D2.1: ULOOP Use-Cases, Assumptions, and Requirements

Deliverable Number	D2.1
Lead Beneficiary	FON
Dissemination Level	Public
Working Group / Task	WP2, Task 2.1
Editor	FON (Valentin Moreno)
List of Authors	ALBLF (Olivier Marcé), ULHT (Rute Sofia, Paulo Mendes, Andrea Nascimento), HWDU (Cornel Pampu, Kostas Pentikousos), ARIA (Alessandro Stagni), CMS (John Thomson, Paulo Trezentos), FON (Valentin Moreno), TUB (Fikret Sivrikaya, Mursel Yildiz), UNIK (Jiangzhou Wang, Huiling Zhou), LEVEL7 (Paolo di Francesco), UNIGE (Carlos Ballester, Jean-Marc Seigneur), UNIURB (Alessandro Bogliolo)
Project Month & Date	Month 7, 01.03.2011
QAT Reviewer	Jiangzhou Wang (UniK)

Executive Summary

The document provides a set of use-cases with assumptions and requirements which shall be the basis for the remaining work in ULOOP, namely, in WP3 and WP4. Constrains, assumptions, and requirements for each use-case are presented. To assist the reader we provide an adequate description and a sound understanding of the terminology applied in the context of the document, the document uses a generic *Metropolitan Area Network (MAN)* model as the basis for all of the terminology and concepts provided in the document.

Table of Contents

List of Figures

List of Tables

Acronyms

Acronym	Meaning
3G	3rd Generation
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AN	Access Node
AP	Access Point
ASP	Application Service Provider
ASN-GW	Access Service Network Gateway element
BRAS	Broadband Remote Access Server
CAPEX	Capital Expenditures
CLEC	Competitive Local Exchange Carrier
CP	Customer Premises
CPE	Customer Premises Equipment
DNS	Domain Name Service
DSL	Digital Subscriber Line
EN	Edge Node
ER	Edge Router
GGSN	Gateway GPRS Support Node (GGSN)

Acronym	Meaning
GPS	Global Positioning System
GPRS	General Packet Radio Service
HSDPA	High Speed Downlink Packet Access
HSIA	High Speed Internet Access
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
ISP	Internet Service Provider
L2	Layer 2
L3	Layer 3
LTE	LongTerm Evolution
MAN	Metropolitan Area Network
NAP	Network Application Provider
NAT	Network Address Translation
NSP	Network Service Provider
nVoD	Near VoD
PPP	Point to Point Protocol
QoE	Quality of Experience
QoS	Quality of Service

Acronym	Meaning
RN	Regional Network
RNP	Regional Network Provider
RTSP	Real Time Streaming Protocol
SIP	Session Initiation Protocol
SNR	Signal to Noise Ratio
SP	Service Provider
UE	User Equipments
ULOOP	User-provided Local Loop
UMTS	Universal Mobile Telecommunication System
VO	Virtual Operator
VoBB	Voice over Broadband
VoD	Video on Demand
VoIP	Voice over IP
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Networks

Acknowledgements

We would like to thank all task elements involved in the discussions and that are not authors of the deliverable.

1. Introduction

This document corresponds to deliverable D2.1 in ULOOP and is dedicated to the description of specific use-cases, basis for the remaining work in ULOOP.

The document is organized as follows. Still in this section we start with a set of definitions and additional terminology based to assist the reader in the understanding of the document. Section 2 is dedicated to the definition of services to be considered in the context of ULOOP, both from an end-user perspective, and from a network perspective. Section 3 covers the ULOOP use-cases, where for each use-case a scene-based description is provided, together with the sets of actors, pre-conditions, assumptions and requirements. Out of the use-cases we then present a list of assumptions and requirements in Section 4. Finally, references are listed in Section 5.

1.1 Terminology and Definitions

The definitions provided in this document have limited scope to D2.1 and are provided for the sake of clarity and to assist the reader in the document understanding. For global and a full set of ULOOP definitions, please refer to Deliverable D2.3. A few initial definitions are provided in *Table 1*.

Table 1: Use-case definitions.

Term	**Definition**
Cloud	See *Community*.
Community	A set of nodes which are ULOOP enabled and with specific characteristics which share some interests regardless of physical location. The notion of community here defined is restricted to this document and provided for the sake of readability. Refer to D2.3 for the ULOOP definition of community.
Handover	Process of transferring an ongoing communication session between two networks, or two communities, from one or several ULOOP enabled devices to other device(s). This definition here is provided for the sake of readability. Refer to D2.3 for the ULOOP notion of handover.
Resources	A physical or virtual element of a global system. For instance, bandwidth, energy, data rate, devices are in ULOOP examples of resources.

Service Provider	An organization (commercial or virtual) that provides some kind of service to Internet stakeholders (users, providers). Examples of services are communication, storage, and trust management. Examples of service providers as of today are Internet service provider (ISP), application service provider (ASP), Wireless Internet Service Providers.
Service	A system that fulfills a specific need.
Application	The tool to provide a service. For instance, VoIP is an example of a user service which can be provided through several applications, e.g. Skype or Gizmo.
Network Service	A system that is required to support, from a network perspective, user services, For instance, Internet connectivity is a network service.
User Service	A system that fulfills a need from an Internet end-user. For instance, VoIP is an end-user service.
Virtual Operator	The VO is the entity or organization that manages ULOOP communities. However, it does not hold a specific infrastructure nor does it specifically sell a service. A VO is therefore not an *Internet Service Provider (ISP),* given that it does not provide Internet access, nor does it provide any type of service, like what is today provided by an *Application Service Provider (ASP)*. The VO is therefore a new type of Service Provider emerging in today's Internet.
Gateway	A translator between two Systems. In ULOOP, gateways are devices owned by users or by operators, which meddle between ULOOP communities and external (non-ULOOP) systems. Refer to deliverable D2.3 for further details on the gateway definition.

1.2 MAN Model and Terminology

This section goes over networking terminology that we consider essential to assist in the synchronization of goals and of results in ULOOP and which is considered starting from a generic, multi-access, MAN model illustrated in *Figure 1*.

Given that ULOOP clouds reside in Internet fringes but require an end-to-end perspective to be addressed, the MAN model illustrates an end-to-end perspective. Therefore, starting from the right-hand side, the figure illustrates the IP backbone where today Service Providers (SPs) reside in the sense that servers, as well as IP routers are located in this region. The region delineated as IP backbone represents the MAN region where *SPs* are located, and encompasses networks operated by one or more *Internet Service Providers (ISP), Wireless Internet Service Providers (WISP)*, *Network Service Providers (NSP)*, as well as *Application Service Providers (ASP)*. This region is therefore IP-

based and is interconnected to one or several *Regional Network Provider (RNP)/Network Application Provider (NAP)*. Such interconnection is normally performed by powerful networking devices which perform mediation/translation between mechanisms from OSI Layer 2/2.5 (the access/regional part) to OSI Layer 3 (the IP backbone). For instance, in WiMAX such mediation is performed through the *Access Service Network Gateway* element (ASN-GW); in 3G it is a task of the *Gateway GPRS Support Node (GGSN)*; in carrier-grade Ethernet it is a job of the Broadband Remote Access Server (BRAS). These are in ULOOP represented by the term *Edge Node (EN)*. Towards the user there is then an Access Network interconnected to the Customer Premises, where ULOOP clouds, as well as other forms of user-centric networks reside.

In addition to the flat, interconnection perspective, the delivery of services across a MAN requires both a data and a control plane. The *data plane* handles all the aspects related to data forwarding, and delivery with reliability. The *control plane* handles all of the aspects related to management of the network operation.

In the next sub-sections further detail is provided into each of these regions, and their elements.

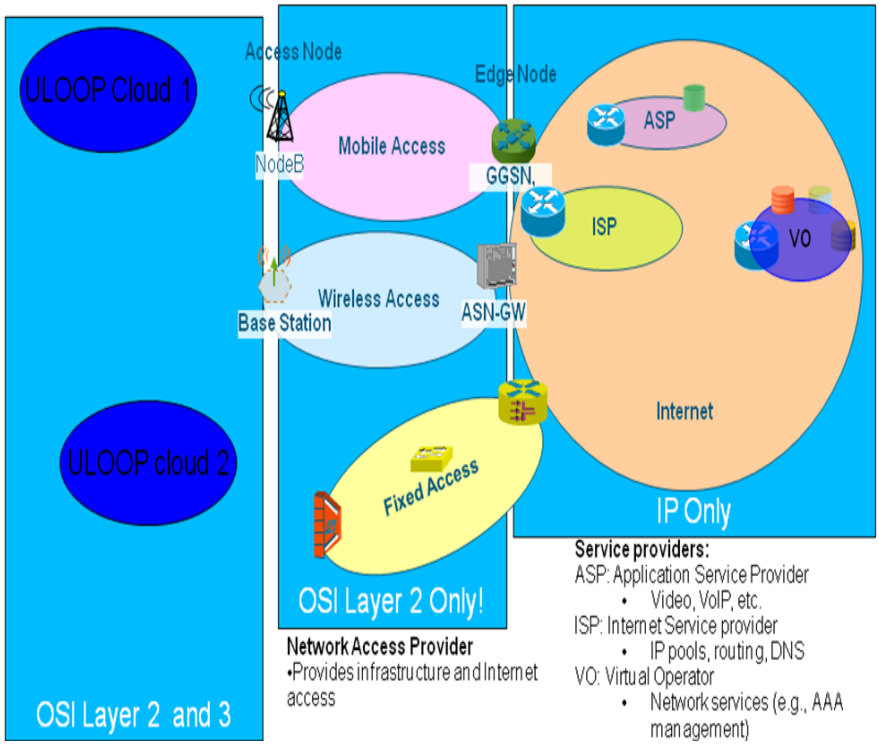

Figure 1: Generic MAN Model.

1.2.1 Customer Premises

Starting from the perspective of the end-user, the *Customer Premises (CP)* is physically within residential households, public spaces, and enterprise market and are, as of today, controlled by the end-user. The *User Equipment (UE)* corresponds to a generic user terminal (for example smart phone or notebook). In terms of UE and for operating systems to address in ULOOP refer to deliverable D2.3. However, the regular and most popular forms of operating systems for portable, *Wireless Fidelity (Wi-Fi)* enabled devices are to be analyzed. In ULOOP, we assume that CP are covered by some form of WLAN: a regular hotspot, infrastructure deployment; a mesh network, etc.

1.2.2 Access Network

The Access network region comprises several networks that provide the connectivity and traffic aggregation between the customer and the Internet backbone.

Access networks are owned by one or more NAP's, which may be *Incumbent Local Exchange Carrier (ILEC's)* or *Competitive Local Exchanger Carrier (CLEC's).* The access network can be further split into *first mile (local-loop)* and aggregation network. The former comprises both the physical connection and optional equipment between a Network Terminator and the so-called *Access Node (AN).* The latter comprises the region where first mile traffic is further aggregated, to be delivered to the regional network.

The Access Network represents a point (in most cases, the first) where several circuits coming from different customers are aggregated. The Access Network performs the required L2 functions (for example port isolation or WLAN support), and may optionally incorporate L3 functionality (for example basic IP routing filtering and/or IP session awareness).

ULOOP relates to the local-loop segments, in particular to the last hop towards the user, where the local-loop is expanded by complementary Wi-Fi technology.

1.2.3 Regional Network

Normally coupled to the access network is the Regional Network. This region interconnects the access network to regional broadband networks. This network is in fact optional, most of the time access and

regional networks are addressed as a group. When present, the regional network is operated by one or several *Regional Network Providers* (RNPs).

1.2.4 IP Backbone

The IP backbone region comprises the region where SPs reside. For instance, ISPs, which are responsible for providing Internet connectivity (routing, addressing, and *Domain Name Service, DNS,* resolution) and which originally were the first type of Internet providers, have their networks within the IP backbone. ASPs (e.g. NetFlix) hold also their server pool and routers in this region.

Through Internet evolution new types of SPs emerged. For instance, *Wireless ISPs (WISPS)* appeared with the introduction of WLANs as a commodity. IP backbone.

2. ULOOP Service Definitions

This section describes a set of user services and network services which are considered in ULOOP as the services to address in any use-case and which serve the purpose to assist in delimiting the concepts to be developed in ULOOP, as well as to assist the evaluation of ULOOP functionality in both experimental and realistic (pilot) environments.

The term service is here applied in a way that is broader than an application. For instance, VoIP as a service can be provided to the end-user by different applications e.g. Skype,

User services correspond to end-to-end services which are provided to Internet end-users. In ULOOP we consider a subset of the most popular Internet services as of today: real-time data sharing; Voice over IP (VoIP); video distribution.

In addition, ULOOP contributes with the definition of two additional categories of end-user services: user-interest based services and context-aware services.

2.1 User Services

The user services here described comprise a subset that is representative in terms of both current and predicted future uses of ULOOP functionality. Concerning today's scenarios we consider the most popular types of Internet services that users have at their disposal:

- **Real-time Sharing:** Born with the purpose of getting a good connectivity between two or more points located on any network and in order to provide real-time data traffic between them. Under this category we consider two specific services: VoIP and Video Streaming as two representative cases of Internet services.

- **Asynchronous Sharing:** This sort of sharing system provides connectivity between two or more points located on any network that don't need a synchronous data sharing flow. Bandwidth will depend on several factors (network latency, network congestion, etc). Under this category we evaluate the support that ULOOP can give to applications able to share user interests (advertising, personal/social networking); location information; multimedia (VoD and near-VoD) and context

information (for example environment; emergency; local information such as tourism). Data sharing is grouped into the following sub-types:

- Multimedia (for example VoD, nVoD).
- User interests.
- Context-aware information (environmental information, emergency; local information).

2.1.1 Real-Time Sharing

2.1.1.1 VoIP

Voice over Internet Protocol (Voice over IP, VoIP) is any of a family of methodologies, communication protocols, and transmission technologies for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms frequently encountered and often used synonymously with VoIP are IP telephony, Internet telephony, *voice over broadband (VoBB),* broadband telephony, and broadband phone.

The *Session Initiation Protocol (SIP)* [7] is a signaling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol. It requires end-to-end signaling and communication. For IPv6 such a scheme is direct; for IPv4 it requires *Network address Translation (NAT)* into private address blocks and end-to-end communication that is a problem. Workarounds have been successfully used like the *Simple Traversal of User Datagram Protocol Through Network Address Translators (STUN) [*4]. STUN allows any UE to connect to a SIP proxy across a *Network Address Translator (NAT)* [8][6], by having the UE sending information (about the global IP address that the NAT will use to represent the UE globally) to a STUN server.

2.1.1.2 Video Streaming

Video services considered in this document are based on the streaming of video content over the network. Streaming here is applied to the case where a subscriber is watching the content he/she receives in real-time, in contrast to services where the subscriber downloads the video streams that are not immediately watched.

Streaming imposes stronger *Quality of Service (QoS)* requirements on the stream delivery, so that the subscriber does not experience degradation or interruption of the streamed content. Consequently, streaming of video traffic has to be treated by the NAP/NSP as high priority traffic with controlled delay, jitter and packet loss. This is the major differentiation factor from the traffic carried over the Internet access.

2.1.2 Asynchronous Sharing

Asynchronous sharing refers to data transmission without the need to synchronize The data transmission rate depends on several factors (network latency, network congestion, etc).

Under this category we consider examples of multimedia services as well as examples for two new categories that are explored in ULOOP user-interest based services, and context-aware based services.

2.1.2.1 Multimedia

Under this category we consider as representative examples Video on Demand and near Video on Demand.

2.1.2.1.1 Video on Demand

Video on Demand (VoD) is a service for which a subscriber can request live or recorded video content from a server located within an ASP. An individual stream, unicast based, of the video content is usually delivered to the subscriber in real-time over the network.

VoD services usually is supported by the *Real Time Streaming Protocol (RTSP*) [3] protocol to provide the user the ability to control the video streams acting as a “network remote control” for streaming servers. The request is sent to the video server and as soon as the request is verified, the video server starts transmitting the content.

2.1.2.1.2 Near Video on Demand

Video distribution is a service where specific content from one source is distributed to several subscribers at the same time. This might be the case for transmitting television over the broadband. This kind of service is called nVoD.

Typically, video distribution content is transmitted through the NAP/NSP domain by means of multi-cast streaming to the customers that have subscribed to the service. However, in low capacity links in the network, the transmission of several simultaneous IPTV channels may lead to overload situations.

Video distribution applications can fully exploit the broadcast/multi-cast capability of the metro/access network. The service architecture can be based on a dedicated point-to-multi-point service connection which is used for the distribution of all video channels.

2.1.2.2 Data Sharing based on User Interests

Data sharing referring to user interests relate not only to personal and individual interests of users but also relates to social interactions on a regular or sporadic basis.

Such data sharing is not just based on social networking, for instance, it may relate to advertisements within geographic locations. Examples of user interests sharing are:

- Social interactions (for example interests of a football fan group in a stadium during a match), which ULOOP may support based on the information about trust relationship.
- New forms of advertising, which may take advantage of locality/proximity information provided by ULOOP.
- Location information, allowing devices to be part of interest-based networks of tourists, for instance, based on localized in time and space. ULOOP will allow low-cost devices to be included by e.g. allowing them to make use of *Global Positioning System (GPS)* information provided by adjacent devices.

2.1.2.3 Context-Aware Services

Context-awareness is a computing technology that incorporates information about the current surrounding of mobile users in order to provide more relevant services.

An example of context information could be real-time traffic information or even a live video feed of a planned route for a motor vehicle driver. Context can refer to real-world characteristics, such as temperature, time or location, as well as human originated information such as advertising. This

information can be updated by the user (manually) or from communication with other devices and applications or sensors on the mobile device.

2.2 Network Services

Network services described in this section correspond to the set of network functionality that an ULOOP architecture must support in order to provide the applications described in the previous section. We consider as main networking services to support:

- Internet connectivity.
- Authentication, Authorization and Accounting (AAA).
- Resource Management.
- Mobility Management.
- Trust Management.

2.2.1 Internet Connectivity

Internet connectivity corresponds to *High Speed Internet Access (HSIA)* and concerns line subscription, IP addressing and routing support; Domain Name Service (DNS) support.

In ULOOP, Internet connectivity is assumed to be provided by cellular, wireless or fixed transport technologies. Relevant to this fact is that Internet connectivity in ULOOP relies on the assumption that the last hop (not to be confused with the local-loop) to the user is based on *Wireless Fidelity (Wi-Fi).* In other words: in ULOOP communities the interface from the user perspective is Wi-Fi based.

2.2.2 Authentication, Authorization and Accounting (AAA)

AAA commonly stands for “authentication, authorization and accounting”. AAA architectures are strongly dependent on access network technologies. AAA functionality is tied to the deployment of auto configuration capabilities/solutions and may be performed at different layers simultaneously.

For PPP scenarios, AAA relies on the basic PPP security features. For non-PPP scenarios, AAA is normally performed by RADIUS. Dialogue between the RADIUS server and EN (or IP-aware AN) permits:

- Configuration of IP filters and firewalls per end-user.
- Configuration of QoS profiles per end-user.
- VPN selection.
- Session accounting.

2.2.3 Resource Management

Resource management is essential to allow the described architectures to grow steadily and to automatically adjust to changes. A user-centric local-loop represents an infrastructure where several entities (individuals) indirectly cooperate to ensure connectivity and reliability in data delivery. The main resource management aspects that are to be addressed in ULOOP relate to the capability of developing a robust and scalable wireless local-loop on-the-fly as well as increasing the spectrum and energy efficiency in the user-centric network.

Cooperative resource management techniques are to be addressed from an OSI Layer 3 and an OSI Layer 2 perspective. Cross-layer aspects will be considered whenever necessary. Aspects that are considered crucial in terms of resource management are to increase the debit of the wireless local-loop up to a level similar to the one provided by the broadband access technology; how to take advantage of overlapping spectrum (instead of trying to prevent it as is the case in cognitive radio research and based on techniques from OSI Layers 3 and 2); how to manage resources efficiently and reliably from a non centralized perspective, in the presence of a multi-operator access network, in neutral based network models.

Another aspect to be considered relates to the optimization of resource distribution, both from a resource admission control perspective, as well as from an attempt to optimize the network behavior based on already existing aspects of the privately owned *WLANs* available. For instance, currently the Wi-Fi infrastructure mode does not take into consideration user expectations which lead to them being incapable of assisting users in terms of *Quality of Experience (QoE);* and also, the fact that a station may be transmitting at a lower rate or at a higher rate, which leads to energy inefficiency.

2.2.4 Mobility Management

Mobility management is an essential issue to wireless networks. Users roaming around the network must be provided with a transparent handover process, taking into account the user's own experience (QoE) and availability of resources in the network.

At the same time, optimized mobility management is also key to reduce *Capital Expenditures (CAPEX)* from the access operator perspective. In what concerns handover support, this task aims at providing support for handover between different networks types (ULOOP to local and between ULOOP and operator network), including session continuity whenever necessary

One additional mobility aspect that is to be considered in ULOOP is the potential application of social-based mobility models which allow the prediction of movement of the ULOOP infrastructure nodes and hence, to be able to optimize different aspects of the network operation (for example, station distribution).

2.2.5 Trust Management

Trust management is a key concept based on the collaborative knowledge of users, devices and additional network components which belongs to the ULOOP network. In ULOOP the service trust management is ensured by the network, which shall consider information systems and information technology trust management systems to assist in developing transparently access control policies, as well as adequate security policies.

3. ULOOP Use Cases

Use-cases in ULOOP serve the purpose of establishing realistic boundaries and requirements for the functionality to be developed in the project. Constraints, assumptions as well as enhancement criteria are assumed to be derived out of the use-cases here described. For each use-case we provide a detailed description including technology and functionality that is available and will be applied, as well as the innovative aspects that ULOOP will pursue. We then derive a set of assumptions and requirements for each use-case.

These use-cases are the basis for all the specification and development to be performed in WP3 and also the basis for the set of scenarios to be implemented in WP4 for the purpose of ULOOP validation and demonstration.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [9].

3.1 Use Case 1: Expanded Coverage and 3G Offloading

Use case name:	Expanded coverage and 3G offloading
Use case ID :	ULOOP-1
Goal:	Complement broadband access by increasing capillary, coverage and providing 3G to ULOOP network handover.

The description here provided stands for a concrete example of application of ULOOP and for this we rely on Figure 2, where we have illustrated two ULOOP clouds represented by Community 1 and Community 2. The term community here is simply representative and identifies a set of users within the same WLAN. It could be, for instance, a mesh network in a city *provided by a municipality), or a hotspot at a coffee. Refer to Deliverable D2.3 for ULOOP definitions.

Communities 1 and 2 profit from Internet access due to one or more users that, through their 3G/Wi-Fi enabled devices, share Internet access. Such users are clients of a 3GPP *Long Term Evolution (LTE)* operator. We highlight that LTE stands for an example of the access technology that interconnects the ULOOP clouds. Such technology could also be WiMAX, or some form of fix network technology e.g. carrier-grade Ethernet coupled to *Digital Subscriber Line (DSL)*. The last hop to the user is Wi-Fi based. Moreover, some of the terminals are also LTE enabled.

ULOOP communities 1 and 2 have an internal connectivity based on Wi-Fi. External community interfacing is provided, in this example, by means of LTE or directly (between communities) by means of Wi-Fi. Moreover, gateways (*Customer Premises Equipment (CPE)*) can be owned by the users (e.g. a smart-phone or notebook) or by the operator (e.g.. an access point). Users have different degrees of mobility, they move with different patterns both within one community and inter-community.

In this scenario, the role of *Virtual Operator* is supported by the LTE provider to its subscribers. ULOOP communities therefore stand for an example of expanded coverage, from the LTE provider to its subscribers.

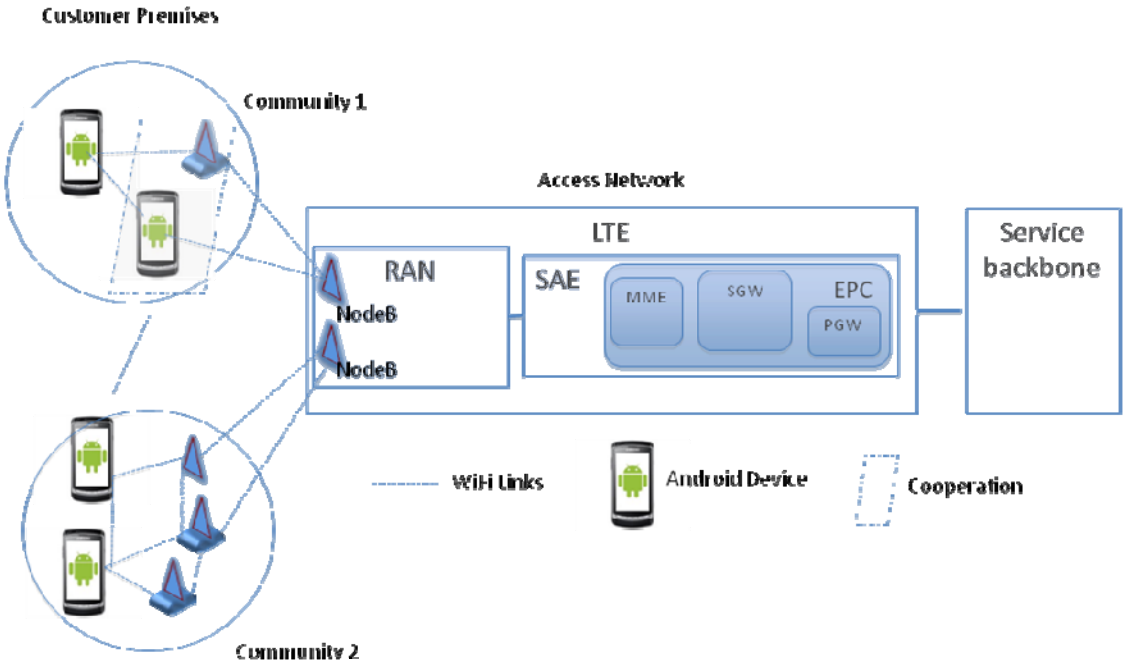

Figure 2: Use-case ULOOP-1 representation.

3.1.1 ULOOP-1 Description

Community 1 stands for an example of a dense wireless network, infrastructure mode (e.g. shopping-mall, football stadium, indoor spaces in a school campus). By dense it is meant that several users may activate devices in AP mode and therefore, there is a strong signal overlap. Hence, the result of this is that despite the fact that spectrum is abundant; signal perceived may in fact be of low quality in some areas (which we name as *gray areas*) Community 2 represents a mesh network also interconnected to the same LTE provider. Community 1 is in Lisbon, while Community 2 is in Paris standing for examples of two distant communities. This is merely for representative purposes, as the description also applies for the case where the communities would be co-located. In other words, there is no strict relation between a community and a geographic location.

Maria is a user in Community 1 carrying her Android smart-phone (UE). Maria's UE selects a specific gateway (AP or UE) to perform association to, and upon the association request (MAC Layer) the ULOOP gateway broadcasts a query both to the Wi-Fi interface and to the LTE interface (to reach the backend) in order to figure out whether Maria is or not an authorised and trusted user. At the same time, the chosen ULOOP gateway also triggers an adequate gateway selection mechanism that takes into consideration not only Maria's expectations but also the potential overlap and electromagnetic noise in the area, as well as the optimization of the load across the entire network.

While roaming in Community 1, the gateway onto which Maria's UE is currently associated detects that she is on the move (due e.g. to Signal to Noise Ratio (SNR) variations) and immediately attempts to estimate/anticipate a potential new anchor for connectivity (new gateway). Upon agreement between the gateways, Maria's UE is automatically attached to a new Access Point (AP), once Maria's expectations can be met.

Tom, another user of Community 1, is in a gray area. His device realizes that Maria's device allows connectivity relaying and therefore Tom's device triggers a request for Maria's device to connect. Maria allows other users with whom her device does not yet have a trust association established to interconnect by providing them a small amount of resources based on specific QoE requirements (e.g. only if her UE has enough battery level and up to 20% of Maria's link capacity). Therefore, Maria and Tom's UE automatically negotiate connectivity and Tom goes online through Maria's device.

Michael, another Community 1 user, is a subscriber of a network operator different than the one Maria is subscribed to and also belongs to Community 1. Given that they share a relation in the context of

Community 1, Michael and Maria can connect and exchange data directly, without going through their respective operators. Moreover, provided that there is such an available device, Michael can also profit from the Internet access while in Community 1.

Every time Michael is within the coverage of Community 1 devices, his UE handovers from the 3G network to the ULOOP community 1 (through Maria's UE). As one of the services provided by the ULOOP network, all the communication between Michael and other users inside Community 1 is performed locally, including voice and video calls, and thus, for Michael, this means that his traffic is offloaded from the 3G network to the ULOOP cloud. Whenever Michael leaves community 1 area, his UE handovers back to the 3G network.

Thanks to the resource optimization and load-balancing features of ULOOP, gateways within Community 1 continuously exchange data and thus offload / transfer some UE's to other elected gateways.

A second group of users belonging to Community 2 gets information about data being shared in Community 1 (e.g. through the ULOOP backend system). The second group is located in Paris, at Bob's place. Bob is using a tethered Android powered smart phone to connect to the LTE network and then uses the ULOOP enabled Wi-Fi on the phone as an access point.

A new company has recently arrived to a contiguous location to community 1 and decides to interconnect to Community 1 (Community 3, not represented in Figure 2). This community holds a specific and private infrastructure which they do not want to open. Therefore, Community 3 stands for a non-ULOOP community example.

In order for community 3 to be part of the ULOOP cloud, the company has to install a ULOOP gateway which is configured to interconnect both communities. Through time and automatically, the ULOOP gateway that interconnects community 1 to 3 will realize that community 3 does not contribute (for example data sharing, resource sharing) to the ULOOP cloud and will therefore restrict privileges based on the policies that Community 1 requires.

Therefore, community 3 will only have access to some ULOOP services (based on the different clouds willingness to share).

3.1.2 Actors

- ULOOP user with a smart-phone, roaming and willing to share its connection and services.
- Group of users within a specific community (groups sharing the same interests).
- Passers-by or social networking connections – e.g. users at Bob's place, with ULOOP-enabled laptops, connected through an ad-hoc network, and accessing the Internet through Bob's connection.
- Non-ULOOP systems.
- ULOOP software that can be downloaded on-the-go to UEs willing to have ULOOP advanced capabilities.
- Network access Providers.
- Service Providers

3.1.3 Pre-conditions

- Some devices in the ULOOP communities are ULOOP enabled support (always the best) connection for ULOOP users, based on their expectations.
- Shared devices are configured properly and have allowed access.
- Not all users belong to communities.
- The new infrastructure of community 3 is set-up with or without independent Internet connectivity.

3.1.4 Basic Sequence

1. User arrives at community 1 and UE automatically connects to a ULOOP gateway that best covers user expectations.

2. UE's roaming can automatically detect that they are starting to loose signal strength and therefore trigger MAC authentication to devices that relay connectivity.

3. A ULOOP gateway gets too many connection requests, and triggers offloading to another device in the community.

4. Michael uses his 3G data plan when he is at home, however when he is in the range of community 1, the ULOOP application installed on his smart-phone detects an ULOOP network and automatically change the connection from 3G to ULOOP. Michael goes out of community 1 and his UE handovers back to the 3G network.

5. Devices connected to Community 1 exchange data to the backend and through the Internet to other far-away ULOOP communities. Example, a remote group is located in Paris, at Bob's place. Bob uses his ULOOP-enabled smart-phone to provide Internet access to his friends, through his subscribed access.

6. A new company (private infrastructure, non-ULOOP community) decides to connect to community 1 and relies on a ULOOP gateway for interconnection. This gateway automatically triggers policies from the community sharing with non-ULOOP communities. Some of the services may therefore not be available to the new enterprise.

3.1.5 Requirements

- The functionality MUST be able to support users roaming in a way that implies minimum or no disruption to the user actions.
- Users MUST achieve their expectations – Quality of Experience – is a profile that the user SHALL define and the network SHOULD consider.
- Gateways MUST provide users with adequate expectations (for example connectivity always; adequate service response).
- Gateways SHOULD be able to load-balance sessions in a transparent way to the user.
- Gateways MUST be able to avoid interference from non ULOOP device.
- Gateways MAY have physical layers able to manage adaptive spectrum.

- UE's SHOULD be capable of resource sharing (for example in terms of battery).
- UE's and gateways MUST be able to create trustful communication communities.
- UE's and gateways MUST be able to ensure data privacy, based on predefined values.
- In ULOOP, the system MUST determine which devices can share (or are willing to share) resources.
- All Users in ULOOP SHOULD receive feedback information concerning their behavior and usage.
- UEs SHOULD get notification concerning availability of surrounding ULOOP communities as well as relevant information concerning the communities.
- ULOOP SHALL support handovers in a way that is the least disruptive to the involved users, and networks.
- ULOOP gateways SHOULD perform intelligent call admission control and not only block potential requests, but also divert them to other neighboring gateways.
- Within ULOOP communities the load SHOULD be fairly distributed among all ULOOP enabled devices and MUST take into consideration users expectations.
- The current Wi-Fi MAC Layer SHOULD be kept intact for backward compatibility.

3.2 Use Case 2: Traceability and Collaborative Monitoring

Use case name:	Traceability and Collaborative Monitoring
Use case ID :	ULOOP-2
Goal:	Provide a collaborative and robust platform for the purpose of data/traffic monitoring and user traceability aspects.

This use-case aims at exploring all the features in ULOOP that attempt to track and monitor user behavior.

Figure 3 provides a schematic representation for use-case 2, where from an end-to-end perspective there is one ULOOP cloud (Community 4) connected to the Internet by means of a fixed operator (carrier-grade Ethernet/DSL). As described, we highlight that the fixed technology stands for an example of access technology. Such technology could also be WiMAX, or LTE. The last hop to the user is Wi-Fi based. We also highlight that the number of ULOOP communities can be variable, being only one here represented for the sake of clarity.

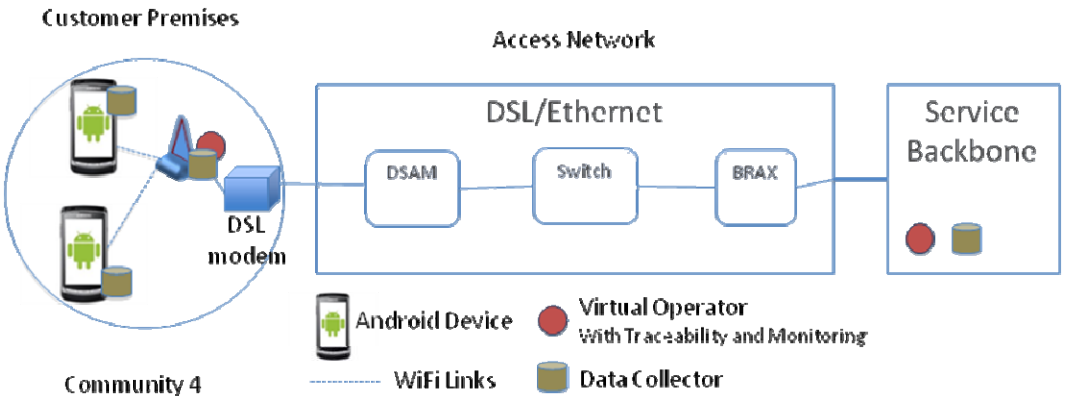

Figure 3: Use-case ULOOP-2 representation.

3.2.1 Description

ULOOP community 4 stands for an example of a regular Wi-Fi hotspot (WLAN operating in infrastructure mode) which is used as complementary to a fixed line subscription. We highlight that in our drawing only one WLAN is present; however, we could have multiple WLANs under the same assumptions and requirements that are going to be described next.

Community 4 (e.g. a hotspot in a coffee-shop) is visited by users that have direct access to the ULOOP gateway (e.g. one or multiple wireless APs) and by users that have access by means of expanded coverage (refer to the ULOOP-1 use-case for details). Moreover, within such community both types of users can profit from services that other users share.

In this use-case the ultimate goal is not to expand coverage but instead to consider ULOOP functionality as an enabling technology platform for cooperative data dissemination. In regular

deployments, such data cannot be available, as it is simply the result of a cooperative effort based on a self-organizing system.

Another main difference in regards to the previous use-case, is the fact that the role of VO can be located on the services backbone, or be located in the ULOOP cloud. Some end-user devices belonging to this community allow service sharing (example printer services sharing) based on specific cooperation incentives which are to be detailed in WP3, task 3.1.

Moreover, end-user devices that are ULOOP enabled may be able to gather open data (data collected from the users' surrounding environment). This is, for instance, the case of Maria, who needs to print her boarding pass at an airport with Wi-Fi coverage. Due to the ULOOP functionality implemented in gateways and also provided directly by other users, Maria can print her boarding pass through John's device, a user that Maria's device trusts through a bi-directional trust association.

In Community 4, ULOOP functionality tracks user expectations and service response. Therefore, users providing expanded coverage have feedback about their resource usage on-the-fly. Moreover, the users are provided with incentives for sharing, e.g. more bandwidth in exchange of receiving some advertisement. Such tracking/monitoring can be performed based on the CPE (UE and gateway) or directly via UE. Moreover, such tracking relates to information that is not personal and that the user always acknowledges to provide beforehand.In this use-case, tracked data does not impose any confidentiality nor privacy risk for the user. The UE serves the purpose of being part of the data dissemination towards users that share some form of interest, or for which there is some interconnection of social strength. Therefore, a component of this use-case is social interaction analysis as the means to adjust network resources being provided adequately. Social interaction analysis shall be dealt with on WP3, task3.1 (Trust management and Cooperation Incentives). Such analysis may pass by understanding the user's behavior in regards to online social networks, for example by tracking (through a plug-in to be developed) such behavior online.

Central also to this scenario is the notion of cooperation among different nodes in the ULOOP cloud. Such articulation contributes not only to a more robust infrastructure and data dissemination but above all to detect abnormal behavior (from the network or from users) in real-time, and to be able to take countermeasures quickly.

An example of abnormal behavior from the network may relate to nodes contributing example due to congestion to downgrading the expected quality. Collaborative monitoring and behavior tracking can assist in estimating a network surge, or preventing network breaks.

An example of abnormal behavior from users relate to potential misuse from malicious users.

3.2.2 Actors

- Set of users that is sharing some form of service, data, or access to peripherals.
- Forwarders, UE's that simply pass information from others.
- Collectors, CPE or servers on the provider side that collect and treat data obtained by cooperation of users.
- Information sources, example advertisement server.
- Service Providers.
- Network Access Providers.

3.2.3 Pre-conditions

- ULOOP plug-in that allows for collaborative data gathering is installed in some UE's of the users belonging to community 4.
- ULOOP functionality capable of collecting and relaying collected data to the access is installed on some gateways (AP's, UE, other CPE).
- ULOOP backend functionality may be available to provide some additional data.
- Users exchanging data have some form (dynamic) of trust association established, or a set of static agreements on how to exchange data has previously been agreed.
- Users allow access to their on-line social networks (through ULOOP plug-in provided to the different social networks), which gives access to a backend trust manager that aggregates and analyses user's social profile.

3.2.4 Basic Sequence

1. ULOOP enabled UE collects information within Community 4 during its owner routine (duration specified by the user) and i) stores it temporarily; ii) passes it to receptive UE's, CPE's, backend device (provided there is Internet access available).

2. ULOOP UE sharing services periodically broadcast such information (regular Wi-Fi beacons).

3. Backend server (or local) gathers collected information directly from the UE and also through the social network plug-in that some users accepted. This information is treated and disseminated through the cloud, example, through gateways. Statistics information are sent to CPE (gateways).

4. Gateways compare information (statistics) received (backend or directly on the wireless slink) and detect traffic abnormal patterns or behavior (example repetitive attempts from an UE to authenticate on different AP's around) and takes a measure (example prevention) while at the same time disseminates the negative behavior to the network and to the dynamic trust management scheme.

3.2.5 Requirements

- User sharing SHOULD state amount of resources to be shared, for example time, bandwidth, energy level of its device.
- User MAY state amount of cooperation incentives which he/she considers reasonable (expectations).
- Users involved in the collaborative behavior SHOULD be informed of the legal regional requirements in place.
- Collaborative data gathering SHOULD prevent data duplication.
- Malicious attacks SHOULD be detected.
- Users sharing some services MUST be provided with a repudiation mechanism to motivate sharing.
- Upon a gray area, UE's MAY rely on other (trusted) UE's to exchange data on-the-fly.

- Trust management MUST ensure that trust associations can be built on-the-fly.
- The current Wi-Fi MAC Layer SHOULD be kept intact for backward compatibility.

4. ASSUMPTIONS AND REQUIREMENTS

This section provides a list of ULOOP assumptions and requirements, which have been collected based on the ULOOP use-cases provided in Section 3.

The full statements of assumptions and of requirements are the basis to delimit ULOOP boundaries in WP2, Task 2.3, and also to drive the concepts in WP3 and the prototyping in WP4.

4.1 Assumptions

Table 2: List of ULOOP Assumptions.

Assumption ID	Use-case	Assumption Description
A-1	ULOOP-1	Some devices in the ULOOP communities are ULOOP enabled support (always the best) connection for ULOOP users, based on their expectations.
A-2	ULOOP-1	Shared devices are configured properly and have allowed access.
A-3	ULOOP-1	Not all users belong to communities.
A-4	ULOOP-1	The new infrastructure of community 3 is set-up with or without independent Internet
A-5	ULOOP-2	ULOOP plug-in that allows for collaborative data gathering is installed in some UEs.
A-6	ULOOP-2	ULOOP firmware capable of collecting and relaying collected data to the access is installed on some devices (e.g. APs, UE, other CPE).

A-7	ULOOP-2	Users may have intermittent connectivity
A-8	ULOOP-2	ULOOP backend functionality may be available to provide some additional data
A-9	ULOOP-2	Users exchanging data have some form (dynamic) of trust association established, or a set of static agreements on how to exchange data has previously been agreed
A-10	ULOOP-2	Some devices in the ULOOP communities are ULOOP enabled support (always the best) connection for ULOOP users, based on their expectations.
A-11	ULOOP-2	Users allow access to their on-line social networks (through ULOOP plug-in provided to the different social networks), which gives access to a backend trust manager that aggregates and analyses user's social profile.

4.2 Requirements

Table 3: List of ULOOP requirements.

Requirement ID	Use-case	Description
R-1	ULOOP-1	Solution MUST be able to support users roaming in a way that implies minimum or no disruption to the user actions.
R-2	ULOOP-1	Users MUST achieve their expectations – Quality of Experience is a profile that the user SHALL define and the network SHOULD consider.

R-3	ULOOP-1	Gateways MUST provide users with adequate expectations (for example connectivity always; adequate service response).
R-4	ULOOP-1	Gateways SHOULD be able to load-balance sessions in a transparent way to the user.
R-5	ULOOP-1	Gateways MUST be able to avoid interference from non ULOOP device.
R-6	ULOOP-1	Gateways MAY have physical layers able to manage adaptive spectrum
R-7	ULOOP-1	UEs SHOULD be capable of resource sharing (for example in terms of battery).
R-8	ULOOP-1	UEs and gateways MUST be able to create trustful communication communities.
R-9	ULOOP-1	UEs and gateways must be able to ensure data privacy, based on predefined values.
R10	ULOOP-1, ULOOP-2	The system MUST determine which devices can share (or are willing to share) resources.
R11	ULOOP-1	All users in ULOOP SHOULD receive feedback information concerning their behavior and usage.
R12	ULOOP-1	UEs SHOULD get notification concerning availability of surrounding ULOOP communities as well as relevant information concerning the communities
R13	ULOOP-1	ULOOP SHALL support handovers in a way that is the least disruptive to the involved users and networks.
R14	ULOOP-1	ULOOP gateways SHOULD perform intelligent call admission control and not only block potential requests, but also divert them to other neighboring gateways

R15	ULOOP-1	Within ULOOP communities the load SHOULD be fairly distributed among all ULOOP enabled devices, and MUST take into consideration user expectations.
R16	ULOOP-1, ULOOP-2	The current Wi-Fi MAC layer SHOULD be kept intact for backward compatibility.
R-17	ULOOP-2	User sharing SHOULD state the amount of resources to be shared, for example time, bandwidth, energy level of its device.
R-18	ULOOP-2	User MAY state amount of cooperation incentives which he/she considers reasonable (expectations).
R-19	ULOOP-2	Users involved in the collaborative behaviour SHOULD be informed of the legal regional requirements in place.
R-20	ULOOP-2	Collaborative data gathering SHOULD prevent data duplication.
R-21	ULOOP-2	Malicious attacks SHOULD be detected.
R22	ULOOP-2	Users sharing some services MUST be provided with a repudiation mechanism to motivate sharing.
R-23	ULOOP-2	Upon a gray area, UEs MAY rely on other (trusted) UEs to exchange data on-the-fly.
R-24	ULOOP-2	Trust management MUST ensure that trust associations can be built on-the-fly.

5. References

[1] IEEE*, IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Broadband Wireless Access Systems*, IEEE Std 802.16-2009 http://standards.ieee.org/getieee802/download/802.16-2009.pdf

[2] R. Sofia, P. Mendes. *User-provided Networks: Consumer as Provider, IEEE Communication Magazine, Feature Topic on Consumer Communications and Networking - Gaming and Entertainment*, 12: 86 - 91. 2008.

[3] H. Schulzrinne, A. Rao, R. Lanphier. *Real-Time Streaming Protocol (RTSP).* IETF RFC 2326 (Standards Track), April 1998.

[4] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy. *STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs),* IETF RFC 3489 (Standards Track), March 2003*.*

[5] W. Simpson. *The Point-to-Point Protocol (PPP),* IETF RFC 1661 ((Standards Track), July 1994.

[6] G. Tsirtsis, P. Srisuresh. *Network Address Translation - Protocol Translation (NAT-PT)*. IETF RFC 2766 (Standards Track), Februrary 2000.

[7] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. *SIP: A Session Initiation Protocol.* IETF RFC 3261 (Standards Track), June 2002.

[8] K. Egevang, P. Francis. *The IP Network Address Translator (NAT).* IETF RFC 1631 (Standards Track), May 1994.

[9] S. Bradner, Key words for use in RFCs to Indicate Requirement Levels. IETF RFC 2119 (Best Current Practice Category), March 1997.