D4.1: Pilot Setup Report

Deliverable Number	D4.1
Lead Beneficiary	TUB
Dissemination Level	Public (PU)
Working Group / Task	WP1, Task 4.1
Editor	TUB (Mursel YILDIZ)
List of Authors	TUB (Mursel YILDIZ, Fikret Sivrikaya), ULHT (Rute Sofia), ZON (Ricardo Mota), UNIGE (Carlos Ballester), UNIURB (Lorenz Cuno Klopfenstein, Andrea Seraghiti, Alessandro Bogliolo), FON (Valentín Moreno, Imanol Fuidio), CMS (Nuno Martins, Alfredo Matos), LEVEL7 (Marzia Mammina, Paolo Di Francesco)
Project Month & Date	Month 26, 24.10.2012
QAT Reviewer	Fikret Sivrikaya (TUB)

Caveat from the Project Scientific Coordinator

After several reviews (which are recorded in the history table) , the project scientific coordinator, together with the Steering Committee of ULOOP, has agreed to release this deliverable with a strong caveat concerning the goals the deliverable should have covered. In our opinion, the deliverable, which corresponds to the outcome of task 4.1, required more time to reach all of the proposed goals of the task. However, in order to ensure minimum impact in the project, and as the pilot is only required in year 3 of ULOOP, **TUB, which is the editor of D4.1 and also the task 4.1 leader, has agreed in taking care of the missing aspects under task 4.2, via a new deliverable – D4.1.1.**

This new deliverable – D4.1.1 – shall be made public, and has as editor TUB. It will be released until month 30 of the project. The deliverable shall be focused on completing at least the following aspects:

- Adequate description of each pilot site, comprising (but not limited to): i) small description and site architecture, as well as site purpose; ii) main features in terms of both hardware and software provided; iii) types of interfacing available within the pilot and to the local community; iv) expected average number of users (e.g. daily, weekly, monthly); v) user profiles; ovi) peration description within ULOOP; vi) how partners can gain access; vii) whether or not access to the external community is provided; viii) types of tests envisioned; ix) limitations and requirements; x) concrete roadmap to set the site (until month 30).

Address the goals that were not met for the pilot, namely, aspects related to interoperability and scalability – what the pilot is intended to analyse, e.g. impact in terms of federated environments – and also aspects related to statistics and traces gathering – if the pilot intends to release traces or statistics to the global community.

24.10.2012, Lisboa, Portugal

The ULOOP Project Scientific Coordinator,

Helena Rute Esteves Coralho Sofia

Executive Summary

This document represents deliverable D4.1 of the EU FP7 ICT project ULOOP (*User-centric Wireless Local Loop,* grant Number 257418). The document is intended to provide a roadmap and instruction sets for successful deployment of ULOOP functionality in experimentation and demonstration sites.

The document corresponds to the outcome of task 4.1 and discusses the specifications as a pilot setup report. In addition to these specifications, guidelines for experimentation and demonstrations are clarified for the WP5.

This deliverable comprises technical description of ULOOP experimentation and demonstration sites, and discussion on federation of sites and assessment methodologies for pilot experimentation.

History

Version	Date	Author	Description
1.0	19.10.2012	Muersel Yildiz	First release
1.1.	20.10.2012	Fikret Sivrikaya	QAT review
1.2.	23.10.2012	Rute Sofia	PSC Review
1.3	24.10.2012	Several partners	SC Review
1.4	24.10.2012	Rute Sofia	Deliverable release

Table of Contents

List of Figures

List of Acronyms

Acronym	Meaning
3G	3rd Generation
3GPP	3rd Generation Partnership Project
AP	Access Point
BOWL	Berlin Open Access Wireless Lab
CAC	Call Admission Control
GUI	Graphical User Interface
IGP	Interior Gateway Protocol
ISP	Internet Service Provider
LIR	Local Internet registry
LTE	3GPP Long Term Evolution
LTE EPC	LTE Evolved Packet Core
MAC	Media Access Control
MPLS	Multiprotocol Label Switching
MM	Mobility Management
NED	Network Description
OSFP	Open Shortest Path First
OS	Operating System

Acronym	Meaning
OSN	Online Social Network
OTcl	MIT Object Tcl
QoE	Quality of Experience
QoS	Quality of Service
RM	Resource Management
SJM-ILL	São João da Madeira – Industrial Living-Lab
SME	Small and Medium Enterprises
SNR	Signal-to-Noise Ratio
SOHO	Small Office Home Office Network
SSID	Service Set Identifier
TM	Trust Management
UE	User Equipment
ULOOP	User-centric Wireless Local Loop
UWiC	University of Urbino Wireless Campus
VIP	Very Important Person
VoD	Video on Demand
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access

Acronym	Meaning
WiMAX CSN	WiMAX Connectivity Service Network
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WP	Work Package

Acknowledgements

We would like to thank all task partners involved in the preparation of this document and those who provided constructive feedback on the deliverable.

1. Introduction

<ULHT: Rute Sofia, Marzia Mammina, LEVEL7: Paolo Di Francesco, TUB: Mursel Yildiz>

Today's mobile and wireless infrastructure networks depend on extremely reliable network elements connected together with high-quality links to provide global broadband connectivity. Although this architectural approach to building networks has been very successful as manifested by the billions of connected devices, it nevertheless has its drawbacks. CAPEX and OPEX, for example, are rapidly increasing while complexity in operation and management hinder the introduction of novel features.

An alternative, unconventional approach to today's mainstream telecommunication standards is to adopt the user-centric Wireless Local Loop (ULOOP) model, which exploits the increasing expansion of wireless access networks in order to deploy autonomic and self-organizing wireless community networks.

This document describes the work developed in task 4.1, which covers aspects related to the specification of the pilot, the environment to be considered, as well as the specific diagram of interconnection of the different sites. The outcome of this task will dictate not only experimentation, but also demonstrations to be performed in WP5. Main topics addressed in this task are:

- To provide the global interconnection scheme of the pilot, including statistical details such as the number of APs and expected number of end-user equipment that each site regularly has access to;
- To assist in the adequate setup of the technical scenarios devised in WP2 and which will be the basis for large-scale experiments as well as for demonstrations.

The pilot setup activity will rely on current best practices in the industrial and academic communities to reach an efficient experimentation and validation phase. This task will consider OneLab2 federation paradigm as one of the main means for pilot setup including several test-beds. It will reuse resource reservation and monitoring concepts and solutions designed in OneLab2 in order to rapidly setup an experimental platform to validate ULOOP concepts.

1.1 Deliverable Organization

This deliverable consists of five main sections. After the very first introductory section, the detailed technical information and the definition of ULOOP pilots are provided in the second section with the title of ULOOP Pilot. This section is also devoted for the technical descriptions of ULOOP demo and experimentation sites, where corresponding roadmaps for successful implementations is additionally included.

After the second section, the deployment considerations are discussed in Section 3, touching briefly on the ULOOP technical use cases. The fourth section, namely, the experiment request template, follows the third section. Finally we provide a summary of the deliverable.

2. The ULOOP Pilot

<ULHT: Rute Sofia, LEVEL7: Marzia Mammina, Paolo Di Francesco>

In addition to simulation tools, the ULOOP consortium has agreed to develop a pilot, which could assist in both experimentation and demonstration of ULOOP concepts, as well as in the dissemination of ULOOP to the global R&D community. This pilot is therefore intended as one possible (but not the single one) embodiment of a ULOOP architecture, being the main motivation to assist ULOOP testing in large scale, and also to acquire information (statistics and traces) concerning user-centric networkings. As the project continues and findings start to be released in terms of milestones, it is possible to have other entities keen to become a demonstration site.

2.1 Assumptions, Requirements

During the development of WP2, and in regards to the overall design of the ULOOP architecture as described in D2.3 [1], a few requirements have been agreed upon and are the basis of current ULOOP operational design choices, as well as implementations. We cover such requirements in this section for the sake of readability.

2.1.1 Customer Premises Equipment

2.1.1.1 End-user Equipment

End-user equipment in ULOOP relates to notebooks but also to smart-phones, or even 3G phones. From a consortium perspective, the **minimum list of support** to be provided is:

- Android OS, versions 2.x (2.2 and above).
- UNIX systems, kernel version 2.36 and above. The default UNIX flavor is Ubuntu.
- Windows 7.
- MacOS.[1]

[1] Windows and MacOS are operating systems that shall be contemplated for specific technical blocks of ULOOP and not necessarily for the integrated ULOOP software suite. For instance, the MTracker

The exact versions of each operating system are to be agreed upon in WP4, for the pilot setup.

From a hardware perspective, the minimum list of support to be provided is:

- Smart-phones
  - Android capable.
  - At least 512Mb RAM.
  - At least 16Gb storage.
  - Wi-Fi: 802.11b/g.
- Laptops
  - NIC chipset: **Atheros**.
  - Ideally, at least 1Gb RAM.

2.1.1.2 Gateways, Access Points

A part of the ULOOP functionality is to go into access points, be it integrated with residential gateways, or isolated. The ULOOP consortium will consider the following guidelines as mandatory for ULOOP access points:

- EU compliant
- 802.11g/b, ideally 802.11n support – 2.4GHz
- NIC chipset: Atheros, ideally AR7240, AR2315.
- Flash memory: 8Mb; SDRAM: 32Mb
- Support for Open-WRT.
- At least 1 Ethernet port.

2.1.2 Access Equipment

Part of the ULOOP functionality shall be interoperable to the access. Concrete tasks that relate to interoperability to the access are:

- Task 3.4, concerning ULOOP to non-ULOOP systems interoperability.
- Task 3.4, 3.3, 3.2, and 3.1 concerning offloading aspects from 3G or LTE to ULOOP systems/nodes.

---

software developed in task 3.3 is expected to run in UNIX and MacOS, as well as Windows, in addition to Android.

The exact access equipment to be considered is expected to be provided by ULOOP partners that are involved in the Access, namely: ALBLF, HWDUand Level7 during the development of Task 4.1.

2.1.3 Backbone Equipment

Parts of ULOOP functionality are expected to be also deployed in servers, which may be part of the service backbone. In what concerns servers, ULOOP experimentation shall be provided for servers running Ubuntu, 64 bits or 32 bits, and where the kernel version is at least 2.36.

2.2 Goals

< ULHT: Rute Sofia, LEVEL7: Paolo Di Francesco>

As briefly explained previously the ULOOP pilot is intended to be an experimental infrastructure that serves both the consortium and also the overall R&D community. There are three main categories of goals to be considered:

- **Experimental / Demo related aspects**. By providing different experimentation sites based on specific and different hardware, the pilot will assist partners to understand implications that cannot be foreseen via local test-beds, with dedicated hardware.

- **Scalability and interoperability aspects**. One of the most critical issues is related to the barriers and challenges that must be taken into account to expand the site from few nodes to hundreds or thousands. For this reason it is essential that scalability should be taken into account to boost the architecture embracement while interoperability aspects make more appealing the possibility of joining the experiments by external entities with little or no effort.

- **Traces and statistics gathering**. One of the main contributions of the ULOOP pilot is the integration of an interface that allows exploiting the diversity of hardware and of users available in the different sites, to extract specific statistics and traces related with ULOOP aspects such as: trust management (e.g. social structures developed based on ULOOP exchange); strength of the cooperation developed; resource management; mobility estimation aspects. This data shall be provided to the public, and the design of the interface is expected to occur in Task 4.2.

3. Experimentation and Demonstration Sites

<ULHT: Rute Sofia, LEVEL7: Marzia Mammina, Paolo Di Francesco>

The next sections go over the experimental sites and the demonstration sites in ULOOP. In the following paragraphs each site is detailed under various aspects.

3.1 Level7 Site

<LEVEL7: Marzia Mammina, Paolo Di Francesco>

Level7 is an Italian WISP that provides commercial Internet access and other added values services (e.g. VoIP). The coverage of each service depends on the service itself: fixed wireless in center-west Sicily (south Italy), xDSL services in Italy, VoIP services in Italy and fiber access across the globe. Level7 has its own infrastructure that consists of servers, access points, radio links (between 500km and 1.000km of proprietary links in Sicily), fiber access and IP address space (both IPv4 and IPv6). Level7 is also a LIR with a specific Autonomous System (AS197506) connected in Rome to other various National and International AS.

3.1.1 Access Network

The Level7 ULOOP access network will consist of two main approaches in order to better investigate the maximum flexibility. The first approach (node type-1) consists in the possibility of “terminating” the access network in a manner that does involve the possibility of terminating the Wi-Fi and/or hiperlan radios towards some central routers/devices. On one side this approach limits the possibility to fully customize the devices and limits the range of possible experiments but on the other side it boosts the technology adoption.

The second approach (node type-2) is more radical and it is based on the implementation of new nodes with the possibility of remotely uploading the firmware directly into the node without the direct intervention or without the need of putting a new compact flash into the device. The technology will consist of the node architecture shown in the following picture.

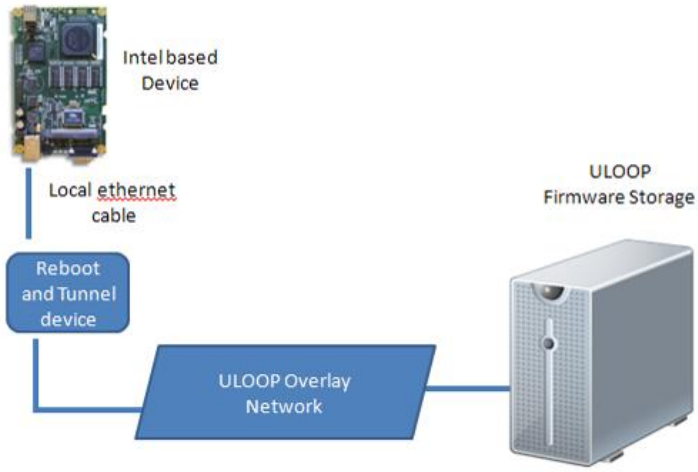

Figure 1: Node type-2 description

The main idea is quite simple, in principle. The Alix board will be the target of the customized firmware. Once the firmware is uploaded into the server the *Reboot and Tunnel device* directly connected to the Alix board will reboot the machine and the firmware will be loaded in real time. From the point of view of the Alix board (the real node), the Ethernet will be directly attached to the TFTP server, making it possible to start from LAN.

Level7 plans to deploy 5 nodes of the architecture shown in the picture in different locations in Sicily and also make them available to possible external entities (see experiment request in order to use those nodes). The overall bandwidth will be 4 megabits, and the connection will be filtered (e.g. no P2P such as emule, bit-torrent).

For the type-1 nodes, Level7 plans to deploy only a few (2-3) of this type of nodes, but in the future the number can grow.

Users' credentials will be provided accordingly to the local law and policies and more details will be available on the ULOOP web site.

Moreover Level7 will also implement some measurements, coherently with the operational constraints due to the fact the ULOOP network is running on top of the real Level7 infrastructure,

3.1.2 Core Network

The Level7 core infrastructure is connected to the global Internet in Rome. As Level7 is an autonomous system it directly announces the route and the address objects to the other autonomous systems via BGP.

Obviously the ULOOP infrastructure and experiments will not directly impact the commercial core network. Indeed the principle is that all the ULOOP nodes, services and server will run in the most transparent way on top of the commercial network but virtually separated.

The ULOOP nodes will be as much “transparent” as possible in regards to the core network, and where possible the access network will be transported over the commercial network and terminated directly (or almost directly) to the Internet.

Level7 can also assist to connect part of the ULOOP network directly with partners, via VPN or other techniques, after credential release.

3.1.3 Addressing

Level7 will allocate 128 Internet-routable public IPv4 and various IPv6 addresses. The IPv4 addresses will also be bound to valid credentials via Level7 AAA-Radius facility or they will be associated to partners requesting a specific experiment accordingly to the local laws.

The IPv4 address space will be in the form of: 31.44.X.Y/25 while the IPv6 address space allocation strategy still must be decided, but at the current date it will be “site-driven”, i.e. a specific IPv6 network address space will be allocated to the single node of the ULOOP infrastructure.

The address release procedure is experiment based, but the default methodology is that the IPv4 address will be taken from an IPv4 pool and dynamically associated to customers.

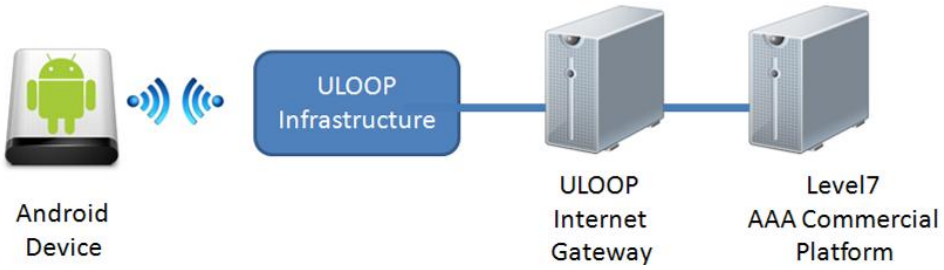

Figure 2: Actors involved in IP release

3.1.4 Interconnection

Level7 ULOOP infrastructure interconnection is possible at the following conditions:

- The entity requesting interconnection should clearly state which part of the Infrastructure / Services should be interconnected.
- The entity should provide a valid reason why “over the Internet” is not enough to carry on the experiments; The procedure to interconnect with the Level7 facilities will be processed on case by case basis sending the request by email to: uloop-project@level7.it

3.1.5 Servers

Level7 will provide the usual services such as:

- DNS
- Radius AAA
- SSH access to selected services

Moreover Level7 makes also available the IDvalidator and the SMS server platform, which are interfaced with the commercial AAA platform, in order to validate the user identity.

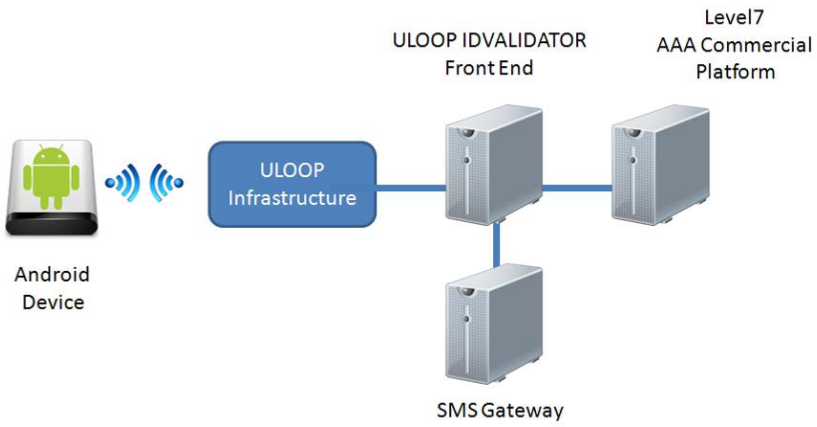

Figure 3: IDvalidator architecture

Another feature that could be open to external entities will be the possibility to upload the operating system image and do the reboot of a specific node. At the current stage this possibility is still under development and any news will be made available via the ULOOP website.

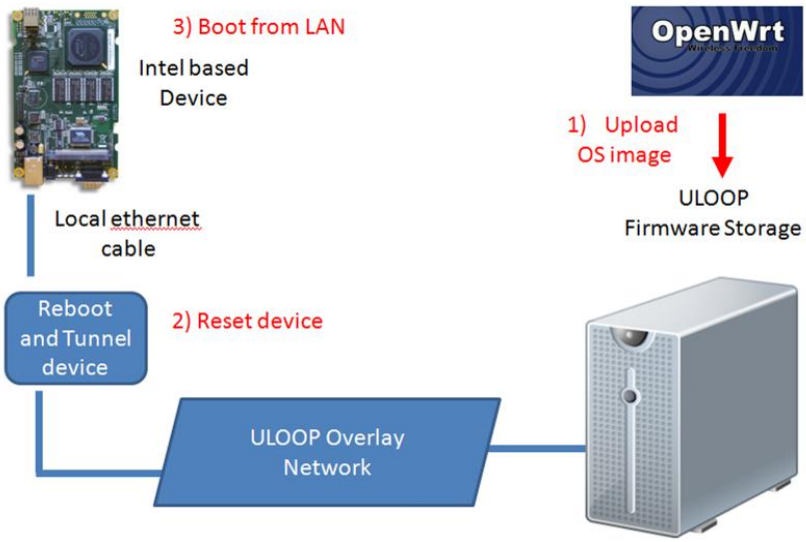

Figure 4: Booting Principle

Restricted access to these facilities can be provided upon request.

3.1.6 Measurement-Taking and Control & Monitor Specifications

Level7 will give to partners the following facilities:

- The IDValidator platform is available to partners requesting strong authentication to Level7. The access, considering that the platform has some operational costs, must be approved before availability.
- The Level7 type-2 nodes will be controlled via a private web based facility.

3.1.7 Experimentation or Control & Monitoring Procedure for Partners in ULOOP

Level7 provides to external entities and to ULOOP partners the following support procedures:

- Leve7 can be contacted by email for any request or support regarding the ULOOP testbed to the following address: uloop-project@level7.it
- Level7 can be contacted for urgent issues at the following phone number: +39-091-8776432 (as for an English speaker). The business hours are Monday-Friday from 9:00am to 17:30pm and out of business hours a message can be left at the vocal message box.

The monitoring facilities access, if public facilities will be made available, will be also be documented on the ULOOP Project website.

3.1.8 Limitations and Challenges of the Site

Level7 ULOOP testbed is lying on top of a commercial network and therefore the ULOOP traffic should not disturb or interfere with the Level7 commercial operations. That is the main challenge in order to validate the ULOOP general architecture. Indeed it is forecasted that before the end of 2012 the architecture will be mostly operative and ready for partners' experiments and it will continue to evolve during year 3 of the project.

The most significant limitation is that anonymous access to the Internet cannot be provided and therefore a real ID must be given to Level7 (that will be stored in its registry) in order to gain real Internet access.

3.2 University of Urbino Site

<UniUrb: Lorenz Cuno Klopfenstein, Andrea Seraghiti, Alessandro Bogliolo>

3.2.1 UWIC Short Description

The Urbino Wireless Campus (UWiC) is a wireless Neutral Access Network (NAN) managed by partner UniUrb in Italy. UWiC is currently composed of more than 100 Wi-Fi hotspots (running either Mikrotik RouterOS or OpenWRT) and 7 Hiperlan base stations (running Mikrotik RouterOS) covering the metropolitan area of Urbino, the University buildings, and students' dorms. The Hiperlan backbone is independent of the University intranet, so that the access network does not expose critical data or services and it is not part of the Internet. Policy constraints can be significantly relaxed, making it possible to share the access infrastructure with third party ISPs and to provide information services to unauthenticated users. Each ISP working on UWiC has his/her own edge router within the access infrastructure, in order to be allowed to provide his/her services without further agreements with the access network manager. In addition, services can be directly hosted within the service sub-network of UWiC in order to be made accessible to users who are not registered with any ISP. The UWIC server farm is composed of 20 virtual machines running Linux OS.

Since 2006, UWiC has been used as a living-lab for interdisciplinary research in the field of access networks. The UWiC project has involved about 50 partners (including municipalities, WISPs, vendors, service providers, wireless communities, and WiMAX operators). UWiC counts with more than 20,000 registered users. Among them, more than 5,000 are active users who used the wireless network at least once and gained access to the Internet through the edge router of UniUrb. On average, the Wi-Fi access network is used by 300 nomadic users simultaneously, with peaks of 500 simultaneous users. The geographic distribution of users changes over time: at night most of the accesses come from the students residences, while during the day most of the accesses come from university buildings and public places.

Figure 5 and Figure 6 show the Wi-Fi and Hiperlan coverage areas.

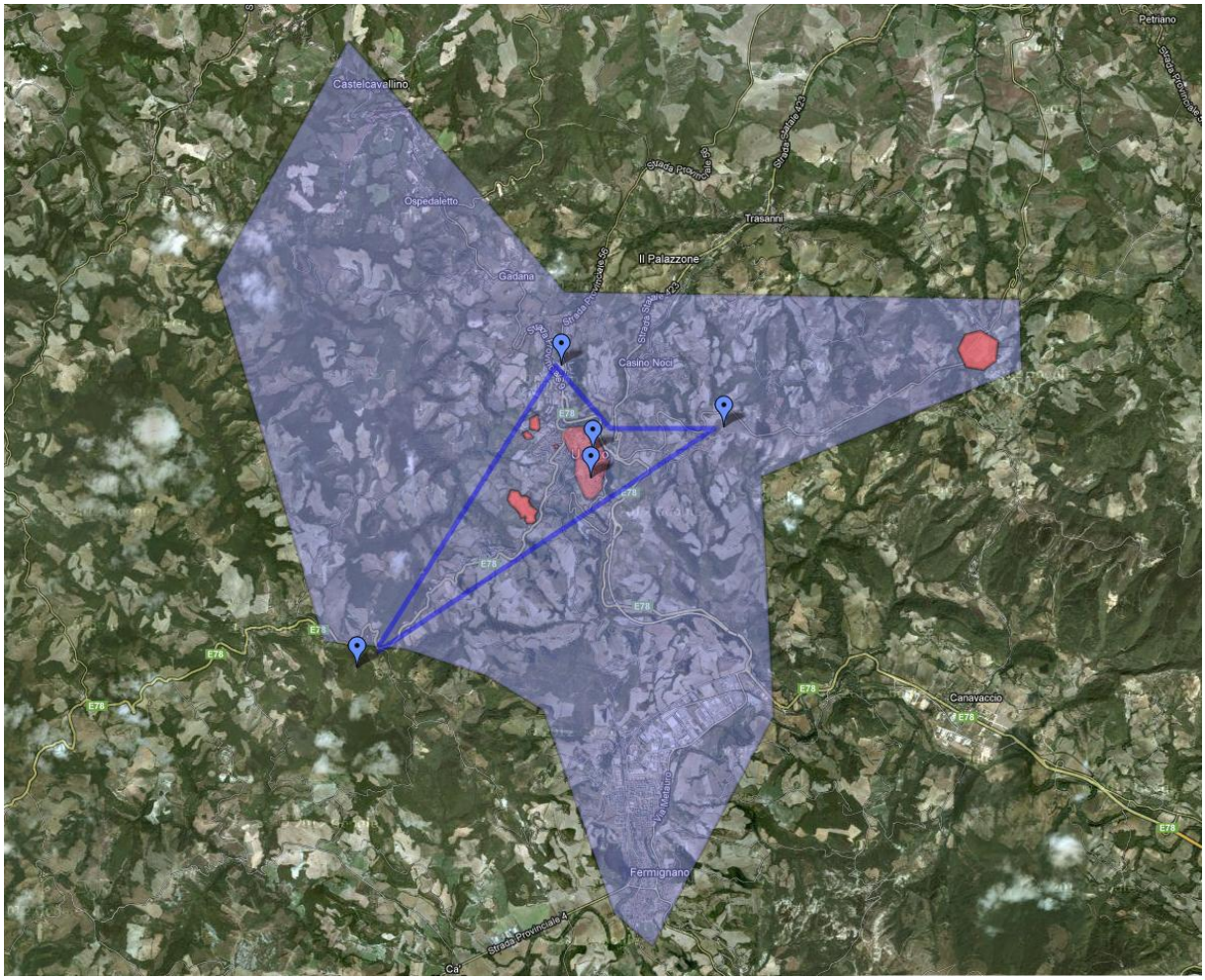

Figure 5: Full coverage of Hiperlan backbone (blue) and Wi-Fi coverage (red).

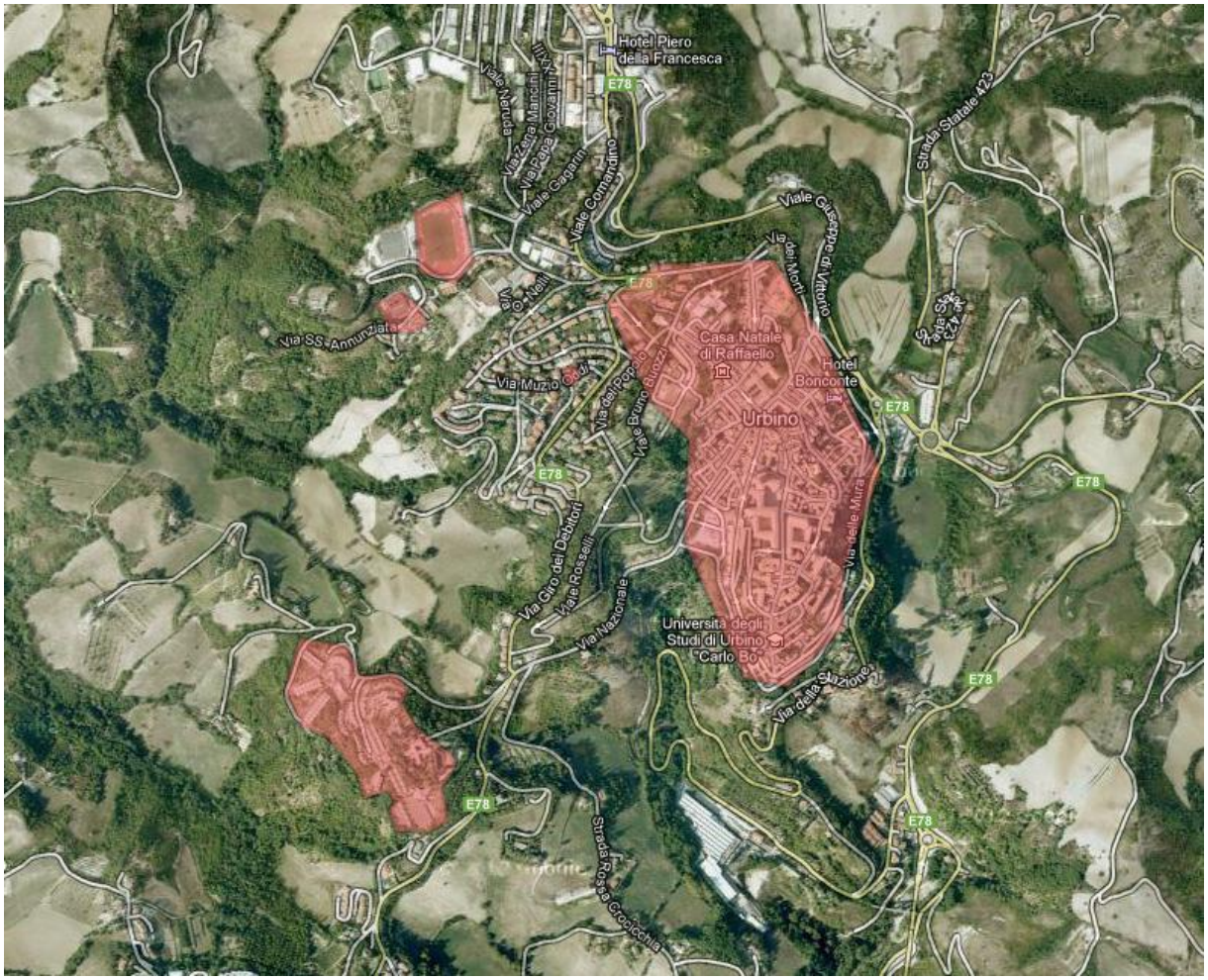

Figure 6: Detailed coverage of the Wi-Fi hotspots on the urban area of Urbino.

3.2.2 Network Architecture

The network architecture encompasses an access network, made of Wi-Fi hotspots and Hiperlan base stations, and a backbone, made of point-to-point Hiperlan bridges and fiber links. The backbone is a closed ring managed by means of dynamic routing to provide link redundancy. The Wi-Fi access network is managed as an open-access MAN with a centralized captive portal which allows end-users to gain access to local services and to the Internet gateways of their choice. The Hiperlan network is protected by means of WPA2 since it is used both to provide access to residential university users and to interconnect university buildings. The Hiperlan backbone also provides backhauling to nomadic users associated with Wi-Fi hotspots.

The different usages of the shared backbone are logically separated by means of different addressing policies, as detailed in the following paragraph.

3.2.3 Addressing

UWiC makes use of private IP addresses in the following ranges: 172.20.0.0/16 for university buildings, 172.31.0.0/16 for Hiperlan devices, and 10.83.0.0/16 for end-users. While addresses in the first two ranges are statically assigned, addresses in the 10.83.0.0/16 range are dynamically assigned by the DHCP server running either on the hot spots or on the base stations. Each one of the 4 nodes of the Hiperlan ring (composed of at least a base station and 2 point-to-point bridges) is seen as an autonomous system by the dynamic routing protocol (i.e., BGP).

The access network has a hierarchical organization: each hot spot is the default gateway of its access island and it routes IP traffic towards a centralized default gateway which plays the role of captive portal by blocking unauthenticated Internet traffic, granting access to local services, and allowing end-users to choose their own ISP.

The gateways of ISPs have their local interfaces in the UWiC service sub-network, with addresses in the range 10.89.42.0/24. As soon as the end-user makes his/her choice, all his/her traffic is forwarded to the corresponding gateway by means of Linux source-based policy routing.

3.2.4 Servers

The UWiC server farm consists of about 20 linux-based VMware virtual machines running on top of a HP DL385 G6 with 2 6-core processors with 16GB of RAM and 1TB RAID 5 HD. The server load is below 60%.

The VLAN support provided by the virtualization system has made it possible to virtualize some of the core routers, including the defaults gateway which implements policy routing.

3.2.5 Interconnection

UWiC adopts the neutral access network (NAN) model, which provides scalability and interoperability features.

Interoperability can be achieved by creating a tunnel (or a physical link) between the service subnetworks of two different NANs. The source-based policy routing mechanism used to provide multi-gateway capabilities to a NAN can be used also to grant access to the services provided by another NAN. To this purpose, the local interface of the tunnel leading to the other NAN has to be treated as a gateway.

Scalability is guaranteed both by the hierarchy (which makes it possible to add at any time new access islands to the networks), and by load balancing among multiple policy routers.

3.2.6 UWiC as a ULOOP Pilot

In order to provide ULOOP-specific services within UWiC it is possible either to instantiate dedicated virtual machines to be added to the server farm, or to create a tunnel providing a local interface to a remote server (possibly hosted and/or managed by a partner).

As for the possibility of granting to the partners full control of some of the hot spots, it is possible to install dedicated ULOOP-enabled hotspots and to make them remotely accessible by means of VPNs.

In addition, it is possible to exploit the modular architecture of UWiC to allow a partner to install a UWiC access island on its own site. The remote access islands can interoperate with UWiC by means of tunneling.

As for the use cases, it is worth mentioning that UWiC is a Wi-Fi open-access network, which allows any end-user to associate with the Wi-Fi hotspots for free without registration/authentication. This means that ULOOP services can be made directly available to end-users from the captive portal and that some Internet connectivity can be provided to support ULOOP bootstrapping.

As a final remark, students, who represent the majority of UWiC users, gain access to the Internet for free through the University gateway, while all other users (citizens, tourists) have to buy Internet bandwidth from the ISPs, which operate in UWiC.

3.3 Technical University of Berlin Site

<TUB: Mursel Yildiz>

This section is devoted to the technical specifications for the Berlin Open Wireless Lab (BOWL). In addition to the technical specifications, two detailed roadmaps are provided for i) the configuration of BOWL site for ULOOP and ii) the experimentation or the control & monitoring procedures. Finally the BOWL operation context in ULOOP is discussed.

3.3.1 Introduction to BOWL

BOWL is established by the Deutsche Telekom Laboratories as a wireless experimental networking platform for mobile Internet research and development. The main perspective of the BOWL testbed is to provide the Wireless Network research community with an open research platform [5]. BOWL provides additionally Internet access for the TUB campus and due to this fact the real-world performance of the proposed ideas might be explored through live-traffic with BOWL testbed.

The main focus areas of BOWL testbed are exploring future Internet architectures, mobile Ad Hoc networks, distributed systems, traffic measurements or analysis and finally the mobile networking and wireless systems. The advantage of BOWL testbed lies on the real-traffic opportunity rather than artificial traffics created for the evaluation of new proposals, when compared to the accustomed indoor-wireless testbeds.

The real Internet access for the campus is prioritized during the experimentation run time through fault-tolerant network architecture. In order to maintain the Internet access for the campus, an experiment on BOWL testbed requires 3 sub-phases, namely, indoor-test, smoke-test and finally the outdoor-test. The aim of these additional progresses is to guarantee an error-free implementation of the proposals. In other words, the experimentation on the outdoor BOWL testbed requires additional countermeasures against contingent system failures due to the proposed solution.

The BOWL testbed deploys more than 100 nodes around the TUB campus of which 54 are indoor nodes around the buildings and 46 are outdoor nodes on rooftop. The rich node capacity and homogenous geographical distribution provides the researchers with the opportunity to separate different testing environments and perform simultaneous experimentation of different approaches for a

specific proposal. *Figure 7* and *Figure 8* illustrate the geographical positions of BOWL nodes and BOWL network coverage respectively.

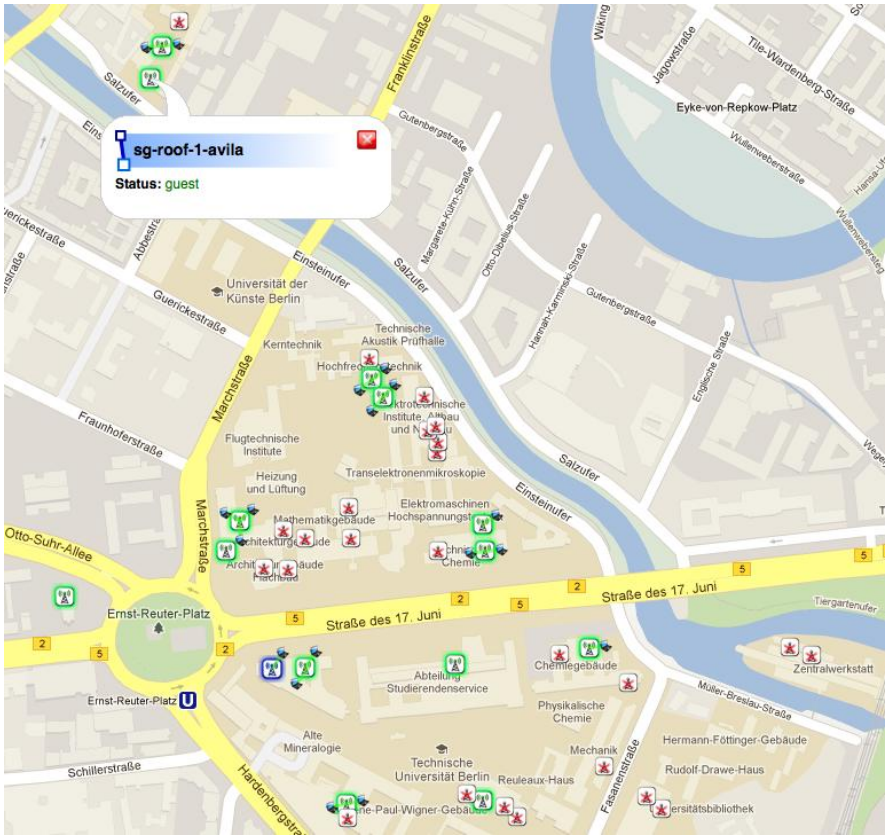

Figure 7: Geographical Positions of BOWL Nodes

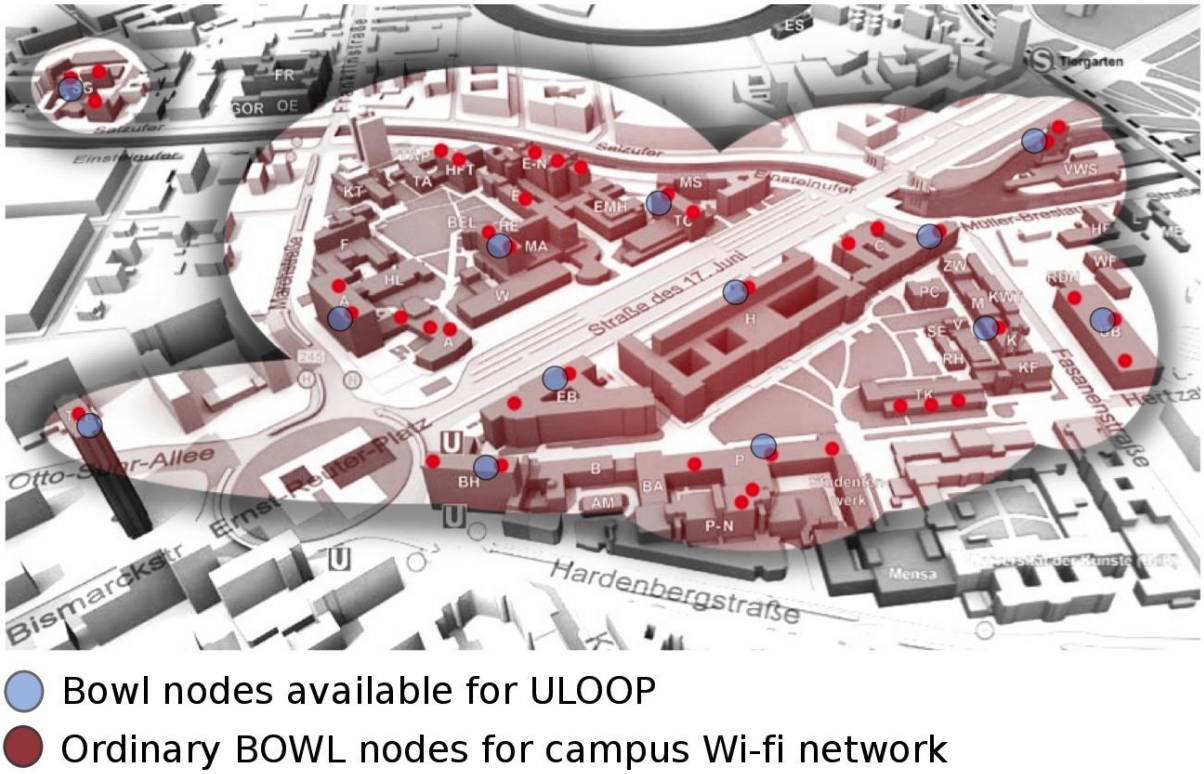

Figure 8: Coverage Area of BOWL Nodes.

3.3.2 BOWL Node Hardware Specifications

A BOWL node is composed of two different architecture boards as illustrated in *Figure 9*. The first board, the Avila GW2342 board [1] is utilized for ordinary campus network and has the Intel x86 architecture. The main campus network board is equipped with 128Mb SDRAM and 32Mb flash size. There exist two physical wireless interfaces of Atheros CM9 chipset equipped with antennas operating at 2.4GHz and 5GHz frequencies.

An additional research and development board is added to the 13 of BOWL nodes. This board is an Asus WL-500gP board with MIPS architecture and is equipped with 32 Mb RAM and 8Mb Flash size. There exist a single Atheros AR5212 [4] wireless module, which is connected to double antennas operating at 2.4GHz and 5GHz frequencies. Detailed technical information on the Asus WL-500gP board can be found in [3].

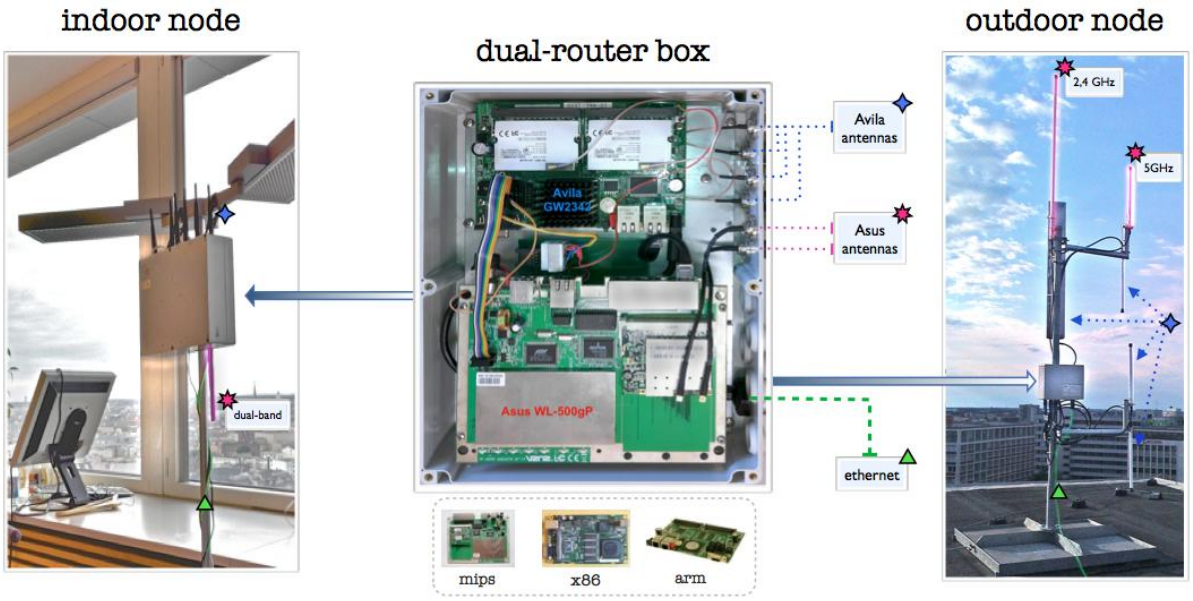

Figure 9: BOWL Node architecture.

3.3.3 BOWL Node Software Specifications

The BOWL nodes are equipped with OpenWrt OS prepared for MIPS and x86 architectures. The ULOOP OpenWrt image is to be flashed on the available MIPS architecture boards.

3.3.4 BOWL Architecture in ULOOP

The additional research and development board, namely, the Asus board is devoted for ULOOP (*ref. to Figure 9*). More than 4 BOWL nodes out of 13 MIPS architecture equipped ones will be available for ULOOP experimentations. The exact numbers and the positions of the available nodes will be provided to the partners with an annex document.

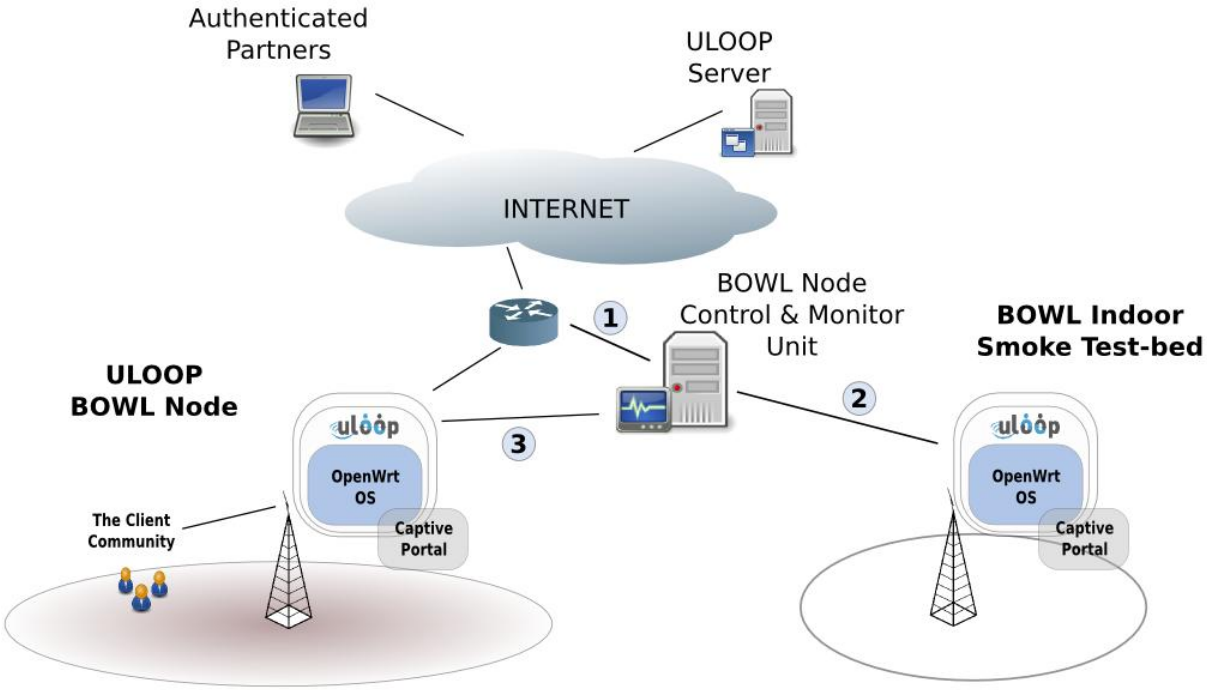

Figure 10: General architecture provided for ULOOP experimentation

As shown in *Figure 10*, an outdoor BOWL node is equipped with an additional research AP board with ULOOP-OS instances. This is due to the restrictions for the maintenance of BOWL ordinary wireless network. A BOWL node operates different AP instances, one of which is allocated for the ULOOP SSID. The ULOOP network will be an open access network, which processes the first authentication requests of client community through the captive portal. The legislation restrictions, limitations and requirements are going to be shown during this time period in order for a client to accept and be authenticated in the ULOOP network. An authenticated client is forced to install the ULOOP application either from the ULOOP server or the ULOOP OpenWrt image depending on the available memory size on the AP.

An account will be established for the partners, who are willing to control and monitor, also perform experimentation on BOWL-ULOOP network. The authenticated partners have an access to the BOWL node control & monitor unit over “SSH” protocol, through which the additional SSH connection can be established to the Smoke-testbed or outdoor BOWL nodes. These activities are restricted for the ULOOP-OpenWrt OS only.

3.3.5 Roadmap for the Configurations of ULOOP BOWL Site

The following items define the steps for the preparation of ULOOP-BOWL site. TUB will assist to the partners at each step if needed:

- The MIPS architecture compatible OpenWrt OS images will be provided to TUB.
- TUB will flash the “Smoke Testbed” indoor BOWL nodes with the provided OS image with the help of BOWL team.
- The accounts will be created for the related partners, who submit an experimentation request document or are responsible for the integration task.
- The partners will be able to sign in Control & Monitor Unit with a remote SSH connection using the created account.
- The maintenance test will be conducted on the Smoke testbed for a while.
- The BOWL team will take the end decision on flashing outdoor BOWL nodes if the ULOOP OS succeeds the maintenance test.
- The experimentation or Control & Monitoring procedure steps will be performed once the outdoor BOWL nodes are flashed with the provided ULOOP OS image.

3.3.6 Experimentation or Control & Monitoring Procedure for Partners in ULOOP

The following procedure should be invoked in order to conduct an experiment or control & monitoring in the BOWL network:

- The partner should perform experiments and evaluation of the related software or the entire ULOOP OpenWrt OS image for various environmental conditions.
- The partner should ensure the operability of the corresponding software or the entire ULOOP OpenWrt OS image.
- An authentication account will be established for the partner for the BOWL Control & Monitoring Unit.
- The partner must conduct initially the experiment in the indoor BOWL Smoke Testbed as illustrated in the *Figure 10*.
- If there exists an installed ULOOP OS image on any of the provided BOWL nodes and the partner aims to control and monitor already existing software, the partner might skip the previous action.
- If the experiment in indoor BOWL Smoke Testbed is successful, the partner might continue the experiment in the outdoor BOWL network prepared for ULOOP.

3.3.7 Measurement Taking and Control & Monitoring in BOWL

As discussed in the preivous sections, some of the research and development boards on the corresponding BOWL nodes are dedicated for ULOOP partners with full functionalities. Once the BOWL-ULOOP network is configured, the authenticated partners will be provided with SSH interface for the “BOWL node control & configuration unit” PC (*ref. to Figure 10)*. From this unit, the partners will be able to connect to the BOWL-ULOOP nodes with root rights, which would provide the researchers in ULOOP with a broad ability of examining BOWL-ULOOP node functionalities. Partners might conduct experiments starting from MAC layer till the application layer considering a translation to the OSI model in the definition of these functionalities. Partners are allowed to install their own measurement and configuration tools on the BOWL-ULOOP nodes.

3.3.8 Limitations and Challenges of BOWL Testbed

BOWL testbed is one of the wireless testbeds providing a perfect environment for not only academic research aspects but also for end-user product development. However, this raises the following additional concerns, which should be taken into account in the utilization of BOWL testbed:

- Any experiment should not disturb the real traffic or the connectivity of clients. Privacy issues, transparent network access and seamless mobility are the main perspectives that require additional attention for the proposals.

- Any software implementation should not disturb the node operation causing OS-freezing. Additional precautions are needed to control maintenance of the whole node operating system.

- Researchers are responsible for the maintenance of their own software implementations taking precautions against possible software failures, e.g. suitable watchdog configurations.

- A detailed documentation is needed for MAC layer implementations and might not be allowed in case of the aforementioned connectivity issues.

- Debugging is one of the most important aspects of the software development and the researchers should not forget about collecting debugging messages; it is not feasible to wait for console print outs.

- The methodology used for measurement taking should minimize or eliminate the influence of proposal-specific parameters on BOWL-ULOOP nodes. Partners should keep the storage limitations in mind and include a memory-freeing mechanism in their software.

- Researchers are expected to have a broad knowledge on OpenWrt, embedded Linux and hardware specifications of BOWL nodes.

- A researcher should apply for a developer-account and get through essential procedures.

3.3.9 BOWL Operation Context in ULOOP

The following items provide a summary on the potential utilization aspects of BOWL in ULOOP:

- AP SON functionalities: The BOWL-nodes are equipped with panel and omni-directional outdoor Wi-Fi antennas. This configuration of the antennas gives the opportunity for the BOWL-nodes being in the coverage of each other. Considering the AP SON mechanism in ULOOP, where the coordination and communication of APs are needed, the BOWL provides an available infrastructure in order to test these mechanisms.

- Scalability: The BOWL infrastructure is deployed in a very active and dynamic site of Berlin, where the instant available number of network clients in the BOWL coverage area is much higher in comparison with many outdoor Wi-Fi testbeds. This is due to the fact that the TU-Berlin Campus is established in the city center rather than in a dedicated rural area. Additionally, BOWL provides campus Wi-Fi network for the TU Berlin. This in turn brings about the opportunity for the ULOOP partners to investigate the ULOOP functionalities in terms of scalability.

- Trust management and incentive mechanism: As temporary and routine clients are present in the campus area with different characteristics, The BOWL testbed provides a suitable medium for experimenting the sufficiency of proposed mechanisms in trust management. Additionally, the incentive mechanisms proposed in ULOOP might be examined in a real-world environment in order to determine to what extend the corresponding incentives attract the clients.

- Various traffic types: The user profiles in the coverage of BOWL are very dynamic in terms of traffic types, depending on the individual interests. The real-world user model provides an experimentation environment in order to investigate the efficiency of the resource management mechanism in ULOOP for various types of users in terms of resource consumption.

- Mobility: Considering the geographical positions of the BOWL nodes and the campus architecture, various clients roam around BOWL coverage area with different mobility patterns as pedestrian or mobilized with a vehicle. The clients might exhibit their regular or fully stochastic mobility behaviors. Moreover, as the deployment directions of BOWL nodes along different paths through the campus and city site differ partially, BOWL can be utilized in testing mobility related proposals in ULOOP.

3.4 The FON Demo Plant

<FON: Imanol Fuidio, Valentin Moreno>

3.4.1 Overview

FON Density projects' objective is turning complete neighborhoods into free and open WiFi Zones. Places where you can always be connected and where WiFi is cheap (for non FON members) or free. They are also grassroots efforts to bring WiFi to all through the contributions of individual business owners and residents. By everyone sharing a bit of their internet connection, we can make Internet access pervasive and available to all. We hope FON Density projects will set an example for neighborhoods and cities of how a community based approach can be successful in creating WiFi coverage.

Residents who want to become Foneros and share some of their broadband with the rest of the FON Community gain free and unlimited access to over 6.000,000 FON Spots around the world. Residents and all of our Foneros visiting the neighborhood will enjoy WiFi coverage.

3.4.2 ULOOP FON Density Project

Argüelles-Moncloa district is within the range of the University district in Madrid, and hence is a highly populated neighborhood, being the student share of the population the target users in ULOOP.

The area is considered as a FON density project, then, partner FON will provide full control to such demonstration area. Nowadays, it counts around 360 FON active hot-spots. Hence, equipment to rely upon is released under the control of FON, with the users being registered within the FON management suite. It should be noted that the FON community users access the Internet by regular subscription, being the access provided by multiple operators.

Figure 11: Moncloa district location

Demographics information

Neighborhood: Argüelles

District: Moncloa

Area: 0,7547 km²

Population: 26.148

Population under 15 years: 10%

Population above 65 years: 25%

Inmigration: 15,85%

Elementary school population: 3%

Graduate population: 34%

3.4.3 Hardware Specifications

For this demo site, FON wants to deploy its own router called Fonera2.0N, with the following technical specifications:

Size & Weight

Dimensions: 30mm (1.18 inches) by 157mm (6.18 inches) by 127mm (5 inches)

Weight: 214 grams (7.5 ounces)

Wireless Protocols (Network Standard Support)

802.11n (300 Mbps)

802.11b/g (54 Mbps) compatible

Ports

1 WAN Ethernet port for connecting ADSL or Cable modem

4 LAN Ethernet port for connecting computers and other network devices

Security

WEP 64/128 bit, WPA, WPA2, WPA mixed

SSIDs

1 Fon network SSID (FON_FREE_INTERNET) for public use

1 private WPA-PSK encrypted SSID (MyPlace) for personal use

Antenna

2 external 3dBi Dipole fixed (2T2R MIMO Technology)

3.4.4 Software Specifications

For the demo site, FON will use the established software suite developed during WP3 and delivered along Year 2 and 3 of the Project.

3.4.5 ULOOP-Node Specifications in this site

The general network schema deployed at the demo site will look like in

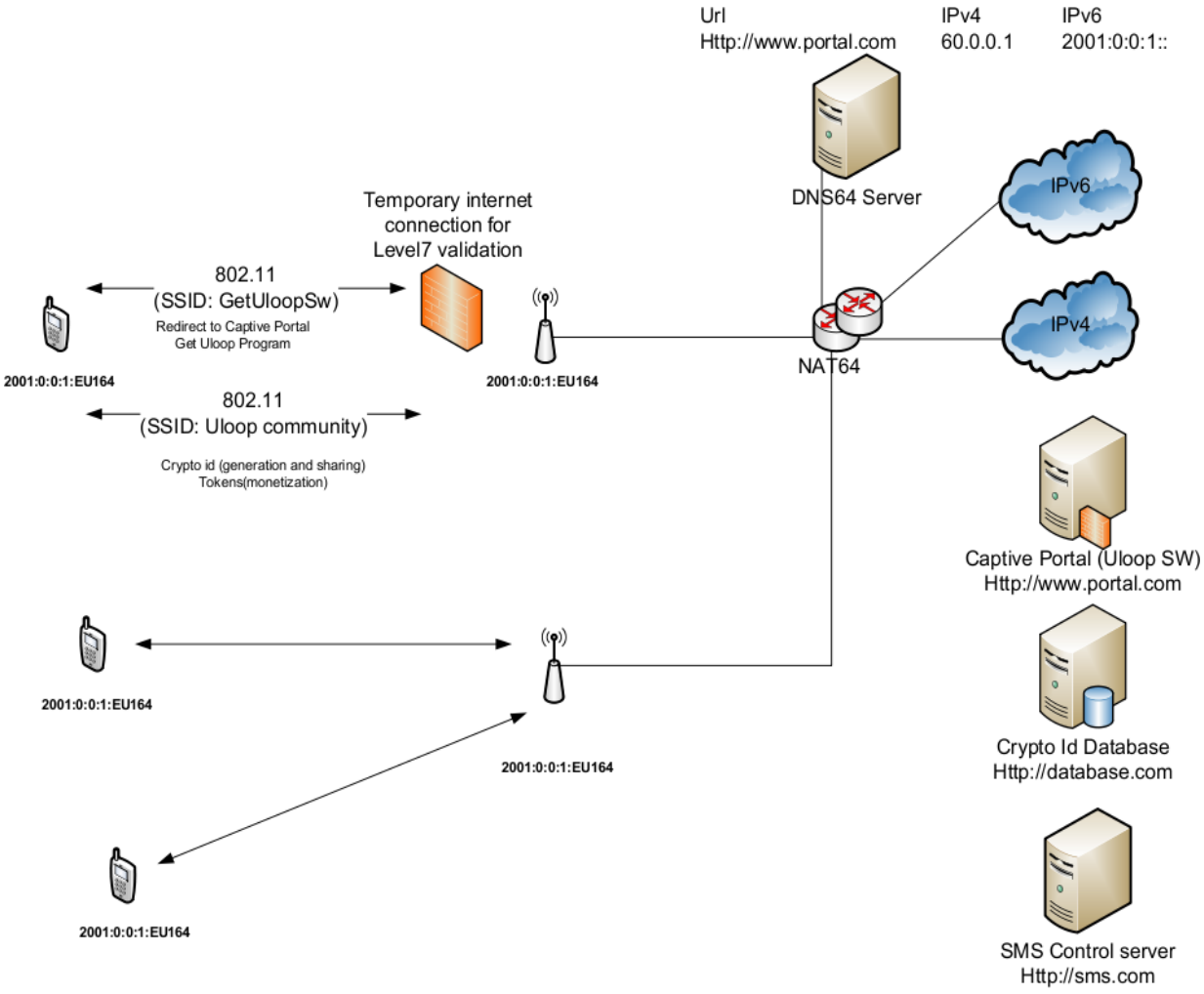

Figure 12:

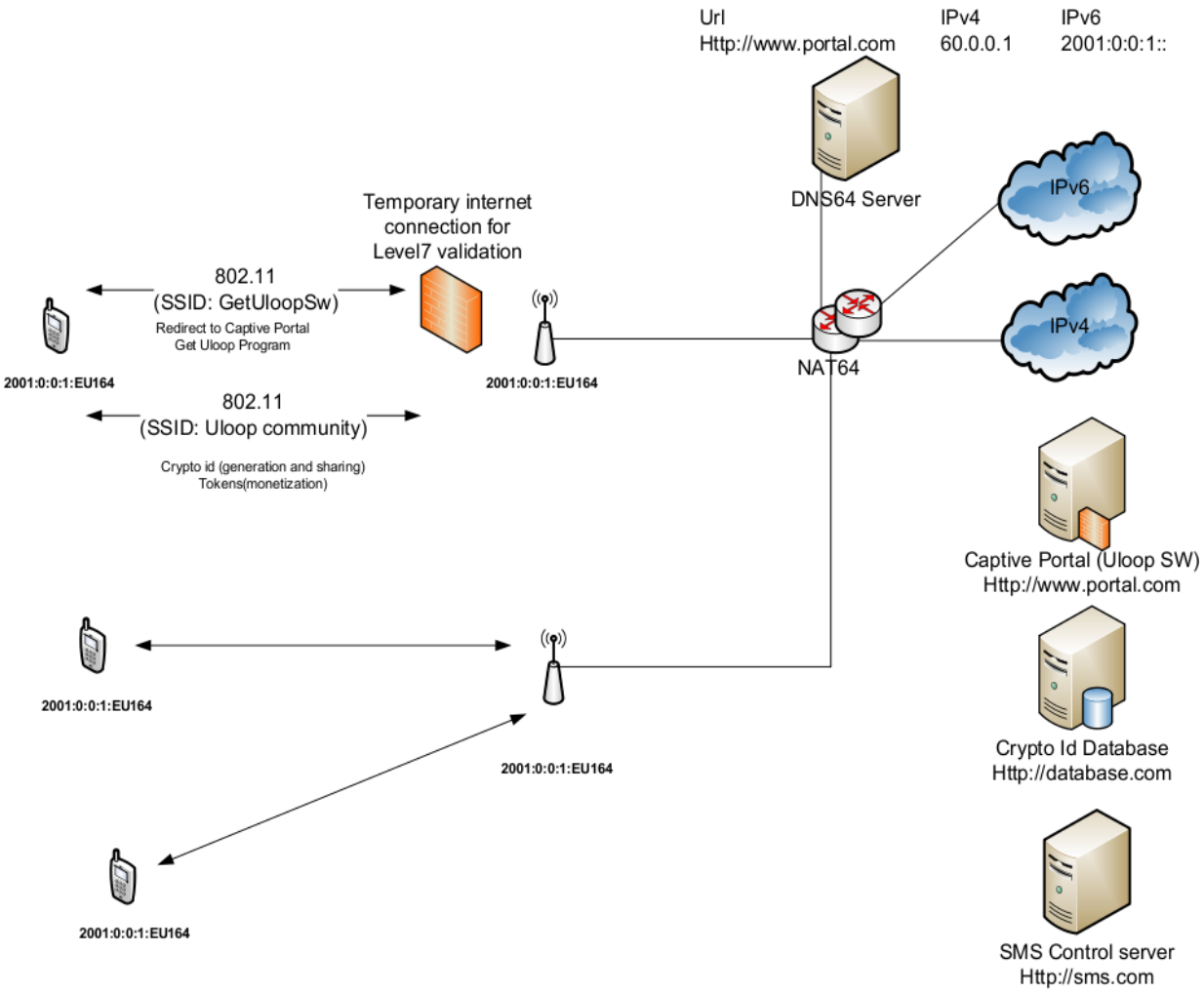

Figure 12: Fon node architecture.

3.5 ZON Multimedia

<ZON: Ricardo Mota>

3.5.1 Background

ZON launched few years ago an integration of FON's software stack into their Cable HomeGateways. It is available today in more than 500.000 devices in Portugal. This integration has been so successful that it has been named as a Zon's product by itself, "Zon@Fon".

Today, this is seen as major advantage over competitors and a functionality that ZON is interested in developing, promoting and innovating, whenever possible.

3.5.2 Pilot Description

As a triple-play services operator (TV, Internet, Phone), ZON keeps a set of residential customers that have been, over the years, used for testing, piloting and even demoing some innovations and new features in existing products.

When the software is ready for it, ZON will manage its integration in a test firmware for those HomeGateways, in place of FON's standard software stack.

Then, approximately 20 of the above mentioned customers will receive units of those HomeGateways for real life situation testing. Those customers will be selected taking into account the profile that is required for this pilot, namely they must be in places where there is high public visibility.

After a given period of time (yet to be defined), ZON will use its customer care service desk to query those customers for usage feedback, and thus enrich any metrics that can be obtained with quality feedback.

3.5.3 Hardware Specifications

ZON's present CPE solution can be generically defined, by its hardware features, as DOCSIS Residential HomeGateway, equipped with:

- RF interface for cable (DOCSIS 3.0)
- 4x GigaEthernet interfaces
- 2x FXS Telephone interfaces
- Wi-Fi 802.11n, 2T2R, based on Ralink's RT3352
- Puma V CPU
- 32MB of Flash
- 128MB of RAM

We have full control of the software running in the device, although we have externalized the development.

3.5.4 ULOOP-Node Specifications in this site

As mentioned before, this isn't a demo site already in place; to be accurate it isn't even a site *per se*, more of a dispersed set of devices that can be located all over the city of Lisbon (depending on which users are selected to be part of this pilot).

With this in mind, the specific needs for ULOOP nodes in terms of servers, firewalls, etc., are not set in place, as we will be waiting for all the applicable specifications to be established and properly finalized. ZON has a considerable server farm for the applications it provides today to its users, and there isn't any foreseeable restriction in setting up a few more machines to provide the necessary services for ULOOP.

As there is a need of more than just individual user testing, but rather a wide approach to the public, in order to access the impact a user-centric network has in a more spread scale; we will select the user database from those more exposed to the public. We are considering also to setup some sort of "real" public hotspot, taking into consideration our new headquarters location – just close to a major public transportation interface.

3.5.5 Measurement-Taking and Control & Monitor Specifications

As mentioned before, there aren't (yet) any specific setups for the server-side components of the demo site(s). We are, nevertheless, committed to put in place whatever is necessary (server-side), as soon as the solution is stable and ready for this real-life environment.

What we have already in place today are tools that we use on a daily basis to monitor the status of each component of the gateways, namely the DOCSIS synchronization status (and values) and the wireless components. We do this via SNMP and TR-069 protocols, which are easily extendable to new software components.

3.5.6 Experimentation or Control & Monitoring Procedure for Partners in ULOOP

We in conditions to discuss how each ULOOP partner can participate in the demo, be it with analysis of collected data, be it in active monitoring, or even hosting hotspots of their own, yet integrated with our Internet service – this, of course, will be limited to those in Portuguese territory, where ZON provides its service.

3.5.7 Limitations and Challenges of the Site

As it was considered from the beginning, ZON wants to put this site in place after all the major developments are closed and the ULOOP software stack (and all necessary server-side components) is in a production stage (or at least a very final beta stage) – therefore, the major constrain we are facing today (as we can see it), is the timing, until all developments are in such stages.

4. Deployment Considerations

<CMS: Nuno Martins, Alfredo Matos>

The deployment of the ULOOP pilots depends on the software and functionality contained in the delivered components, which were delivered as part of Tasks 3.1, 3.2 and 3.3. However, the actual pilot deployment is realized through the ULOOP uses cases, and how they can be instantiated into the actual deployment sites.

While the deployment of the different components towards the pilot sites is to be mostly considered as part of Task 4.2 and Deliverable 4.2, it is important to understand early on the interconnection requirements of the different sites, as well as understanding how the ULOOP use cases can be related to the different pilots. Considering these aspects will allow us to prepare the deployment plan in the upcoming Task 4.2 through the definition of what pilots can be deployed on which sites, and especially, how they need, if at all, to be interconnected.

4.1 Global Interconnection Aspects

When initially considering the deployment of the ULOOP functionality, it is important to understand the relationships that need to be established between the different sites. This directly translates into the different possibilities of strong federation between all the test sites, or a light interconnection, which can be achieved through administrative tools (e.g. providing assess credentials to different test sites, depending on the deployment requirements).

The federation of the Pilot sites may increase the complexity of the network, as different geographical locations are required to establish a transparent link between them. This may also decrease network performance (or negatively impact the quality of user experience), due to the use of tunnels or other network mechanisms to inter-connect the sites over the internet. Such an approach requires strong coordination mechanisms to ensure the compatibility and connectivity across the different sites. This imposes a strong and unified coordination layer across the different layers, which, as already mentioned, can greatly increase the complexity of maintaining such strong couplings between the different sites.

From an integration perspective, regardless of the deployment options, in order to have smooth integration process, the different pilot sites need to have a common set of software packages, similar network policies and compliant address schemes. Having the same structure on every Pilot site enables a broader test of the software, developed on top of different hardware. This opens the door to a light weight approach, which ensures the required software is capable of being installed on the target site, followed by an administrative process of accessing the site for both deployment and testing.

While in the future it is possible to have all pilot sites interconnected through strong federation mechanisms, at this point in time there is not a strong need to share the resources across the different pilot boundaries, which also imply different service providers and a complete different set of users.

Another aspect to consider is that while different test facilities provided by other projects such as OneLab2 [6] consider aggregating nodes on very different geographical and (network) topological locations under the same unified testbed (and thus creating strong need for federation), in ULOOP all nodes can be assumed to be in the same network, corresponding to each site.

The conclusion of this preliminary analysis is that in ULOOP it is possible to consider only loosely connected sites over the Internet, where each site provides their own domain and addressing scheme (reachable through public addressing when necessary), and without tunnels or other federation mechanisms. This approach will reduce the complexity of both the deployment and of the actual testing procedures, without compromising the pilot goals.

4.2 Preparing Use Cases to Pilot site mapping

While most of the deployment aspects should be considered part of D4.2, “Pilot validation and deployment Report”, due Month 34 under the guidance of Task 4.2, it is important to start preparing the deployment of the different use cases to the test sites. Therefore, there should be a concrete understanding of the actual ULOOP use cases in terms of requirements, and if they match the resources provided by each Pilot. The goal of such an assessment is to understand if there are constraints imposed by the Pilot sites, concerning the hardware and resources provided. In this section we highlight the starting point for Task 4.2, by discussing the initial limitations that should be considered for Pilot deployment.

The ULOOP use cases were defined on ULOOP deliverable D2.1 and should be mapped onto the Pilot sites to analyze their impact and feasibility on the real test sites. Therefore, we analyze the implementation of each use case on the specific Pilot site, by providing, first, a generic mapping between the use case and the delivered software (D3.4, D3.5 and D3.6), and then using this mapping to understand which are the technical requirements for each use case.

4.2.1 Methodology Overview

The software delivered by the different tasks in WP3 defines several levels of functionality. The most important building blocks are Trust Management (Task 3.1), Resource Management (Task 3.2), and Mobility Aspects (Task 3.3). Each of these blocks has features that operate on different layers of the operating system. Therefore, for each of these components, there should be an assessment of the requirements for the nodes present at each pilot site. These should consider different levels of requirements:

- Modification of core operating system features (e.g. Kernel level modifications)
- Required external dependencies on libraries and applications (i.e. software dependencies)
- Impact of the provided features on the communication layers, and standard operation modes of the devices (e.g. L2, L3).

When these requirements are identified for each of the ULOOP building blocks, it will be possible to identify which of the Pilots can adequately provide the required functionalities in order to realize the ULOOP use case on the site. This initial overview, which should be carried under Task 4.2, will provide the first deployment map towards the sites.

Below, we provide a preliminary identification of the functionality covered by each use case, and consequently which building blocks are required to realize the use-case, as to determine which sites can host the Pilot demos.

4.2.1.1 Use Case 1: Expanded Coverage and 3G Offloading

This use case covers different aspects of the usage of the ULOOP network such as: connection of user equipments to the ULOOP gateways, interconnection of different communities across the

internet, relaying internet from user equipments (user equipment as a gateway), handover of connections, roaming between gateways, etc. [9].

The fundamental building blocks for this use-case start by Trust Management deployed on Task 3.1, which enables users to be able to connect to the gateway, and to each other with different levels of trust.

Regarding Resources Management and Mobility Aspects, this use case will have contributions from Task 3.2 and 3.3, which open the range of requirement to the entire set of building blocks. In particular, from Task 3.2, it will be required the contribution of the Resource Management blocks so that users and the gateway to be able to share resources, namely the Internet access. Similarly, the roaming of users and the handover of connections will be provided by Task 3.3 (Mobility Aspects) from the Mobility Prediction, Mobility Coordination and Mobility Management.

The first complete assessment is to consider that in order to deploy USE Case 1, on the Pilot sites, the target site must support the entire building block requirements, which in most cases was already expected, given the integration of the ULOOP software and functionality.

4.2.1.2 Use Case 2: Traceability and Collaborative Monitoring

This use case intends to investigate all features in ULOOP that attempt to track and monitor user behavior. Providing the necessary functionality involves monitoring the user equipment as well as the different gateways. On the gateways the work developed on Task 3.2 and Task 3.3 for User Management and Traffic Behavior and Mobility Tracking, respectively, could be accomplished gathering data of every new connection. That data is also comprised with which user and at time and date it happened, can give a good starting point.

While a deployment can be foresee of the two building blocks from Task 3.2 and Task 3.3, there should be a consideration to also provide the modules from Task 3.1, since Trust Management can be considered a fundamental dependency for each of these operations. As such, the starting point for the entire use case deployment, should also take into account all of the building blocks developed in ULOOP. In any case, partial or parallel deployments can be considered in the future work of Task 4.2, which should follow, to be best extent possible, the guidelines and recommendations highlighted in these sections.

5. Experiment Request Template

<CMS: Alfredo Matos>

The experiment request documents describe experiment requests that either an internal or external partner would need to fill out in order to explain the goals, instruction sets and technical details for the successful deployment of the corresponding experiment in either experimentation or the demonstration sites. This can also be applied internally for the deployment of ULOOP use case functionalities.

The document provides the place to describe the experiment goal and the corresponding expected results, which should be filled in the requesting entity in order to understand requirements that should be met by the hosting site. Following the generic description of the experiment, there should be the detailed technical description where the infrastructure requirements should be outlined, especially concerning network details, such as what sort of network access is required, and what are the addressing needs for the experiment (e.g. all global and public address, private addresses, node interconnection, etc.)

This document is particularly useful to understand the potential requirements stemming from the experiments that are going to be executed on the pilot sites. Using this document, we provide two different example requests to, first, fine-tune the template document so that it can easily meet the expectations of the requesters and, second, to allow a first understanding of the information that should be available from each site, as to complete the information in this deliverable. The experiment request examples are described below.

5.1 Example Experiment Request: SMS Validation

< UNIGE: Carlos Ballester>

To better understand the purpose of the experiment request document, we provide an example document [8] that relies on the template for formally requesting an experiment on ULOOP SMS VALIDATION in one of the ULOOP testbeds. In this document UniGe, acting as an internal entity to ULOOP, requests resources in one of the ULOOP testbeds to carry out an experiment, along with the technical information.

The requested experiment deals with the validation and authentication mechanisms in ULOOP. Once a node is introduced in the system for the first time, a crypto-id (public-private key pair) is generated and the user chooses a nickname. This nickname should be subsequently validated in order to be linked to the crypto-id and to ensure its uniqueness in the system. ULOOP includes an SMS validation mechanism, which is provided by Level7 as part of ULOOP consortium.

The goal of this experiment is to test the ULOOP nickname SMS validation mechanism in a realistic setup, in order to verify and compare with the previous simulation results. For this purpose, several new nodes (Android clients) should be introduced to the system. Crypto-ids will be generated for each of them and afterwards they will try to register nicknames. Nodes with the same nickname should be introduced in order to test the resilience of the system under this type of event, as it is expected that nicknames are unique in the system.

5.2 Example Experiment Request: ULOOP Messages

<CMS: Alfredo Matos>

To better undestand the purpose of the experiment request document, we provide an example document [7] that relies on the template for formally requesting an experiment on ULOOP MESSAGES in one of the ULOOP testbeds.

In this document, elaborated by CMS, acting as an internal entity to ULOOP requests resources in one of the ULOOP testbeds to carry out an experiment, along with the technical information. This experiment request is intended to allow the testing of the ULOOP Message API in C. It requires that at least two different deployed nodes communicate using ULOOP message (over TCP sockets). To this end, we require access to two (Linux) devices where we can run the software. The goal of this experiment is to test the provisional ULOOP Messages API implementation, which is a cross-platform, cross-device message passing application written in C using the Protocol buffers technology.

The result from this example experiment enabled Task 4.1 to better understand the requirements and the resources involved in providing an experimentation site towards internal and external entitites. The end result can be found in the provided annex document.

6. Summary and Conclusions

<TUB: Mursel Yildiz>

In this deliverable, the technical details on the ULOOP experimentation are provided. Different experimentation sites and the demo plants are introduced, which provides the first important steps of the technical roadmap for successful experimentation and demonstrations of ULOOP results. These sections are devoted for the technical instruction sets, which the partners should follow not only for the infrastructure but also for further experimentations.

The overview of deployment considerations is discussed for the next tasks in WP4 informing the corresponding partners in terms of the possible difficulties and complexities. As followed by the deployment considerations, example annex documents are provided for the experimentation requests from the partners to the owner partners of either experimentation or the demonstration sites. The main purpose of these documents is to prepare related partners, who are responsible for the deployment and the maintenance of ULOOP sites.

These guidelines and main site framework discussions are references for the tasks 4.2 and 4.3 of this work package.

7. References

[1] Deliverable D2.3

[2] “Avila Board Hand book”, *online,* available at: https://wiki.opennet-initiative.de/w/images/4/49/Avila_handbuch.pdf

[3] “Asus WL-500g Premium – OpenWrt Wiki”, *online*, available at: http://wiki.openwrt.org/toh/asus/wl500gp

[4] “ath5k – Linux Wireless”, *online*, available at: http://wireless.kernel.org/en/users/Drivers/ath5k

[5] “Berlin Open Wireless Lab”, *online*, available at: http://www.bowl.tu-berlin.de

[6] “OneLab2”, *online*, available at: https://www.onelab.eu/index.php/projects/past-projects/onelab2.html

[7] “Deliverable Annex Document for Experiment Request ULOOP-MESSAGES”

[8] “Deliverable Annex Document for Experiment Request SMS-Validation”

[9] “ULOOP Technical Use Cases”, *online,* available at: http://siti.ulusofona.pt/~uloop/wp-content/uploads/2011/04/ULOOP_D2.1_2011-03-29.pdf