1 (7.1)
			Data via Mesh WiFi	2 (7.2)
			Data via UMTS/HSPA	3 (7.3)
			Data via Ethernet/FTTH	4 (7.4)
	Other	8	Data via LTE (prioritized)	1 (8.1)
			Data via Mesh WiFi	2 (8.2)
			Data via UMTS/HSPA	3 (8.3)
			Data via Ethernet/FTTH	4 (8.4)

Table 3-7: Service prioritization

Service priority defines importance/urgency of the group of services per content. Service priority in the A-ERCS is used for admission control and in situations when network resources are limited and not all requesting services can be ranted resources. In other words, if resources are scarce, voice and messaging services have priority over data transfer, while for data transfer service access to shared web applications, image and file transfer have priority over video streaming. Altogether, 8 priority classes are considered.

Each service (service type and content defined) can be provided via several networks; therefore an order of network selection is required. In while Table 3-7 order of selection for voice and messaging is defined based on the expected reliability of the service via different networks (with the exception of Ethernet/FTTH, which is ordered last given its lower convenience due to being a fixed network; in case this network is selected, connectivity must be available locally and the team needs to gain access to it while the intervention is undergoing). For data services, the order of selection is defined based on the expected bit rate capacities (with the exception of Ethernet/FTTH, which is ordered last given its lower convenience due to being a fixed network). For all service types and networks/technologies, the prioritization implemented in the A-ERCS node is subject to availability and might change throughout the project.

Furthermore, prioritization is also subject to the following criteria:

- Security requirements – in this respect no differentiation is considered for the order of selection as security is expected at an appropriate level; professional and commercial networks provide sufficient security while the Mesh WiFi is planned as a closed network with applied security mechanisms.
- Quality requirements – quality requirements are take into consideration throughput prioritization based on the expected reliability.
- Multimedia intensity – this criteria applies to video streaming service and is taken into consideration in the order of selection based on bitrate capacities.
- Resource requirements – this criteria is taken into consideration in the order of selection based on bitrate capacities.
- Real-time characteristics.

For each of the above criteria, further service studies are required throughout A-ERCS system and services design phase, based on which admission control and micro prioritization can be defined. The outline of study, in preparation in close collaboration with the external stakeholders, foremost the SECCSU, is presented in Table 3-8 along with some initial application examples. A methodology was defined that comprises:

- Network service parameters:
  - Priority group.
  - Protocols.
  - Ports.

- Addressing plan:
    - IPv6.
    - IPv4.
- QoS parameters (end-to-end):
    - Delay.
    - Jitter.
    - Packet loss.
    - Bitrate.

This methodology will be employed in further steps towards the design and pilot plan of the A-ERCS system and services.

Application	Description	Network service parameters			Addressing plan		QoS parameters			
		Priority group	Protocols	Ports	IPv6	IPv4	Delay	Jitter	Packet loss	Bitrate
Access to inventory data RAKI	PFFS equipment inventory	7	HTTP	TBD	TBD	TBD	TBD	TBD	TBD	TBD
VoIP	Voice service over IP, codec g711	1	RTP/UDP, SIP/TCP, SIP/UDP	TBD	TBD	TBD	150 ms	150 ms	0.2%	110 kbit/s
Internet service	Access to Internet	7	various	various	TBD	various	/	/	/	/
Analogue voice	Analogue voice	1	analogue	/	/	/	/	/	/	/
DISPATCHER	Application for fire fighter unit dispatching logging	7	HTTP	TBD	TBD	TBD	TBD	TBD	TBD	TBD
ICS	Integrated communication services solution for professional use in case of massive accidents	2	HTTP	TBD	TBD	TBD	TBD	TBD	TBD	TBD
GPS tracker	GPS tracking for vehicles and users	5	HTTP	TBD	TBD	TBD	TBD	TBD	TBD	TBD
RFID tagging	Detection of presence of persons, equipment, system components in the vehicle or on site	5	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
Environmental measurements	Measurements of CO2, humidity and temperature in the vehicle	5	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD
	Measurements of CO2, humidity and temperature on site	5	TBD	TBD	TBD	TBD	TBD	TBD	TBD	TBD

Table 3-8: Service and application requirements study

3.5 Study of Various available IPv6-based mechanisms for secure and QoS-enabled data transmission

This chapter provides an overview of available Quality of Service (QoS) and security mechanisms, applicable to IPv6-based systems. There are many mechanisms for providing QoS and data security for data transmission services with IPv6. Typically, a combination of mechanisms is implemented to fulfil to the requirements.

3.5.1 QoS mechanisms

3.5.1.1 Traffic class and Flow labels

IPv6 packet header contains two fields, which are used for QoS - Traffic class (TC) and Flow label (FL). TC is used to classify packets into different classes, depending on the requirements and priorities. Network devices read each TC field and perform prioritization depending on the value – this is usually done by giving scheduling priorities or by bandwidth limiting. Highest priority is usually given to network signalization (routing, management, etc.), and then to real-time services (VoIP, messaging), followed by different services such as IPTV etc. Random Internet traffic (www traffic, data downloads, peer-to-peer, etc.) is usually assigned the lowest priority. There are no major differences when compared to IPv4.

A user can set the traffic class values by himself, but most commercial providers ignore and/or replace the value on their devices, thus applying classification and QoS only to services provided by themselves. IPv6 introduces the 20 bits Flow label (FL) field that allows the user to further classify and prioritize traffic flows within its TC. Any user application can set the FL field to a desired value for each flow thus allowing for more granular prioritizing of traffic. While both being HTTP traffic, large HTTP file download can be given lower priority than a webpage currently being opened. Currently, most network devices don't support QoS enforcement based on IPv6 flow label.

3.5.1.2 Multi-Protocol Label Switching - MPLS

MPLS can be used to provide high-performance simplex links between two endpoints. Similarly as with IP, the TC field is used for QoS. Since the IP packets are encapsulated within MPLS packets, the MPLS traffic class value is set by the MPLS endpoints and does not have to be the same as the IP traffic TC value.

3.5.1.3 Other tunnelling solutions

Other tunnelling solutions (6to4, 6in4, 6rd, etc.) rely on outer packets to set the required traffic class.

3.5.1.4 Overview of QoS requirements in the A-ERCS system

Overview of QoS requirements in various segments of the A-ERCS system are gathered in Table 3-9, Table 3-10 and Table 3-11. An IPv6 QoS mechanism (e.g. DiffServ model, Traffic Class, Flow

Label) enables end-to-end control and data plane for QoS enforcement in the A-ERCS system. Due to the fact that the A-ERCS system is a unified solution based on integration of professional, commercial and ad-hoc communication systems, an interconnection point must exist to provide heterogeneous networks and technologies interconnect (e.g. TETRA to IPv6/Ethernet, HSPA to IPv6/MPLS). In the interconnection point, support for QoS interworking function (IWF) must be provided, which enables translation of QoS control and data plane attributes between different technologies domains.

A-ERCS segment/capability	Requirement		Status
	A-ERCS node QoS requirements		
A-ERCS Node	DiffServ model based on TC	Core router	Required
		Core firewall	Required
	DiffServ model based on Flow Label	Core router	Optional
		Core firewall	Optional
A-ERCS Node extension	Sensor system QoS support		Optional
	WiFi (802.11a/g/n) QoS support		Optional
	DMR and Analog radio		Optional

Table 3-9: A-ERCS node QoS requirements

A-ERCS segment/capability	Requirement	Status
Backhaul QoS network capabilities		
Backhaul over professional networks (DMR, analogue radio, TETRA, satellite or other)	IPv6 QoS to Tetra QoS IWF	Optional
	IPv6 QoS to DMR QoS IWF	Optional
	IPv6 QoS to Satellite QoS IWF	Optional
Backhaul over commercial networks (UMTS/HSPA, LTE, WiFi/WiMAX)	IPv6 QoS to UMTS/HSPA IWF	Required
	IPv6 QoS to LTE IWF	Required
	IPv6 QoS to WiFi/WiMAX IWF	Required
Backhaul over xDSL/FTTH	IPv6 QoS to xDSL/FTTH IWF	Optional

Table 3-10: QoS requirements for backhaul networks

A-ERCS segment/capability	Requirement	Status
SECC QoS capabilities		
SECC networks	DiffServ model based on TC	Required
	DiffServ model based on Flow Label	Optional

Table 3-11: SECC QoS capabilities

3.5.2 Security mechanisms

3.5.2.1 Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) is a group of protocols for encryption and authentication of IP packets. Internet Security Association and Key Management Protocol (ISAKMP) is used for authentication and key exchange. IPsec support is one of the requirements for the IPv6 protocol stack. Further security details on this mechanism are represented in the following.

3.5.2.1.1 IPsec Authentication Header (AH)

Authentication header (AH) guarantees data integrity and endpoint authentication of IP packets. Source device calculates an Integrity Check Value (ICV) using a cryptographic hash function with the non-changing part of the IP header, IP payload and the IPsec key. End device does the same, and compares the values. Other devices along the path don't have access to the IPsec key and are unable to calculate a correct ICV. Since cryptographic hash functions are one-way, it is practically impossible to derive the IPsec key from captured packets. Since both source and destination addresses are used in the ICV computation, it is impossible to use AH with any kind of Network Address Translation (NAT).

3.5.2.1.2 IPsec Encapsulating Security Payload (ESP)

Encapsulating Security payload offers authentication, data integrity and encryption. Unlike AH it provides authentication and/or encryption only of payload data and not the IP header itself so it can be used in combination with NAT. The encryption algorithm is not enforced, but usually AES, blowfish or (Triple)DES is used. Authentication-only or encryption-only (null encryption) modes are also possible, but the latter is discouraged due to security issues.

3.5.2.1.3 IPsec Transport and Tunnel mode

Both IPsec AH and ESP can work in two modes. In transport mode, the authenticated/encrypted data is from a higher protocol (usually TCP or UDP). The IP header is kept intact (but authenticated with AH). This is mostly used with host-to-host communication.

Tunnel mode is mostly used with Virtual private network (VPN) connection. The whole IP packet is encapsulated within another IP packet with AH header or ESP. With ESP the whole inner IP packet is encrypted (header too), and a potential eavesdropper can only read the IPsec endpoints IP addresses and not the source and destination of the encrypted packet.

3.5.2.1.4 IPsec QoS

IPsec relies on IP Traffic Class (TC) fields and other mechanisms to provide QoS. With transport mode, the packet source sets the TC field, but with the tunnel mode, the TC field has to be set by the device doing the encapsulating and tunnelling.

3.5.2.2 Secure Sockets Layer (SSL)

Where IPsec is impossible or impractical, data encryption and authentication can be done with Secure Sockets Layer (SSL). SSL is a set of cryptographic protocols, which use asymmetric cryptography with public-key infrastructure (PKI) for authentication and symmetric encryption for privacy. The SSL connection begins with a handshake where public keys are exchanged and (symmetric) session keys are generated. After that, all data is encrypted with the selected session keys.

SSL is most widely used with secure HTTP – HTTPS, but it can also be used to securely tunnel TCP/UDP connections, or even as a VPN solution where IP or even Ethernet packets are carried over SSL tunnels. Many vendors provide commercial SSL VPN solutions.

As with IPsec, QoS is managed by lower protocols (usually IP).

3.5.2.3 Overview of security requirements in the A-ERCS system

An overview of security requirements in the targeted segments of the A-ERCS system is gathered in the following tables. Fixed and core segments of the A-ERCS system represent secure and controlled environments where the users of the A-ERCS system are well known and under closed supervision of system administrators. Therefore, in these segments, the A-ERCS system will rely on the integrated security mechanisms and will not deploy additional ones.

Commercial and professional communication systems (e.g. TETRA, DMR radio, HSPA and LTE) inherently support security mechanisms (e.g. encryption and integrity service) for data and voice communications. Uses of external security protocols (e.g. IPsec and TLS) on these segments of the A-ERCS system are not required.

Due to the fact that any communication within the A-ERCS system crosses several administratively and technically diverse domains, security protocols IPsec and TLS will be used for selected services according to requirements (to be specified later in the pilot planning).

A-ERCS segment/capability	Requirement		Status
A-ERCS node security requirements			
A-ERCS Node	IPsec support	Core router	Optional
		Core firewall	Required
		User stations	Optional
		System management station	Required
	TLS/SSL	User stations	Optional
		Servers	Required
A-ERCS Node extension	IPsec support	Sensors	Optional
		Cameras, PDA	Optional
	TLS/SSL	Sensors	Optional
		Cameras, PDA	Required

Table 3-12: A-ERCS node security requirements

A-ERCS segment/capability	Requirement	Status
Backhaul security network capabilities		
Backhaul over professional networks (DMR, analogue radio, TETRA, satellite or other)	Tetra security support	Optional
	DMR security support	Optional
	Satellite system security support	Optional
Backhaul over commercial networks (UMTS/HSPA, LTE, WiFi/WiMAX)	UMTS/HSPA security support	Required
	LTE security support	Required
	WiFi/WiMAX security support	Required
Backhaul over xDSL/FTTH	xDSL/FTTH	No support

Table 3-13: Security requirements for backhaul networks

A-ERCS segment/capability	Requirement		Status
SECC security capabilities			
SECC networks	IPSec support	Firewall / router	Required
	TLS/SSL support	Servers	Required

Table 3-14: SECC security capabilities

4. CHARACTERISTICS OF THE AVAILABLE LIVE PILOT FIELD ENVIRONMENT

4.1 Analysis of the characteristics of professional systems: service capabilities of TETRA and DMR radio systems

4.1.1 TETRA

Terrestrial Trunked Radio (TETRA) is a telecommunications standard for Private Mobile Radio (PMR) systems developed by the ETSI. The main purpose of the TETRA system is to complement existent 2G and 3G systems for prioritized delivery of voice and data services in critical situations when commercial mobile systems might fail to operate. TETRA is mainly used for professional services by organizations and units such as the police, fire departments and rescue centres, as well a maintenance services, taxi services, delivery services and security. The evolution of digital technology allows for high spectrum efficiency and coexistence with present analogue systems.

TETRA supports the following key applications that correspond to the needs of a variety of professional users:

- Secure speech and data transfer.
- Automatic vehicle location.
- Railway applications.
- Road transport information.
- File transfer & access to databases.
- Fax transfer.
- Picture transfer.
- Low definition video stream.
- Fleet management.

From the technological point of view, TETRA is based on trunking technology, where the intelligence is inside the network and not on the user terminal. It uses TDMA (Time Division Multiple Access) technology and provides 4 channels on a 25 kHz bandwidth carrier, ensuring medium/high volume traffic. Higher data transfer rates up to 28.8kbit/s are implemented by reserving up to four channels for the same user connection. Bandwidth is allocated on demand.

TETRA is a trunked system, which manages a number of calls through a Trunking Controller. It assigns the radio resource through one or more control channels. The control channel acts as a signalling communication link between the Trunking Controller and all mobile radio terminals operating on the system. The links between the radio base stations typically require 2Mb/s of bandwidth. Each repeater uses different frequencies thus the network is of cellular type, providing a cell size smaller than analogue network system (usually well under 40 km).

Three different data transmission modes are available in TETRA:

- Circuit mode, where a fixed data communication channel is established between two points. A fixed data rate of up to 7.2 kbps per channel is assigned to a connection; since data transmission is normally bursty by its very nature, this mode can be quite inefficient from the viewpoint of channel usage, and hence expensive.
- SDS (Short Data Service), which is a special service, similar to SMS in GSM, suitable for low data rate packet transmission.
- Packet data, which is a fully featured packet data communication suitable for IP (Internet Protocol) traffic; single channel net bit rate is 4800 bps.

TETRA uses three different standards for voice or data transmission:

- V+D (Voice+Data) – this standard is used for voice calls and various modes of data transmission (Circuit Mode, SDS, or Packet Data).
- DMO (Direct Mode Operation) is similar to V+D but operates without a base station; the set of available services is restricted compared to V+D.
- PDO (Packet Data Optimized) – as the name implies, this standard is specially designed and optimized for packet data transmission.

Error protection	**Data rate (kbps)**			
	1-slot	**2-slot**	**3-slot**	**4-slot**
High	2.4	4.8	7.2	9.6
Low	4.8	9.4	14.4	19.2
None	7.2	14.4	21.6	28.8
V+D	x	x	X	x
DMO	x	/	/	/
PDO	/	/	/	/

Figure 4-1: TETRA data transmission

In Slovenia, the Slovenian Ministry of Interior built the first Slovenian TETRA network in 2004 for the purposes of the Slovenian Police. The main reasons for choosing this technology were:

- Digital open standard – Multi vendor.
- IOP certification for infrastructure and terminals.
- Secure communications – Authentication, AIE & E2EE.
- Voice clarity, especially in noisy environments.

- Various possibilities for data applications (SDS, multi-slot circuit and packet switched data).
- Concurrent voice and data services.
- Efficient use of radio spectrum.
- Possibility of future enhancement – TETRA Release 2.
- Improvement of user efficiency and safety.
- EU police cooperation – cross border communications.

Advantages and benefits that were also considered when selecting TETRA for the professional system were:

- Fulfilment of Schengen requirements:
    - 2-way voice and data communications.
    - Status messaging and SDS.
    - Network controlled communications channels.
    - Fast access to the system (< 500ms).
    - Short transmission delay (< 150ms).
    - Terminal disabling (stolen or lost), priority levels etc.
- Advanced dispatcher functions.
    - Group patching and Dynamic Group Number Assignment.
    - End-to-end encryption (E2EE).
    - Data applications (e.g. file & image transfer).
    - Subscriber and group management.
- Reliability – BS local site trunking mode.
- DMO with repeater and gateway functions.

The existent Slovenian TETRA network used by the Slovenian Police comprises 25 base stations, 6 dispatchers and a central switching node with authentication and E2EE management centre. It enables connection to analogue and digital telephone networks, analogue radio networks and existent data networks. The infrastructure has capacity for approx. 20.000 users and implements 64 base stations.

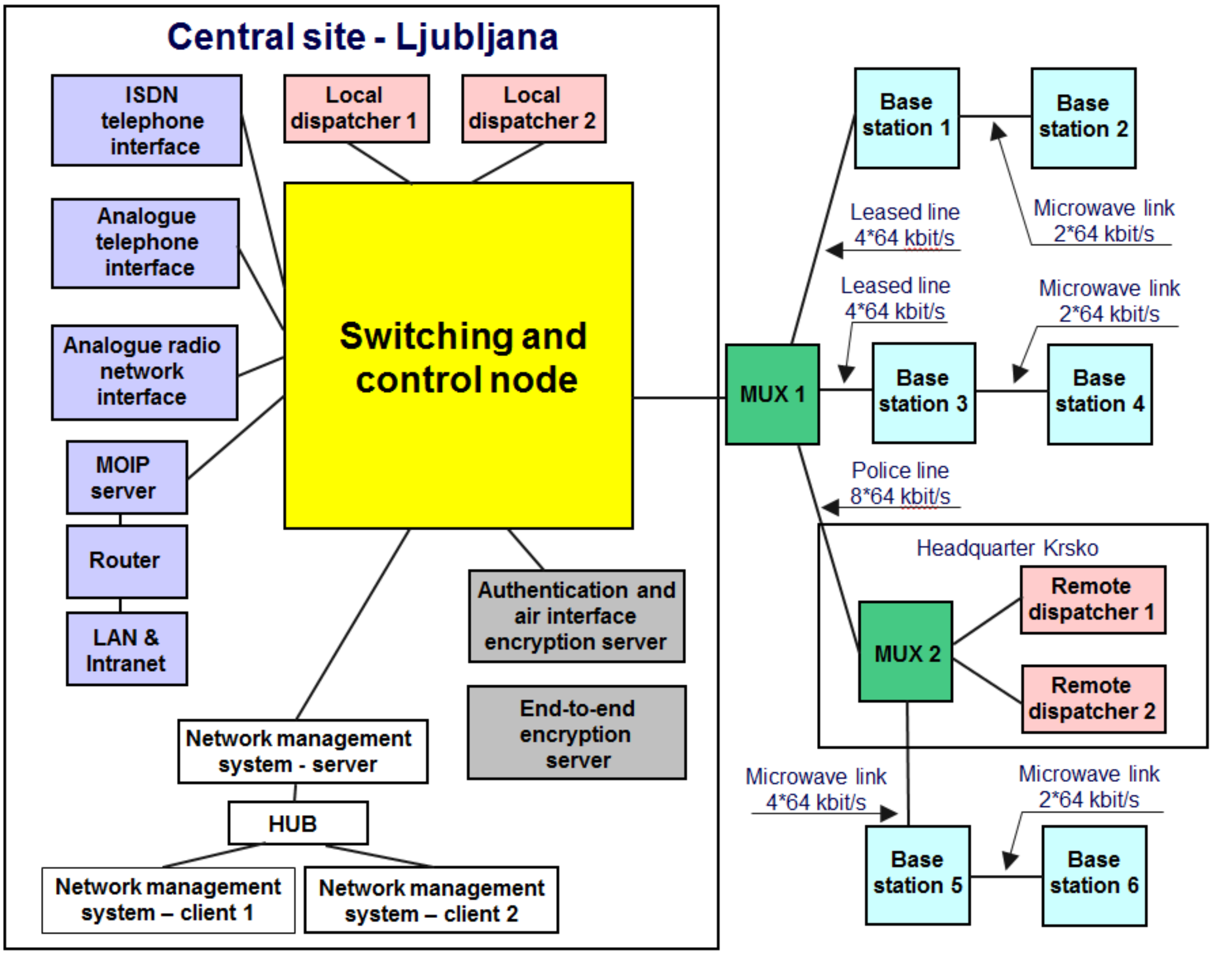

Central site - Ljubljana
ISDN telephone interface
Local dispatcher 1
Local dispatcher 2
Analogue telephone interface
Analogue radio network interface
Switching and control node
MOIP server
Router
LAN & Intranet
Authentication and air interface encryption server
End-to-end encryption server
Network management system - server
HUB
Network management system – client 1
Network management system – client 2
MUX 1
Base station 1
Base station 2
Leased line 4*64 kbit/s
Microwave link 2*64 kbit/s
Leased line 4*64 kbit/s
Microwave link 2*64 kbit/s
Base station 3
Base station 4
Police line 8*64 kbit/s
Headquarter Krsko
MUX 2
Remote dispatcher 1
Remote dispatcher 2
Microwave link 4*64 kbit/s
Microwave link 2*64 kbit/s
Base station 5
Base station 6

Figure 4-2: The Slovenian Police TETRA network topology

The Slovenian Army uses another TETRA system in Slovenia. No further information is available regarding this network.

For the time being, however, TETRA networks that exist in Slovenia are not available for the purposes of the A-ERCS pilot for administrative reasons.

4.1.2 DMR

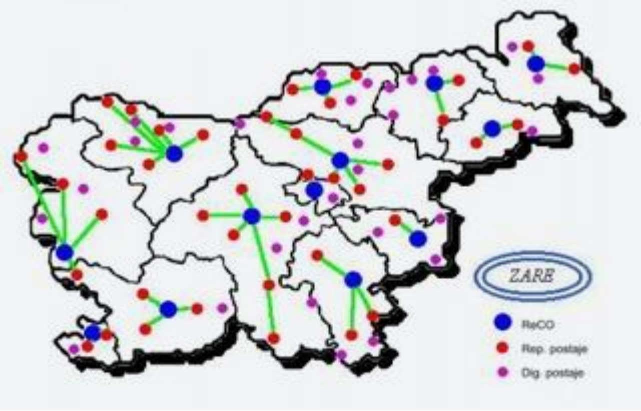
Digital Mobile Radio (DMR) is another technology that is more recent than TETRA and was developed by ETSI to grant gradual migration from the analogical conventional system to digital mode without new licenses and without changing the existing network architecture. DMR uses 2 time slots on a 12.5 kHz bandwidth carrier, using TDMA and 4-FSK modulations. The modulated signal has constant envelope, a transmitter can work in saturation (clipping) mode (C class or superior) with very low consumption (e.g., photovoltaic power sources can be used for base stations). DMR has a maximum bitrate of 9.6 kbps, and can works in simulcast mode (in star configuration, one master station and one or more satellite station) to provide a wider coverage area (up to 80 km), using a frequency pair only. Network and terminals can be dual mode, thus granting the coexistence of analogue and digital devices.

In Slovenia, the Slovenian Rescue Centre ZIR on VHF radio uses DMR system. It is used for voice communication and data communication. For example, DMR is used for national alarm system where sirens are connected to a central point at ZIR using DMR radio repeaters.

4.1.2.1 ZARE system

Also based on the DMR technology as well as on analogue radio technology, a uniform (autonomous) system of radio communications (ZARE) is in use on a national level for civil protection and rescue services in Slovenia [4]. It is used by all rescue services in the country.

The Administration of the Republic of Slovenia for Civil Protection and Disaster Relief is in charge of the technical aspect and of ensuring the disturbance-free operation of the system. The system's communication centres are located in regional notification centres, where radio traffic is managed and used to connect users to public and functional telecommunications systems. The ZARE system guarantees 95% coverage of the territory by radio signal from a stationary network, and complete territorial coverage by means of mobile repeaters.



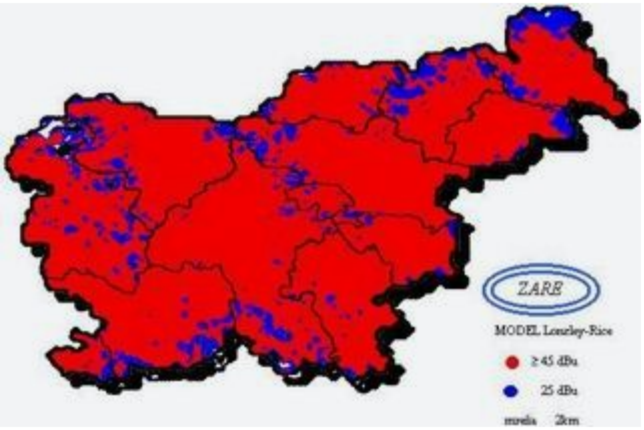


Figure 4-3: ZARE communication system [4]

The ZARE communications system is the largest single professional system of radio links (PMR) in the country. Its network consists of 40 repeaters of the high network and 56 digital base stations of the lower network. Lower network is being constantly rebuilt. Current network capabilities are limited to up to 9.6 Kbit/s with no direct support for IPv6 data transfer.

Currently, only voice communications are supported over ZARE system, either on DMR technology or analogue radio. Bearing in mind that the system is narrowband, it does not correspond to the requirements of an advanced modern ERCS system.

4.2 Analysis of the characteristics of commercial systems: IPv6 service capabilities of GPRS/UMTS/HSxPA from Slovenian mobile operators

4.2.1 Slovenian mobile operators

This chapter briefly summarizes and compares current status and stage of IPv6 deployments in commercial mobile networks in Slovenia. There are three major mobile operators in Slovenia, Mobitel (Telekom Slovenije Group), Simobil and Tušmobil. All of them are actively involved in IPv6 deployment. A short IPv6 deployment status overview for each of them is presented in the following.

4.2.1.1 Mobitel (Telekom Slovenije group)

Mobitel is the oldest Slovenian GSM/UMTS/HSxPA mobile operator. The company is in 100 percent ownership of Telekom Slovenije, d.d. It holds a 51.8%[6] market share, which also makes it the largest mobile operator in Slovenia.

4.2.1.1.1 Coverage and capabilities

The Mobitel's radio coverage and capabilities by technologies are shown in the tables and figures below.

[6] *APEK 2011 (Post and Electronic Communications Agency of the Republic of Slovenia)*

Technology	Coverage	Capacity
GSM	99.70%	
UMTS	90.60%	384 kbps
HSDPA	80.63%	7.2 Mbps (download)
HSUPA	80.63%	1.4 Mbps (upload)
HSPA+		21.6 Mbps (download)
		5.76 Mbps (upload)

Table 4-1: Mobitel – network coverage and capacity by technology

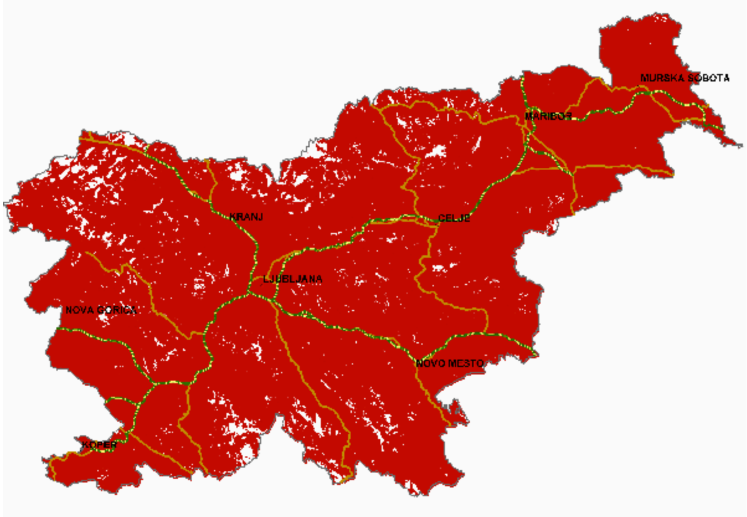


Figure 4-4: Mobitel – GSM coverage

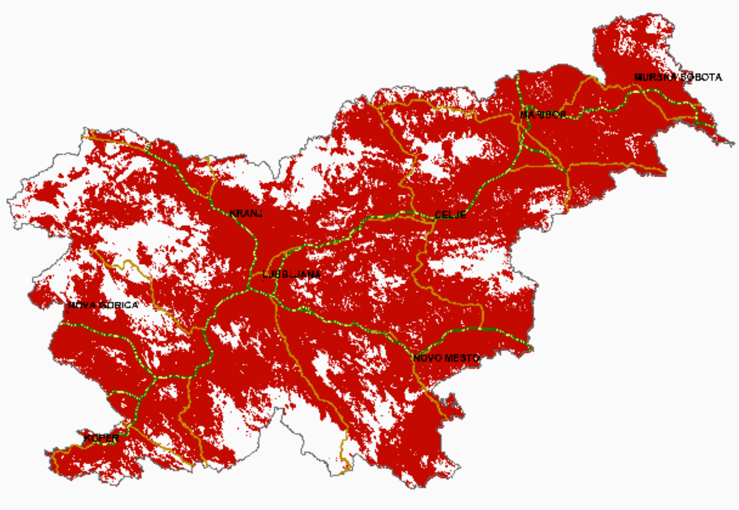


Figure 4-5: Mobitel – HSxPA coverage (outside)

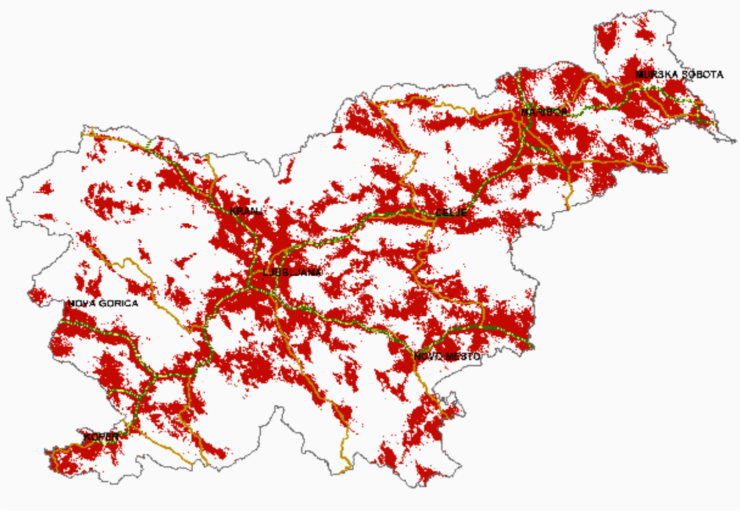


Figure 4-6: Mobitel – HSxPA coverage (inside)

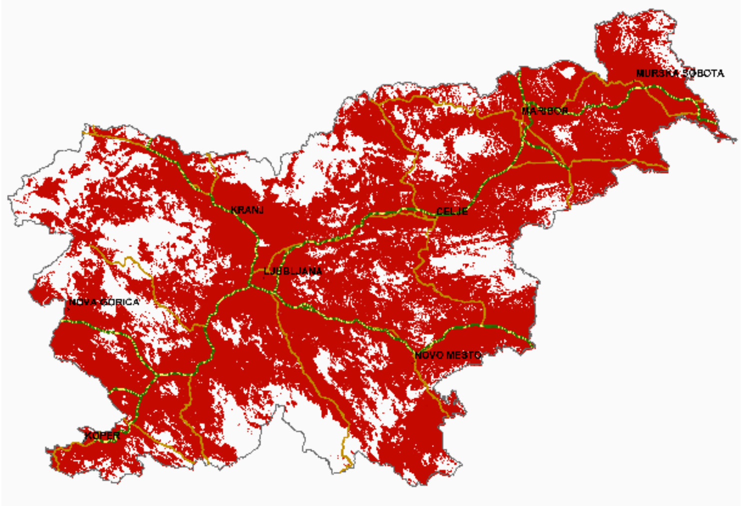


Figure 4-7: Mobitel – HSPA+ coverage (outside)

4.2.1.1.2 IPv6 support

Mobitel's address allocation scheme is as follows:

- IPv6: 2a02:e20::/32.
- AS number: 29276.

Mobitel's packet core is IPv6-ready. Currently it supports IPv6-only PDP context, IPv4 and IPv6 in the same PDP context is not supported yet.

Network equipment used in Mobitel's IPv6 network comprises:

- SGSN Ericsson Mk IV 2008B Dual Access.
- GGSN Ericsson/Juniper J120 2009A.
- MPLS Cisco 7609 Version 12.2(33)SRC2.

The network topology of Mobitel’s IPv6 network is shown below (Figure 4-8).

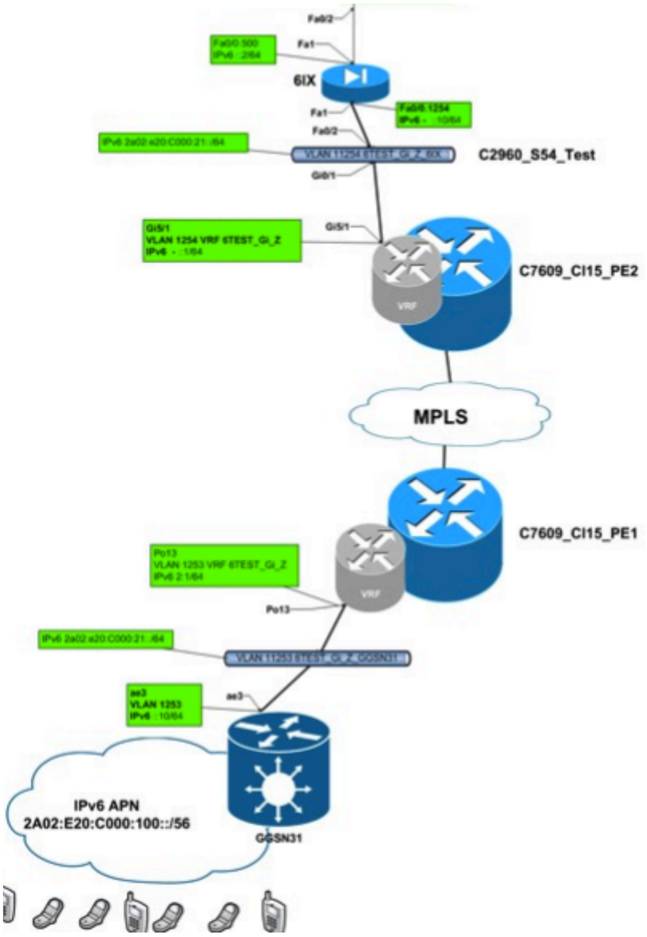


Figure 4-8: Mobitel’s IPv6 Network

Mobitel also provides IPv6 to mobile end users, each of them gets /64 prefix. Fort the time being, there is a limited set of terminals supported.

4.2.1.2 Simobil

Simobil is the second largest mobile operator in Slovenia with a 29.5%[7] market share.

4.2.1.2.1 Coverage and capabilities

The Simobil’s radio coverage and capabilities are shown below.

[7] *APEK 2011 (Post and Electronic Communications Agency of the Republic of Slovenia)*

Technology	Coverage	Capacity
GSM	99.6%	
EDGE	99.6%	236 kbps (download)
HSxPA/HSPA+	over 90%	21.6 Mbps (download)

Table 4-2: Simobil – network coverage and capacity by technology

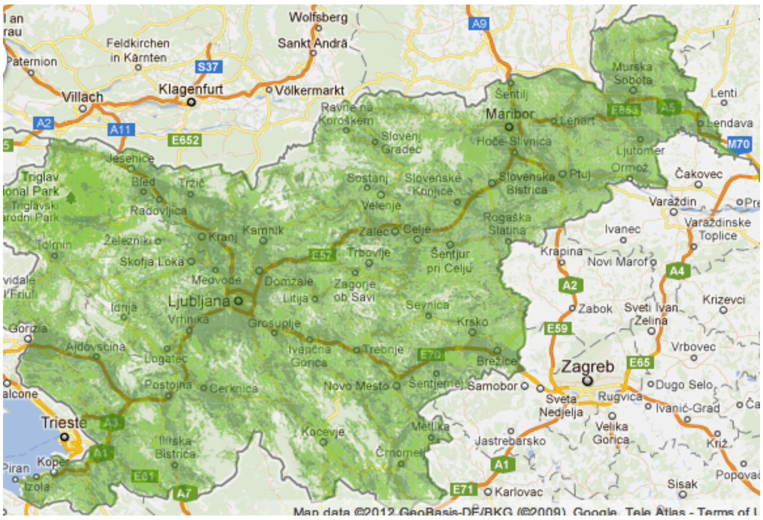


Figure 4-9: Simobil – GSM/EDGE coverage

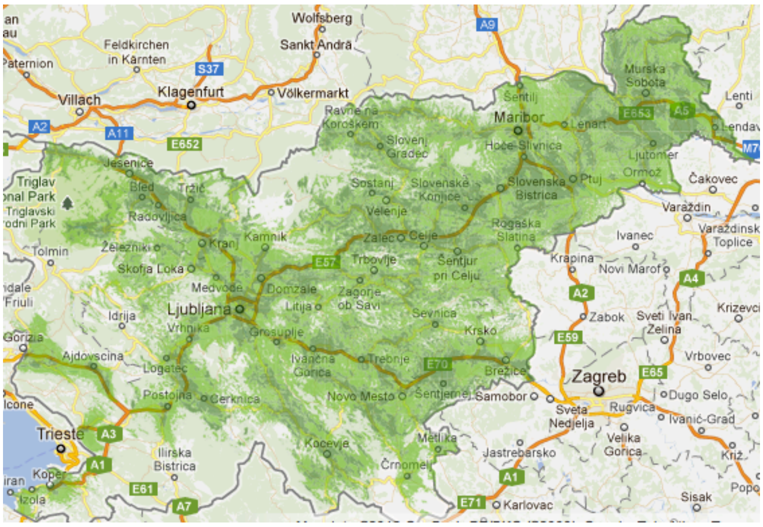


Figure 4-10: Simobil – 3G coverage

4.2.1.2.2 IPv6 support

Simobil's address allocation is as follows:

- IPv6: 2a00:1a20::/32.
- AS number: 21283.

Simobil is currently testing its IPv6 network. Their test IPv6 APN currently supports IPv4-only PDP contexts and IPv6-only PDP contexts.

4.2.1.3 Tušmobil

Tušmobil is the third largest Slovenian mobile operator with an 8.2%[8] market share.

4.2.1.3.1 Coverage and capabilities

The Tušmobil's radio coverage and capabilities are shown below.

Technology	Coverage	Capacity
GSM/EDGE	98.01%	
UMTS	77.61%	

Table 4-3: Simobil – network coverage and capacity by technology

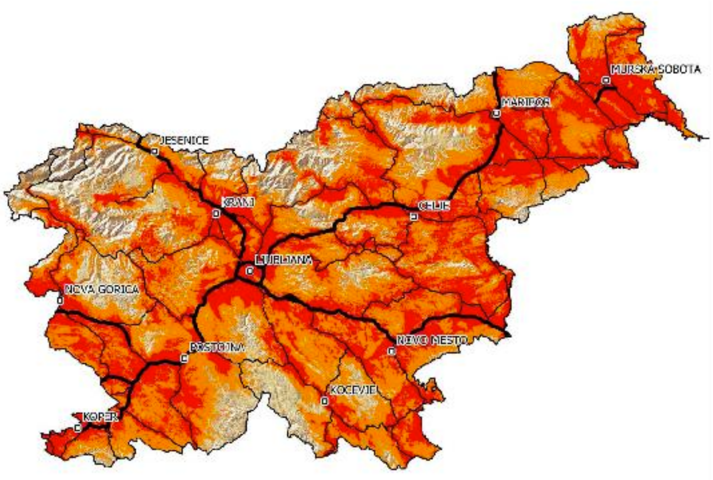


Figure 4-11: Tušmobil – GSM coverage

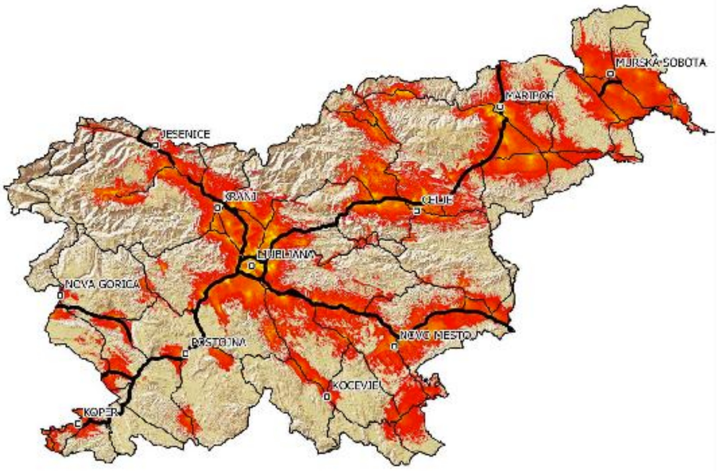


Figure 4-12: Tušmobil – UMTS coverage

[8] *APEK 2011 (Post and Electronic Communications Agency of the Republic of Slovenia)*

4.2.1.3.2 IPv6 support

Tušmobil's address allocation is as follows:

- IPv6: 2a02:840::/32.
- AS number: 41828.

Tušmobil has a packet core that is IPv6-ready.

Network equipment used in Tušmobil's IPv6 network comprises:

- SGSN NSN, SG6.
- GGSN NSN, FlexiISN v 3.2 CD7.
- Firewall Cisco ASA v7.2.
- DNS64 totd 1.5.1.
- NAT64 ecdysis-nf-nat64-20100226 @gentoo 2.6.3.

The network topology of Tušmobil's IPv6 network is shown below (Figure 4-13).

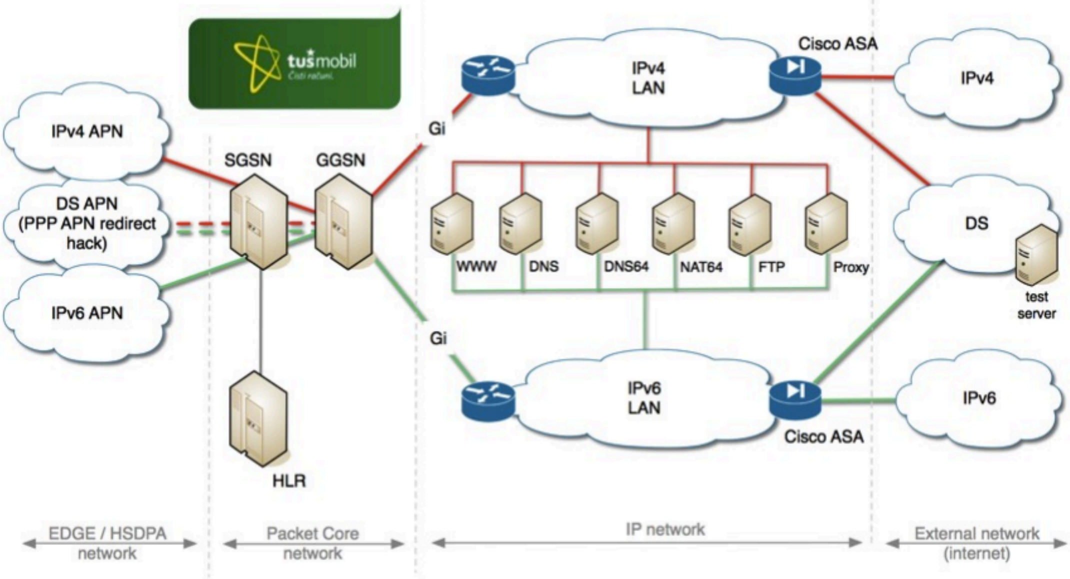


Figure 4-13: Tušmobil's IPv6 network

Tušmobil currently provides IPv6 to test users only. It has also a test implementation of a DSMIPv6 mobility system, the network scheme is shown below.

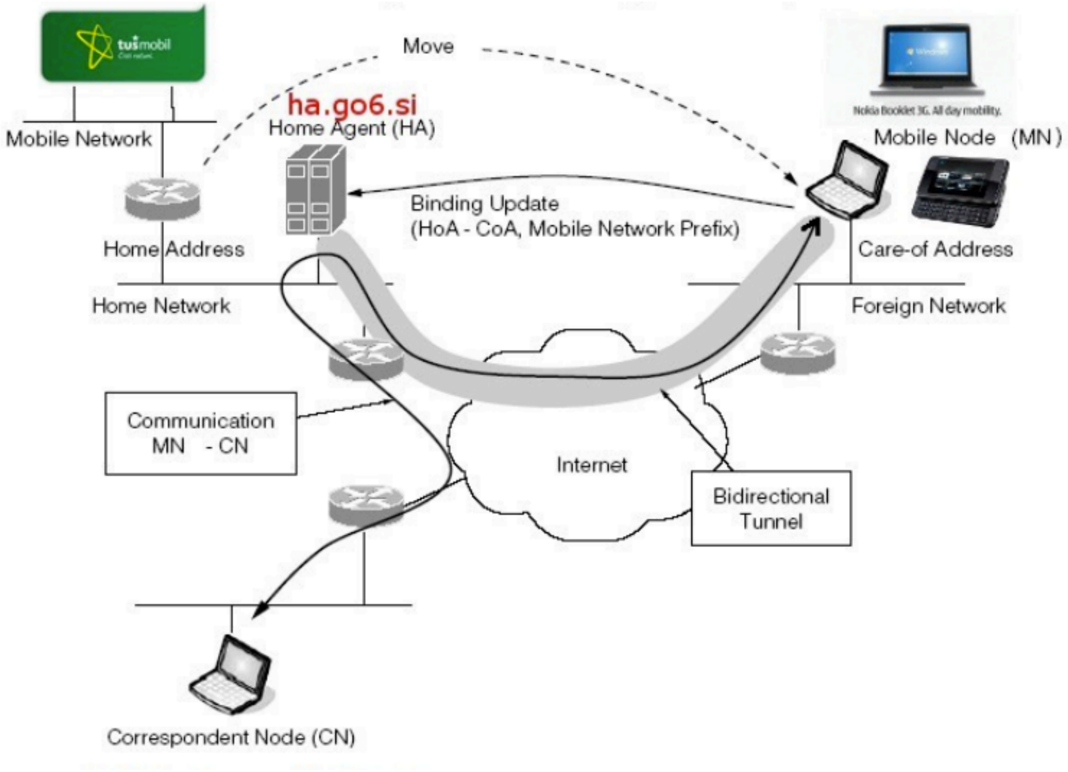


Figure 4-14: Tušmobil – DSMIPv6 mobility system

4.2.2 Comparison of IPv6 capabilities of the Slovenian mobile operators

The table below shows the comparison of IPv6 capabilities and functionalities offered by the Slovenian mobile operators.

IPv6 capability	Mobitel	Simobil	Tušmobil
Global address allocation	2a02:e20::/32	2a00:1a20::/32	2a02:840::/32
AS number	29276	21283	41828
IPv6 enabled packet core	yes	yes	yes
IPv6 enabled access network	yes	yes	yes
IPv6 PDP context	yes	yes	yes
IPv4 and IPv6 PDP context	no	no	no info
Commercial availability	yes[9]	no	yes[10]
IPv6 UE Mobility	Mobile IPv6 DSMIPv6	DSMIPv6	Mobile IPv6 DSMIPv6
Stateless autoconfiguration	yes	yes	yes
DNSv6	yes	no info	yes
DNS64	no info	yes	yes
NAT64	no info	yes	yes

Table 4-4: Comparison of IPv6 capabilities of Slovenian mobile operators

[9] *Limited terminal support*

[10] *Currently only for test users*

4.3 Analysis of the characteristics of alternative ruggedized COTS – professional mobile router network and ULFE ad-hoc mobile system

Ruggedized professional mobile router network can be used based on a mobile ad-hoc router used as the ad-hoc node. For A-ERCS purposes, such networks are built using ruggedize embedded platform with several connectivity interfaces. For this specific pilot, WiFi technologies are considered for ad-hoc network implementation on site for a range of advantages, as described in the following.

4.3.1 Wireless ad-hoc networks

A wireless ad-hoc network is a decentralized wireless network. The decentralized nature of wireless ad-hoc networks makes them suitable for a variety of applications where central nodes cannot be relied on. Minimal configuration and quick deployment make ad-hoc networks suitable for emergency situations like natural disasters and military applications. Furthermore, decentralized nature can also improve the scalability of wireless ad-hoc networks compared to wireless managed networks. However, theoretical and practical limits to the overall capacity of such networks have been identified and need to be taken into consideration.

The network topology is mesh, so each node is willing to forward data for other nodes. The data forwarding topology is determined dynamically using ad-hoc routing protocols. The decentralized nature may also improve the scalability of wireless ad-hoc networks compared to wireless managed networks. To connect the devices in an ad-hoc network we have to provide access points, which are implemented in each separate node. An ad-hoc node can interchange data between protocol incompatible networks and serve as a gateway.

The ad-hoc network has to provide special routing protocols to ensure proper routing of data packets to the nearest node based on the best routing metrics. In a robust ad-hoc network many nodes can be used to provide better distribution of traffic and increase network capacity.

For the purpose of the A-ERCS pilot, the Core Router of the A-ERCS node will be used to host the ad-hoc packet radio network. In addition to routing functions between nodes, network will support several service functions, such as:

- DHCP.
- Implementation of NAT and PAT.
- Traffic Filtering and Firewall functionalities.
- User authentication.
- Support for various end user terminals.
- Implementation of QoS features.

- Network security features.

To correspond to the requirements of the ad-hoc networks, an embedded hardware platform will be used, which must be sufficiently powerful, reliable and resistant to environmental influences and provided in a small case (small enough to fit into the SECCSU vehicle). Because of a rather large amount of traffic and various applications, it is necessary to provide sufficient peripheral capacity.

To connect nodes in the backbone network and to enable network connectivity for multiple user devices we have to provide several communication interfaces (for the purposes of the A-ERCS a selection of the following will be implemented):

- Fast Ethernet
- WiMAX (and LTE).
- WiFi.
- UMTS / HSPA.
- Bluetooth, ZigBee and RFID.
- USB and serial interface.
- I2C and SPI interfaces.
- GPIO interface.

In terms of further requirements, an ad-hoc node must ensure best possible autonomy and must rely on its own power supply. It should contain power supply regulator that adapts to a wide range of available power supply voltages, since nodes can be used in various types of vehicles. If the node will be used in the field, we must ensure autonomy with its own battery pack and with additional solar panels. Power over Ethernet (IEEE 802.3af) can be also used to power the node.

The node must operate in extreme environment conditions (wide range of temperatures and high humidity of the surroundings). Therefore the requirements are also:

- Installation of elements in a robust casing, resistant to liquid and dust - IP67 standard.
- Use of connectors that are mechanically strong, resistant to liquids, dust, vibration, EMI.

The design of packet radio system will encompass civil standards (IETF, IEEE, ITU-T, ETSI), allowing easy upgradeability and scalability of the system in the future.

A-ERCS segment/capability	Requirement	Status
Requirements for Mesh WiFi network in the A-ERCS system		
Core Router (A-ERCS node) functionalities	DHCP	Required
	Implementation of NAT and PAT	Required
	Traffic Filtering and Firewall functionalities	Required
	User authentication	Optional
	Support for various end user terminals	Optional
	Implementation of QoS features	Optional
	Network security features	Optional
Core Router (A-ERCS node) interfaces	Fast Ethernet	Required
	WiMAX (and LTE)	Optional
	WiFi	Required
	UMTS / HSPA	Required
	Bluetooth, ZigBee and RFID	Optional
	USB and serial interface	Optional
	I2C and SPI interfaces	Optional
	GPIO interface	Optional
A-ERCS node (general requirements)	Power supply regulator	Optional
	Autonomy with own battery pack	Optional
	Solar panels	Optional
	Power over Ethernet (IEEE 802.3af)	Optional
	Robust casing, resistant to liquid and dust - IP67 standard	Optional
	Mechanically strong connectors	Optional
	Support for civil standards (IETF, IEEE, ITU-T, ETSI)	Optional

Table 4-5: Requirements for Mesh WiFi network in the A-ERCS system

5. Fire Fighter Unit Proprietary Requirements Analysis

5.1 Analysis of proprietary fire fighter unit communications infrastructure

This chapter summarizes fire fighter specific requirements that are of relevance to the A-ERCS system, pilot and services planning and requirement analysis. The majority of these specific requirements are already incorporated in the requirement analyses of previous chapters. The intention of this chapter is to additionally clarify the specifics and limitations that the A-ERCS pilot is subject to.

5.1.1 Civil services organization

This chapter summarizes civil services organization and requirements as defined by the Department for Protection, Rescue and Civil Defence (URSZR). The Public Fire Fighter Service (PFFS) is one segment of the URSZR and consists of one professional and 35 Voluntary Fire Brigades (VFBs).

In general, the URSZR of the MOL uses a plan for protection and rescue that comprises:

- A plan for protection against fire – an operative fire fighter plan, covering procedures for informing and operation of fire brigades.
- An operational fire fighter plan for MOL.
- A plan for protection and rescue in case of accidents with dangerous substances.
- A plan for protection and rescue in case of flooding.
- Protection and rescue in case of massive accidents.
- Protection and rescue in case of earthquake.

Each on-site operation of the VBS is called an intervention. The procedure of executing the intervention is clearly defined along with the involved bodies, services and departments. Figure 5-1 depicts the procedures for a “rescue and protection plan in the case of massive accidents”, a case covered for the purposes of the A-ERCS pilot. As evident from the procedures, the SECSSU (marked as the leader of the intervention on site – “vodja intervencije na mestu nesreče)” communicates with fire fighter teams on the location (downward communication) and with the SECC (marked as the leader of the intervention as a whole – “vodja intervencije kot celote”). Also, additional communication of the SECCSU is fore seen to communicate with the helicopter unit of the Slovenian Army and with the operational management of the intervention, both according to individual intervention requirements. Each on-site intervention requires its own SECSSU unit.

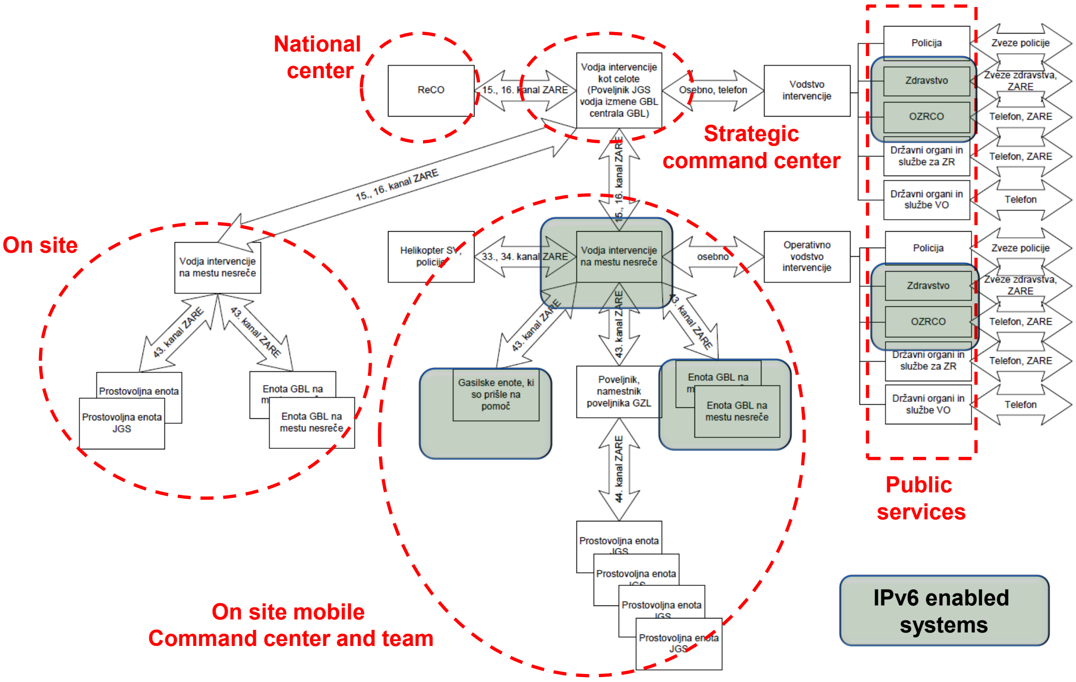


Figure 5-1: Fire Fighter department organization in the Ljubljana Municipality and entities involved in the chain of command on the national level

5.1.2 The plan of intervention and role of the VFB and the SECCSU in case of a massive accident

For the purpose of A-ERCS pilot planning and establishment, we have decided together with the SECCSU unit (representing the major external stakeholder in this project) to define the A-ERCS system and services for the purpose of interventions in case of a massive accident. An important requirement in this respect is a precondition that the A-ERCS implementation and demonstration must not in any case breach or interrupt the regular command chain, operations and specifics as defined by the OZRCO. Therefore, the following are the basic preconditions and limitations that need to be considered throughout the pilot activities.

A-ERCS segment/capability	Requirement	Details	Status
Specific URSZR and SECCSU preconditions			
A-ERCS as a whole	A plan for protection and rescue in case of massive accidents	Command chain	Required
		One SECSSU per on-site intervention	Required
		SECSSU communicates with SECC	Required
		SECSSU communicates with on-site fire fighter team	Required
		URSZR in command for fire fighter services	Required
	Communication system	ZARE, analogue voice services	Required

Table 5-1: Specific URSZR and SECCSU preconditions

Public Fire Fighter Service (PFFS) of the MOL is responsible for operating an on-site mobile command centre, operated from a specialized vehicle depicted in Figure 5-2.

5.1.3 The SECSSU unit and vehicle

The Strategic Emergency Control Centre Support Unit (SECCSU) is the on-site command centre for the intervention. It consists of 4 operatives, 1 driver/mechanic and a specialized SECCSU vehicle. Together they are able to set up an on-site mobile command centre with the entire communication infrastructure and team. The command centre is set up either directly on site or on a remote location, depending on the current situation.

In the vehicle there are four operator posts. Three operators are responsible for communication and coordination of individual on-site fire fighter teams while the fourth operator, called the controlling operator, is in command of the intervention from this unit and responsible for communication with the SECC. Each operator is equipped with ZARE system; for the time being only analogue radio (UKV) for voice services is used (even though DMR channels are also supported in the ZARE system as well as narrowband data transfer). Each operator also uses a laptop to record the intervention information and to exchange information among the SECSSU operators using LAN connectivity. In addition, connectivity to the Internet using UMTS/HSPA router is available to the SECSSU operators for situation surveillance services (exchange of intervention reports with the SECC, access to weather reports and weather forecasts, acquisition of water flow levels, Internet access).

In this project, the SECSSU vehicle will be equipped to establish the A-ERCS, more specifically, the A-ERCS node will be implemented inside the vehicle as an ad-on element (in addition to existent systems and equipment).

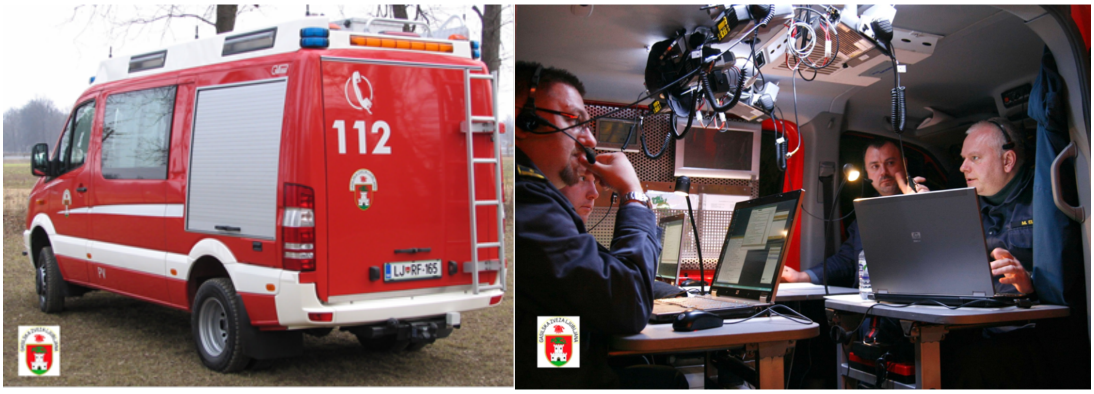


Figure 5-2: SECCSU on-site mobile command centre

6. 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.

A major phase in designing and implementing such a pilot is the requirements analysis study. This deliverable includes identification and analysis of aspects relevant to IPv6 introduction in the A-ERCS pilot with clear definition and planning of possible services, as well as initial guidelines and analyses for A-ERCS pilot planning, design and specification.

In summary, in-depth system requirements were specified from network and service aspects of the A-ERCS system. First, a high-level A-ERCS architecture was briefly presented followed by requirement analysis of the following segments: local and backhaul connectivity, self-x functionalities, automatic network planning and deployment, routing and mobility, and seamless connectivity.

Also, service requirements analysis is included, covering the following aspects: general A-ERCS service requirements, specification of target service scenarios, reuse of existent services, and aspects of urgency, security, reliability and QoS. An in-depth plan of service planning and prioritization is also provided as required by the specified service scenarios.

Added value and usability of the A-ERCS system and services for civil protection and fire fighting purposes is one of the main goals of these efforts. Therefore, special attention was given to the requirements specific to the fire fighter domain. Domain-specific requirements were studied in-depth along with an analysis of current systems and services available to the fire fighter unit, representing the basis for the implementation of the A-ERCS pilot. Proprietary communications infrastructure was studies along with organizational requirements for the fire fighter unit and the civil services organization. Also, in the entire A-ERCS requirement analysis fire fighter specifics were considered and incorporated appropriately.

The requirements study was completed in close collaboration of all involved internal and external stakeholders, foremost in close cooperation with the Strategic Emergency Control Centre Support Unit (SECCSU), with an attempt to gather realistic requirements that will serve as the core input into the A-ERCS system and services design and planning.

7. References

[1] 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

[2] IPv6 Address Prefix Reserved for Documentation, http://tools.ietf.org/html/rfc3849

[3] 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

[4] IETF RFC2080, "RIPng for IPv6"; http://datatracker.ietf.org/doc/rfc2080/

[5] IETF RFC5308, "Routing IPv6 with IS-IS"; http://datatracker.ietf.org/doc/rfc5308/

[6] IETF RFC5340, "OSPF for IPv6"; http://datatracker.ietf.org/doc/rfc5340/

[7] IETF RFC4760, "Multiprotocol Extensions for BGP-4"; http://datatracker.ietf.org/doc/rfc4760/

[8] IETF RFC3344, "IP Mobility Support for IPv4, Revised"; http://datatracker.ietf.org/doc/rfc5944/

[9] IETF RFC5213, "Proxy Mobile IPv6"; http://datatracker.ietf.org/doc/rfc5213/

[10] IETF RFC5555, "Mobile IPv6 Support for Dual Stack Hosts and Routers"; http://datatracker.ietf.org/doc/rfc5555/

[11] IETF RFC4862, "IPv6 Stateless Address Autoconfiguration"; http://datatracker.ietf.org/doc/rfc4862/

[12] RFC3315, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"; http://datatracker.ietf.org/doc/rfc3315/

[13] RFC3736, "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6"; http://datatracker.ietf.org/doc/rfc3736/