Global Access to the Internet for All
Internet-Draft
Intended status: Informational
Expires: July 25, 2015

J. Saldana, Ed.
University of Zaragoza
A. Arcia-Moret
Universidad de Los Andes
B. Braem
iMinds
L. Navarro
U. Politecnica Catalunya
E. Pietrosemoli
ICTP
C. Rey-Moreno
University of the Western Cape
A. Sathiaseelan
University of Cambridge
M. Zennaro
Abdus Salam ICTP
January 21, 2015

# Alternative Network Deployments. Taxonomy and characterization
draft-manyfolks-gaia-community-networks-02

## Abstract

This document presents a taxonomy of "Alternative Network deployments", and a set of definitions and shared characteristics. This term includes a set of network access models emerged in the last decade with the aim of bringing Internet connectivity to people, using topological, architectural and business models different from the so-called "traditional" ones, where a company deploys the network infrastructure for connecting the users, who pay for it.

Several initiatives throughout the world have built large scale networks that are alternative to the traditional network operator deployments using predominately wireless technologies (including long distance) due to the reduced cost of using the unlicensed spectrum. Wired technologies such as Fiber are also used in some of these alternate networks. There are several types of such alternate network: networks such as community networks are self-organized and decentralized networks wholly owned by the community; networks owned by individuals who act as wireless internet service providers (WISPs), networks owned by individuals but leased out to network operators who use such networks as a low-cost medium to reach the underserved population and finally there are networks that provide connectivity by sharing wireless resources of the users.

The emergence of these networks can be motivated by different causes such as the reluctance, or the impossibility, of network operators to

provide wired and cellular infrastructures to rural/remote areas. In these cases, the networks have self sustainable business models that provide more localised communication services as well as Internet backhaul support through peering agreements with traditional network operators. Some other times, networks are built as a complement and an alternative to commercial Internet access provided by "traditional" network operators.

The present classification considers different existing network models such as Community Networks, open wireless services, user-extensible services, traditional local Internet Service Providers (ISPs), new global ISPs, etc. Different criteria are used in order to build a classification as e.g., the ownership of the equipment, the way the network is organized, the participatory model, the extensibility, if they are driven by a community, a company or a local (public or private) stakeholder, etc.

According to the developed taxonomy, a characterization of each kind of network is presented, in terms of specific network characteristics related to architecture, organization, etc.

Table of Contents

# 1. Introduction

Several initiatives throughout the world have built large scale networks that are alternative to the traditional network operator deployments using predominately wireless technologies (including long distance) due to the reduced cost of using the unlicensed spectrum. Wired technologies such as Fiber are also used in some of these alternate networks. There are several types of such alternate network: networks such as community networks are self-organized and decentralized networks wholly owned by the community; networks owned by individuals who act as wireless internet service providers (WISPs), networks owned by individuals but leased out to network operators who use such networks as a low cost medium to reach the underserved population and finally there are networks that provide connectivity by sharing wireless resources of the users.

The emergence of these networks can be motivated by different causes, as the reluctance, or the impossibility, of network operators to provide wired and cellular infrastructures to rural/remote areas [Pietrosemoli]. In these cases, the networks have self sustainable business models that provide more localised communication services as well as Internet backhaul support through peering agreements with traditional network operators. Some other times, they are built as a complement and an alternative to commercial Internet access provided by "traditional" network operators.

One of the aims of the Global Access to the Internet for All (GAIA) IRTF initiative is "to document and share deployment experiences and research results to the wider community through scholarly publications, white papers, Informational and Experimental RFCs, etc." In line with this objective, this document is intended to propose a classification of these "Alternative Network deployments". This term includes a set of network access models emerged in the last decade with the aim of bringing Internet connectivity to people, following topological, architectural and business models different from the so-called "traditional" ones, where a company deploys the infrastructure connecting the users, who pay for it. The document is intended to be largely descriptive providing a broad overview of initiatives, technologies and approaches employed in these networks. Research references describing each kind of network are also provided.

## 1.1. Requirements Language

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 [RFC2119].

# 2. Classification

This section classifies Alternative Networks (ANs) according to their intended usage. Each of them has different incentive structures, maybe common technological challenges, but most importantly interesting usage challenges which feeds into the incentives as well as the technological challenges.

This classification is agnostic from the technical point of view. Technology in this case must be taken as implementation. Moreover, many of these networks are implemented in a way that several technologies (Ad-Hoc Wi-Fi, Infrastructure Wi-Fi, Optical Fiber, IPv4, IPv6, RFC1918, OLSR, BMX6, etc.) coexist.

## 2.1. Community Networks

Community Networks are large-scale, distributed, self-managed networks sharing these characteristics:

- They are built and organized in a decentralized and open manner.

- They start and grow organically, they are open to participation from everyone, sometimes agreeing to an open peering agreement. Community members directly contribute active network infrastructure (not just passive infrastructure).

- Knowledge about building and maintaining the network and ownership of the network itself is decentralized and open. Community members have an obvious and direct form of organizational control over the overall operation of the network in their community (not just their own participation in the network).

- The network CAN serve as a backhaul for providing a whole range of services and applications, from completely free to even commercial services.

Hardware and software used in Community Networks CAN be very diverse, even inside one network. A Community Network CAN have both wired and wireless links. The network CAN be managed by multiple routing protocols or network topology management systems.

These networks grow organically, since they are formed by the aggregation of nodes belonging to different users. A minimum governance infrastructure is required in order to coordinate IP addressing, routing, etc. A clear example of this kind of Community Network is described in [Braem]. These networks are effective in enhancing and extending digital Internet rights following a participatory model.

The fact of the users adding new infrastructure (i.e. extensibility) can be used to formulate another definition: A Community Network is a network in which any participant in the system may add link segments to the network in such a way that the new network segments can support multiple nodes and adopt the same overall characteristics as those of the joined network, including the capacity to further extend the network. Once these link segments are joined to the network, there is no longer a meaningful distinction between the previous extent of the network and the new extent of the network.

In Community Networks, the profit can only be made by services and not by the infrastructure itself, because the infrastructure is neutral, free, and open (traditional Internet Service Providers, ISPs, base their business on the control of the infrastructure). In Community Networks, everybody keeps the ownership of what he/she has contributed.

Community Networks MAY also be called "Free Networks" or even "Network Commons". [FNF]. The majority of Community Networks accomplishes the definition of Free Network, included in the next subsection.

#### 2.1.1. Free Networks

A definition of Free Network (which MAY be the same as Community Network) is proposed by the Free Network Foundation (see http://thefnf.org) as:

"A free network equitably grants the following freedoms to all:

Freedom 0 - The freedom to communicate for any purpose, without discrimination, interference, or interception.

Freedom 1 - The freedom to grow, improve, communicate across, and connect to the whole network.

Freedom 2- The freedom to study, use, remix, and share any network communication mechanisms, in their most reusable forms."

The principles of Free, Open and Neutral Networks have also been summarized (see http://guifi.net/en/FONCC) this way:

- You have the freedom to use the network for any purpose as long as you do not harm the operation of the network itself, the rights of other users, or the principles of neutrality that allow contents and services to flow without deliberate interference.

- You have the right to understand the network, to know its components, and to spread knowledge of its mechanisms and principles.

- You have the right to offer services and content to the network on your own terms.

- You have the right to join the network, and the responsibility to extend this set of rights to anyone according to these same terms.

## 2.2. Wireless Internet Service Providers WISPs

WISPs are commercially-operated wireless Internet networks that provide Internet and/or Voice Over Internet (VoIP) services. They are most common in areas not covered by incumbent telcos or ISPs. WISPs often use wireless point-to-point or point-to-multipoint in the unlicensed frequencies but licensed frequency use is common too especially in regions where unlicensed spectrum is either perceived as crowded or where unlicensed spectrum may have regulatory barriers impeding its use.

Most WISPs are operated by local companies responding to a perceived market gap. There is a small but growing number of WISPs, such as AirJaldi [Airjaldi] in India that have expanded from local service into multiple locations.

Since 2006, the deployment of cloud-managed WISPs has been possible with companies like Meraki and later OpenMesh and others. Until recently, however, most of these services have been aimed at industrialised markets. Everylayer [Everylayer], launched in 2014, is the first cloud-managed WISP service aimed at emerging markets.

## 2.3. Shared infrastructure model

These networks are owned by individuals but leased out to network operators who use them as a low cost medium to reach the underserved population.

### 2.4. Crowdshared approaches, led by the people and third party stakeholders

These networks can be defined as a set of nodes whose owners share common interests (e.g. sharing connectivity; resources; peripherals) regardless of their physical location. The node location exhibits a space and time correlation which is the basis to establish a robust connectivity model over time.

These networks conform to the following approach: the home router creates two wireless networks: one of them is normally used by the owner, and the other one is public. A small fraction of the bandwidth is allocated to the public network, to be employed by any user of the service in the immediate area. Some examples are described in [PAWS] and [Sathiaseelan_c]. Other example is constituted by the networks created and managed by City Councils (e.g., [Heer]).

In the same way, some companies [Fon] develop and sell Wi-Fi routers with a dual access: a Wi-Fi network for the user, and a shared one. A user community is created, and people can join the network in different ways: they can buy a router, so they share their connection and in turn they get access to all the routers associated to the community. Some users can even get some revenue every time another user connects to their Wi-Fi spot. Other users can just buy some passes in order to use the network. Some telecommunications operators can collaborate with the community, including in their routers the possibility of creating these two networks.

A Virtual Private Network (VPN) is created for public traffic, so it is completely secure and separated from the owner’s connection. The network capacity shared may employ a low priority, a less-than-best-effort or scavenger approach, so as not to harm the traffic of the owner of the connection [Sathiaseelan_a].

The elements involved in a crowd-shared network are summarised below:

- Interest: a parameter capable of providing a measure (cost) of the attractiveness of a node towards a specific location, in a specific instance in time.

- Resources: A physical or virtual element of a global system. For instance, bandwidth; energy; data; devices.

- The owner: End users who sign up for the service and share their network capacity. As a counterpart, they can access another owners’ home access for free. The owner can be an end user or an entity (e.g. operator; virtual operator; municipality) that is to be made responsible for any actions concerning his/her device.

- The user: a legal entity or an individual using or requesting a publicly available electronic communications’ service for private or business purposes, without necessarily having subscribed to such service.

- The Virtual Network Operator (VNO): An entity that acts in some aspects as a network coordinator. It may provide services such as initial authentication or registering, and eventually, trust relationship storage. A VNO is not an ISP given that it does not provide Internet access (e.g. infrastructure; naming). A VNO is neither an Application Service Provider (ASP) since it does not provide user services. Virtual Operators MAY also be stakeholders with socio-environmental objectives. They CAN be a local government, grass root user communities, charities, or even content operators, smart grid operators, etc. They are the ones who actually run the service.

- Network operators, who have a financial incentive to lease out the unused capacity [Sathiaseelan_b] at lower cost to the VNOs.

VNOs pay the sharers and the network operators, thus creating an incentive structure for all the actors: the end users get money for sharing their network, the network operators are paid by the VNOs, who in turn accomplish their socio-environmental role.

### 2.5. Testbeds for research purposes

In some cases, the initiative to start the network is not from the community, but from a research entity (e.g. a university), with the aim of using it for research purposes [Samanta], [Bernardi].

## 3. Scenarios where Alternative Networks are deployed

Alternative Network deployments are present in every part of the world. Even in some high-income countries, these networks have been built as an alternative to commercial ones managed by traditional network operators. This section discusses the scenarios where Alternative Networks have been deployed.

### 3.1. Digital Divide and Alternative Networks

There is no definition for what a developing country represents that has been recognized internationally, but the term is generally used to describe a nation with a low level of material well-being. In this sense, one of the most commonly used classification is the one by the World Bank, who ranks countries according to their Gross National Income (GNI) per Capita: low income, middle income, and high income, being those falling within the low and middle income groups considered developing economies. Developing countries have also been defined as those which are in transition from traditional lifestyles towards the modern lifestyle which began in the Industrial Revolution. Additionally, the Human Development Index, which considers not only the GNI but also life expectancy and education, has been proposed by the United Nations to rank countries according to their well-being and not solely based on economic terms. These classifications are used to give strong signals to the international community about the need of special concessions in support of these countries, implying a correlation between development and increased well-being.

However, at the beginning of the 90's the debates about how to quantify development in a country were shaken by the appearance of Internet and mobile phones, which many authors consider the beginning of the Information Society. With the beginning of this Digital Revolution, defining development based on Industrial Society concepts started to be challenged, and links between digital development and its impact on human development started to flourish. The following dimensions are considered to be meaningful when measuring the digital development state of a country: infrastructures (availability and affordability); ICT (Information and Communications Technology) sector (human capital and technological industry); digital literacy; legal and regulatory framework; and content and services. The lack or less extent of digital development in one or more of these dimensions is what has been referred as Digital Divide. This divide is a new vector of inequality which - as it happened during the Industrial Revolution - generates a lot of progress at the expense of creating a lot economic poverty and exclusion. The Digital Divide is considered to be a consequence of other socio-economic divides, while, at the same time, a reason for their rise.

In this context, the so-called "developing countries", in order not to be left behind of this incipient digital revolution, motivated the World Summit of the Information Society which aimed at achieving "a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life" [WSIS], and called upon "governments, private sector, civil society and international organisations" to actively engage to accomplish it [WSIS].

Most efforts from governments and international organizations focused initially on improving and extending the existing infrastructure in order not to leave their population behind. As an example, one of the goals of the Digital Agenda for Europe [DAE] is "to increase regular internet usage from 60% to 75% by 2015, and from 41% to 60% among disadvantaged people."

Universal Access and Service plans have taken different forms in different countries over the years, with very uneven success rates, but in most cases inadequate to the scale of the problem. Given its incapacity to solve the problem, some governments included Universal Service and Access obligations to mobile network operators when liberalizing the telecommunications market. In combination with the overwhelming and unexpected uptake of mobile phones by poor people, this has mitigated the low access indicators existing in many developing countries at the beginning of the 90s [Rendon].

Although the contribution made by mobile network operators in decreasing the access gap is undeniable, their model presents some constraints that limit the development outcomes that increased connectivity promises to bring. Prices, tailored for the more affluent part of the population, remain unaffordable to many, who invest large percentages of their disposable income in communications. Additionally, the cost of prepaid packages, the only option available for the informal economies existing throughout developing countries, is high compared with the rate longer-term subscribers pay.

The consolidation of many Alternative Networks (e.g. Community Networks) in high income countries sets a precedent for civil society members from the so-called developing countries to become more active in the search for alternatives to provide themselves with affordable access. Furthermore, Alternative Networks could contribute to other dimensions of the digital development like increased human capital and the creation of contents and services targeting the locality of each network.

## 3.2. Urban vs. rural areas

The Digital Divide presented in the previous section is not only present between countries, but within them too. This is specially the case for rural inhabitants, which represents approximately 55% of the world’s population, from which 78% inhabit in developing countries. Although it is impossible to generalize among them, there exist some common features that have determined the availability of ICT infrastructure in these regions. The disposable income of their dwellers is lower than those inhabiting urban areas, with many surviving on a subsistence economy. Many of them are located in geographies difficult to access and exposed to extreme weather conditions. This has resulted in the almost complete lack of electrical infrastructure. This context, together with their low population density, discourages telecommunications operators to provide similar services to those provided to urban dwellers, since they do not deem them profitable.

The cost of the wireless infrastructure required to set up a network, including powering it via solar energy, is within the range of availability if not of individuals at least of entire communities. The social capital existing in these areas can allow for Alternative Network set-ups where a reduced number of nodes may cover communities whose dwellers share the cost of the infrastructure and the gateway and access it via inexpensive wireless devices. Some examples are presented in [Pietrosemoli] and [Bernardi].

In this case, the lack of awareness and confidence of rural communities to embark themselves in such tasks can become major barriers to their deployment. Scarce technical skills in these regions have been also pointed as a challenge for their success, but the proliferation of urban Community Networks, where scarcity of spectrum, scale, and heterogeneity of devices pose tremendous challenges to their stability and the services they aim to provide, has fuelled the creation of robust low-cost low-consumption low-complexity off-the-shelf wireless devices which make much easier the deployment and maintenance of these alternative infrastructures in rural areas.

# 4. Technologies employed

## 4.1. Wired

In many (developed or developing) countries it may happen that national service providers may decline to provide connectivity to tiny and isolated villages. So in some cases the villagers have created their own optical fiber networks. It is the case of Lowenstedt in Germany [Lowenstedt].

## 4.2. Wireless

Different wireless technologies [WNDW] can be employed in Alternative Network deployments. Below we summarise topics to be considered in such deployments:

### 4.2.1. Antennas

Three kinds of antennas are suitable to be used in these networks: omnidirectional, directional and high gain antennas.

For local access, omnidirectional antennas are the most useful, since they provide the same coverage in all directions of the plane in which they are located. Above and below this plane, the received signal will diminish, so the maximum benefits are obtained when the client is at approximately the same height as the Access Point.

When using an omnidirectional antenna outdoors to provide connectivity to a large area, people often select high gain antennas located at the highest structure available to extend the coverage. In many cases this is counterproductive, since a high gain omnidirectional antenna will have a very narrow beamwidth in the vertical plane, meaning that clients that are below the plane of the antenna will receive a very weak signal (and by the reciprocity property of all antennas, the antenna will also receive a feeble signal from the client). A moderate gain omnidirectional of about 8 to 10 dBi is normally preferable. Higher gain omnidirectional antennas are only advisable when the farthest way client is roughly in the same plane.

For indoor clients, omnidirectional antennas are generally fine, because the numerous reflections normally found in indoor environments negate the advantage of using directional antennas.

For outdoor clients, directional antennas can be quite useful to extend coverage to an Access Point fitted with an omnidirectional one.

When building point-to-point links, the highest gain antennas are the best choice, since their narrow beamwidth mitigates interference from other users and can provide the longest links [Flickenger], [Zennaro].

24 to 34 dBi antennas are commercially available at both the unlicensed 2.4 GHz and 5 GHz bands, and even higher gain antennas can be found in the newer unlicensed bands at 17 GHz and 24 GHz.

Despite the fact that the free space loss is directly proportional to the square of the frequency, it is normally advisable to use higher frequencies for point-to-point links when there is a clear line of sight, because it is normally easier to get higher gain antennas at 5 GHz. Deploying high gain antennas at both ends will more than compensate for the additional free space loss. Furthermore, higher frequencies can make do with lower altitude antenna placement since the Fresnel ellipsoid (the volume around the optical line occuppied by radio waves, which should be free from obstacles), is inversely proportional to the square root of the frequency.

On the contrary, lower frequencies offer advantages when the line of sight is blocked because they can leverage diffraction to reach the intended receiver.

It is common to find dual radio Access Points, at two different frequency bands. One way of benefiting from this arrangement is to attach a directional antenna to the high frequency radio for connection to the backbone and an omnidirectional one to the lower frequency to provide local access.

In the case of mesh networking, where the antenna should connect to several other nodes, it is better to use omnidirectional antennas.

The same type of polarisation must be used at both ends of any radio link. For point-to-point links, some vendors use two radios operating at the same frequency but with orthogonal polarisations, thus doubling the achievable throughput, and also offering added protection to multipath and other transmission impairments.

#### 4.2.2. Link length

##### 4.2.2.1. Line-of-Sight

For short distance transmission, there is no strict requirement of line of sight between the transmitter and the receiver, and multipath can guarantee communication despite the existence of obstacles in the direct path.

For longer distances, the first requirement is the existence of an unobstructed line of sight between the transmitter and the receiver. For very long path the earth curvature is an obstacle that must be cleared, but the trajectory of the radio beam is not strictly a straight line due to the bending of the rays as a consequence of non-uniformities of the atmosphere. Most of the time this bending will mean that the radio horizon extends further than the optical horizon.

Another factor to be considered is that the Fresnel zone (the volume around the optical line) must be unencumbered from obstacles for the maximum signal to be captured at the receiver. The size of the Fresnel ellipsoid grows with the distance between the end points and with the wavelength of the signal, which in turn is inversely proportional to the frequency.

For optimum signal reception the end points must be high enough to clear any obstacle in the path and leave extra "elbow room" for the Fresnel zone. This can be achieved by using suitable masts at either end, or by taking advantage of existing structures or hills.

##### 4.2.2.2. Transmitted and Received Power

Once a clear radio-electric line of sight (including the Fresnel zone clearance) is obtained, one must ascertain that the received power is well above the sensitivity of the receiver, by what is known as the "link margin". The greater the link margin, the more reliable the link. For mission critical applications 20 dB margin is suggested, but for non critical ones 10 dB might suffice.

The sensitivity of the receiver decreases with the transmission speed, so more power is needed at greater transmission speeds.

The received power is determined by the transmitted power, the gain of the transmitting and receiving antennas and the propagation loss.

The propagation loss is the sum of the free space loss (proportional to the square of the the frequency and the square of the distance), plus additional factors like attenuation in the atmosphere by gases or meteorological effects (which are strongly frequency dependent), multipath and diffraction losses.

Multipath is more pronounced in trajectories over water. If they cannot be avoided special countermeasures should be taken.

In order to achieve a given link margin (also called "fade margin"), one can:

a) Increase the output power.The maximum transmitted power is specified by each country’s regulation, and for unlicensed frequencies is much lower than for licensed frequencies.

b) Increase the antenna gain. There is no limit in the gain of the receiving antenna, but high gain antennas are bulkier, present more wind resistance and require sturdy mounts to comply with tighter alignment requirements. The transmitter antenna gain is also regulated and can be different for point-to-point as for point-to-multipoint links. Many countries impose a limit in the combination of transmitted power and antenna gain, EIRP (Equivalent Isotropically Irradiated Power) which can be different for point-to- point or point-to-multipoint links.

c) Reduce the propagation loss, by using a more favorable frequency or a shorter path.

d) Use a more sensitive receiver. Receiver sensitivity can be improved by using better circuits, but it is ultimately limited by the thermal noise, which is proportional to temperature and bandwidth. One can increase the sensitivity by using a smaller receiving bandwidth, or by settling to lower throughput even in the same receiver bandwidth. This step is often done automatically in many protocols, in which the transmission speed can be reduced from 150 Mbit/s to 6 Mbit/s if the receiver power is not enough to sustain the maximum throughput.

##### 4.2.2.3. Medium Access Protocol

A completely different limiting factor is related to the medium access protocol. Wi-Fi was designed for short distance, and the transmitter expects the reception of an acknowledgment for each transmitted packet in a certain amount of time; if the waiting time is exceeded, the packet is retransmitted. This will significantly reduce the throughput at long distance, so for long distance applications it is better to use a different medium access technique, in which the receiver does not wait for an acknowledgement of the transited packet. This strategy of TDMA (Time Domain Multiple Access) has been adopted by many equipment vendors who offer proprietary protocols alongside the standard Wi-Fi in order to increase the throughput at longer distances. Low cost equipment using TDMA can offer high throughput at distances over 100 kilometers.

### 4.2.3. Layer 2

#### 4.2.3.1. 802.11 (Wi-Fi)

Wireless standards ensure interoperability and usability to those who design, deploy and manage wireless networks. The standards used in the vast majority of Community Networks come from the IEEE Standard Association’s IEEE 802 Working Group.

The standard we are most interested in is 802.11 a/b/g/n, [IEEE.802-11A.1999], [IEEE.802-11B.1999], [IEEE.802-11G.2003], [IEEE.802-11N.2009] as it defines the protocol for Wireless LAN. Different 802.11 amendments have been released, as shown in the table below, also including their frequencies and approximate ranges.

| 802.11 prot | Release date | Freq (GHz) | BWdth (MHz) | Data Rate per stream (Mbit/s) | Approx range (m) indoor | outdoor |
|---|---|---|---|---|---|---|
| a | Sep 1999 | 5 | 20 | 6,9,12, 18, 24, 36, 48, 54 | 35 | 120 |
| b | Sep 1999 | 2.4 | 20 | 1, 2, 5.5, 11 | 35 | 140 |
| g | Jun 2003 | 2.4 | 20 | 6,9,12, 18, 24, 36, 48, 54 | 38 | 140 |
| n | Oct 2009 | 2.4/5 | 20 | 7.2, 14.4, 21.7 28.9, 43.3, 57.8, 65, 72.2 | 70 | 250 |
| n | Oct 2009 | 2.4/5 | 40 | 15, 30, 45, 60, 90, 120, 135, 150 | 70 | 250 |
| ac | Nov 2011 | 5 | 20 | Up to 87.6 | | |
| ac | Nov 2011 | 5 | 40 | Up to 200 | | |
| ac | Nov 2011 | 5 | 80 | Up to 433.3 | | |
| ac | Nov 2011 | 5 | 160 | Up to 866.7 | | |

In 2012 IEEE issued the 802.11-2012 Standard that consolidates all the previous amendments. The document is freely downloadable from IEEE Standards [IEEE].

###### 4.2.3.1.1. Deployment planning for 802.11 wireless networks

Before packets can be forwarded and routed to the Internet, layers one (the physical) and two (the data link) need to be connected. Without link local connectivity, network nodes cannot talk to each other and route packets.

To provide physical connectivity, wireless network devices MUST operate in the same part of the radio spectrum. This means that 802.11a radios will talk to 802.11a radios at around 5 GHz, and 802.11b/g radios will talk to other 802.11b/g radios at around 2.4 GHz. But an 802.11a device cannot interoperate with an 802.11b/g device, since they use completely different parts of the electromagnetic spectrum. More specifically, wireless interfaces must agree on a common channel. If one 802.11b radio card is set to channel 2 while another is set to channel 11, then the radios cannot communicate with each other.

When two wireless interfaces are configured to use the same protocol on the same radio channel, then they are ready to negotiate data link layer connectivity. Each 802.11a/b/g device can operate in one of four possible modes:

1. Master mode (also called AP or infrastructure mode) is used to create a service that looks like a traditional Access Point. The

wireless interface creates a network with a specified name (called the SSID, Service Set IDentifier) and channel, and offers network services on it. While in master mode, wireless interfaces manage all communications related to the network (authenticating wireless clients, handling channel contention, repeating packets, etc.) Wireless interfaces in master mode can only communicate with interfaces that are associated with them in managed mode.

2. Managed mode is sometimes also referred to as client mode. Wireless interfaces in managed mode will join a network created by a master, and will automatically change their channel to match it. They then present any necessary credentials to the master, and if those credentials are accepted, they are associated with the master. Managed mode interfaces do not communicate with each other directly, and only communicate with an associated master.

3. Ad-hoc mode creates a multipoint-to-multipoint network where there is no single master node or AP. In ad-hoc mode, each wireless interface communicates directly with its neighbours. Nodes must be in range of each other to communicate, and must agree on a network name and channel. Ad-hoc mode is often also called Mesh Networking.

4. Monitor mode is used by some tools (such as Kismet) to passively listen to all radio traffic on a given channel. When in monitor mode, wireless interfaces transmit no data. This is useful for analysing problems on a wireless link or observing spectrum usage in the local area. Monitor mode is not used for normal communications.

When implementing a point-to-point or point-to-multipoint link, one radio will typically operate in master mode, while the other(s) operate in managed mode. In a multipoint-to-multipoint mesh, the radios all operate in ad-hoc mode so that they can communicate with each other directly. Managed mode clients cannot communicate with each other directly, so a high repeater site is required in master or ad-hoc mode. Ad-hoc is more flexible but has a number of performance issues as compared to using the master / managed modes.

#### 4.2.3.2. GSM

GSM has also been used in Alternative Networks as Layer 2 option, as explained in [Mexican].

#### 4.2.3.3. Dynamic Spectrum

Some Alternative Networks make use of TV White Spaces - a set of UHF and VHF television frequencies that can be utilized by secondary users in locations where it is unused by licensed primary users such as television broadcasters. Equipment that makes use of TV White

Spaces is required to detect the presence of existing unused TV channels by means of a spectrum database and/or spectrum sensing in order to ensure that no harmful interference is caused to primary users. In order to smartly allocate interference-free channels to the devices, cognitive radios are used which are able to modify their frequency, power and modulation techniques to meet the strict operating conditions required for secondary users.

The use of the term "White Spaces" is often used to describe "TV White Spaces" as the VHF and UHF television frequencies were the first to be exploited on a secondary use basis. There are two dominant standards for TV white space communication: (i) the 802.11af standard [IEEE.802-11AF.2013] - an adaptation of the 802.11 standard for TV white space bands and (ii) the IEEE 802.22 standard [IEEE.802-22.2011] for long-range rural communication.

##### 4.2.3.3.1. 802.11af

802.11af [IEEE.802-11AF.2013] is a modified version of the 802.11 standard operating in TV White Space bands using Cognitive Radios to avoid interference with primary users. The standard is often referred to as White-Fi or Super WiFi and was approved in February 2014. 802.11af contains much of the advances of all the 802.11 standards including recent advances in 802.11ac such as up to four bonded channels, four spatial streams and very high rate 256-QAM modulation but with improved in-building penetration and outdoor coverage. The maximum data rate achievable is 426.7 Mbps for countries with 6/7 MHz channels and 568.9 Mbps for countries with 8 MHz channels. Coverage is typically limited to 1km although longer range at lower throughput and using high gain antennas will be possible.

Devices are designated as enabling stations (access points) or dependent stations (clients). Enabling stations are authorized to control the operation of a dependent station and securely access a geolocation database. Once the enabling station has received a list of available white space channels it can announce a chosen channel to the dependent stations for them to communicate with the enabling station. 802.11af also makes use of a registered location server - a local database that organizes the geographic location and operating parameters of all enabling stations.

##### 4.2.3.3.2. 802.22

802.22 [IEEE.802-22.2011] is a standard developed specifically for long range rural communications in TV white space frequencies and first approved in July 2011. The standard is similar to the 802.16 (WiMax) [IEEE.802-16.2008] standard with an added cognitive radio ability. The maximum throughput of 802.22 is 22.6 Mbps for a single 8 MHz channel using 64-QAM modulation. The achievable range using the default MAC scheme is 30 km, however 100 km is possible with special scheduling techniques. The MAC of 802.22 is specifically customized for long distances - for example, slots in a frame destined for more distant CPEs are sent before slots destined for nearby CPEs.

Base stations are required to have a GPS and a connection to the Internet in order to query a geolocation spectrum database. Once the base station receives the allowed TV channels, it communicates a preferred operating white space TV channel with the Client Premises Equipment (CPE) devices. The standard also has a co-existence mechanism that uses beacons to make other 802.22 base stations aware of the presence of a base station that is not part of the same network.

# 5. Network and architecture issues

## 5.1. Layer 3

### 5.1.1. IP addressing

Most known Alternative Networks started in or around the year 2000. IPv6 was fully specified by then, but almost all Alternative Networks still use IPv4. A survey [Avonts] indicated that IPv6 rollout presents a challenge to Community Networks.

Most Community Networks use private IPv4 address ranges, as defined by RFC 1918 [RFC1918]. The motivation for this was the lower cost and the simplified IP allocation because of the large available address ranges.

### 5.1.2. Routing protocols

Alternative Networks are composed of possibly different layer 2 devices, resulting in a mesh of nodes. Connection between different nodes is not guaranteed and the link stability can vary strongly over time. To tackle this, some Alternative Networks use mesh network routing protocols while other networks use more traditional routing protocols. Some networks operate multiple routing protocols in parallel. For example, they use a mesh protocol inside different islands and use traditional routing protocols to connect islands.

#### 5.1.2.1. Traditional routing protocols

The BGP protocol, as defined by RFC 4271 [RFC4271] is used by a number of Community Networks, because of its well-studied behavior and scalability.

For similar reasons, smaller networks opt to run the OSPF protocol, as defined by RFC 2328 [RFC2328].

#### 5.1.2.2. Mesh routing protocols

A large number of Alternative Networks use the OLSR routing protocol as defined in RFC 3626 [RFC3626]. The pro-active link state routing protocol is a good match with Alternative Networks because it has good performance in mesh networks where nodes have multiple interfaces.

The Better Approach To Mobile Adhoc Networking (BATMAN) [Abolhasan] protocol was developed by members of the Freifunk community. The protocol handles all routing at layer 2, creating one bridged network.

Parallel to BGP, some networks also run the BMX6 protocol [Neumann]. This is an advanced version of the BATMAN protocol which is based on IPv6 and tries to exploit the social structure of Alternative Networks.

### 5.2. Upper layers

From crowdshared perspective, and considering just regular TCP connections during the critical sharing time, the Access Point offering the service is likely to be the bottleneck of the connection. This is the main concern of sharers, having several implications. There should be an adequate Active Queue Management (AQM) mechanism that implements a Less than Best Effort (LBE) policy for the user and protects the sharer. Achieving LBE behaviour requires the appropriate tuning of the well known mechanisms such as ECN, or RED, or others more recent AQM mechanisms such as CoDel and PIE that aid on keeping low latency RFC 6297 [RFC6297].

The user traffic should not interfere with the sharer’s traffic. However, other bottlenecks besides client’s access bottleneck may not be controlled by the previously mentioned protocols. Therefore, recently proposed transport protocols like LEDBAT [Ros], [Komnios] with the purpose of transporting scavenger traffic may be a solution. LEDBAT requires the cooperation of both the client and the server to achieve certain target delay, therefore controlling the impact of the user along all the path.

There are applications that manage aspects of the network from the sharer side and from the client side. From sharer's side, there are applications to centralise the management of the APs conforming the network that have been recently proposed by means of SDN [Sathiaseelan_a], [Suresh]. There are also other proposals such as Wi2Me [Lampropulos] that manage the connection to several Community Networks from the client's side. These applications have shown to improve the client performance compared to a single-Community Network client.

On the other hand, transport protocols inside a multiple hop wireless mesh network are likely to suffer performance degradation for multiple reasons, e.g., hidden terminal problem, unnecessary delays on the TCP ACK clocking that decrease the throughout or route changing [Hanbali]. There are some options for network configuration. The implementation of an easy-to-adopt solution for TCP over mesh networks may be implemented from two different perspectives. One way is to use a TCP-proxy to transparently deal with the different impairments (RFC 3135 [RFC3135]). Another way is to adopt end-to-end solutions for monitoring the connection delay so that the receiver adapts the TCP reception window (rwnd) [Castignani_c]. Similarly, the ACK Congestion Control (ACKCC) mechanism RFC 5690 [RFC5690] could deal with TCP-ACK clocking impairments due to inappropriate delay on ACK packets. ACKCC compensates in an end-to-end fashion the throughput degradation due to the effect of media contention as well as the unfairness experienced by multiple uplink TCP flows in a congested Wi-Fi access.

### 5.2.1. Services provided by Alternative Networks

This section provides an overview of the services between hosts inside the network. They can be divided into Intranet services, connecting hosts between them, and Internet services, connecting to nodes outside the network.

#### 5.2.1.1. Intranet services

Intranet services can include, but are not limited to:

- VoIP (e.g. with SIP)

- Remote desktop (e.g. using my home computer and my Internet connection when I am on holidays in a village).

- FTP file sharing (e.g. distribution of Linux software).

- P2P file sharing.

- Public video cameras.

- DNS.

- Online games servers.

- Jabber instant messaging.

- IRC chat.

- Weather stations.

- NTP.

- Network monitoring.

- Videoconferencing / streaming.

- Radio streaming.

5.2.1.2.  Access to the Internet

5.2.1.2.1.  Web browsing proxies

A number of federated proxies MAY provide web browsing service for the users.  Other services (file sharing, skype, etc.) are not usually allowed in many Alternative Networks due to bandwidth limitations.

5.2.1.2.2.  Use of VPNs

Some "micro-ISPs" may use the network as a backhaul for providing Internet access, setting up VPNs from the client to a machine with Internet access.

5.3.  Topology

Alternative Networks follow different topology patterns, as studied in [Vega].

Regularly rural areas in these networks are connected through long-distance links (the so-called community mesh approach) which in turn convey the Internet connection to relevant organisations or institutions.  In contrast, in urban areas, users tend to share and require mobile access.  Since these areas are also likely to be covered by commercial ISPs, the provision of wireless access by Virtual Operators like [Fon] may constitute a way to extend the user capacity (or gain connection) to the network. Other proposals like Virtual Public Networks [Sathiaseelan_a] can also extend the service.

As in the case of main Internet Service Providers in France, Community Networks for urban areas are conceived as a set of APs sharing a common SSID among the clients favouring the nomadic access. For users in France, ISPs promise to cause a little impact on their service agreement when the shared network service is activated on clients' APs. Nowadays, millions of APs are deployed around the country performing services of nomadism and 3G offloading, however as some studies demonstrate, at walking speed, there is a fair chance of performing file transfers [Castignani_a], [Castignani_b]. Scenarios studied in France and Luxembourg show that the density of APs in urban areas (mainly in downtown and residential areas) is quite big and from different ISPs. Moreover, performed studies reveal that aggregating available networks can be beneficial to the client by using an application that manages the best connection among the different networks. For improving the scanning process (or topology recognition), which consumes the 90% of the connection/reconnection process to the Community Network, the client may implement several techniques for selecting the best AP [Castignani_c].

## 6. Acknowledgements

This work has been partially funded by the CONFINE European Commission Project (FP7 - 288535).

The editor and the authors of this document wish to thank the following individuals who have participated in the drafting, review, and discussion of this memo:

Paul M. Aoki, Roger Baig, Jaume Barcelo, Steven G. Huter, Rohan Mahy, Rute Sofia, Dirk Trossen.

A special thanks to the GAIA Working Group chairs Matt Ford and Arjuna Sathiaseelan for their support and guidance.

## 7. Contributing Authors

Ioannis Komnios
Democritus University of Thrace
Department of Electrical and Computer Engineering
Kimmeria University Campus
Xanthi 67100
Greece

Phone: +306945406585
Email: ikomnios@ee.duth.gr

Steve Song
Village Telco Limited

Halifax
Canada

Phone:
Email: stevesong@nsrc.org

David Lloyd Johnson
Meraka, CSIR
15 Lower Hope St
Rosebank 7700
South Africa

Phone: +27 (0)21 658 2740
Email: djohnson@csir.co.za

## 8. IANA Considerations

This memo includes no request to IANA.

## 9. Security Considerations

No security issues have been identified for this document.

## 10. References

### 10.1. Normative References

[IEEE.802-11A.1999]
"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - High-speed Physical Layer in the 5 GHZ Band", IEEE Standard 802.11a, Sept 1999, <http://standards.ieee.org/getieee802/download/802.11a-1999.pdf>.

[IEEE.802-11AF.2013]
"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 5: Television White Spaces (TVWS) Operation", IEEE Standard 802.11af, Oct 2009, <http://standards.ieee.org/getieee802/download/802.11af-2013.pdf>.

[IEEE.802-11B.1999]
"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Higher-Speed Physical Layer Extension in the 2.4 GHz Band", IEEE Standard 802.11b, Sept 1999, <http://standards.ieee.org/getieee802/download/802.11b-1999.pdf>.

[IEEE.802-11G.2003]
"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band", IEEE Standard 802.11g, Jun 2003, <http://standards.ieee.org/getieee802/download/802.11g-2003.pdf>.

[IEEE.802-11N.2009]
"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 5: Enhancements for Higher Throughput", IEEE Standard 802.11n, Oct 2009, <http://standards.ieee.org/getieee802/download/802.11n-2009.pdf>.

[IEEE.802-16.2008]
"Information technology - Telecommunications and information exchange between systems - Broadband wireless metropolitan area networks (MANs) - IEEE Standard for Air Interface for Broadband Wireless Access Systems", IEEE Standard 802.16, Jun 2008, <http://standards.ieee.org/getieee802/download/802.16-2012.pdf>.

[IEEE.802-22.2011]
"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands", IEEE Standard 802.22, Jul 2011, <http://standards.ieee.org/getieee802/download/802.11af-2013.pdf>.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC3135] Border, J., Kojo, M., Griner, J., Montenegro, G., and Z. Shelby, "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations", RFC 3135, June 2001.

[RFC3626] Clausen, T. and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003.

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC5690] Floyd, S., Arcia, A., Ros, D., and J. Iyengar, "Adding Acknowledgement Congestion Control to TCP", RFC 5690, February 2010.

[RFC6297] Welzl, M. and D. Ros, "A Survey of Lower-than-Best-Effort Transport Protocols", RFC 6297, June 2011.

## 10.2. Informative References

[Abolhasan] Abolhasan, M., Hagelstein, B., and J. Wang, "Real-world performance of current proactive multi-hop mesh protocols", In Communications, 2009. APCC 2009. 15th Asia-Pacific Conference on (pp. 44-47). IEEE. , 2009.

[Airjaldi] Rural Broadband (RBB) Pvt. Ltd., Airjaldi., "Airjaldi service", Airjaldi web page, www.airjaldi.net , 2015.

[Avonts] Avonts, J., Braem, B., and C. Blondia, "A Questionnaire based Examination of Community Networks", Proceedings Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 8th International Conference on (pp. 8-15) , 2013.

[Bernardi] Bernardi, B., Buneman, P., and M. Marina, "Tegola tiered mesh network testbed in rural Scotland", Proceedings of the 2008 ACM workshop on Wireless networks and systems for developing regions (WiNS-DR ’08). ACM, New York, NY, USA, 9-16 , 2008.

[Braem] Braem, B., Baig Vinas, R., Kaplan, A., Neumann, A., Vilata i Balaguer, I., Tatum, B., Matson, M., Blondia, C., Barz, C., Rogge, H., Freitag, F., Navarro, L., Bonicioli, J., Papathanasiou, S., and P. Escrich, "A case for research with and on community networks", ACM SIGCOMM Computer Communication Review vol. 43, no. 3, pp. 68-73, 2013.

[Castignani_a] Castignani, G., Loiseau, L., and N. Montavont, "An Evaluation of IEEE 802.11 Community Networks Deployments", Information Networking (ICOIN), 2011 International Conference on , vol., no., pp.498,503, 26-28 , 2011.

[Castignani_b]
Castignani, G., Monetti, J., Montavont, N., Arcia-Moret, A., Frank, R., and T. Engel, "A Study of Urban IEEE 802.11 Hotspot Networks: Towards a Community Access Network", Wireless Days (WD), 2013 IFIP , pp.1,8, 13-15 , 2013.

[Castignani_c]
Castignani, G., Arcia-Moret, A., and N. Montavont, "A study of the discovery process in 802.11 networks", SIGMOBILE Mob. Comput. Commun. Rev., vol. 15, no. 1, p. 25 , 2011.

[DAE] European Commission, EC., "A Digital Agenda for Europe", Communication from the Commission of 19 May 2010 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Agenda for Europe , 2010.

[Everylayer]
former Volo Broadband, Everylayer., "Everylayer", Everylayer web page, http://www.everylayer.com/ , 2015.

[FNF] The Free Network Foundation, FNF., "The Free Network Foundation", The Free Network Foundation web page, https://thefnf.org/ , 2014.

[Flickenger]
Flickenger, R., Okay, S., Pietrosemoli, E., Zennaro, M., and C. Fonda, "Very Long Distance Wi-Fi Networks", NSDR 2008, The Second ACM SIGCOMM Workshop on Networked Systems for Developing Regions. USA, 2008 , 2008.

[Fon] Fon Wireless Limited, Fon., "What is Fon", Fon web page, https://corp.fon.com/en , 2014.

[Hanbali] Hanbali, A., Altman, E., and P. Nain, "A Survey of TCP over Ad Hoc Networks", IEEE Commun. Surv. Tutorials, vol. 7, pp. 22-36 , 2005.

[Heer] Heer, T., Hummen, R., Viol, N., Wirtz, H., Gotz, S., and K. Wehrle, "Collaborative municipal Wi-Fi networks-challenges and opportunities", Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on (pp. 588-593). IEEE. , 2010.

[IEEE] Institute of Electrical and Electronics Engineers, IEEE, "IEEE Standards association", 2012.

[Komnios] Komnios, I., Sathiaseelan, A., and J. Crowcroft, "LEDBAT performance in subpacket regimes", IEEE/IFIP WONS, Austria, April 2014 , 2014.

[Lampropulos] Lampropulos, A., Castignani, G., Blanc, A., and N. Montavont, "Wi2Me: A Mobile Sensing Platform for Wireless Heterogeneous Networks", 32nd International Conference on Distributed Computing Systems Workshops (ICDCS Workshops), 2012, pp. 108-113 , 2012.

[Lowenstedt] Huggler, J., "Lowenstedt Villagers Built Own Fiber Optic Network", The Telegraph, 03 Jun 2014, available at http://www.telegraph.co.uk/news/worldnews/europe/germany/10871150/German-villagers-set-up-their-own-broadband-network.html , 2014.

[Mexican] Varma, S., "Lowenstedt Villagers Built Own Fiber Optic Network", The Times of India, 27 Aug 2013, available at http://timesofindia.indiatimes.com/world/rest-of-world/Ignored-by-big-companies-Mexican-village-creates-its-own-mobile-service/articleshow/22094736.cms , 2013.

[Neumann] Neumann, A., Lopez, E., and L. Navarro, "An evaluation of bmx6 for community wireless networks", In Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on (pp. 651-658). IEEE. , 2012.

[PAWS] Sathiaseelan, A., Crowcroft, J., Goulden, M., Greiffenhagen, C., Mortier, R., Fairhurst, G., and D. McAuley, "Public Access WiFi Service (PAWS)", Digital Economy All Hands Meeting, Aberdeen , Oct 2012.

[Pietrosemoli] Pietrosemoli, E., Zennaro, M., and C. Fonda, "Low cost carrier independent telecommunications infrastructure", In proc. 4th Global Information Infrastructure and Networking Symposium, Choroni, Venezuela , 2012.

[Rendon] Rendon, A., Ludena, P., and A. Martinez Fernandez, "Tecnologias de la Informacion y las Comunicaciones para zonas rurales Aplicacion a la atencion de salud en paises en desarrollo", CYTED. Programa Iberoamericano de Ciencia y Tecnologia para el Desarrollo , 2011.

[Ros] Ros, D. and M. Welzl, "Assessing LEDBAT's Delay Impact", Communications Letters, IEEE , vol.17, no.5, pp.1044,1047, May 2013 , 2013.

[Samanta] Samanta, V., Knowles, C., Wagmister, J., and D. Estrin, "Metropolitan Wi-Fi Research Network at the Los Angeles State Historic Park", The Journal of Community Informatics, North America, 4 , May 2008.

[Sathiaseelan_a] Sathiaseelan, A., Rotsos, C., Sriram, C., Trossen, D., Papadimitriou, P., and J. Crowcroft, "Virtual Public Networks", In Software Defined Networks (EWSDN), 2013 Second European Workshop on (pp. 1-6). IEEE. , 2013.

[Sathiaseelan_b] Sathiaseelan, A. and J. Crowcroft, "LCD-Net: Lowest Cost Denominator Networking", ACM SIGCOMM Computer Communication Review , Apr 2013.

[Sathiaseelan_c] Sathiaseelan, A., Mortier, R., Goulden, M., Greiffenhagen, C., Radenkovic, M., Crowcroft, J., and D. McAuley, "A Feasibility Study of an In-the-Wild Experimental Public Access WiFi Network", ACM DEV 5, Proceedings of the Fifth ACM Symposium on Computing for Development, San Jose , Dec 2014 pp 33-42, 2014.

[Suresh] Suresh, L., Schulz-Zander, J., Merz, R., Feldmann, A., and T. Vazao, "Towards Programmable Enterprise WLANs with ODIN", In Proceedings of the first workshop on Hot topics in software defined networks (HotSDN '12). ACM, New York, NY, USA, 115-120 , 2012.

[Vega] Vega, D., Cerda-Alabern, L., Navarro, L., and R. Meseguer, "Topology patterns of a community network: Guifi. net.", Proceedings Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on (pp. 612-619) , 2012.

[WNDW] Wireless Networking in the Developing World/Core Contributors, "Wireless Networking in the Developing World, 3rd Edition", The WNDW Project, available at wndw.net , 2013.

[WSIS] International Telecommunications Union, ITU, "Declaration of Principles. Building the Information Society: A global challenge in the new millenium", World Summit on the Information Society, 2003, at http://www.itu.int/wsis, accessed 12 January 2004. , Dec 2013.

[Zennaro] Zennaro, M., Fonda, C., Pietrosemoli, E., Muyepa, A., Okay, S., Flickenger, R., and S. Radicella, "On a long wireless link for rural telemedicine in Malawi", 6th International Conference on Open Access, Lilongwe, Malawi , Nov 2008.

## Authors' Addresses

Jose Saldana (editor)
University of Zaragoza
Dpt. IEC Ada Byron Building
Zaragoza 50018
Spain

Phone: +34 976 762 698
Email: jsaldana@unizar.es

Andres Arcia-Moret
Universidad de Los Andes
Facultad de Ingenieria. Sector La Hechicera
Merida 5101
Venezuela

Phone: +58 274 2402811
Email: andres.arcia@ula.ve

Bart Braem
iMinds
Gaston Crommenlaan 8 (bus 102)
Gent 9050
Belgium

Phone: +32 3 265 38 64
Email: bart.braem@iminds.be

Leandro Navarro
U. Politecnica Catalunya
Jordi Girona, 1-3, D6
Barcelona  08034
Spain

Phone: +34 934016807
Email: leandro@ac.upc.edu

Ermanno Pietrosemoli
ICTP
Via Beirut 7
Trieste  34151
Italy

Phone: +39 040 2240 471
Email: ermanno@ictp.it

Carlos Rey-Moreno
University of the Western Cape
Robert Sobukwe road
Bellville  7535
South Africa

Phone: 0027219592562
Email: crey-moreno@uwc.ac.za

Arjuna Sathiaseelan
University of Cambridge
15 JJ Thomson Avenue
Cambridge  CB30FD
United Kingdom

Phone: +44 (0)1223 763781
Email: arjuna.sathiaseelan@cl.cam.ac.uk

Marco Zennaro
Abdus Salam ICTP
Strada Costiera 11
Trieste  34100
Italy

Phone: +39 040 2240 406
Email: mzennaro@ictp.it