CELTIC-PLUS/EUREKA
Smart Connected World

Project-ID: C2012/1-1 ACEMIND

Deliverable *D3.1*

Manageable ACEMIND features

Contractual Date of Delivery:	*30/09/2014*
Actual Date of Delivery:	**30/09/2014**
Editor(s):	**Abdesselem Kortebi (Orange Labs)**
Author(s):	**Abdesselem Kortebi, Pierre Jaffré, Olivier Bouchet, Jean-Philippe Javaudin, Marcin Brzozowski, Oliver Maye, Pavel Celeda, Jan Pazdera, Helmut Lucht, Anil Mengi**
Work package:	*WP3*
Security:	*PU*
Nature:	Report
Version:	*1*
Total number of pages:	32

Abstract

In this deliverable, we present the ACEMIND hybrid network elements. In fact, it introduces the basic components of the ACEMIND hybrid demonstrator which will be detailed in another deliverable. It describes the associated architecture and the implementation of IEEE 1905.1 convergence layer on ACEMIND hybrid devices. In addition, it deals with network management and traffic monitoring aspects. It relies on a specific GUI named dashboard to display pertinent network information such as topology, links metrics and data traffic information. To do so, it is necessary to gather information provided by the appropriate modules which are described through the document. Finally, security, legal and privacy issues are also discussed.

Keyword list

Home network management, IEEE 1905.1, traffic monitoring

Executive Summary

Home network complexity is increasing with the multiplication of the devices (including end devices such as PCs, tablets, smartphones, TVs, etc. and infrastructure devices such as Ethernet switches, wireless APs, PLC plugs, etc.) and services. Moreover, heterogeneous connectivity technologies are used, typically: Ethernet, WiFi and PLC (Power Line Communication). In this context, it is important to rely on efficient management tools to hide the complexity to end users.

This deliverable deals with ACEMIND manageable features; it focuses on the hybrid demonstrator elements. In fact, a recent IEEE 1905.1 standard about convergent digital home network has been proposed. Its aim is to handle the heterogeneous connectivity technologies in a transparent and efficient way. It offers various features including improved diagnostic and user experience. In this document, we describe the implementation of IEEE 1905.1 software convergence layer on hybrid ACEMIND devices. Then, we present the dashboard component that aims to provide a GUI for the user and the operator to help with troubleshooting issues and display network pertinent information. The different information needed by the dashboard are listed:

- Network topology (devices and links)
- Links metrics (e.g., physical rate, packet losses, etc.)
- Traffic monitoring (flows, applications and statistics)
- Smart home elements (devices and power consumption)

The traffic monitoring task is performed thanks to FlowMon probes and collector modules based on IPFIX standard as described through the management and monitoring section of this document. In fact, the dashboard will interact via appropriate APIs with the different defined modules to gather the needed information: 1905.1 manager to obtain network topology and links metrics, FlowMon collector module to get traffic monitoring information and smart home coordinator.

Finally, security and privacy issues are discussed as they represent an important aspect when it comes to home network management. It is intended to rely on TLS over TCP protocol to secure exported monitoring data with IPFIX.

All these components constitute the basics of the ACEMIND hybrid demonstrator which will be described in a successive deliverable.

Impact on the other Work-packages

The ACEMIND architecture and the components described in this document: 1905.1 hybrid devices, dashboard (GUI), traffic monitoring modules (probes and collector) are the basic elements for the ACEMIND hybrid demonstrator. Therefore, there is an impact of this deliverable on WP4 which defines ACEMIND demonstrators.

List of Authors

First name	Last name	Beneficiary	Email address
Abdesselem	Kortebi	Orange Labs	abdesselem.kortebi@orange.com
Pierre	Jaffré	Orange Labs	pierre.jaffre@orange.com
Olivier	Bouchet	Orange Labs	olivier.bouchet@orange.com
Jean-Philippe	Javaudin	Orange Labs	jeanphilippe.javaudin@orange.com
Marcin	Brzozowski	IHP	brzozowski@ihp-microelectronics.com
Helmut	Lucht	Devolo	helmut.lucht@devolo.de
Anil	Mengi	Devolo	anil.mengi@devolo.de
Pavel	Celeda	Invea-Tech	celeda@invea.com
Jan	Pazdera	Invea-Tech	pazdera@invea.com
Oliver	Maye	IHP	maye@ihp-microelectronics.com

Document History

First name	Last name	Version	Comments

List of Acronyms

Acronym	Meaning
<ACEMIND>	<Advanced Convergent and Easily Manageable Innovative Network Design>
PLC	**Power Line Communication**
QoS	**Quality of Service**
QoE	**Quality of Experience**
SIM	**Subscriber Identification Module**
UICC	**Universal Integrated Circuit Card**
TLS	**Transport Layer Security**
REST	**Representational State Transfer**
API	**Application Programming Interface**

Table of contents

List of Tables

List of Figures

1 Introduction

Home network complexity is growing as there are more and more devices (ranging from end devices such as PCs, tablets, smartphones, TVs, etc. to infrastructure devices such as Ethernet switches, wireless APs, PLC plugs, etc.) and services. Furthermore, heterogeneous connectivity technologies are used, including Ethernet, WiFi and PLC (Power Line Communication). In this context, it is important to rely on efficient management tools to hide the complexity to end users.

This deliverable deals with ACEMIND manageable features; it focuses on the hybrid demonstrator elements. Section 2 describes operator and users requirements. Section 3 presents the ACEMIND hybrid network. Section 4 describes the implementation of IEEE 1905.1 convergence layer on ACEMIND hybrid devices. Section 5 is related to the ACEMIND network management. In particular, it presents the dashboard and the traffic monitoring architecture. Finally, Section 6 discusses security, legal and privacy issues.

2 Requirements: Users and Operators

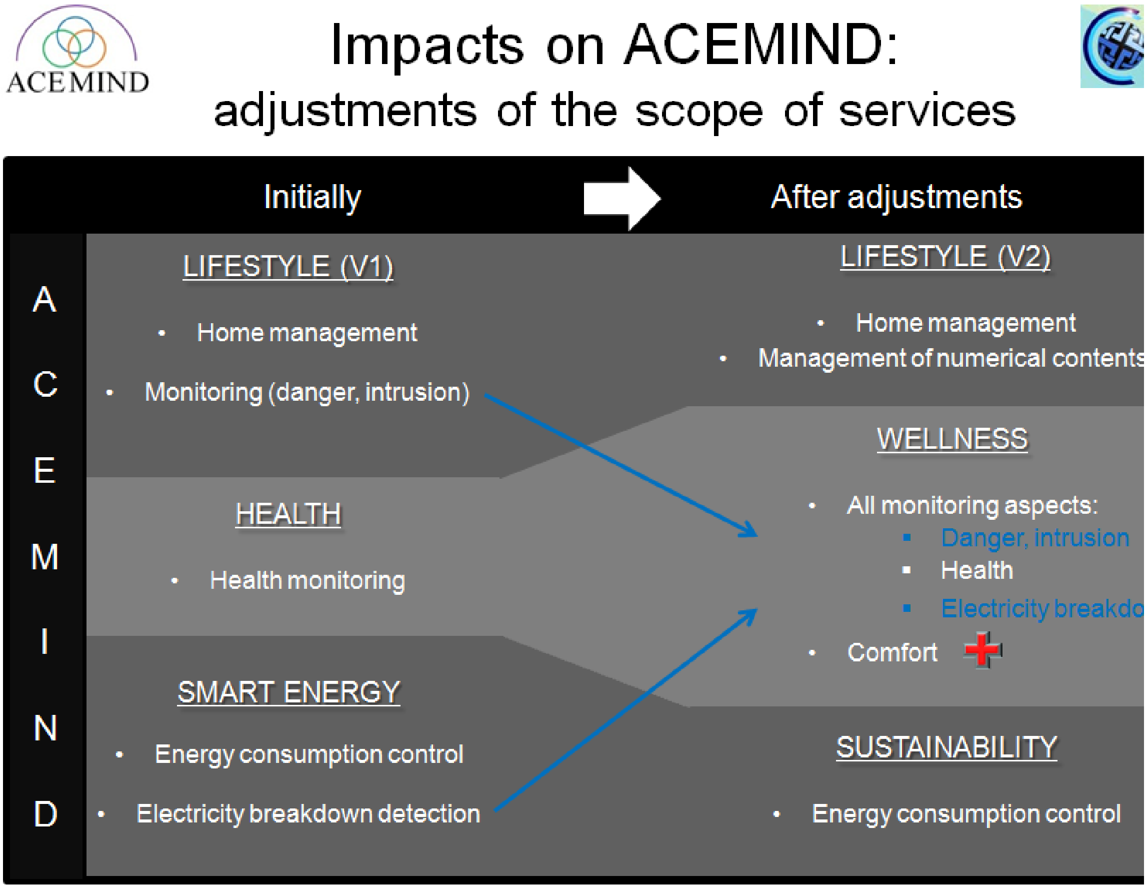
2.1 Users requirements

In the context of the CELTIC ACEMIND project face-to-face interviews were organized with end users to get feedback on user expectations and fears regarding the installation and operation of their home network.

Initially, before the interviews, three main services were defined so that the participants can comment and enrich them:

- Lifestyle (including home management and monitoring (danger, intrusion))
- Health monitoring
- Smart Energy (energy consumption control and electricity breakdown detection)

After the analysis of the interviews, the scope of services was adjusted in the following way:



Impacts on ACEMIND: adjustments of the scope of services

Initially → After adjustments

A C E M I N D

LIFESTYLE (V1)
- Home management
- Monitoring (danger, intrusion)

HEALTH
- Health monitoring

SMART ENERGY
- Energy consumption control
- Electricity breakdown detection

LIFESTYLE (V2)
- Home management
- Management of numerical contents

WELLNESS
- All monitoring aspects:
  - Danger, intrusion
  - Health
  - Electricity breakdo
- Comfort ➕

SUSTAINABILITY
- Energy consumption control

Figure 1 Example of categorization of M2M applications in the home network

Features such as high technology or ergonomics appeared not as a need in themselves. They should be intrinsically in the service and remain transparent from a user's point of view.

At the end of the ACEMIND project, five demonstrators are planned:

- **SECURE HOME (SOL)**: Smoke/CO (mandatory in 2015/2017 in France), Intrusion detector.
- **LIFE STYLE HOME:** Smart Plug, Heating Control, Motion detector
- **GREEN HOME (HOPE):** Self-sufficient house, Arcelik-White Goods, EMI Reduction. The demonstrator will present a home solution to flatter the consumption peak.
- **Hybrid Connected HOME (UNIC):** Hybrid 1905.1 network and an ACEMIND dashboard for monitoring and management of the hybrid network (could also be proposed on each language, i.e. English, French, German, Turkish, Czech, etc.).

- **LiFi Extender**: Propose an alternative wireless communication solution by using optical waves.

The following picture illustrates the three services emphasized and consolidated thank to the users' interviews. On this picture, each demonstrator is positioned in order to make the connection:

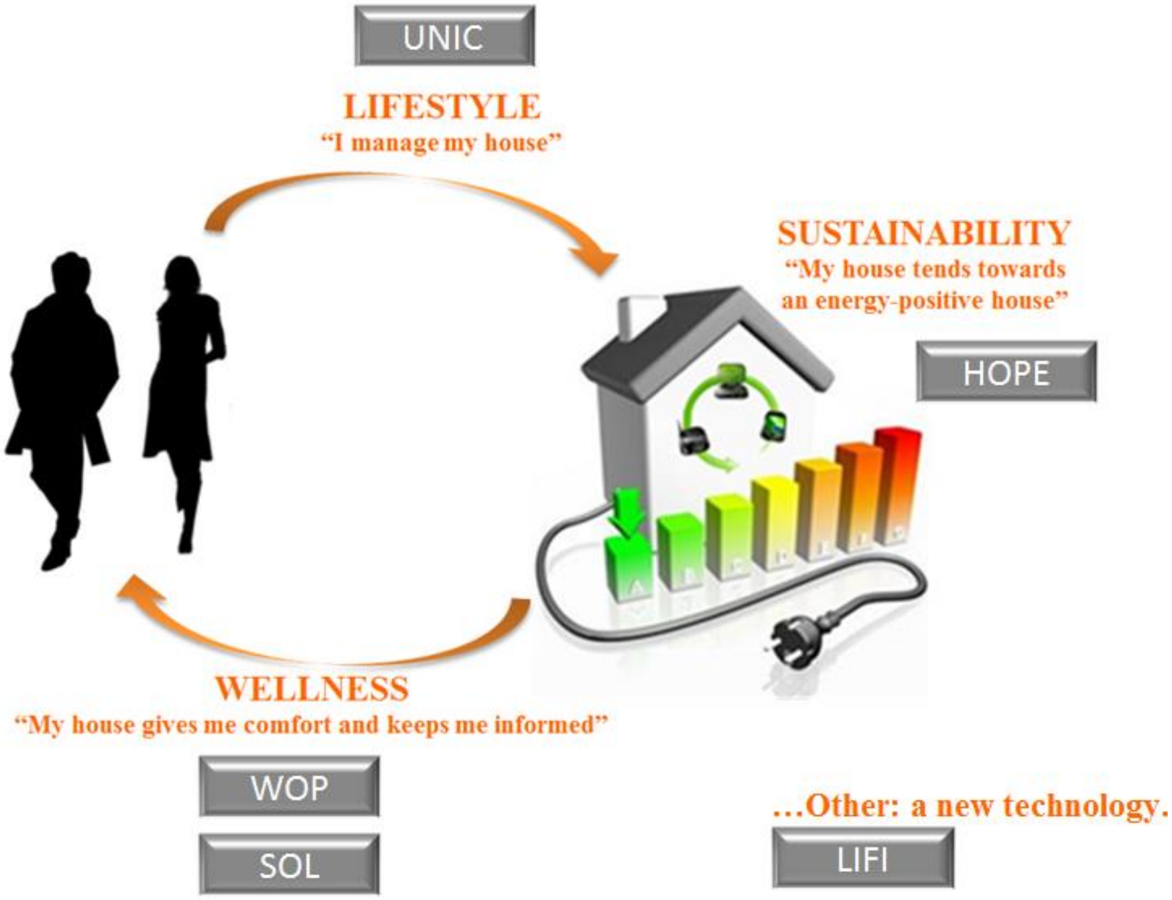

UNIC
LIFESTYLE
"I manage my house"
SUSTAINABILITY
"My house tends towards an energy-positive house"
HOPE
WELLNESS
"My house gives me comfort and keeps me informed"
WOP
SOL
...Other: a new technology.
LIFI

Figure 2 Connection between the three services "lifestyle", "wellness" and "sustainability" and the five demonstrators defined in the Acemind project

Regarding "LiFi", the demonstrator is a case apart from the other demonstrators. Indeed, it is included in ACEMIND project as a new wireless technology alternative to radio (WiFi). It is not part of the home automation services strictly speaking.

2.2 Operator expectations

2.2.1 Meet quality of experience customer expectations

2.2.1.1 Quality of service and quality of experience

Most of the requirements of the operator regarding the Quality of Service (QoS) concern the classification of services to manage potential congestion in the home gateways and home network infrastructure devices (HNIDs). As stated in the HGI QoS approach is class-based i.e. a service signature identifies a class and all members of that class share the same queue. The alternative would have been to have a queue per service instance, but this has several drawbacks. First, the number of queues is unbounded and could be large, and in the case of round robin queues, there would be many more weightings to configure. Second, identifying service instances is more difficult than classes, and cannot be done in advance.

In the upstream direction, the main requirement is to avoid excessive delay for voice, provide sufficient bandwidth for voice and video, and to prevent best-efforts traffic being completely starved by higher priority queues. There are three fundamentally different types of traffic with regard to QoS: voice, video and data. This would require three queues. However there is a need to further distinguish between at least two different types of data (e.g., for higher priority control data or to support a premium data service). Further, the overload protection mechanism mentioned above requires an additional queue; making **the total number of upstream queues required at least five**.

In the downstream direction there are two concerns, ensuring that WAN traffic is not blocked by transit traffic, and if there is downstream congestion due to a rate mismatch caused by a slow HN technology, that the managed traffic gets priority. There may be two different types of transit traffic, simple data and streaming (e.g., from a media player). **The downstream needs a somewhat simpler queue structure, with four queues**.

Additionally, on both downstream and upstream directions, as most of home network connectivities are likely subject to congestions due to varying total bandwidth (WiFi, PLC), an appropriate mapping is necessary between the DSCP QoS marking performed at layer 3 and the underlying layer 2 QoS marking. Note that in the downstream, DSCP marking is already performed in the access link but remarking is performed in the Home Gateway for the LAN segment. Regarding layer 2 marking, IEEE 802.11e standard specifies 4 classes for the WiFi connectivity, HomePlug AV specifies as well 4 classes for powerline communications (with a possible extension to 8 classes). Additional requirements about the QoS monitoring and control are defined as well at the HGI in:

- The home gateway shall be able to check the list of the QoS classes and the mapping between these classes and the queues.
- Regarding the queues, it shall be possible to measure its main characteristics (average and max queue length, # of dropped packets, throughput, …).

To ensure satisfactory Quality of Experience (QoE), home network performance monitoring is key. In fact, different standardization bodies address performance measurement. For example, BBF TR-143 provides an active monitoring test suite which can be leveraged by Network Service Providers to monitor and/or diagnose their broadband network. It allows computing parameters such as: one way delay variation, round trip delay, one way loss ratio and HTTP/FTP throughput. Furthermore, IEEE 1905.1 defines a set of home network local metrics which are agnostic to the underlying connectivity technology and a way to retrieve them. Such metrics include: packets losses, physical rate, link availability, MAC throughput capacity, etc.

Moreover, it is important for an operator to remotely manage the home network. In particular, Home gateway management can be performed using BBF TR-069; among other functions, it allows to upgrade the firmware of the device.

2.2.1.2 Ease of installation and use

As for end users, simple installation and use of the home networks by its clients is a key factor of economic success. This applies both to the HNIDs infrastructure (extenders) and the operator boxes (Home Gateway, SetTopBox) and the deployment of services on top of this network. Regarding the HNIDs, plug and play solutions are a key requirement for the operators to save OPEX in the aftersales support (hotlines), which may cost up to some tens of euros a year per customer.

In addition, the design of non-intrusive, educative, and user friendly dashboard to monitor the status of the services and the network, and manage them, is the second pillar for the operators to let users troubleshoot themselves their home networks.

2.2.1.3 User assistance and troubleshooting

The main expectations of major European operators regarding user assistance and troubleshooting are contained in the following document: Home Gateway and Home Network Diagnostics Module Requirements, updated in April 2013 [HGI2]

These requirements concern both the network functionalities and the hardware/software capabilities and status of the devices of the home network. From a high level point of view, the network oriented requirements consist into:

- Getting a view (graphical interface) of the presence of all connected devices to the home network is mandatory. Recommended functions are historisation via a log of changes or additional information about the devices (e.g. OS, …).
- A determination of the links connecting the devices in the home network (e.g. to the Home Gateway) is also important. This may be done either passively of via active probing. Type of connectivity and information about PHY rate in the LAN is recommended.

- The home gateway shall be able to test the IP reachability of all connected devices via a ping test. The Home Gateway shall also be able to maintain a table of local IP addresses of the home network and end devices.

2.2.2 Improvement of existing services and deployment of new services

2.2.2.1 Existing services

Triple / Quadruple play are the services provided today by most European Internet Service Providers (ISP). The Quality of Service requirements listed above often constraint operators to recommend direct Ethernet connections or simple network configuration for QoS demanding services such as IP TV.

Regarding the service themselves the trends for their improvement lie in the increase of the capacity required.

- For the internet access the capacity already jumps today from tens of Mbps with ADSL/ADSL2+ to hundreds of Mbps with fibre access with first launches of Gbps offers, waiting for multi-Gbps access before 2020.
- For the IP TV services, HD TV services demand today 5-8 Mbps and future 4K possibly combined with 3D will demand 10 to 20 Mbps. The improvement of the video compression efficiency will likely limit the increase of the video throughput demand. Nevertheless, the multiplication of simultaneous TV flows in the home is the main factor of throughput demand for video (watch and record, multiple TV sets …).

2.2.2.2 New services

Most of new services for the home networks concern smart applications and devices. Smart Home is often considered as a fifth play for the ISP service bundles.

These services often do not require large bandwidth but are very sensitive to disconnection such as security oriented services part of the wellness service type identified in Section 1, i.e. they require a 100 % availability of the end to end link from the service platform (server) in the cloud up to the sensor/actuator in the home. This may go through the need of multiple links in parallel both in the access and the LAN (home) segments of the network.

2.2.3 Profitability

2.2.3.1 Investment costs (CAPEX)

- Initial Deployment

Most of the initial costs are usually supported by the internet service provider and lies into two main parts.

Access segment
This cost is for the deployment of copper cable and/or fibre infrastructure to connect the home. This cost represents the main CAPEX for the internet service provider and has to be made prior to customer subscriptions.

As an example Orange announced in 2010 an investment of 2 billion euro over 5 years to deploy fibre at the access in France.

It can be noted that this cost is often shared with public authorities.

Home segment
Home Network Equipment package usually comprises the Home Gateway, the Set Top Boxe(s), the Network extenders (HNIDs) and some end devices (smart home devices, …).

Costs of such packages may vary from dozens euro to several hundreds of euro depending on the quality and the composition of the package. Customers may share the cost of this initial equipment (e.g. network extenders are typically at the charge of the end customer whereas gateways may be lent, rent, or sold by the ISP).

- Material renewal

Depending on the equipment quality and the operator, 5 to 15% of home gateways are refurbished every year. For a typical European operator with 10M customers this may represents several million (5 – 20 millions) Euro each year. The reduction of this cost goes essentially through new design of home gateways with the consideration of the refurbish from the initial design phase.

2.2.3.2 Operational costs (OPEX)

- Customer assistance

A large part of the operational costs for the operators lies in the customer assistance. Hotlines cost for typical European operators (5-20 million customers) represents every year several hundreds of millions of euro. This large total makes even more attractive the development of self-care solutions as ACEMIND will provide with the development of smart monitoring and management dashboards.

- Maintenance

As part of the global network, the access segment represents operational costs for any internet service provider. This could be a renting cost of a maintenance cost depending on the case where the operator owns or not its access network.

2.2.3.3 Expected profitability

Due to the large investment necessary for the deployment of ultra-high rate and reliable access networks (e.g. fibre) the profitability and the return on investment have to be considered over large periods such as 10 years or more.

When considering the home network segment only, as the investment is much lower for the operator (provision of a bundle of devices), profitability should be measured over a shorter period, maximum 3 years.

3 ACEMIND Hybrid Network

3.1 IEEE 1905.1 Standard

The IEEE 1905.1 standard enables seamless integration of four different communication technologies, that is, Ethernet, Wireless LAN, Power Line Communication, and MoCa. It introduces a new abstraction layer above the MAC layer, as depicted in Figure 33. The major benefits of this standard include the following:

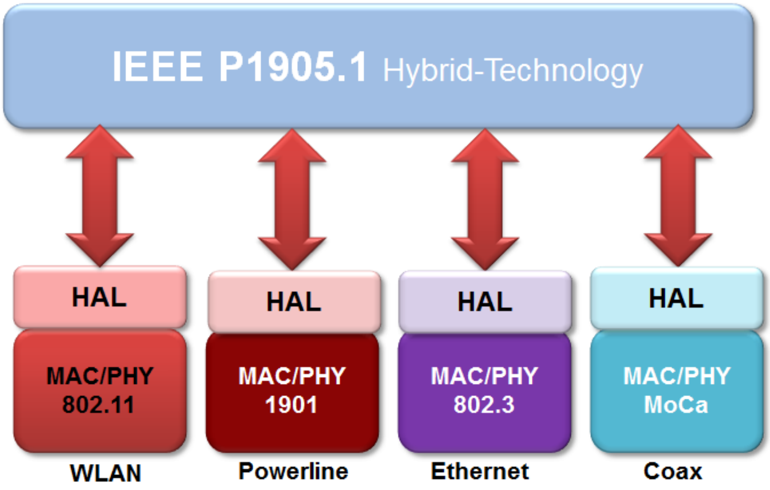


Figure 3 IEEE 1905.1 abstraction layer

- Ease of use; the users do not have to set up the network on their own, as the standard provides common setup procedures and access points auto configuration
- Improved diagnostic: the standard defines a topology discovery protocol for the home network along with a set of link metrics

Furthermore, other features beyond IEEE 1905.1 are possible:

- Aggregate throughput: transfer data over several technologies in parallel to increase throughput
- Load balancing: network traffic is split among several technologies to limit congestion and increase reliability
- Fallback: if a specific technology suffers from problems and stops working, an alternative route is quickly selected, reducing the number of problems and interruptions that the users experience
- Energy management: optimized network usage across home networks based on hybrid communication technologies

3.2 Beyond IEEE 1905.1

Users may benefit from features provided by the IEEE 1905.1 standard, as stated before. However, the standard does not define the implementation details of these features. For example, it lists the aggregate throughput as one of the benefits, but does not provide information how to support this feature. Therefore, we will investigate means to support two challenging features that are not really supported by the IEEE 1905.1 standard. These features include parallel data streams and energy savings.

3.2.1 Parallel data streams

If network devices are connected over multiple technologies, for example PLC and WiFi, they can send traffic over all these technologies simultaneously. It provides the following benefits and scenarios:

1. Various streams can be transmitted over different technologies and to limit congestion and maintain reliability. For example, in **Erreur ! Source du renvoi introuvable.**4 an SD stream is transmitted over PLC and HD Video over WiFi.

2. A single stream can be split and transmitted among many technologies to achieve higher throughput. For instance, the upcoming ultra HD streams may not be transmitted neither over WiFi nor PLC technologies because of high demand for throughput. However, if we split the stream into over two data paths, WiFi and PLC, it can be still transmitted over the network.
3. To achieve higher reliability, a stream and its copies can be transmitted over several technologies. In case a certain technology suffers from communication problems, the receiver still gets data from another path.

In this work package, we will investigate means to **s**upport the above-mentioned features and evaluation of various approaches to support parallel data streams.

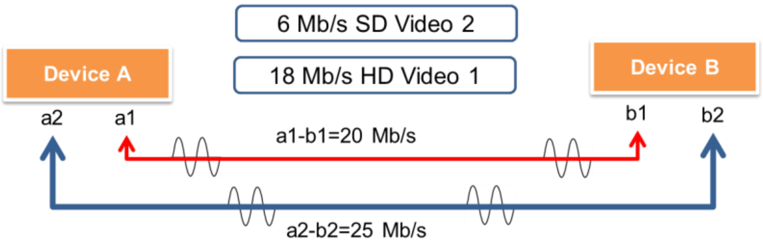


Figure 4 Parallel data streams

3.2.2 Energy management

With the increasing number of network technologies at home, energy consumption is higher than before. However, home networks usually provide more capacity than needed. Therefore, we will investigate the idea of powering down hybrid communication technologies when they are not needed. Further, we will have to detect quickly the increased demand on throughput in order to power up those technologies to avoid network delays and interruptions that degrade users experience.

3.3 ACEMIND hybrid Architecture

The hybrid ACEMIND infrastructure network consists of several device demonstrators, which enable the seamless integration of three different communication technologies: Ethernet, Wireless LAN, and PLC. The first-phase of the demonstrators contains the implementation of ACEMIND hybrid architecture based on the IEEE 1905.1 standard. This implementation builds up an ACEMIND network that can periodically measure the quality of all possible connections between the devices. These quality indicators are used to determine the best possible routes for the data transmission. Each device provides an interface for collecting local statistics based on IEEE 1905.1 frames. That is an external client such as dashboard, introduced later in this document, collect network statistics from devices and display them to the user.

4 ACEMIND Hybrid Network Devices

4.1 Hardware

At first time the 1905.1 software will be implemented on the Devolo devices dLAN 500 WiFi. The dLAN 500 WiFi is configured as a low cost system with small clock rate (MIPS 24 Kc V7.4 | 400 MHz) and represents the smallest device on which the 1905.1 software will be implemented.

Figure 5 Devolo dLAN 500 WiFi

Platform	
Processor	Qualcomm/Atheros AR9331 "Hornet" (based on MIPS 24Kc V7.4 | 400 MHz)
Memory	64MB DDR2-RAM, 8MB NOR-Flash
Network	WiFi 802.11 a/b/g/n/r and integrated Fast-Ethernet-Switch, PLC (Atheros 7420)

The following home network technologies are supported by the ACEMIND demonstrator:

PLC	IEEE 1901
Wireless	IEEE 802.11
Ethernet	IEEE 802.3

Erreur ! Source du renvoi introuvable.6 shows the internal block diagram of the ACEMIND demonstrator. The ACEMIND abstraction layer based on the IEEE 1905.1 standard is implemented into the flash memory of the WiFi controller chip (AR9331). The AR9331 has an integrated 5 port switch. This switch provides the external Ethernet connection and the interface to the PLC Chip (AR7420).

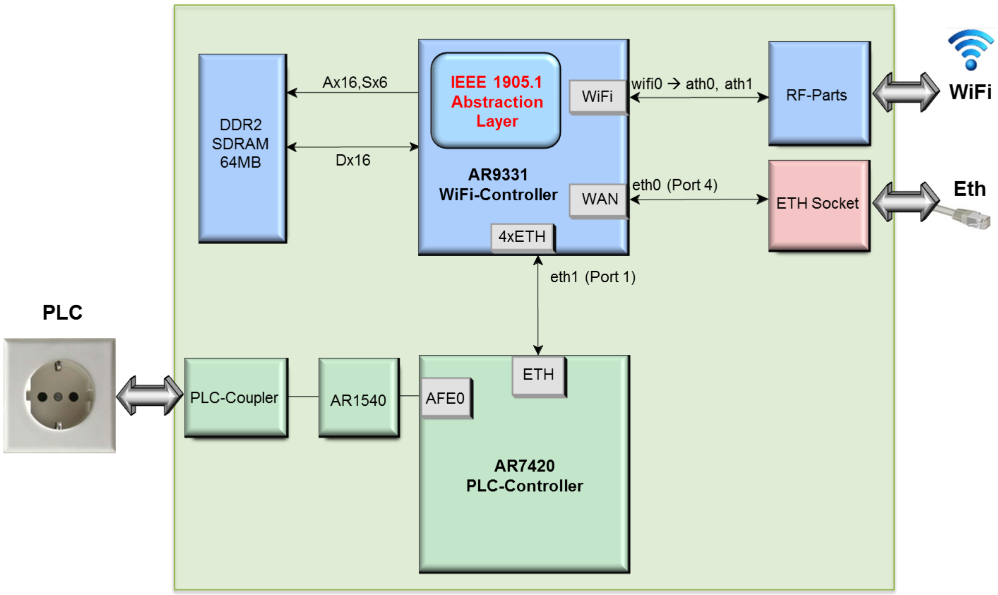


Figure 6 Hardware Structure of the ACEMIND demonstrator device

4.2 Software

Within this project, the ACEMIND abstraction layer based on the 1905.1 standard is implemented, which runs mainly on Devolo plugs. However, the 1905.1 implementation is not limited to these devices. The software is written to allow portability to other hardware platforms, for instance, to potential new versions of Devolo plugs that are not available yet.
To support the SW portability, we applied a Cross-Platform (C-P) architecture presented in **Erreur ! Source du renvoi introuvable.**7. In this case, a Cross-Platform implementation includes two groups of modules:

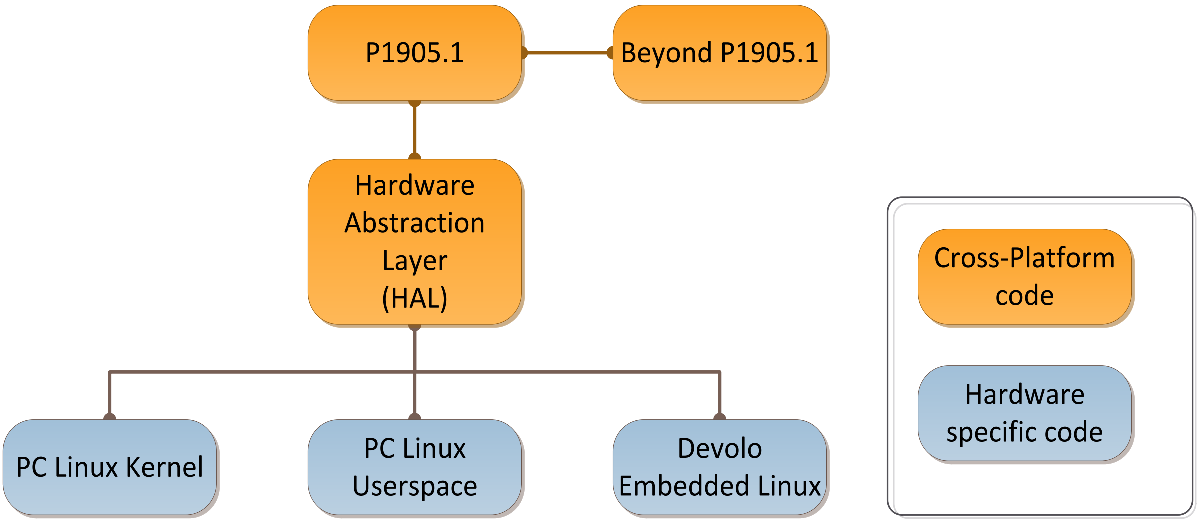


Figure 7 Cross-platform software architecture of 1905.1 implementation

1. Hardware- and operating-system independent implementation:
   It includes only ANSI C instructions, without any platform-specific function calls, data types, etc. Clearly, modules of this group must also access OS-specific functions, such as frame transmission or reception. In this case, the modules access a set of functions defined in Hardware Abstraction Layer. Obviously, each hardware platform must provide the implementation of HAL functions.
2. Hardware-specific adapters:
   These adapters allow to compile 1905.1 implementation on various hardware platforms. They provide the implementation of all functions, variables and data types defined in the Hardware Abstraction Layer. Furthermore, these adapters include also the appropriate build system (e.g. Makefiles).

As already stated, we will implement the 1905.1 module in a Cross-Platform way (see Figure 7). The features beyond 1905.1, such as path selection or energy efficiency, will also be implemented as Cross-Platform code too. By doing so, we will be able to easily adapt the standard, and the new features beyond 1905.1, to new hardware platforms.
Devolo plugs are the primary hardware platforms in this project, and therefore we will provide hardware adapters for these devices. However, we will also implement adapters that allow to execute 1905.1 standard on common personal computers (PCs), running Linux. In this way, we will be able to examine and trace bugs in 1905.1 implementation on PCs, in both user space and kernel space, which is more efficient than working directly on embedded platforms. Furthermore, it will allow us to test interoperability between different hardware platforms.

The cross-platform code of the 1905.1 implementation is modularized into a set of functional blocks called main modules. Each of these modules is nearly self-contained and interacts with other modules or the HAL through only a sparse common interface. Most modules implement certain functions of the 1905.1 standard, such as security, link-metrics, topology discovery or access-point auto-configuration. The module-design is sketched in **Erreur ! Source du renvoi introuvable.**9.

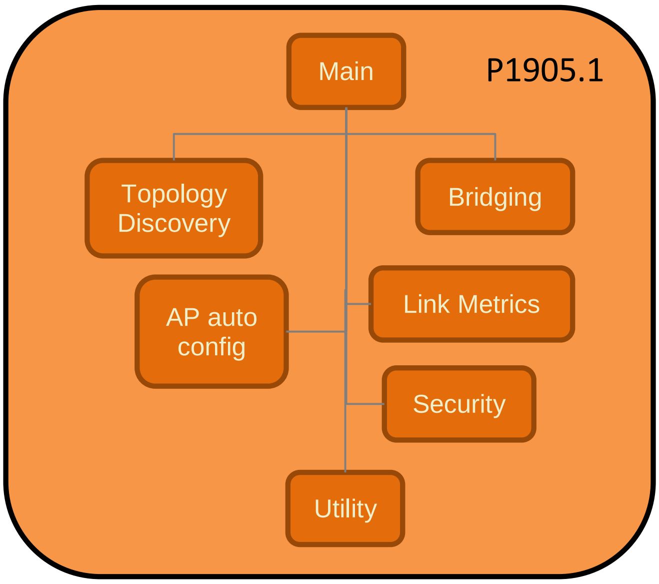


Figure 8 Internal module design of the 1905.1 protocol engine

One module is dedicated to the main control. It provides initialization and frame reception routines. Beside some helper routines and the complete LLDP handling, also the administration of the message ID, which is part of the CMDU header, is done here. Once a CMDU frame has been received and categorized, further processing is delegated to the corresponding functional module. Those modules are expected to take necessary actions like sending response frames, so as to behave consistently with the 1905.1 standard.

The modules for topology discovery, bridging, link metrics, access-point (AP) auto-configuration and security are mostly concerned with interpreting and constructing the involved TLVs. Especially bridging and security use variable-length TLV and thus, behave quite dynamically at run-time. This is well reflected in a more complex implementation of this part of the protocol software, when compared to others.

Finally, there is a utility module that provides helper functions and commonly shared code. Both, fragmentation of long frames into multiple fragments as well as re-assembly of those frame fragments are examples for this kind of code. Also, functions to access transmitted data throughout different levels of the 1905.1 protocol are grouped into this module. So, computing offsets into the CMDU header, the CMDU payload, a TLV-header or TLV data or even finding a certain TLV throughout multiple frame fragments can be done with the help of this module.

Usually, the source code of a module is stored in a single C file having the module’s name. The module-specific types and external functions are declared through a corresponding header file.

5 Monitoring and Management

The objective is to develop tools for monitoring reliability of hybrid networks by identifying slow or failing components and the causes of their misbehavior, security by providing secure network visibility to intrusion detection systems and performance by collecting traffic measurements and figures of merit (drop rates, response time, ...). This task has also to focus on developing tools for network management. Network management refers to the overall configuration and parameterization of the network.

5.1 Dashboard description

In this section, we describe the ACEMIND dashboard which is a graphical user interface allowing to show pertinent information about the network. The user interface (dashboard) is designed to enable users with different levels of expertise to setup, reconfigure and optimize their network. The feasibility of management methods will be demonstrated. The dashboard could also be accessible remotely by the operator for troubleshooting and home network diagnostic purpose (e.g. based on TR-069 protocol).

In a previous work, we showed the pertinence of the Home Network Assistant concept to improve the home network diagnostics [KLD13]. The aim of the dashboard is to provide additional information about the home network including typically:

- Network topology: it includes devices (e.g. PCs, tablets, 1905.1 Devolo plugs, etc.) and links (e.g. tablet connected to home gateway with a wireless link, plug 1 connected to plug 2 with a PLC link, etc.)
- Network metrics: IEEE 1905.1 metrics (link availability, packets errors, etc.), available bandwidth …
- Paths used by flows.
- Traffic monitoring and anomaly detection.
- Smart home information and energy consumption monitoring.

Figure 10 shows an example of what the dashboard could look like on a tablet (it is just for matter of illustration, as the GUI has not yet been developed). The graphical interface should be accessible on every device (PC, tablet, smartphone). The different ACEMIND modules will feed the dashboard with the needed information as we will describe in the next sub sections. The information provided by the dashboard will be classified into two categories (levels):

- Basic: it means that this kind of information will always be displayed on the dashboard
- Advanced: the information will be displayed on demand only

The idea is to have a simple default display containing only basic information. Then, it will be possible to add other information according to the user needs (typically, the user will have to click on the corresponding tab on the GUI to access it).

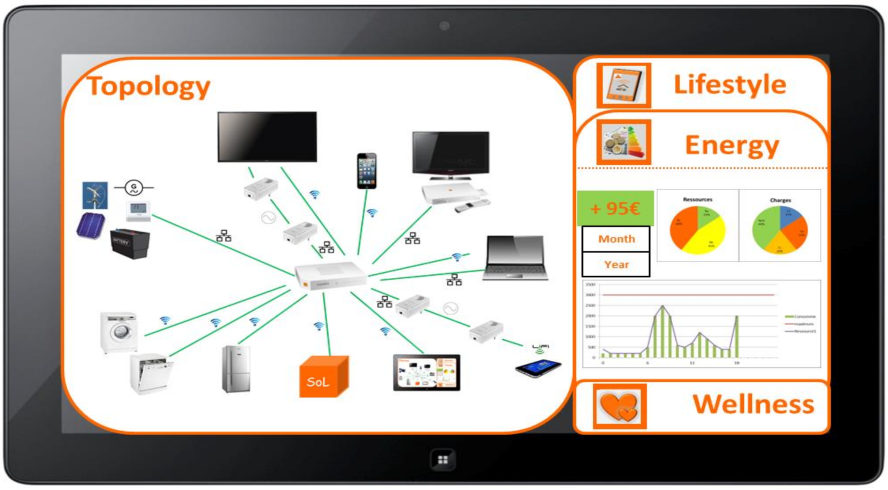


Figure 9 Dashboard example

5.2 Dashboard information

In this section we describe the information that the dashboard will provide. The dashboard will gather different kinds of information related to the ACEMIND network (1905.1, traffic, smart home, etc.). The aim is to present them on a single GUI that can be shown on ACEMIND final demonstrator.

5.2.1 Topology and metrics information

The dashboard will show the network topology as basic level information. It consists of the devices of the network and how they are connected (links between them: Ethernet, WiFi and PLC). Usually, home network devices include end devices (TVs, PCs, tablets, smartphones, …) and infrastructure devices (Ethernet switches, wireless access points, PLC plugs, etc.). Home network topology discovery is a tricky task mainly because of the heterogeneous nature of the home network, as it contains devices pertaining to various manufacturers and supporting multiple protocols. In fact, there is no universal protocol allowing to detect all devices and links. Typically, several protocols are available: LLDP, HTIP, LLTD, UPnP, etc. Furthermore, IEEE 1905.1 standard defines a topology discovery mechanism. In the ACEMIND project context, we will rely on 1905.1 protocol to detect infrastructure devices (1905.1 Devolo plugs). The detection of other ACEMIND demonstrator devices will depend on the supported protocols and the target use cases.

The dashboard will provide 1905.1 metrics as advanced level information. IEEE 1905.1 defines the following metrics:

- At transmitter side:
  - Interface type
  - Intermediate 802.1 legacy bridge flag
  - Packet errors (during a measurement period)
  - Transmitted packets (during a measurement period)
  - MAC throughput capacity (expressed in Mbps)
  - Link availability (expressed in % of time the link is idle)
  - PHY rate (expressed in Mbps)
- At receiver side:
  - Interface type
  - Packet errors (during a measurement period)
  - Received packets (during a measurement period)
  - RSSI (if the interface type is WiFi)

The interface type and intermediate 802.1 legacy bridge flag are not useful for the dashboard 1905.1 metrics as they are part of topology information. All remaining metrics are of interest to the dashboard. The final implementation will depend whether all 1905.1 metrics will be supported or not. In addition, we could support other metrics such as energy consumption on the dashboard in a second step (depending on available information).

Furthermore, the dashboard could indicate the paths used by flows. Typically, it would be possible to click on a given link to obtain information about ongoing flows. However, this kind of information needs interaction with path selection module. For the moment, it is not considered as mandatory information for the dashboard.

5.2.2 Traffic monitoring information

The following traffic monitoring information will be available on the dashboard at advanced level:

- Top web servers: visited http and https sites.
- Top clients of web servers
- Top mail senders and SMTP servers
- Top mail users and POP3/IMAP servers

- Hosts with top data transfers: devices with highest download and upload traffic volume. It would allow to identify devices having highest utilization of home network links.
- Top network services over TCP : application protocols (http …) and port numbers (flows) using TCP protocol
- Top network services over UDP
- AS statistics : top used AS (autonomous system) by bytes
- Top source autonomous systems : AS with most data volume transferred from them
- Hosts with top upload transfers in the network: identifies devices with highest upload utilization
- Hosts with top download transfers in the network: identifies devices with highest download utilization
- Application identification (e.g. skype, youtube, dailymotion, etc.)
- Active devices in the network (those sending traffic).

Most information can also be presented in terms of evolution during time showing for example the structure of overall traffic, services, etc. Table 1 summarizes all these information.

Table 1 Traffic monitoring information summary

Information	**Presentation**
Hosts with top data transfers *- Top clients of web servers* *- Hosts with top upload transfers in the network* *- Hosts with top download transfers in the network*	Statistics
Top network services - Over TCP - Over UDP	Statistics + graphs (overall traffic, per protocol traffic)
Top mail senders and SMTP servers	Statistics + graphs
Top mail users and POP3/IMAP servers	Statistics + graphs
AS statistics & top source autonomous systems	Statistics + graphs
Top web servers	Statistics
Applications identification and traffic proportions for each application	Statistics + graphs

It will be possible to the user to reset/delete the corresponding information through the GUI. Moreover, some of these information will be useful for the operator.

5.2.3 Smart home information

The dashboard will provide the following information at advanced level with respect to the smart home white goods appliances:

- For each Arcelik device:
  - Current instantaneous power consumption in W
  - Current program cycle
  - Forecast cycles consumption (remaining duration, estimated average power consumption in Wh and perhaps maximum power consumption in W
  - Status of the appliance (off, on, play, pause) if available
- Green Home demonstrator topology
  - List of devices with friendly name, model, manufacturer, appliance’s type

It could also be possible to launch some actions from the dashboard.

As we can see, only topology information is provided at basic level, all other information are displayed at advanced level to avoid complex GUI.

5.3 Architecture and modules interaction

The information described in the previous section will be provided to the dashboard thanks to dedicated software modules (managers/coordinators) developed by the ACEMIND partners.

As the dashboard will interact with each ACEMIND demonstrators modules, two options are conceivable to get needed information. One possible way to monitor the network is to rely on a central manager. The manager will retrieve pertinent information by interrogating the corresponding network modules (traffic monitoring, path selection, etc.). Then, the manager will provide this information to the dashboard to display them on laptop, tablet or smartphone. The second option consists of relying on multiple managers, one for each type of demonstrator: Hope (smart home), SoL (sign of life), 1905.1 manager (topology and metrics) and traffic monitoring collector. In this case, the dashboard will communicate with each manager to obtain needed information and displays it.

For the moment, the second option seems more appropriate as there is no need to aggregate information at an intermediate level with a central manager. Therefore, Figure 14 indicates the following interactions:

- Dashboard gets topology and metrics information through 1905.1 manager. The API needs to be defined, it has to allow dynamic notifications as topology might change and metrics information need to be updated periodically.
  - 1905.1 manager will be responsible of computing 1905.1 network topology and obtaining 1905.1 metrics based on standard 1905.1 messages.
  - Path selection information will be provided based on 1905.1 vendor specific TLVs or messages.
- Dashboard obtains traffic monitoring information through collector module based on REST API.
- Dashboard retrieves smart home information through Green home demonstrator coordinator based on REST API.

5.4 Traffic Monitoring

A typical example of the architecture of the proposed monitoring solution for the ACEMIND environment is shown in Figure 11. The basic ideas are:

1. Allow to generate IP flow statistics supplemented by additional application information and IEEE 1905.1 statistics directly by the network devices located in the home network.
2. Transfer data in an open (IPFIX) and secure (TLS) protocol to the cloud environment.
3. Collect, evaluate and access data via web interface and service.
4. Special web interface for ordinary users – customers of a big telecommunication operator. The architecture of the proposed solution was accepted throughout the consortium.

5. The FlowMon probe modules will be installed on Devolo 1905.1 plugs.
6. The FlowMon collector module can be installed on a local PC or in the cloud.

Devices used in home networks do not yet have the functionality defined by the IEEE 1905.1 standard and they do not allow to create information about the network traffic. Thus, the first year of the project was focused on research in this area.

Current form of displaying network statistics is not well suited for ordinary users. Therefore, the Orange research team within WP2 is trying to find appropriate display format. Web application should use REST API technology, which allows ACEMIND Dashboard application to access selected graphs, tables and other statistics. This application will be designed to simply provide the user with information about his home network and the devices in it.

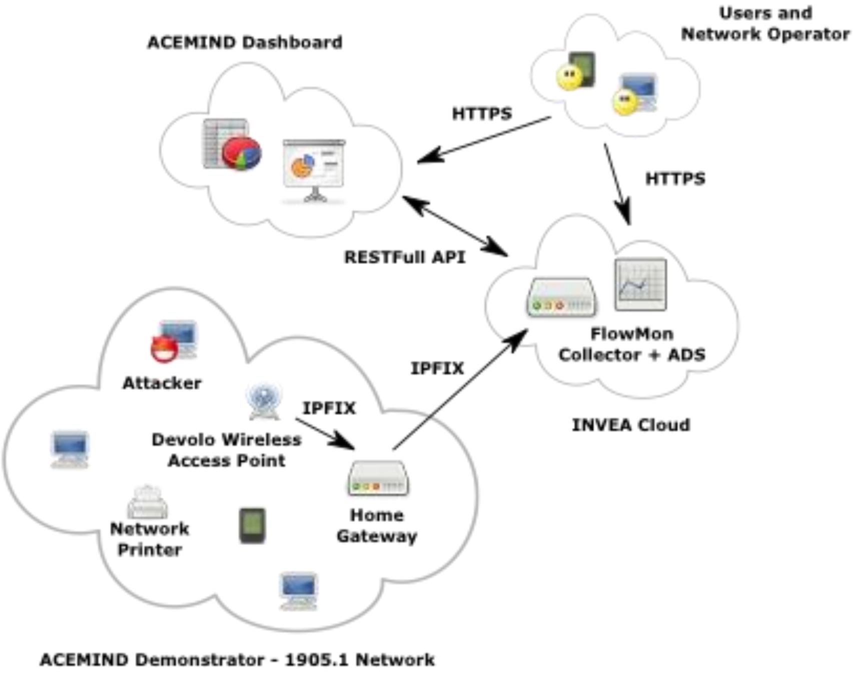


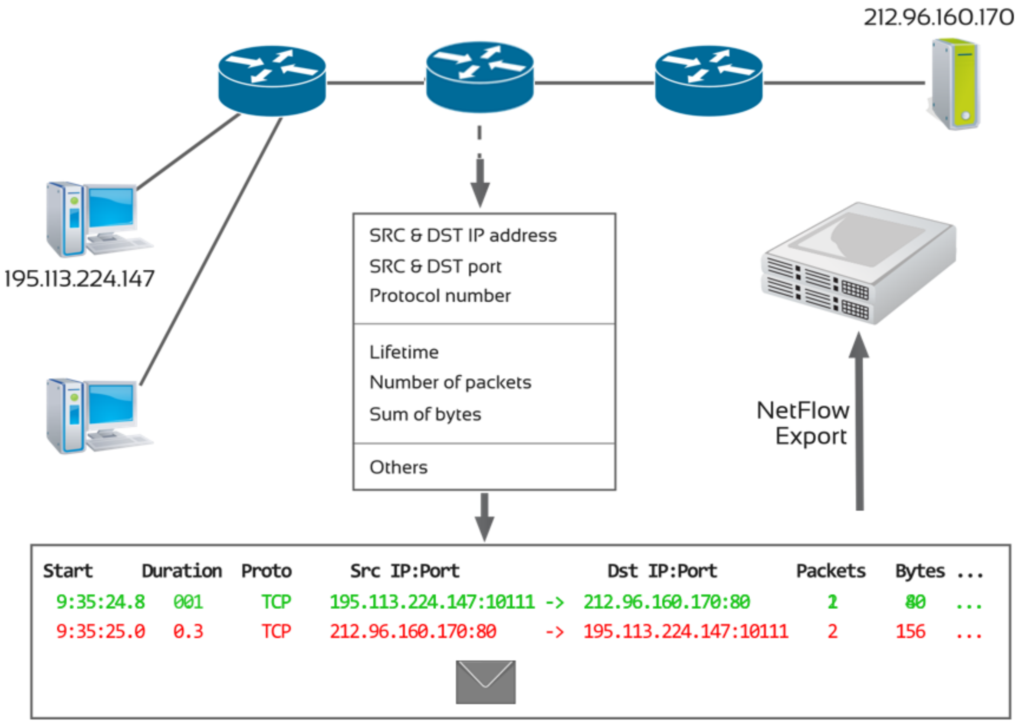
Figure 10 Architecture of the proposed monitoring solution for ACEMIND environment

5.4.1 The Principle of Measuring IP Flows in the Home Network

IP flow is defined as a sequence of packets with the same key items (see RFC 7011). Typically, these items include information from the IP packet header:

- Source and destination IP address
- Source and destination port
- Number of network (L3) and transport (L4) protocols

A flow is defined as a one-way connection of two entities using a computer network. Every recorded packet is either added to the existing flow, or a new flow is created for it, if there is not one already. Flow records can store any information from the packet headers. The basic record includes number of packets, first packet arrival time (start of the flow), last packet arrival time (end of the flow), total amount of data, VLAN tag, TCP flags etc. Traditionally, these are the items in L3 and L4 packet header. Modern monitoring tools allow to record information from the headers of other layers, especially L2 (e.g. MAC address, MPLS tags, VLAN tags). Current research and development is focused on monitoring at the application layer (L7). Principal of IP flows measuring is schematically shown in Figure 12.



```
Start      Duration  Proto   Src IP:Port                Dst IP:Port           Packets   Bytes ...
 9:35:24.8   001       TCP   195.113.224.147:10111 -> 212.96.160.170:80         1        80   ...
 9:35:25.0   0.3       TCP   212.96.160.170:80     -> 195.113.224.147:10111     2       156   ...
```

Figure 11 Principle of creating IP flows from the network traffic

Figure 12 illustrates a computer network with monitored end stations and two switches. The link between these switches is monitored and the passing traffic is recorded. A fixed size part containing the analyzed header is extracted from every packet and the header is then processed. Created flows are stored in flow cache. Flow is stored in the cache for as long as the connection, which generated the flow, is active, or until one of the set time intervals expires. Usually, this includes active and inactive timeouts. Active timeout specifies the maximum time of the flow existence. Inactive timeout defines the time during which the flow is stored in the memory when no additional packet from the same flow is captured. If the flow is removed from the flow memory, it is stored with additional flows into the packet and sent to the collector. The process which handles the monitoring and sends flow packets is called exporter. The device collecting, storing and processing flow packets is called collector.

The transfer of packets from exporter to collector is specified by a protocol. The most widely used protocol is currently NetFlow protocol developed by Cisco. It is practically an industry standard. The NetFlow protocol is currently being replaced by its modern variant – protocol IPFIX (IP Flow Information Export), which is already standardized by IETF standard and described in RFC 7011, 7015 and 5103. Together with these protocols, several other flow protocols were developed. They are more or less based on NetFlow, such as jFlow, sFlow, NetStream, appFlow, cflowd.

Flow exporter can be implemented on routers or in autonomous probes that are placed in important locations in the network. For example in the point of connecting the local network to the Internet, DMZ or to central active element on his SPAN port. For the purpose of measuring home networks and operation statistics derived from the IEEE1905.1 standard it seems appropriate to measure traffic on the central element of such network. For this purpose, Devolo network devices (dLAN 500) are used in the ACEMIND project and the software IPFIX exporter is currently being integrated to these devices. This exporter is currently used in the FlowMon probe and it was modified to be able to measure traffic from the hybrid networks.

5.4.2 FlowMon Probe

Probes are passive network devices designed for the collection of packets, calculating statistics about IP flows and exporting these statistics to the collector in the NetFlow v5/v9 or IPFIX format. The probes are equipped with one administrative port for remote configuration and export of the flow data and also with one or more monitoring ports for the network monitoring.

Probes are controlled remotely using web user interface or command line. Administrative port is used for configuration which is always encrypted (HTTPS, SSH). After the initial configuration, the probe works automatically without external interventions.

The subject of this project is to explore new additions to the current functionality of the FlowMon exporter such as:

Overview of the main functions of the probe

- Export of statistics in NetFlow v5/v9, IPFIX format
- IPv4/IPv6/MPLS/VLAN
- L2 monitoring – MAC address exporter
- Autonomous system number export
- Native geolocation (part of the flow statistics)
- 10/100/1000 Mbps data link support

Overview of the newly implemented functions of the probe

- Measurement of IEEE 1905.1 characteristics
- Measurement and analysis of HTTP – URL exporter
- Measurement and analysis of ARP traffic

5.4.3 FlowMon Collector

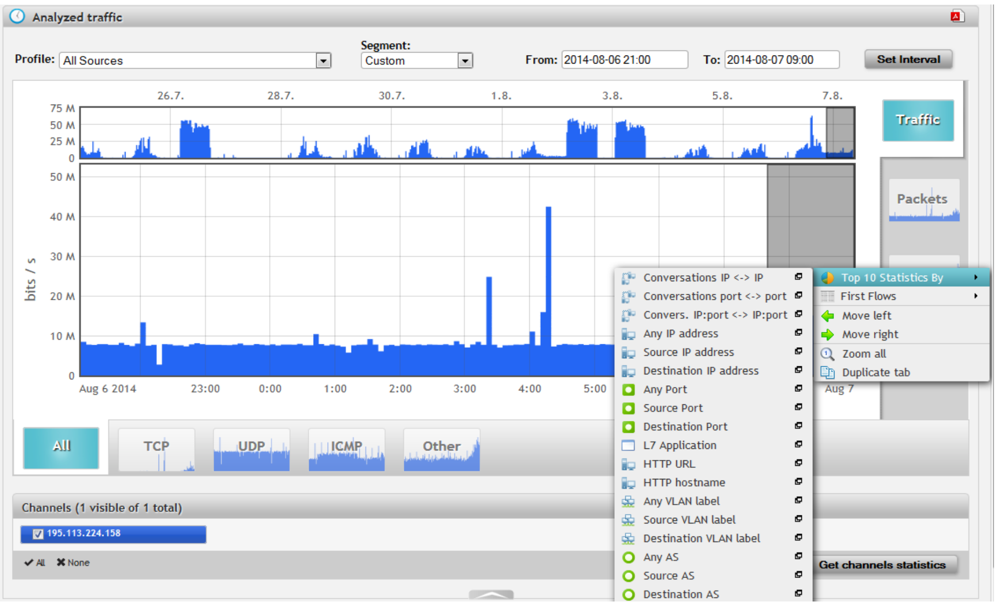
The goal of this project is to collect IP flows by a collector running in a virtual (cloud) environment for large group of users (home networks) and create appropriate access to this information using “network dashboard”. The center of this is the IPFIX collector which collects, analyses and visualizes statistics of IP flows supplemented by specific information available in home networks. In the third year, the process of collecting and analyzing IP flows will be expanded to include a system of anomaly detection and undesirable behavioral patterns in hybrid networks.

Displaying of saved IPFIX (or NetFlow or sFlow) data and their analysis (searching, aggregation, outputs, etc.) is done using secured web interface. The core of the collector is FlowMon Monitoring Center application for statistics storage and visualization.

Overview of the main functions

FlowMon Monitoring Center enables to view and analyze data stored on the collector. Application is used to perform following operations:

- Create long-term charts and reports with various types of views divided into categories according to size (number of transferred bytes, flows, packets), IP traffic (TCP, UDP, ICMP, others) or protocol (HTTP, IMAP, SSH, etc.)
- Generate statistics and detailed listings over optional time intervals
- Listing top N statistics by various criteria (number of transferred bytes, packets, flows, etc.) allowing to list the most active or the most anomalous computers participating in the network traffic
- Alert administrators by e-mail in the case of user-defined situations (e.g. excessive data transfer, the occurrence of dangerous anomalies, use of forbidden application, etc.)
- Create profiles to store data matching the defined filters (e.g. HTTP, FTP, SMTP, SSH traffic, autonomous systems, HTTP information, etc.)


Analyzed traffic

Profile: All Sources

Segment: Custom

From: 2014-08-06 21:00

To: 2014-08-07 09:00

Channels (1 visible of 1 total)

☑ 195.113.224.158

Figure 12 Displaying data in the FlowMon monitoring center

FlowMon Monitoring Center provides clear reports containing statistics on network traffic in the form of pie charts, continuous graphs and tables, which are important reports for automatic monitoring of the traffic structure and used services, revealing hosts generating the highest traffic on the key lines, correct planning of link capacity and much more, for example:

- Top reports –list of stations, services and communications dominating in the particular traffic, displayed using table and pie charts.
- Traffic reports – describes traffic for the selected time period and displays it's intensity in the graph.
- Sending of the selected reports for the chosen time period to e-mail of the user, ability to export to PDF, CSV.

Solution can be further customized using your own set of reports built from pre-defined chapters containing tables and graphs, or user-defined chapters. Working with chapters does not require any technical knowledge about computer networks. A set of predefined chapters can be extended by a network administrator or other technician based on the user requirements.

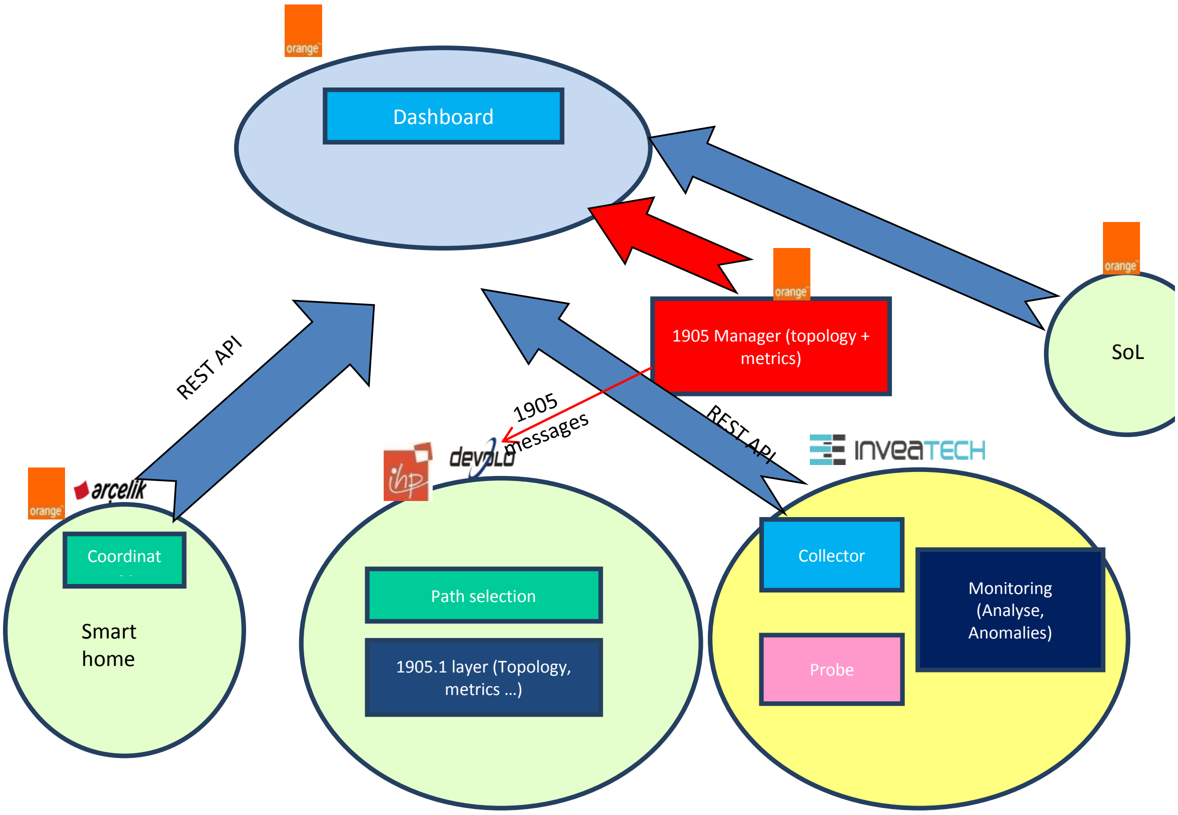

Dashboard
1905 Manager (topology + metrics)
SoL
REST API
1905 messages
REST API
Coordinat
Smart home
Path selection
1905.1 layer (Topology, metrics …)
Collector
Monitoring (Analyse, Anomalies)
Probe

Figure 13 Modules interaction

6 Security, Privacy and Legal Issues

This section provides recommendations and specifications for security, privacy and legal issues related to management of hybrid home networks. We research the security aspects to achieve secure visibility and management in heterogeneous home networks. We evaluate available security technologies and solutions to be used in an ACEMIND network as well as to identify potential gaps to be fulfilled.

There are several sensitive issues that must be assessed and resolved concerning privacy. We research privacy issues arising in proposed ACEMIND scenarios. The emphasis is put on advanced techniques to ensure privacy. Privacy and security cannot be enforced without an analysis of legal aspects, issues and impacts. We present results of our observation on current legal, policy, and regulation situation. The requirements and recommendations for ACEMIND demonstrators are set to evaluate compliance with common legal aspects.

6.1 Security Considerations

The ACEMIND project aims to provide secure network visibility (network security monitoring) and management in heterogeneous home networks. The visibility is based on flows passing through network (see Section Monitoring and Management). The flow information (IPFIX data) carries important traffic and user information. In this section, we describe security requirements and potential security threats for flow monitoring in home networks. The considerations are based on relevant parts from IPFIX standard [RFC7011] and they are further adopted to fit ACEMIND scenarios. The proposed system must be capable of transporting data over public networks (e.g., Internet), where attackers can capture, modify or insert packets.

The security requirements for flow monitoring in heterogeneous home networks are as follows:

- ***Confidentiality*** – data transferred from a probe to a collector must be encrypted to prevent disclosure of information transported via IPFIX.
- ***Integrity*** – communication protocol must prevent the injection of incorrect data or data loss or duplication of transferred data from a probe to a collector. The involved devices must be able to check the integrity of the data they receive.
- ***Authentication*** – to avoid unauthorized access to data all exporting and collecting processes must mutually authenticate. The authentication must be completed between the involved devices before any transfer of data.
- ***Exclusivity*** – if the device embeds a SIM application (which is not the case for all Smart Home devices), it must not be possible to use the UICC associated to the Smart Home device for other applications. The presence of a SIM application is much more secure than the login/password procedure and allows to use the Generic Authentication/Bootstrapping Architectures (GAA/GBA). Unfortunately until now some manufacturers do not give access to the driver of their SIM card, which compromises that approach. In any case precautions must be taken in order to avoid that a given thing can connect itself to any application, and vice versa.
- ***Anonymity*** – the device identity must remain secret.

6.2 Disclosure of Monitored Data

Transport Layer Security (TLS) [RFC5246] and Datagram Transport Layer Security (DTLS) [RFC6347] ensures the requirements of confidentiality, integrity, and authentication. They are nowadays used to secure data exchange on Internet. IPFIX standard [RFC7011] requires implementation of TLS for TCP transport and DTLS for UDP or SCTP. Unfortunately, this requirement is not fulfilled and implemented by many vendors. In the ACEMIND project we will focus on TLS over TCP implementation and evaluation.

Encryption Key Length

Key length is the crudest way of determining how long a cypher will take to break, as it is the raw number of ones and zeros used in a cypher. Similarly, the crudest form of attack on a cypher is known as a brute force attack (or exhaustive key search), which involves trying every possible combination until the correct one is found.

Encryption used in TLS is invariably between 128-bits and 256-bits in key length (with higher levels used for handshake and data authentication). It should be noted that the US government uses 256-bit encryption to protect “sensitive” data (and 128-bit for “routine” encryption needs). However the method it uses is AES (Advanced Encryption System).

Ciphersuites

While encryption key length refers to the amount of raw of numbers involved, ciphers are the mathematics used to perform the encryption, and it is weakness in these algorithms, rather than in the key length, that often leads to encryption being broken.
By far the most common ciphers are Blowfish and AES. In addition to this, RSA is used to encrypt and decrypt the cipher's keys, and SHA-1 or SHA-2 are used as a hash function to authenticate the data.
AES is now generally considered the most secure cipher, and its adoption by the US government has only increased its perceived reliability, and consequently its popularity.

Securing the Collected Data

The security of the collected data is important. The storage and access to flow data must be protected via technical as well as policy means to ensure that the privacy of monitored networks is protected. Requirements for flow collection in heterogeneous home networks are as follows:

- ***Secure access*** – the ability to communicate over secure channel (HTTPS) and strong authentication to confine flow visibility to authorized users.
- ***Multi-user access (multitenancy)*** – the ability to define precisely what data each user has access to and what operations he is authorized for.
- ***Automated detection of data sources*** – detection and overview of new connected and monitored networks.

Privacy Considerations

The flow data contains information about activities on the observed network and may identify users. It is very important to take the user privacy in consideration. For example, the project Turris [TUR] is a service helping to protect its user's home network with the help of a special router. It is a not-for-profit research project of CZ.NIC, the registry of the Czech national top level domain .CZ. The goal of Turris project is to analyze the traffic between Internet and the home network, and identify suspicious data flows.

6.3 Legal Issues

The concern of securing the collected data is also related to the more global concern of cyber criminality.

Conflict of laws in cyberspace has become a major cause of concern for computer security community. Some of the main challenges and complaints about the antivirus industry are the lack of global web regulations, a global base of common rules to judge, and eventually punish, cyber crime and cyber criminals. There is no global cyber law and cyber security treaty that can be invoked for enforcing global cyber security issues.

International legal issues of cyber attacks are really tricky and complicated in nature. For instance, even if an antivirus firm locates the cyber criminal behind the creation of a particular virus or piece of malware or again one form of cyber attack, often the local authorities cannot take action due to lack of laws under which to prosecute. This is mainly caused by the fact that many countries have their own regulations regarding cyber crime. Authorship attribution for cyber crime and cyber attacks has become a major problem for international law enforcement agencies.

"Computer viruses switch from one country to another, from one jurisdiction to another – moving around the world, using the fact that we don't have the capability to globally police operations like this. So the Internet is as if someone had given free plane tickets to all the online criminals of the world" (Mikko Hyppönen).

Businesses are eager to expand to less developed countries due to the low cost of labor, says White et al. (2012). However, these countries are the ones with the least amount of Internet safety measures, and the Internet Service Providers are not so focused on implementing those safety measures (2010). Instead, they are putting their main focus on expanding their business, which exposes them to an increase in criminal activity.

In response to the growing problem of cyber crime, the European Commission established the European Cybercrime Centre (EC3) [EUROPOL]. The EC3 effectively opened on 1 January 2013 and will be the focal point in the EU's fight against cyber crime, contributing to faster reaction to online crimes. It will support member states and the EU's institutions in building an operational and analytical capacity for investigations, as well as cooperation with international partners.

And from the US side, on May 12, 2011, the White House sent Congress a proposed cybersecurity law designed to force companies to do more to fend off cyber attacks, a threat that has been reinforced by recent reports about vulnerabilities in systems used in power and water utilities.

Executive order 13636 Improving Critical Infrastructure Cybersecurity was signed February 12, 2013. And on the 12th of February 2014, the NIST (National Institute of Standards and Technology) published the version 1.0 of a document categorizing the legal and regulatory requirements regarding cybersecurity, and their related informative references [NIST].

Recurrent incidents of cyber criminality have led the countries to elaborate efficient security recommendations Below is a partial listing of European, United Kingdom, Czech Republic, Canadian and U.S. governmental laws and regulations that have, or will have, a significant effect on data processing and information security. Important industry sector regulations have also been included when they have a significant impact on information security.

UK Data Protection Act 1998 makes new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The European Union Data Protection Directive (EUDPD) requires that all EU members must adopt national regulations to standardize the protection of data privacy for citizens throughout the EU.

The Computer Misuse Act 1990 is an Act of the UK Parliament making computer crime (e.g., hacking) a criminal offence. The Act has become a model upon which several other countries including Canada and the Republic of Ireland have drawn inspiration when subsequently drafting their own information security laws.

Czech Republic – the Act no. 181/2014 Coll. on the Cyber Security and on the Amendments of the Related Acts (Cyber Security Law) has been published in the Collection of Laws on August 29, 2014. It will be effective as of January 1, 2015.

EU Data Retention laws requires Internet service providers and phone companies to keep data on every electronic message sent and phone call made for between six months and two years.

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232 g; 34 CFR Part 99) is a US Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.

Federal Financial Institutions Examination Council’s (FFIEC) security guidelines for auditors specifies requirements for online banking security.

Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the adoption of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. And, it requires health care providers, insurance providers and employers to safeguard the security and privacy of health data.

Gramm–Leach–Bliley Act of 1999 (GLBA), also known as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process.

Sarbanes–Oxley Act of 2002 (SOX). Section 404 of the act requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in annual reports they submit at the end of each fiscal year. Chief information officers are responsible for the security, accuracy and the reliability of the systems that manage and report the financial data. The act also requires publicly traded companies to engage independent auditors who must attest to, and report on, the validity of their assessments.

Payment Card Industry Data Security Standard (PCI DSS) establishes comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

State security breach notification laws (California and many others) require businesses, nonprofits, and state institutions to notify consumers when unencrypted "personal information" may have been compromised, lost, or stolen.

Personal Information Protection and Electronics Document Act (PIPEDA) – An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act.

Loi Informatique et Libertés, Act N°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties. This act, elaborated by the CNIL (Commission Nationale de l'Informatique et des Libertés) defines the conditions according which the processing of private data collected by a third party is legal in France [CNIL]. In parallel the French telecommunications regulation authority (named ARCEP) proposes a site collecting private data, compliant with the CNIL recommendations, in the purpose of improving the quality of the telecommunications services [ARCEP].

A further analysis about constrains regarding home network data monitoring will be conducted in the upcoming months within ACEMIND project.

7 Conclusion

In this deliverable, we presented the main components of the ACEMIND hybrid network. It will be based on dLan hybrid devices implementing IEEE 1905.1 convergence layer. This layer will enable several features including topology discovery, links metrics, wireless APs auto configuration and secure pairing enhancing user experience. Furthermore, these hybrid devices will embed FlowMon probes modules which will allow, along with the collector module (which can be installed on a local PC or in the cloud), to collect data about traffic monitoring. A GUI available for the end users and the operator named dashboard was described. It aims to display useful network information gathered through an interaction with other modules: 1905.1 manager for network topology and links metrics, FlowMon collector for traffic monitoring (flows, applications and statistics) and smart home coordinator. Finally, some security and privacy issues were discussed. It is intended to rely on TLS over TCP protocol to secure exported monitoring data with IPFIX standard.

So far we have:

- Presented the different components of the ACEMIND hybrid network
- Implemented IEEE 1905.1 convergence layer on dLan hybrid devices
- Specified the dashboard pertinent information
- Defined traffic monitoring architecture based on FlowMon probes and collector
- Defined the global architecture and interactions between the different modules

Next steps will include:

- Implementation of the dashboard and the associated APIs to communicate with corresponding modules
- Implementation of the beyond 1905.1 features, in particular, path selection
- Integration of FlowMon probes on dLan 1905.1 hybrid devices
- Implementation of TLS over TCP for FlowMon exported data
- Setup of the ACEMIND hybrid demonstrator (subject of task 3.3 and deliverables D3.3 and D3.4)

References

[HGI2] “Home gateway and home network diagnostics module requirements”, http://www.homegatewayinitiative.org/publis/HGI-RD016_HG-Home-Network-Diag-Modul-Req.pdf, April 2013.

[KLD13] A. Kortebi, P. Le Dain, F. Duré, “Home Network Assistant: towards better diagnostics and increased customer satisfaction”, IEEE GIIS 2013.

[NIST] “Framework for Improving Critical Infrastructure Cybersecurity”, Version 1.0, National Institute of Standards and Technology, February 12, 2014

[RFC5246] T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, Internet Engineering Task Force, August 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5246.txt

[RFC6347] E. Rescorla and N. Modadugu, “Datagram Transport Layer Security Version 1.2”, RFC 6347, Internet Engineering Task Force, January 2012. [Online]. Available: http://www.ietf.org/rfc/rfc6347.txt

[RFC7011] B. Claise, B. Trammell, and P. Aitken, “Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information”, RFC 7011 (Internet Standard), Internet Engineering Task Force, September 2013. [Online]. Available: http://www.ietf.org/rfc/rfc7011.txt

[TUR] CZ.NIC, “Project Turris”, September 2014. [Online]. Available: https://www.turris.cz/en/

[EUROPOL] https://www.europol.europa.eu/ec3

[CNIL] http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

[ARCEP] https://extranet.arcep.fr/portail/privacy.aspx