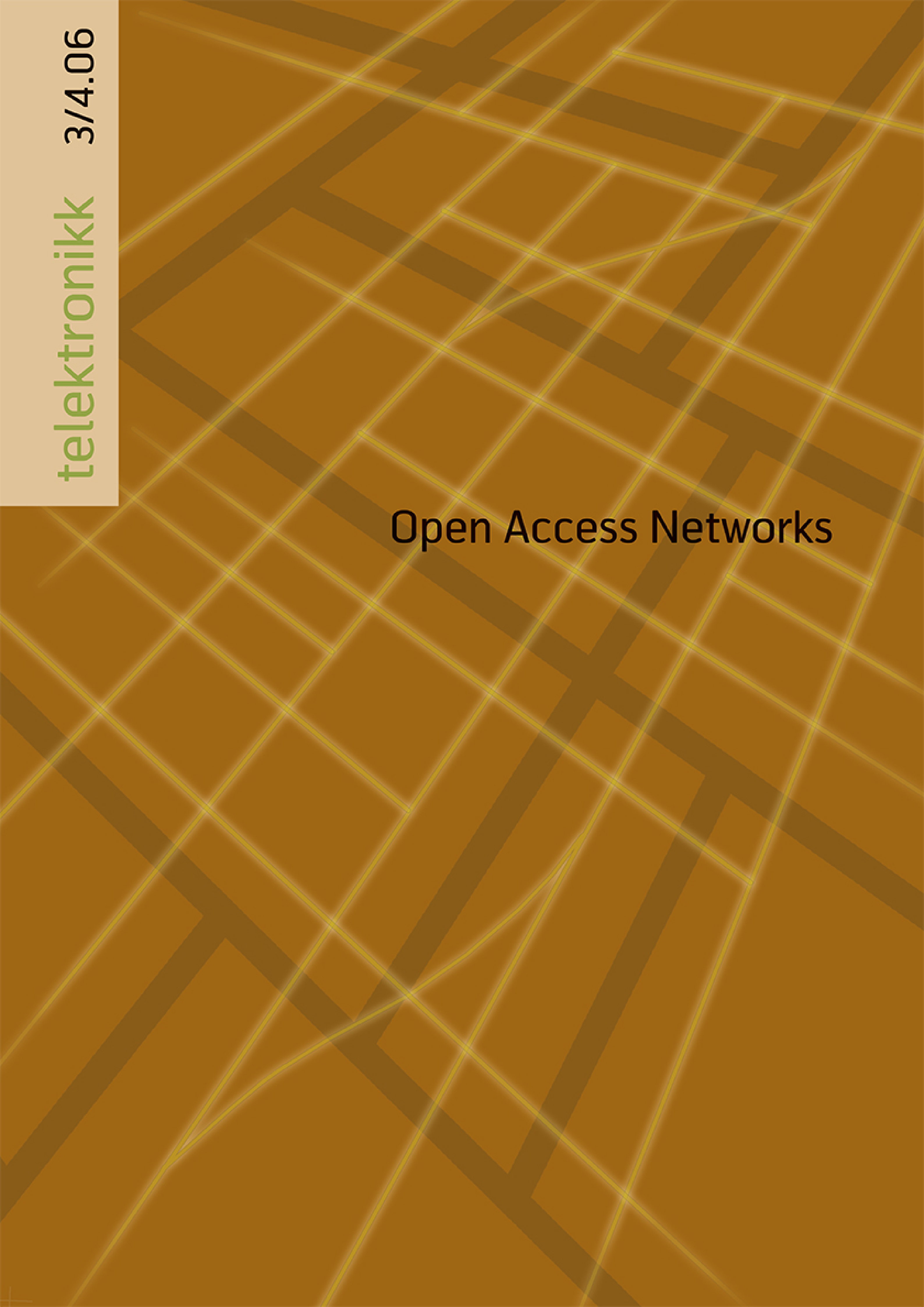
telektronikk 3/4.06

Open Access Networks



Contents

Telektronikk
Volume 102 No. 3/4 – 2006
ISSN 0085-7130

Editor:
Per Hjalmar Lehne
(+47) 916 94 909
per-hjalmar.lehne@telenor.com

Editorial assistant:
Gunhild Luke
(+47) 415 14 125
gunhild.luke@telenor.com

Editorial office:
Telenor R&I
NO-1331 Fornebu
Norway
(+47) 810 77 000
telektronikk@telenor.com
www.telektronikk.com

Editorial board:
Berit Svendsen, VP Telenor Nordic
Ole P. Håkonsen, Professor NTNU
Oddvar Hesjedal, VP Project Director
Bjørn Løken, Director Telenor Nordic

Graphic design:
Design Consult AS (Odd Andersen), Oslo

Layout and illustrations:
Gunhild Luke and Åse Aardal,
Telenor R&I

Prepress and printing:
Rolf Ottesen Grafisk Produksjon, Oslo

Circulation:
3,700

Networks on networks

Connecting entities through networks – in technological, societal and personal terms – enables telecommunication. Networks occur on different levels, form parts of larger networks, and exist in numerous varieties. The artist Odd Andersen visualises the networks on networks by drawing interconnected lines with different widths. Curved connections disturb the order and show that networks are not regular but are adapted to the communication needs.

Per H. Lehne, Editor in Chief

Open Access Networks

Guest Editorial

EINAR EDVARDSEN

Einar Edvardsen is Senior Adviser in Telenor R&I

The fixed broadband access network – the most powerful, fine-grained and ***inaccessible*** network there is.

This is of course a "to-the-point" formulation, but there are components of truth in it – how?

The only spot on the earth from which a person can access the network is over the line identified by his subscription with the service provider. As soon as he moves outside the reach of his home/office network, he will be unable to obtain connection. To be able to establish a broadband session away from home, he must sign up other agreements with service providers (scratch card, hotel, mobile, ...). In the role of a fixed line subscriber it is impossible to connect anywhere else than at home, because the subscription is limited to communication over one particular line terminated at his premises.

The fixed broadband network is powerful in respect of total capacity, access capacity and coverage. Every household and business will soon be connected to a common high capacity core network. The infrastructure for these access networks builds predominantly on the old telephone cables and the coaxial cable networks used for TV distribution. Other physical infrastructures do also exist, but play minor roles. These cable infrastructures are continuously being upgraded to offer capacities up to 20 – 25 Mbits/sec per line dependent on the applied technology. When demand for capacity exceeds the threshold of today's network, optical cables will be installed and offer more or less unlimited bandwidth.

The mobile networks on the other hand are optimised to provide telecommunication services to travelling people. They aim at offering services to people wherever they are on the earth, but the drawback is that these networks do not provide the bandwidth the users are used to at home/office over the fixed network. Though mobile networks go through a capacity upgrade similar to the fixed, these networks will never catch up with the latter networks' performance, unless more radio frequencies are released for such purposes. Compared to the fixed networks, the capacity of the mobile networks is only a fraction, but they have a great advantage; they are accessible where people are, not only at certain access points.

The appearance of cheap wireless technology used as local area networks may become the catalytic force sewing together fixed and mobile networks (FMC – Fixed and Mobile Convergence). WLAN has become a popular technology and is now widely deployed in people's homes and enterprise premises to interconnect computer equipment. It gives people the freedom to locate PCs, servers and printers where they want them to be, not only where the cables terminate. Since radio waves to some degree penetrate walls and windows and do not see the borders between the private and public domains, they will also cover public areas and enable people passing by to connect provided that the necessary functionality is installed in the network. WLAN may accordingly become a medium and mean for providing public access to the fixed broadband network in wide areas. Broadband will no longer be limited to applications at home/office, but will also be available to people when they are walking in the street, sitting at a café, visiting friends, visiting business relations, etc.

However, inviting anybody to connect to private wireless networks and allowing them access to the Internet over the present subscribers' access lines, is controversial and feared by people. The basic access to Internet can very easily be realised. Leaving the WLAN unprotected – without using encryption, hidden SSID or MAC address filtering – anybody may use it and obtain access. Nothing needs to be done to realise this, except disabling all security mechanisms and offer them to public disposal. Many reasons make it impossible to follow such an approach in viable commercial business models.

For the users, subscribers as well as visitors, privacy reasons may be one of them. Nor will subscribers be willing to 'give away' bandwidth they are paying for, or at least: They want to be assured that they have the bandwidth they pay for when they need it. From a commercial point of view it is important to identify users, i.e. the operators need to know who the users are in order to bill for communication. Also the society has its interests in this image as information about usage often is requested in legal disputes. The 9-11 syndrome has even made these aspects more important. Secure identification of users and traffic records are demanded by the telecom regulator authorities to comply with community interests.

ISSN 0085-7130 © Telenor ASA 2006

In a few years most households will have broadband and the majority will also use WLAN as home networks for interconnecting electronic devices. As the number of WLANs increases they will form continuous coverage indoors as well as outdoors, thus giving the subscribers of the fixed network the opportunity to connect everywhere. An intuitive follow-up question might be whether such networks would perform well enough to oust GSM/UMTS by providing better and cheaper services than offered by the mobile network. Would it be possible to develop the fixed network to support mobile services as they are provided by the mobile network? WLAN in stand-alone situations offers basically much more bandwidth than the mobile networks. Tens of Megabits per user are achievable under optimal conditions, but how do they perform in crowded situations? When WLANs overlap and interfere with each other? Or when the number of users increases? The most popular WLAN products of today are based on the IEEE802.11b/g standard, which offers only three non-overlapping channels. With only three independent channels available severe interference cannot be avoided, but how severe will it be?

These and many other questions connected to extensive deployment of WLANs are sought answered in this issue of *Telektronikk*. Most of the articles in this issue of *Telektronikk* are based on the 6th Framework Programme Project OBAN – Open Broadband Access Networks (see: http://www.ist-oban.org). The articles are grouped into four different thematic sections.

First, an overview article explains and discusses different aspects of some approaches to "Open Access Networks" (OAN) and attemps to draw some overall technical and commercial conclusions. A second paper presents the regulatory framework, which viable commercial OANs have to comply with.

Section two addresses some over-all issues like a brief discussion of some of the present approaches to open access networks. Open access to broadband over WLAN is being offered by existing as well as new operators on the market (FON, Boingo, LinSpot, ...). From the mobile side the UMA standard defines how WLAN can be integrated in the mobile network. The section also contains an architectural overview of the OBAN approach to open access networks.

In section three the commercial aspects of open access networks are covered. Implementation of open access is in fact a radical change of today's fixed networks towards a network supporting nomadic and mobile services. New business models will be required to enable this transition. The increased performance of the fixed network will give a pulse to service providers to develop new services and applications that rely on new multi-function terminals that are able to connect to different networks.

Section four addresses the main properties that must be present in an open access network. These properties involve a range of security aspects in order to meet requirements from users as well as the commercial players and the community around. They also cover requirements to service quality – how to maintain service quality while users are roaming from access point to access point.

The last section, number five, contains three articles related specifically to the wireless aspects of an OAN. An overview of relevant radio technologies used for short-haul communications is given. Further, an estimation of expected capacity and coverage of typical open access networks is presented. Open access networks based upon WLAN will be exposed to severe interference. Two papers present results from analytic studies and simulation that attempt to give an answer to the fundamental question of how much capacity is available for casual visitors given that the fixed subscribers consume bandwidth as normal (given by some scenarios).

Einar Edvardsen

Einar Edvardsen obtained his MSc in Data and Telecommunication from the Norwegian University of Science and Technology (NTNU) in 1978. After finishing his education he joined the R&D division of Telenor. In 1984 he established his own company, Cable Engineering AS, active in the field of optical fibre installation and product development. From 1994 and up to the present time, he has been employed at Telenor R&D (now Telenor R&I), dealing with broadband communication – the broadband access network. During this period (interrupted by a short period as CTO in the company inAxxess AS), he has participated in national as well as international research projects and has been project manager in two of them – AC309 ITUNET and IST 001889 OBAN.

email: einar-paul.edvardsen@telenor.com

Introduction to Open Access Networks

EINAR EDVARDSEN

Einar Edvardsen is Senior Adviser in Telenor R&I

The article opens by defining the Open Access Network (OAN) and giving a brief overview of different aspects related to making the fixed network publicly accessible over wireless LANs. Three approaches are discussed: 1) Use of unsecured WLANs, 2) Solutions on the market, 3) The OBAN solution. The popularity of WLAN may become a catalyst for the introduction of OAN. Together with enablers like people's take-up of broadband and an assumed market demand for services that can be offered in OANs, it is concluded that the conditions required by operators to realise open access networks and develop adequate services also are present. Finally, the expected performance of such networks is analysed.

1 Introduction

Open Access Networks (OAN) is nowadays a popular buzz word or notation often used in telecommunication as well as in completely different relations. A superficial search on the WEB reveals a span of interpretations of the three words. It may mean a network of specialists (doctors, engineers, education, training etc), who jointly offer their services to the public, i.e offer open access to the network of specialists. Some private companies include Open Access in their company names. One example is the American company Open-Access who provides global data storage services.

From telecommunication we find a range of broadband networks established by communities, private initiatives, organisations, etc, offering Internet access to their members. A number of community operated WiFi networks use the term OAN in their marketing. The meaning of the term in these connections may for instance be that the network has been established by non-profit organizations (local authorities, interest-groups, ...) which offer services free of charge or at very low charges.

Though OAN often is interpreted as a network that can be used free of charge, this is not a stringent rule. First of all – the access to such free of charge networks is often restricted to a group of individuals or companies that either pay a membership fee or provide something else in return. In fact, nothing is free of charge. You will normally have to pay indirectly, for instance as an integrated expense of the hotel bill.

The Wikipedia database defines a telecommunication related OAN like this:

> Open Access Network (OAN) refers to horizontally layered network architecture and business model that separate physical access to the network from service provisioning. The same OAN will be used by a number of different providers that share investment and maintenance costs. The term was coined by Roberto Battiti in 2003 in his article "Global growth of open access networks: from warchalking and connection sharing to sustainable business"[1].

Though the term OAN says nothing about technology it is particularly often mentioned in connection with Wireless Local Area Networks (WLAN). WLAN is a widely deployed radio based technology used to realize wireless local networks in enterprises as well as in the public room and in private homes. Key drivers for its popularity are the low cost, simplicity of use and availability of WLAN in almost all portable terminals.

WLANs, which now are extensively deployed in portable terminals and home/business networks, have also shown up in the public room like railway stations, airports, cafés and have become a necessity at any hotel and overnight stop. The technology has become so important among people that hotels which cannot offer WLAN as a service, lose customers. A hotel today without WLAN is like a hotel ten years ago who did not have telephones in the rooms. The situation is rather the opposite now. Since everybody has their own mobile phones, they do not request wire-line phones in the rooms, but WLAN. This change of behaviour among people has happened very fast. Five years ago it was only a trend, which one could argue and question.

WLAN based wide area networks have also popped up. Network operators are blanketing city areas with WLANs allowing people to connect to Internet also outside buildings – in streets, parks or anywhere they may stay or pass through. This is happening very fast and often in parallel to similar network expansion performed by the traditional telecom networks.

[1] *See: http://en.wikipedia.org/wiki/Open_Access_Network*

ISSN 0085-7130 © Telenor ASA 2006

Though still suffering from many shortcomings compared to traditional telecommunication networks, it has become evident that WLAN is a viable access technology for years to come.

To a certain degree all these applications of WLANs can be considered as OAN according to the definition above and according to common sense thinking. People get access to the 'huge Internet' and to all the services and applications that are offered over it. There is a clear separation between the access network and all the services offered by the Internet.

However, the definition above does not match Open Access Network in the way we want to use it. As we shall see the new interpretation of the term should refer to opening up the fixed access network for public use. In today's fixed access networks each telephone subscriber has a dedicated copper line from the telephone exchange to the residence or office. These copper lines are the most commonly used infrastructure for broadband provisioning in many countries. Each line is equipped with a xDSL modem (ADSL, ADSL2, VDSL, ...), which is able to transfer some Megabits capacity to the users. Alternative infrastructures used are the cable networks (CATV), optical fibres and the power distribution lines. In some countries or areas the latter ones may have dominant market shares.

Since normally only a few persons share the capacity of the access line the utilization of it is often very poor. Most of the time it is not used at all and even during the periods of the day that can be considered as 'busy time', the utilization is low. Good statistics for the utilization has not been found, but simple calculations based upon estimates can easily be done. Unless people use video streaming services extensively it can be shown that the utilization of the access capacity is less than 1 %, which means that 99 % of the capacity is wasted[2)]. Observed from a network provider's point of view this may look like a very unsatisfactory situation, and good proposals for how to exploit the wasted capacity should therefore be in their interest as well as in the interest of other players, like service providers and end-users. The question is how to make more efficient use of the access capacity. Efficient utilization of network resources should theoretically lead to lower cost and indirectly give birth to new services and more traffic in the network.

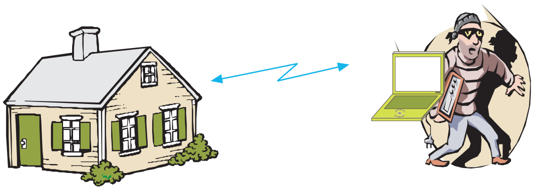


Figure 1 A casual by-passer steals access to broadband

One way of improving utilization of the access network is to invite more users to access the network, but how?

The popular WLAN technology has actually become the enabling technology for opening up the fixed access network more users. Developed for a different market, these radio solutions may now serve a new application, namely as an access technology for the fixed network. WLAN was developed to connect computers in local networks, like in offices and residential environments, but as radio waves also propagate into the public areas other users may also connect to the network if they have the necessary access permissions. Inviting third parties to access today's privately disposed access lines and home/office networks is in fact a more radical transition than immediately conceived. It transforms the access lines to become public lines in the sense that they are not anymore restricted to individual subscribers, but open to the general public. It also expands the control area of the network operators, since they will have to care more about 'residential equipment' than today. The most important changes, however, are the ones connected to security and privacy issues, since the approach invites third parties to connect over devices in the network that up to now have been considered as privately administered.

Figure 1 illustrates a casual by-passer who enters within the coverage of an access point and who illegally is able to connect to the network, i.e. he is stealing network access and communication time.

Accordingly the new definition of an Open Access Network is as follows:

> *Open Access Networks (OAN) refers to a public network architecture and business model that utilize the existing fixed access network as an infrastructure for providing wireless broadband services to both the existing subscribers and any other party acquiring access. Wireless LAN is often used as access medium between terminals and access point, but other wireless or wired technologies can also be applied.*

[2)] *Example: A user who on average downloads 10 Gb/month and has subscribed to a 5 Mb/s Internet access. Average consumption is 0.8 % of total available capaciy.*

The definition requires that the OAN must be a commercial implementation of a public network. If people leave their accesses open to anybody, this cannot be considered as an OAN, though the services it offers may be similar.

The definition does also exclude cases where a few households share a common access line. If the intention is only to share the access line between limited numbers of users, it is not considered an OAN. For instance, people living in multi-dwelling apartments or in houses located relatively close to each other may share a common WLAN access point. The parties may share the expenses according to a formal or informal agreement between them. As long as ISPs do not implement volume charging for use there is no real incentive for subscribers to charge for others' use, which often involves neighbours surfing on the Internet free of charge on other people's subscriptions. However, security and access control mechanisms in the WLAN can be activated to prevent persons not concerned connecting and this is what has happened recently. More and more people protect their WLANs with appropriate encryption and access control mechanisms. There are many reasons for that – see below.

2 Open Access Networks (OAN)

The following discussion uses this latter definition of OAN, which means that the word 'Open' refers to making the fixed access line accessible (open) for others than the original subscriber. An OAN, according to the definition is recognized by the following:

1 Utilization of individual access lines as a common access for both residents and casual visitors and by-passers;

2 Offering access to broadband to the public; i.e it cannot be restricted to employees of a company or such like;

3 It must be commercially viable.

Since WLANs installed in homes and offices often cover public areas as well as the targeted areas, people staying in the vicinity of an access point may connect to the network unless precautions are taken to prevent it. This makes the introduction of OAN-like services simple because the technology is there; it is widespread and by its pure existence one of the basic requirements above (1) of an OAN can easily be met. However, the two other requirements remain unsolved – how to launch a viable commercial service offering for the general public. In fact, using WLAN, which is running in unlicensed frequency bands and also without supporting the primary requirements known from legacy telecommunications, one must be prepared to make compromises as regards the requirements that are common in telecommunications.

Offering a public service has many implications. One has to investigate what are the requirements from regulatory authorities, such as lawful interception, retention of traffic data, communication protection, emergency calls, etc. One also has to meet users' requirements on security and privacy. Commercial viability also means that the business model must encompass all parties that are contributing to the complete service offering, and that all of them are ensured their share of the value creation. Thus there is a long list of conditions that must be met in order to state that it is an Open Access Network in accordance with the definition.

The OAN definition does not define what kind of services shall be offered over the network. The choice of services to be offered over an OAN impacts largely the complexity of the network and the choice of technology used to realise the network. Thus it follows that the exact answer to how an OAN performs and how it should be implemented and run does not exist.

Open access networks may be looked upon as a compelling alternative to cellular networks for obtaining Internet access on the move. Mobile network operators have so far managed to take control of this sector through aggressive pre-emptive strategies. However, the rapid emergence of private WLAN networks and broadband Internet connections among households has raised the crucial issue of the sharing of Internet access through these networks. This has generated interesting opportunities to a variety of players to position them in the mobile industry as Open Access Service Providers (OASP).

In the following a few possible OAN implementations will be discussed with regard to their properties.

2.1 OANs based on unsecured WLANs

The easiest way to establish an OAN is to leave the WLAN unsecured and open for anybody to access. This means that neither data encryption nor hidden SSID nor MAC address filtering are used to prevent unauthorised people accessing the network in any way. In reality this has been the situation up to the present time where most of the APs have been left open without any protection. People have not cared about communication security nor that other people could use their networks free of charge and by-passers could connect over any such AP at no cost. They may connect in the street or in the park as long as they are within the reach of an open WLAN and nobody cares about paying for the service. It is an approach very similar to the original one of Internet – that Internet should be an open infrastructure allowing everybody to utilise it free of charge or at low cost.

The two visions together, the one from Internet and the one of OAN, complement each other in a pretty way. While OAN provides the *free access to Internet*, the latter provides the *backbone infrastructure for free communication*, but is it possible to establish and run such a full scale OAN without involving commercial partners who will charge for their services? Hardly – there must be partners involved that take the responsibility to run the network, making the necessary investments and implement all the functionality that is needed by state authorities as well as all other commercial partners involved in the concept. Accordingly, an OAN based upon these principles does not comply with the definition of an OAN, which requires it to be commercially viable. An examination is nevertheless interesting, because the solution reveals some of the problems that viable solutions must deal with.

In spite of the OAN definition and logical commercial thinking, open access to Internet over private access lines does already exist and will possibly also continue to exist. Some people will leave their networks open for public access whatever the threats are, thus allowing other to connect, but the trend is that many of them will be closed over time. This trend is caused by concerns among people as well as among network providers and telecommunication regulator authorities.

First of all – while people in the beginning left their wireless networks open to the public, they have now become aware of the risks connected to using unprotected WLANs. More and more people activate the available security features of their networks to protect against intrusion:

1 They fear wiretapping and that unauthorised people can get access to their communication and stored documents.

2 People do not accept the risk to be charged with illegal use of the network, for instance charged with breach of property rights in connection with down-loading of music and films, or for downloading paedophile material done by some casual by-passers.

3 People do also care about the product they are paying for; i.e. if they have paid for 2 Mbit access capacity they expect that this capacity is available when they need it. They may not allow unknown by-passers to occupy the line when they need it for themselves. Some kind of economic incentive must be in place to allow that.

Also network operators will resist such unregulated OANs mainly for economic reasons. One cannot expect operators to support unregulated use of open access without any economic compensation. The relation between the operator and each individual legal subscriber is regulated by a subscription agreement giving the subscriber an exclusive right to use the services provided by the operator. Nobody else is in principle allowed to connect over that particular access line. Therefore – allowing third parties to connect may be considered as a contractual breach. Of course, there are a lot of grey areas in which such third party access is acceptable – for instance to allow a guest of the family to connect over the host's network and other similar cases of sporadic and small volume use. A technical argument in favour of the operator is also that the network is planned for only 'one' user per line. If more users connect over the same line the traffic may exceed the upper capacity limit the network is designed for, which may reduce the communication quality for all.

The major concerns for the authorities are related to matters like traceability of users, which often is needed in legal trials. People who connect over other people's networks cannot be identified. It is the legal subscriber who must take the responsibility of any illegal activity that takes place over his line – refer point 2 above. The new Data Retention Directive [1] approved by the European Parliament even enjoins the requirements on data communication by demanding records of traffic and identification of users that connect. When this directive is implemented it will be illegal to leave WLANs open to third parties. All users of communication networks will have to identify themselves before accessing the network, and records of relevant information will have to be stored in the network for a certain period of time.

2.2 Open Access Service Providers on the market today

The concerns listed above pave the way for operators who are assumed to have the ability to comply with requirements from regulatory authorities and other commercial players and users. A number of start-ups have adopted this idea and established companies based upon it. Others have consciously organized themselves to form free wireless communities aiming at providing free Internet access to members or even to the public. Three of the most interesting initiatives, FON, Boingo and The Cloud, illustrate what is happening on the market. It is, however, worth mentioning that only one of the three, the FON community, positions themselves as an OAN provider (sharing subscribers' access lines). The two others, Boingo and The Cloud, should more correctly be named roaming providers and/or wireless ISP since their core business is not aimed at providing public Internet access over subscribers' access lines, but rather enabling users of one WLAN operator to communicate over another operator's network.

Further information about these three operators and others can be found in the article by Thor Gunnar Eskedal and Tor Hjalmar Johannessen [2] and the article by Muslim Elkotob et al. [3] in this issue.

All three companies mentioned above market products that intend to open up the fixed access network to the public, but there are concerns about these approaches. One concern is whether they can meet the regulatory requirements. The second concern relates to commercial aspects on whether they determine the rights and obligations of all involved parties – network operator, ISP, site owner, etc.

ISPs do not normally allow sharing Internet access with neighbours or among community members. Such sharing is only lawful with the consent of the ISP. This consent must be explicitly stipulated in the contract between the ISP and the user. Allowing other people to access the line can be considered as illegal resale according to the contract. Whether money is involved or not, does not matter – it does not change the fact that it is forbidden by the contract. In such cases, the ISP may intervene by terminating the contract. It is therefore questionable whether some of the present OAN initiatives on the market can be considered viable. Legal disputes are actually going on in some countries.

On the other hand, it may prove to be difficult to regulate and prevent people forming communities in order to share cost and to improve network availability, and network operators and ISPs have to meet this challenge wisely. The contractual weapon mentioned above, terminating the subscription agreement, is also a double-edged sword for the operator if the competing operators allow access sharing. Terminating a contract on such grounds may give the wrong signals to the market and a subsequent loss of many customers. Accordingly, the best way to meet such challenges is to offer better alternatives and services to people and by realising them in ways that comply with public regulations and common rules among players in the market.

The requirements from regulatory authorities may also be crucial for initiatives like the three mentioned here. The main reason for this is that the community demands more control over telecommunication due to the fight against terrorism and crime. The authority requires users of public networks to be identified and geographically located. More control of communication increases the complexity of the network and will possibly impose trouble for 'sharing access communities' without a strong back-up from stable operators – see the paper by Malin Tønseth et al. [4] in this issue.

2.3 The OBAN project

Open access networks where network operators are not involved will suffer from certain drawbacks. For instance, extensive demands on QoS cannot be met because the OAN providers do not have access to the necessary functionalities in the network. Another similar example is how to offer mobile services to customers.

Accordingly – if OAN should meet the same requirements with regard to quality, functionality and legal orders that are imperative in legacy communication networks then the network operators must be involved. Such services must be supported by functionalities in the network.

The European project OBAN [5] (Open Broadband Access Networks) of the EC's 6th Framework Programme is one attempt to design an Open Access Network meeting all the requirements of visitors and AP owners, the operators and service providers and towards the public authorities. Extensive studies were carried out on how to realise viable open access networks. The results from these studies constitute much of the fundament for this issue of *Telektronikk*. The project has addressed the most important aspects of opening up the fixed access network for public use. Many of the authors of articles in this issue have participated in the project. They have through their work gained excellent knowledge about the various challenges that must be solved to establish viable Open Access Networks.

Figure 2 illustrates a visiting user (guest) communicating over a casual host's access to broadband. The visitor is identified by the operator as a separate subscriber and given the necessary resources in the network. The two users do not need to know about each other.

A comprehensive study has been done on commercial, legal and regulatory aspects connected to Open Access Networks. The present implementations of OANs are still to be considered immature – the achievements in OBAN may therefore have important impact on how OANs are developing in the future.

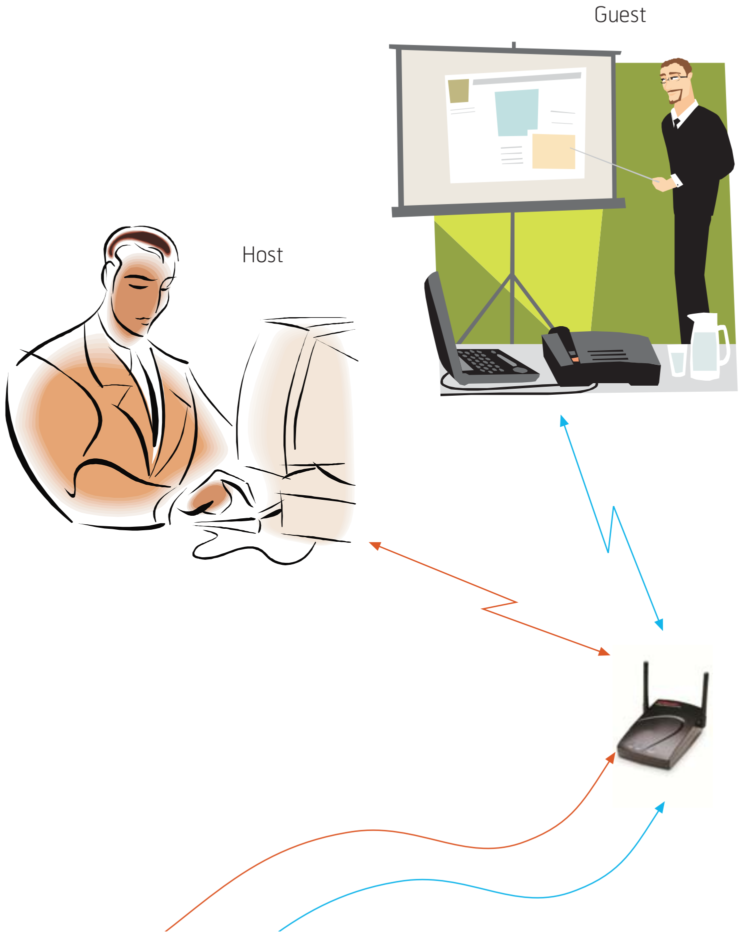


Figure 2 Sharing of access

The 9-11 syndrome has changed the world after 2001. Security and control have become hot topics in the public debate. Legal orders that will enjoin the "freedom on Internet" have already been passed (see Data Retention Directive [1]). Operators of all communication networks will have to deal with them. However, since small and professional OAN operators are not supposed to hold the human and technical resources needed to implement the required functionalities in the network, a likely consequence may be that they disappear from the market. The OBAN project has considered all these aspects and proposed a future proof architecture meeting these fundamental requirements.

While many of today's implementations of OANs limit their QoS support to providing a simple QoS mechanism for the wireless section (WLAN), the OBAN project has developed a solution for end-to-end QoS provided that the core network supports QoS per session. The latter is, however, not a given feature.

Handover when users move from one access point to another, is an important feature in OAN networks. Not necessarily because users are mobile or travelling, but because strong output power limitations for radio transmitter in the unlicensed frequency band limit the reach of WLAN to a few tens of metres. Another factor is obstacles along the radio wave path resulting in reflections and signal loss and which the receiver will detect as strong signal level variation. A stationary user's terminal, which for some reason has been moved from "one side of the table to the other" may lose the signal and try to connect to another access point. In an Open Access Network according to the OBAN specification, this will be possible – of course without terminating the session, but also without noticeable disruption.

None of the existing OAN implementations on the market today support mobility with seamless handover for people roaming between different access points and to/from 3G networks; especially in multiple ISP environments. Though the IEEE 802.11r [6] addresses mobility and specifies that hand-off shall be less than 50 msec, it is not relevant for an OAN since it relates to a network of WLANs interconnected with broadband links and operated by one single operator. The latter presumption differs fundamentally from OBAN, since OBAN assumes that people are roaming between WLANs operated by different ISPs. Each time a user enters a new WLAN zone, the user has to be re-authenticated; the time the re-authentication takes is a show-stopper for fast handover in such environments. A technical solution for how fast handover can be managed in multiple-ISP networks is an important contribution from the OBAN project.

When people move from one access point to another and they use applications with requirements to QoS like voice, it is not possible in advance to know whether the next access point has resource available to support the application. Another problem is to meet security requirements while roaming within time limits given by a seamless fast handover. The OBAN project has presented solutions to these problems by proposing an architecture that preserves all requirements to QoS and security while performing a fast seamless handover. More about this can be found in the article by Jaatun et al. in this issue [7]. The QoS requirements are of course only met if resources are available or can be made available.

WLAN is actually not designed to meet the requirements of a public network, but rather to be used in private areas, but the deployment of WLAN has developed beyond the original scope and one of the objectives in the project was also to investigate the potential of deploying WLAN in public areas. The most commonly used WLAN today is the one following IEEE802.11b/g. This standard is lacking non-interfering radio channels. There are only three of them. This makes it very difficult to design networks of WLANs which are overlapping, because MAC-layer interference will severely reduce their performance. The project therefore carried out a comprehensive study based upon analytic calculation and simulation to estimate its performance. Results from these studies are presented in the article by Ormhaug et al. in this issue [8].

An objection against approaches like the one presented by OBAN is that open access free of charge already exists on the market. People leaving their networks unsecured and open to the public and initiatives like the aforementioned FON, provide something similar at a very low cost. This is true, but it is assumed to change over time. The present telecom operators as well as national/EU telecom regulation authorities will force changes to the present situation. Commercial interests will spur the operators to try to obstruct so-called 'free-riders', while the authorities will be driven to act in the interest of the general public and community. All together this will be the crowbar that forces OANs into regular forms. This latter sentence may sound provoking, but seen from a technology point of view it will make it possible to create new and better services for people; with regard to both service quality and security/privacy.

3 Drivers and stoppers for Open Access Networks

The WLAN technology and fixed broadband access are today most important enablers for OANs. This does not mean that the technology is perfect – that it meets all requirement and expectations, but it has opened the eyes of users and service providers for how telecommunications may develop in order to meet people's demand for electronic communication. So what are the drivers for a trend towards an open access network? But first of all, how can people benefit from OANs?

3.1 Enabling a market demand

The potential market demand for open access networks is apparent for most of us, especially for those who are travelling and who want to connect to Internet, either to check their emails or to read the news while they are away. When, for instance, Ms Jones visits an office or private home, she should be allowed to connect without asking anybody in advance; she should receive the bill in an ordinary manner and the subscriber at the site should not have to worry about neither security issues nor bills. This can be interpreted as the basic (minimum) service offered to users in open access networks.

However, there are some obstacles to overcome before this imaginable need can convert to a real market demand among the general public. *Simplicity, availability, inexpensiveness* are key words characterizing these obstacles.

Firstly, simplicity embraces a lot of aspects connected to the terminals people use while they are away from home and how it is to connect to a network. It may mean things like low weight, ease of use, small size, large screen, but also issues related to simplicity of use and surveyable relations to service providers. Many of these requirements have found acceptable solutions during the last years. The weight and size of mobile equipment in many cases meet the requirements, while in others they are conflicting. It is difficult to design small devices with large displays.

Simplicity of use is possibly the biggest challenge to meet in modern communication. How to overcome the barriers people often have against adapting new technologies? Easily understandable user interfaces with a minimum of user interactions have always been aspired at, but often with moderate success. All who have struggled with PCs, laptops, PDAs, mobile phones know that.

Simplicity of use also applies to log-on procedures, which often can be troublesome with a number of passwords and interactions on the screen. The procedure used to log on away from home should not differ from what the users are accustomed to at home and it should function with as little involvement by the user as possible.

Secondly, availability to open access networks is at the moment insufficient and must be substantially improved. Broadband access to fixed networks is today only possible at hot-spots and over relatively few private WLANs if we look away from those private WLANs which are left unsecured and accessible to the public by the owners. The appearance of newcomers like the aforementioned FON community bridges towards more open networks and also for existing operators to take a more active role in this development. This is already happening to a certain extent – an example is Telenor's product "Trådløs Sone" ("Wireless Zone")[3].Thus it is assumed that the availability of open broadband services for mobile users will improve significantly in few years and give people the ability to connect not only at home, but also while visiting friends, sitting in a café or in a park.

[3] *See: http://www.telenor.no/bedrift/produkter/mobil/tradlos_sone.html (In Norwegian)*

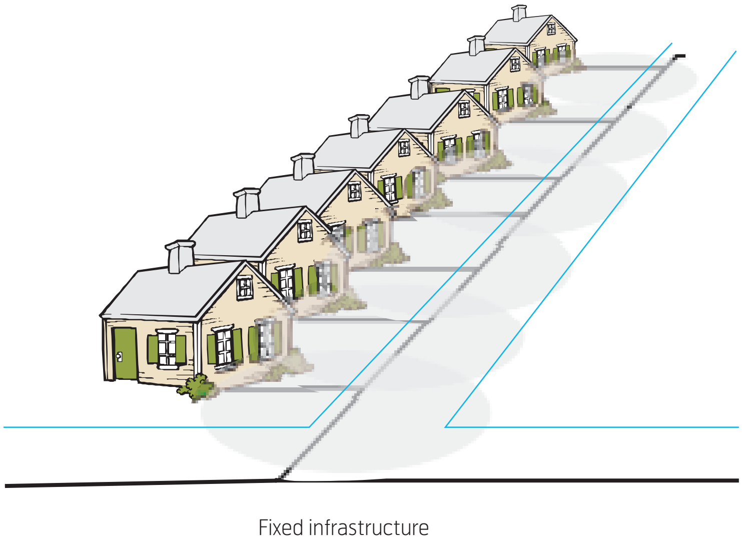


Figure 3 Open access network will make the fixed network publicly available everywhere

Thirdly, inexpensiveness is an important factor of success for any product, so also for open access networks. The cost of equipment, terminals and WLAN access points, as well as the charge for communication must be low enough also for people with low incomes. The cost of terminals and WLANs has fallen dramatically during recent years and is not considered to become a hinder for the introduction of Open Access Networks. The communication cost is a matter for the future market to decide. The OAN approach has, however, the qualifications needed to become an inexpensive service. The approach is predominantly based upon utilisation of existing infrastructures and equipment in the network, thus large investments are not expected to be needed.

3.2 Broadband availability

The availability of broadband availability is an enabler for implementation of open access networks, but can be perceived in at least two ways. The first one is connected to establishing open access in mature markets where the main objective is to make broadband available to people away from home and office, thus broadband is an assumption for establishing an OAN. The other one is connected to the use of open access to provide broadband in areas where the main objective is primarily to improve broadband availability to people in general and not particularly those on the move, thus the OAN concept is used to improve broadband take-up among people.

In the first case, open access in mature markets, the take-up of broadband is an important parameter for establishment of open access networks. People will not request broadband access when they are away if they do not have it at home and/or in the office.

The broadband access networks are predominantly based upon the old legacy telephone networks and the cable TV networks. In the industrialised countries the physical infrastructure is reaching more or less every household and business and is now being upgraded to carry broadband traffic. The number of broadband subscribers is actually increasing rapidly world-wide and the increase is even higher than we have seen for any other new technology up to the present time including the mobile boom. In few years most of the population will be connected.

In parallel with the present deployment of existing infrastructure for providing broadband to the people, new access networks based upon optical fibres are also appearing. By using optical fibres people will be

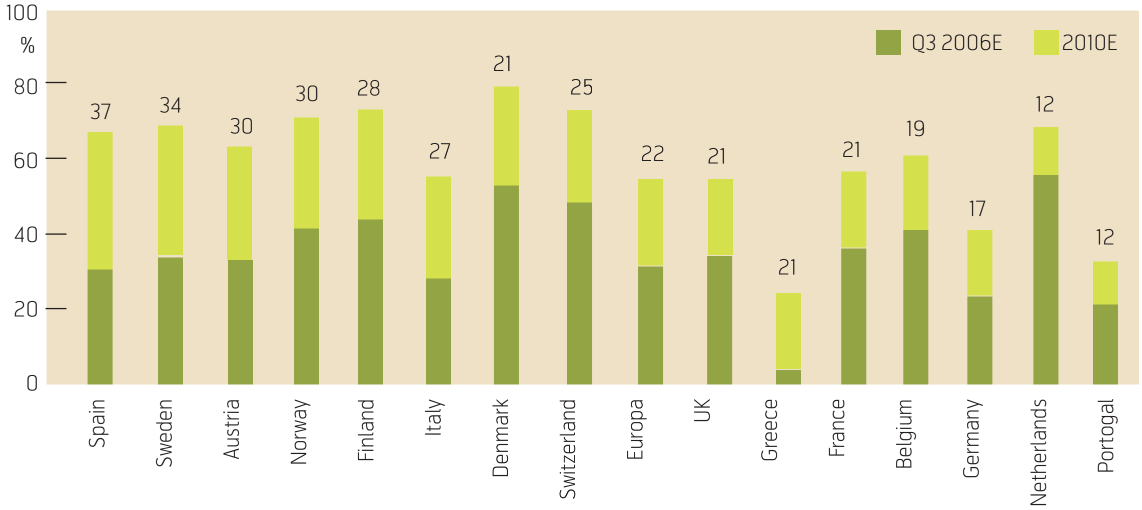


Figure 4 Broadband penetration in percent of population. Source: Meryl Lynch Estimates

offered access capacities possibly up to 1 Gb/s. When access rates increase the potential of OANs will even be more evident. Combining the high capacity of optical fibres with appropriate wireless technology can be perceived as a major step towards the future ubiquitous networks, which everybody is talking about.

The average broadband coverage in Western Europe was already in 2004 about 91 %, which means that the network has capacity to offer broadband to 91 % of the population [9]. The broadband access market is currently still in very rapid growth and the goal of 100 % coverage is accordingly soon within reach.

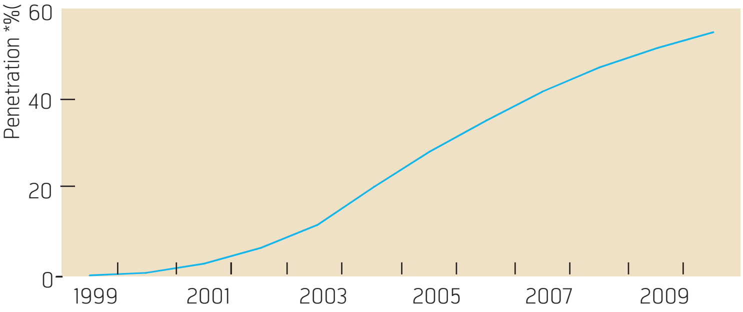


Figure 5 Trendline for broadband penetration in percent of population (Western Europe). Source: EU project ECOSYS, D14 "Updated forecasts for the mobile and fixed broadband networks and services"

Figure 4 gives an overview of broadband penetration in percent of population in some European countries. The dark green parts of the columns give the penetration by Q3 2006 and the light green parts give an estimate for the expected penetration by the end of 2010. The chart shows a rapidly increased availability of broadband among people. It is expected that the penetration will reach about 80 % of the population over time – see Figure 5.

The availability of broadband is rapidly increasing and will reach the expected 80 % in a few years, but there are large variations between regions (digital divide). Some regions are lagging behind others for several reasons. One of them is due to the lack of adequate infrastructure to feed and distribute broadband. The digital divide is considered as a severe obstacle for social inclusion and economic progress.

Though the OAN approach is not a method to build infrastructure, it is an architecture that makes optimal use of the existing infrastructure. It offers an efficient way of resource sharing in the access network. Implementation of OAN features in the network is an attractive means for increasing broadband availability among the public. People who do not have private broadband subscription of a broadband access line can be offered less expensive access by an OAN service provider. This possibility of using the OAN approach to improve broadband take-up can be beneficial both in countries without adequate network infrastructure and to people with less ability to pay for normal broadband access. Thus opening up the fixed broadband access network to the general public may also be a tool to reach the overall goal of providing broadband to 100 % of the population.

In addition to being a tool for increasing broadband take-up in general, it also implicitly offers the main feature of open access networks, namely that users are free to connect to the network anywhere. This can be considered as given, but it is worth underlining here because it is important in areas with inadequate infrastructure since the network may be overloaded at some locations and less loaded in other locations, thus it opens the opportunity for people to seek out access points with less traffic load.

3.3 Incentives for access network providers (ANP)

The utilisation of today's fixed broadband access networks is very low. The reason is that each physical line is dedicated only one legal subscriber, which in residential areas equals to one or a few persons. Though it is foreseen that new applications of the network will appear and that people will consume more and more capacity, it is unlikely that people in general will use all the available capacity all the time – most of the time these lines will carry nothing. As indicated above an average of less as 1 % of the available capacity during the day is used, thus 99 % of the capacity can be made available for public use.

From a commercial point of view these 99 % is a waste of money or said in a more positive way; the fixed network operators have a huge opportunity to make more money from the network by utilising it better. An OAN is not only a new service on an 'old network', which can be used by the present subscribers, but it has the ability to attract new customers – and new customers mean opportunities to make more money. It can also be looked upon as an improved service offering to the existing customers, because these customers will now have the possibility to access the network when they are away from home or office.

Since the ANPs do not always have direct contact with end-users, but rather with ISPs, it is the latter that often are their customers. By implementing OAN functionality in the network, the ANPs can offer improved services to the existing ISPs as well as Open Access Service Providers (OASP). The separation between ISP and OASP may be considered

ISSN 0085-7130 © Telenor ASA 2006

irrational, since they could be merged into one role. This is however for the future to decide. The separation is made to better illustrate the opportunities an open access approach can offer to infrastructure owners – namely to sell the same access line to more than one ISP/OASP.

Network operators today suffer from low earning capability; they are only providing a bit-pipe. OANs open new opportunities for network operators to profit more on their assets and it gives needed incentives to invest in new infrastructure in the access network. The latter is possibly most important. The LLUB (Local Loop UnBundling) has created a market for ANPs, but the LLUB product (copper line in the telephone network) does not give the right incentive for investment. Creating a market for 'access sharing' opens a range of opportunities.

The ANPs have access to the total bandwidth of the physical access line and not only the part paid for by a fixed subscriber. He may utilise this asset and develop differentiated products by implementing various levels of QoS, for instance dynamic bandwidth sharing or fixed bandwidth sharing or possibly other combinations. Dynamic bandwidth sharing may be attractive in some cases where the fixed subscribers are active in the evening, while the roaming users may be busier during day time. In total this is expected to give more income to the infrastructure owner and give a necessary incentive for investment. It will also create dynamics on the end-user market since the ISP/OASPs may choose and offer different products to end-users.

3.4 Incentives for ISP/OASPs

The main objective of a service provider is to develop value added services and applications that users are willing to pay for. The discussion on these matters is therefore closely related to how users perceive the services, thus users must be offered services that are requested at an acceptable price. This is, however, not the whole truth, because the situation on the market is more complex. The competition between service providers and their need to distinguish themselves from each other, lead to charging models that cannot directly be mirrored into the relation between one service provider and his customers. Accordingly, paying for communication may also be done more indirectly, for instance through advertising means, but such alternatives are considered to be outside the scope of this article.

An OAN brings a number of value added services and features to the end-users. Users in OANs are either communicating from their home locations (home users) or as visitors (visitors) at other broadband subscribers' access points. Dependent on where they are, they experience the OAN service from different perspectives. For instance: When you are in your garden you may get better connection via your neighbour's network than by using your own. Thus, users at home may perceive their home networks as borderless since they may switch to their neighbour's network when they are outside the reach of their own. This may be considered a value added feature of an OAN, which may create increased income to the ISP/OASP.

The basic OAN feature is however that visitors (guests, customers or casual by-passers) can connect to the network as if they were at home or in their business premises. They do not need to ask the host for permission and they are individually billed by their own service provider:

Making the fixed access network ubiquitously accessible to the public improves network availability dramatically. People should be able to log on to the network anywhere as if they were at home. They will be connected to the fixed access network, which offers 10–100 folds higher capacity than any public mobile network does today and experience the same performance as they do at home.

The increased availability of broadband will open new arenas for service providers, who will develop new products adapted to the performance and properties of the network and the needs of people. Since users of OANs are individually authenticated it is possible to register when connecting users are away from their home location and consequently charged extra.

However, the above are only possible opportunities and the market may drive the development in different directions – for instance towards fixed fees for the basic OAN service or in the direction of bundling it with others.

3.5 Wireless home networks and terminals

Wireless home networks based upon WLANs have become popular among people. One main reason for this is that broadband subscribers need local networks to connect printers, more PCs, data storage units, etc. WLAN offers a simple way to connect these devices and also the freedom to locate them where you want and not where the Ethernet cable is installed. Wireless technology is now established as a convenient and inexpensive alternative to cables for the general broadband subscribers who need to connect data related equipment in a network. We are no longer satisfied by being tied to the wall with a cable while using the network.

A side-effect of the above popularity seems to be that WLAN is positioning itself to become the catalyst for a transformation of the fixed network towards an open access network, which will be forced upon operators with or without their active participation. The reason is that radio waves do not see the borders between private and public areas. WLANs, which ideally should only cover inside the building, do it as well outside. The 'outside coverage' opens a potential gateway for casual by-passers to access private networks without the owners' knowledge unless something is done to protect the network against unintentional access.

PCs and laptops with WLAN capability are often default features in such terminals today. The same may happen with hand-held terminals. Multiple radio interface telephones are already available and make it possible to connect over the fixed broadband network with WLAN when it is available and when the user needs more bandwidth than offered by the cellular network.

The need for more bandwidth will increase as the functionality of terminals is increasing. The integration of digital cameras and video cameras in mobile phones, or rather integrating the mobile phone into a camera/video camera, gives us only a feeling of what is going to happen.

Real time video filming may become the next capacity demanding service commonly used by the general public. But even before this becomes popular uploading digital photos and videos during travels may spread and demand wireless and fixed access surpassing today's offering. Used in mobile phones the bandwidth demand for transferring a video film is rather low and can even be supported by today's 3G network. However, laptops have bigger screens and are more demanding and they shall in some cases relay video films to large screen TV monitors resulting in increasing bandwidth demand.

3.6 Individual authentication

A secure and trusted authentication system is a mandatory requirement in any business model. The service providers need to know who is using the network and to whom the bill should be sent.

Authentication in the fixed network is based upon 'line authentication'; i.e. that the access router or modem in the home performs the authentication towards the service provider and not the individual users. The consequence is that service providers cannot identify each individual user's traffic, for instance traffic from a casual by-passer who has been able to connect. Since the subscriber is responsible to his service provider and to public authorities for all use of the line, he runs the risk of being taken to court for illegal use [1], [11]. Such incidents around the world have led to a change in people's minds as regards security issues for data communication over wireless. The trend is now that more and more people protect their wireless networks with encryption and/ or MAC filtering, thus making them inaccessible to the public.

In order to identify users in an OAN individual authentication must be deployed as it is already done in mobile networks. However, to introduce individual authentication and abandon the line authentication is a radical system change and also a cost issue. All terminals must have an authentication mechanism installed. A simplified method of authentication is to use the mobile phone as an authentication device either by requesting authentication via the mobile network, or by transferring SIM information by Bluetooth or Infrared from the mobile phone to the terminal to be connected. The latter method is described in the article by Corrado Derenale and Simone Martini [12] in this issue. The consequence of these methods is that visitors' access to the fixed network will be considered as a service offered by mobile operators, which sometimes is undesired.

Individual authentication allows subscribers of an ISP to connect to any network where the ISP offers his services – at home, in other people's homes, on the street or at any other location. Individual authentication is like a key (see Figure 6) that opens the door to the broadband network.

As mentioned in section 2 above regulatory authorities have legal requirements to operators of telecommunication networks, such as identification of users,

Figure 6 Individual authentication is like a key that opens the door to the public broadband network

ISSN 0085-7130 © Telenor ASA 2006

storage of traffic data, etc. Operators are required to maintain records of such data for a period of time. To comply with the regulations of open access networks operators will have to introduce individual authentication. The regulatory requirements may become the joker giving premises for what kind of operators that can run open access networks. The smaller and possibly less professional operators/committees will not be able to comply with these requirements.

3.7 Consequences for operators

The liberation of the telecommunication market has during the past years enforced changes on how the incumbent telecom operators run their networks and provide their services. One of the effects is that operators have less responsibility for user equipment than before. People buy their ADSL modems and routers. They install the equipment themselves or pay somebody else to install it. Nor is the operator responsible for keeping it in service. If the home router fails, the operator does not care – it is in the hands of the owner. If the equipment is installed in dirty and humid environments, it is still not the operator's responsibility. The users may disconnect the equipment and they may turn off the power. The operator does not care.

In an OAN the operators will have to care more about the equipment installed also in private environments. The reason is that the Residential Gateway (RGW) which is installed in subscribers' premises now will become a part of the network and must also be treated as such. Important functionalities crucial for the network will reside in this equipment. The equipment must, among other things act as a public access node equal to DSLAMs and access routers in today's networks. The functionality of the RGW is explained further by Panken et al. in this issue [13].

Since crucial functionalities of the network reside in equipment installed in private premises, there are a number of security related issues to solve. Privacy is one of them. Subscribers will not accept the possibility that their communication may be wire-tapped by casual by-passers. Users of the network, home users as well as visiting users, must be convinced that they do not interfere with each other or that they are wire-tapped. They must also feel assured that content cannot be accessed and manipulated by intruders.

Operational reliability is another important issue. Since the RGW often will be located in private environments, the physical access to the equipment may be restricted and influence on network reliability. Power supply is also a concern for operators. How can they prevent the power being turned off by the owner?

3.8 Obstacles for realisation of open access networks

The main uncertainty and possible obstacle for realisation of open access networks is people's adaptation to the possibilities offered by new electronic equipment, terminals and modern communication like open access networks. Would they use broadband away from home/office if it were available? What kind of communication needs in their daily life would be satisfied? Some of the answers may be deduced by analysing how mobile phones are used in 3G networks – looking at news, listening to the radio, etc.

The second question is related to their willingness to pay for the services. Answers to these questions cannot be given yet.

The third question is related to subscribers' willingness to share the WLAN and access point with third parties. Since this question is related to how you implement an OAN, it is considered to be less severe. Priority and QoS mechanisms can be implemented in the network in such a way that home users will be undisturbed by the existence of other connected users. Similar arguments can be used as regards security/privacy issues. They can be solved.

4 Potential performance of an open access network

The following summary of potential performance is mainly deducted from results obtained in the OBAN project. It gives a brief overview of the most important properties of the network and how users will benefit from it.

4.1 Availability of broadband

Realisation of an OAN will improve the accessibility to broadband substantially compared to the present situation. The fixed access network is today inaccessible to people everywhere except from their homes/offices. Each subscriber in the fixed broadband network will now host a public access point. The number of places where people on the move may access the network will increase from 'a few tens to millions'.

4.2 Mobility features

It is assumed that the basic service offered by an OAN is broadband access for people in nomadic situations or people moving at pedestrian speed. The latter may sound like a substantial drawback, but is probably not. People are normally not in motion when they make use of broadband services. Most of the communication takes place while people are sitting and standing somewhere – at home, in an office, in a café or similar. The obvious reason is that many services require the user's full attention. Browsing the Internet while walking in the street is convenient for nobody, nor would you want to watch a video while walking and even phone calls mostly take place while people are stationary and not on the move.

The above does not mean that mobility, fast and seamless handover is superfluous. Since the WLAN covers only a limited area – a few tens of metres – and many WLANs may be accessible from the same location, micro movement may cause a demand for handovers. Multi-path propagation and interference from other access points create large variations in signal level, thus moving the wireless terminal from one side of the table to the other may request handover. Fast handover is therefore required and it can be implemented in the network. The requirement specification worked out in the OBAN project specified that disruption during handover should be less than 120 msec [12].

Nevertheless, it is not expected that an OAN will offer mobile services in the same way that 2G/3G networks do. Mobile networks are designed to cover wide areas and to meet the requirements of voice communication. This can hardly be achieved in OANs.

4.3 Service quality

Up to the present time WLAN has been suffering from a lack of QoS mechanisms. This has however changed with the completion of the IEEE802.11e standard. Thus, by deploying this standard it is possible to meet the requirements to QoS that are common in telecommunications, but only in stable situations – see explanation below.

QoS should be observed in an end-to-end perspective and the QoS implementation on the wireless sector must be matched with QoS on the access line and in the core network. DiffServ [15] is one of the available mechanisms for QoS that can be used in public IP networks.

QoS in OANs is however much more complicated and unpredictable. Due to the fact that WLAN operates in the unlicensed frequency band, severe MAC-interference from other WLAN access points must be expected. These disturbing access points can belong to the actual open access network, but they may as well be any other access point installed by people. The available capacity at one particular access point will therefore depend upon the traffic in other access points. This makes the situation unpredictable and unmanageable in respect of providing guaranteed QoS to users, but certain approximations can be realised [12].

4.4 Security issues

Security embraces a range of aspects related to the users of the networks, the operators and the community. The aspects that are solved in the OBAN project are user authentication, anonymity, separation of users, authentication of access points, confidentiality and security during fast handover. In addition there are issues that relate to regulatory demands such as storage of traffic/user data – see section 2 above.

Further information can be found in the OBAN documents – among others [14].

4.5 Capacity and coverage

Capacity and radio coverage can relatively easily be estimated in networks consisting of non-overlapping access points, but this will most probably not cover the situation in a realistic OAN. As mentioned above in section 4.3 there will be a number of access points that are interfering with each other. Interference may be sorted into two classes – the MAC layer interference and physical layer interference. Further information about these two terms and also about coverage and capacity simulation and calculation is presented by Jan Erik Håkegård [16] and Terje Ormhaug et al. [8] in this issue.

MAC layer interference has severe impact on available capacity for a user compared to a stand-alone situation where access points are located in interference free distance from each other. If three access points can listen to each other, they have to share the airtime. The effect is that the average capacity per access point is 1/3 of the maximum.

The effect of MAC interference is in contradiction to the objective of obtaining full radio coverage in an area in order to enable seamless handover between access points. Thus, seamless handover will only be possible in OANs with moderate capacity demands and high capacity can only be achieved in networks consisting of stand-alone access points.

5 Conclusion

The evaluation presented in this article substantiates that the present situation where people often leave their WLANs open for anybody to access, will fade out due to the general increased fear among people of misuse and pressure from operators. It is also argued that other initiatives based upon separate agreements between a service provider and the subscriber without involving the ISP/network provider will fade out as well. Public security issues and commercial reasons will probably make this happen and leave the arena to bigger operators who have resources to implement the required functionalities in the network and to

ISSN 0085-7130 © Telenor ASA 2006

comply with regulatory demands. Results from the OBAN project [5] have concluded that all the major functionalities needed in an OAN can be implemented.

6 References

1 European Parliament – The legislative Observatory. *Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes* (amend. direct. 2002/58/EC) (The Data Retention Directive). Procedure File COD/2005/0182. [online], 11 December 2006, URL: http://www.europarl.eu.int/oeil/file.jsp?id= 5275032

2 Eskedal, T G, Johannessen, T H. Actors, activities and business opportunities in open broadband access markets today. *Telektronikk*, 102 (3/4), 72–84, 2006. (This issue)

3 Elkotob, M et al. The Open Access Network Architectural Paradigm Viewed Versus Peer Approaches. *Telektronikk*, 102 (3/4), 33–47, 2006. (This issue)

4 Tønseth, M et al. Open access networks – regulatory aspects. *Telektronikk*, 102 (3/4), 17–25, 2006. (This issue)

5 *IST project OBAN (Open Broadband Access Networks)*. Available from: www.ist-oban.org

6 IEEE. *P802.11r – Standard for 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*. Approval Letter – 30 May 2006. [online] 11 December 2006, URL: http://standards.ieee.org/ board/nes/projects/802-11r.pdf

7 Jaatun, M G, Tøndel, I A, Johannessen T H. Security in fast handovers. *Telektronikk*, 102 (3/4), 111–124, 2006. (This issue)

8 Ormhaug, T, Lehne, P H, Østerbø, O. Traffic capacity and coverage in a WLAN-based OBAN. *Telektronikk*, 102 (3/4), 171–194, 2006. (This issue)

9 Celtic Project ECOSYS. *Updated forecasts for mobile and fixed broadband networks and services*. Deliverable D14, December 2005.

10 *Boycott-RIAA.com. Forum: Serious Legal Discussions, Subject: RIAA defeated by WLAN defense*. [online], 11 December 2006, URL: http://www.boycott-riaa.com/forums/ legalissues/3153.

11 Camponovo, G, Cerutti, D. WLAN Communities and Internet Access Sharing : A regulatory overview. *Proc. International Conference on Mobile Business (ICMB'05)*, Sydney, 281–287, 2005.

12 Derenale, C, Martini, S. An EAP-SIM based authentication mechanism to open access networks. *Telektronikk*, 102 (3/4), 135–144, 2006. (This issue)

13 Panken, F, Hoekstra, G, van der Gaast, S. Resource allocation and guarantees for real-time applications in WLANs. *Telektronikk*, 102 (3/4), 125–134, 2006. (This issue)

14 Panken, F et al. *Condensed OBAN architecture*. Deliverable D30, IST Project 001889, OBAN, 23 August 2006.

15 Blake, S et al. *An Architecture for Differentiated Services (DiffServ)*. IETF Request for Comments RFC2475. December 1998, [online], URL: http://www.ietf.org/rfc/rfc2475.txt

16 Håkegård, J E. Multi-cell WLAN coverage and capacity. *Telektronikk*, 102 (3/4), 159–170, 2006. (This issue)

For a presentation of the author, please turn to page 2.

Open Access Networks – Regulatory Aspects

MALIN TØNSETH, ØYSTEIN HOEL, HÅKON STYRI, CHRISTIAN A. NØKLEBY, EINAR MELING, RUNAR LANGNES

Malin Tønseth is Legal Adviser at Norwegian Post and Telecommunications Authority

Developments in wireless access networks raise new challenges from a regulatory point of view. Networks that used to be private are opening up and becoming part of public networks. How do existing laws and directives apply on emerging networks and services in this new situation? The regulatory issues generally fall into two categories: Those related to security and lawful interception, and those concerning fair and effective competition in the market. Regarding traffic data both protection of privacy and legal authorities' right to interception have regulatory requirements that will affect demands on storage solutions. Location information in case of emergency calls is another potentially important matter. Finally, market regulations could be applicable in order to promote competition in favour of the users. In this paper we give an overview of relevant regulations and discuss possible requirements that might be put on network solutions and on operators.

Øystein Hoel is Senior Adviser at Norwegian Post and Telecommunications Authority

Håkon Styri is Senior Adviser at Norwegian Post and Telecommunications Authority

Christian A. Nøkleby is Senior Engineer at Norwegian Post and Telecommunications Authority

1 Introduction

Emerging open access networks present new challenges to regulatory authorities. The requirements put on providers of electronic communication services are well established. Nevertheless, in a new environment it is not trivial to classify the services and decide which legal entities that take the different roles and consequently where to place the responsibility. The separation between access providers and service or application providers that is considered advantageous in many cases, makes some requirements more challenging. Furthermore, in open access networks, access is likely to be provided in a close cooperation between different players. In particular the role and responsibility of private owners or hosts of equipment providing public access is a new issue. It is important to identify which players to whom the regulations apply.

The background for this paper is the Norwegian Post- and Telecommunications Authority's (NPT)[1] participation in the IST OBAN[2] project. Although we observe also other initiatives in this field, our discussion here will have OBAN as the most important reference.

Regulatory measures in a market are primarily used to correct real problems and not to anticipate hypothetical issues. One important objective is to avoid making it more difficult to introduce new technologies and services. However, to protect critical infrastructure and the security needs of our society there are some requirements that will be imposed on technologies and services that are widely adapted. Some choices made in the development phase may benefit from anticipating such requirements in order to avoid cumbersome and expensive adaptations at a later stage. Thus, in a development project it is more appropriate that regulatory issues are considered after a technology, service or business model is outlined, rather than the work on regulatory issues being used to suggest technologies, services or business models. The various regulations are only broadly explained and specific counsel should always be sought for a particular case.

The remaining chapters in this paper are arranged as follows: First we introduce some useful definitions. In chapter 3 we discuss security and lawful interception issues while in chapter 4 we go through current market regulation. In both chapters we first introduce the relevant legal basis and then give examples of how this might be applied on open access networks. For market regulations the focus of this paper is on the Norwegian market. Finally we sum up our discussion.

2 Definitions

For the purpose of this paper the following definitions from the Norwegian Electronic Communications Act [1] are considered useful:

- *Provider:* any physical or legal person that offers others access to an electronic communications network or service;

- *Electronic communications network:* electronic communications system that includes radio equipment, switches, other connection and routing equipment, associated equipment or functions;

[1] *The views of the authors do not necessarily reflect those of the Norwegian Post and Telecommunications Authority.*

[2] *Open Broadband Access Network. EU funded research project under the Information Society Technologies (IST) priority of the Sixth Framework Programme (FP6).*

ISSN 0085-7130 © Telenor ASA 2006

Einar Meling is Senior Advisor at Norwegian Post and Telecommunications Authority

Runar Langnes is Senior Advisor at Norwegian Post and Telecommunications Authority

- *Electronic communications service:* service that wholly or primarily comprises arrangement of electronic communications and that is normally provided for a fee;
- *Public electronic communications service:* electronic communications service that is accessible to the public or intended for use by the public;
- *Telephone service:* electronic communications service that transmits speech between terminal equipment connected to network termination points in an electronic communications network.

The term *private network* is not defined in the act, but the following definition could be derived from the regulation on electronic communications [2]:

- A private network is an electronic communications network from the point of connection to an electronic communications network used for the provision of public electronic communications services up to the private network termination point(s). It is assumed that the owner has the network for his own use or leasing and does not offer electronic communications services to others.

3 Security and lawful interception

3.1 Legal background

In the combat of terrorism and crime, information about the use of different electronic services is extremely useful. In some cases the content of the communication is also of interest. This poses certain requirements to the communication equipment, which are defined in laws and regulations.

These laws and regulations will affect the possibility of realising different open access network solutions. In this first part of the paper the focus will be on security related laws and regulations.

The relevant paragraphs in the Norwegian Electronic Communication Act will be referred to relevant EC Directives [3] in which this act has its legal basis. It should be noted that member states may have implemented the EC directives into national regulations in various forms and with various content. However, in general the legal consequences for the member states' national regulatory framework ought to be in harmony with the directives. The relevant articles in the EC directives are to a large extent detailed and do not leave much room for differences in national implementation.

In this paper NPT will use the Norwegian national legislation as a starting point of our analysis. There is quite a good mapping between the directives and the Norwegian national legislation. However, NPT does not guarantee that this is the case with the national legislation of all EU member states. A survey of any discrepancy with national legislation of the EU member states has not been conducted by us.

Please note that the law text and description of practices in this chapter are translated from Norwegian by NPT, and NPT cannot guarantee that this is strictly correct from a legal point of view.

3.2 Scope of the Electronic Communications Act

The Electronic Communications Act applies to activity connected to transmission of electronic communications and the associated infrastructure, services, equipment and installations (section 1-2).

Electronic communication is defined in section 1-5 as transmission of sound, text, pictures or other data using electromagnetic signals in free space or by cable in a system for signal transmission.

Open access networks transmit data using electromagnetic signals in free space and on this background it is quite clear that this kind of networks falls within the subject scope of the Electronic Communications Act.

3.3 Regulation on private networks

A useful starting point for this discussion could be to examine the legal situation for private networks. The regulation based on the Electronic Communications Act contains special requirements for private networks.

Examples of such requirements are:

- Duty to maintain secrecy of the content of electronic communications;
- Implement measures to prevent others from acquiring knowledge of such information;
- Make sure that the private network has a satisfactory quality.

These duties will apply regardless of whether the private network is based on fixed or wireless systems.

3.3.1 The distinction between private and public networks

According to the Electronic Communications Act a network becomes public when it is made accessible to the public or it is intended for use by the public. In other words, a network will only become public if the owner deliberately makes it accessible to the public. The deliberation may express itself in the form of making the network technically accessible (opening it) to the public and making the public aware of its existence, e.g. by ads in the media. In practice, this means that merely opening a previously closed private wireless network will not automatically make it public.

3.3.2 Private electronic communication service

In order for it to be a service there should normally be a fee involved. The term *fee* is not explained in the act or in the preparatory sources to the act, but according to the directive on electronic commerce the term must be understood in a broad sense. This means that also indirect profits from the service could be considered as a fee. On the other hand, if a group of people form a club, share the costs and have no intention of making a profit, this could fall outside the term *fee*.

3.4 Relevant provisions in the Electronic Communication Act

On the assumptions that services based on open access networks will be defined as electronic communication services, the following sections in the Electronic Communications Act will apply:

§ 2-1 Duty to register

§ 2-2 Measurement and information on quality

§ 2-3 Requirements for networks, services, associated equipment and installations

§ 2-4 Terms of supply

§ 2-5 Permitted restrictions on use

§ 2-7 Communications protection etc.

§ 2-8 Provide statutory access to information (legal interception)

§ 2-9 Duty of confidentiality

§ 2-10 Security and preparedness

Furthermore, based on the assumption that the services based on open access networks can be considered as a public telephony service, the following sections in the Electronic Communications Act will apply in addition to those mentioned above:

§ 2-6 Calls to emergency call services and geographic location of emergency calls

The first five paragraphs are general in nature. For the purpose of this discussion we focus on the security related paragraphs.

§ 2-6 Calls to the emergency call services and geographical locating of emergency calls

According to section 1 of this provision it shall be possible to make calls to the emergency services' emergency call service from all terminals connected to public telephone services.

The provision has its legal basis in the EC Universal Directive 2002/22/EC (Universal Service Obligation (USO) Directive) [3]. The Directive defines a minimum set of services of specified quality which shall be made available to all end-users on their territory, independently of geographical location and in the light of specific national conditions and at affordable prices.

According to the USO Directive Article 26 the member states shall ensure that all end-users of publicly available telephone services are able to call the emergency services free of charge. (§2-6 only applies for "public telephony service".)

§ 2-7 Communications protection etc.

According to this provision "The provider shall implement the necessary security measures for the protection of communications in the provider's electronic communications networks and services. In the event of a particular risk of breach of security the provider shall inform the subscriber of the risk. Traffic data shall be deleted or rendered anonymous as soon as they are no longer necessary for communications or invoicing purposes, unless otherwise determined in or pursuant to the law. Any other processing of traffic data requires the consent of the user."

The provision has its legal founding in the 2002/58/EC Directive [3] concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. This directive is a continuation of and a supplement to the principles set out in the 95/46/EC Directive on the Processing of Personal Data by way of adapting those principles according to the developments in markets and technologies in order to provide for a technology neutral set of rules. On this basis provision § 2-7 on Communication Protection sets out some rules of obligation related to the providers' security measures and also related to the providers' processing of traffic data.

§ 2-8 Provide statutory access to information (legal interception)

This provision states that "Providers of electronic communications networks that are used for public electronic communications services and providers of such services shall operate networks and services so that statutory access to information on end users and electronic communications is assured. The provider's running costs connected with fulfilling this operating duty will be met by the state in regard to those additional costs resulting from these services."

The aim of this provision is to ensure that the arrangement of networks and services allows for certain means of police investigation (monitoring) in connection with combatting crime. The obligation of arranging for statutory access to information also includes the arrangements necessary to allow for obtainment of information on end users in relation to electronic communication. The provision lies within an area of legal issues not governed by EC legislation since Norwegian regulations which are implemented in order to combat crime lies within the national freedom of action. However, we assume that other member states have similar provisions in national legislation.

§ 2-9 Duty of confidentiality

As a consequence of this provision the "Providers and installers have a duty to maintain secrecy on the content of electronic communications and others' use of electronic communications, including information on technical systems and methods. They have a duty to implement measures to prevent others than those to whom the information applies having the opportunity to acquire knowledge of such information."

Similar to provision § 2-7 provision § 2-9 has its legal founding in the 2002/58/EC Directive concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. The relevant articles of the Directive are article 4 and 5. The provision is supplemented by the Norwegian Regulations on Electronic Communications Networks and Services chapter 7 which provides detailed guidelines on the processing of traffic data and of location data According to Section 7-1 of the Regulations on Electronic Communications Networks and Services providers shall keep traffic data confidential and shall erase traffic data or render it anonymous. According to Section 7-2 Location data other than traffic data may only be processed in an anonymized form.

§ 2-10 Security and preparedness

This provision states that "Providers shall offer electronic communications networks and services with the necessary security for the users in peace, crises and war. Providers shall maintain the necessary preparedness and entities important to the community shall be prioritised when necessary.

Similar to provision § 2-8 this provision lies within an area of legal issues not governed by EC legislation since Norwegian regulations which are implemented in order to maintain national security lies within the area of national freedom of action.

3.5 The directive on the retention of traffic data

Each and every move over electronic communications networks generates so-called 'traffic data'; i.e. data processed for the purpose of conveyance of a communication on an electronic communications network or for the billing thereof.

The availability of such traffic data is important for purposes related to law enforcement and security, such as the prevention, investigation, detection and prosecution of serious crime, such as terrorism and organised crime.

Following the Madrid terrorist bombings in March 2004, the EC Commission stated that it has now become urgent to adopt harmonised provisions at EU level on this subject. The Commission has found it necessary to apply rules that guarantee the availability of traffic data for anti-terrorism purposes. These rules are defined in the Data Retention Directive[3]. On this basis provisions on data retention might be implemented in the different member states' national legal framework.

One cannot predict how national legislative authorities will treat this directive. However, players should be aware of the possibility of stronger requirements on traffic data storage in future.

3.6 Communications protection

The Norwegian Electronic Communication Act as well as directive 2000/58/EC have provisions on security. They cover protection of communication content and traffic data. It is the responsibility of the provider to make sure that necessary effort is made to protect the information. The technological development is running fast and the wording of the act cannot be too specific in defining what is "necessary". This has to be assessed in the actual context. In Norway this field is regulated by assessing the actual solutions in retrospect if a user submits a complaint. If the regulator finds the measures implemented by the operator insufficient, then requirements might be imposed on the operator. There will always be a possibility that players with access to great resources can break security. However, the regulator will expect that the most obvious threats have been met with adequate means. Examples of reasoning would be:

- If there are well known and effective countermeasures to typical threats, these should be implemented to the appropriate extent.

[3] *Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006.*

- In the case of wireless access systems, encryption over the radio link would be an obvious expectation.

- Crypto algorithms with published severe weaknesses should be avoided.

- In a strongly decentralised open access network, e.g. OBAN, steps should be taken to avoid illegal access to information through equipment placed in private domains or poorly controlled public environment. Equipment could be protected by physical/mechanical means and locally installed software could have cryptographic integrity protection. When a wired connection partly runs through this kind of insecure environment, then the whole path to the operator controlled building should be protected.

There are a number of aspects associated with the requirements on traffic data. Data must be protected from illegal access and must be deleted or anonymised when no longer necessary for invoicing purposes. Another aspect is the obligation to prepare for statutory access to information on end users. When implementing measures to fulfil the requirements on security, both aspects have to be taken into account. Furthermore the proposed directive on the retention of "traffic data" may lead to stronger requirements on secure data storage.

It is important to stress that the player that appears to the user as the provider of the electronic communication service as well as the access network provider are both responsible for fulfilling the requirements.

3.7 Lawful interception

Lawful interception must satisfy three important requirements. The first and basic requirement is to provide the ability to intercept all communication sessions originating from or terminating at a specific subscriber. The second requirement is that the subscriber or any third party should not be aware of such intercepts. This is usually more difficult in a packet switched network than in a circuit switched network, in particular there are several issues that must be addressed when the subscriber is nomadic or mobile and free to roam between several network access providers. The third requirement is that the access mechanisms to establish an intercept must be secure and only allow authorized lawful intercepts. For an introduction of the basics of lawful IP interception, please refer to ETSI TR 101 944 *Telecommunications Security; Lawful Interception; Issues on IP Interception* [4].

One important issue in a packet switched system where nomadic or mobile subscribers may connect to any access point is where the actual intercept points can be placed. Assuming voice over IP technology where the content streams are routed directly between end terminals a system using a small number of centralized intercept points may influence the quality of service and thus risk revealing the intercept.

Another technical solution would be to move the interception points to the edge of the network. As a mobile subscriber moves from access point to access point each interception point may be able to collect only a fraction of the communicated content. In practice, such an interception system must be able to concatenate several fractions of an intercepted communication session. A vulnerability of this system is the security of the interception points. As several interception units must have a list of potential interception candidates, the confidentiality and integrity of the list is paramount. A systems design that minimizes the number of interception points may be the preferred solution.

Traffic data is part of the data collected in a lawful intercept. Collecting call setup information does not create any issues that have not been addressed in lawful interception of circuit switched telephony, but it should be noted that several IP telephony providers do not collect call duration information for some categories of calls. This should not represent any problem in the cases where the content of the communication is intercepted.

3.8 Emergency calls and location data

The Electronic Communications Act sets forth an obligation for operators to transfer subscriber data and location information to emergency services in conjunction with emergency calls. This implies that there has to be technical means as to:

- Identify the emergency caller
- Identify the caller location
- Route the call to the correct Public Safety Answering Point (PSAP).

The emergency services have expressed a need for more accurate location information and additional information about the emergency caller. NPT's current stand on this matter is that the information in question should be limited to information telecom operators have available for invoicing and operational purposes. The Ministry of Transport is however considering a proposal to change the regulation in order to facilitate the transfer of a wider range of information to emergency services.

3.8.1 Related initiatives

In the 1980s Televerket in Norway developed a solution identifying the emergency caller based on the Caller Line Identification (CLI – the caller's telephone number). Further, an inquiry was made to a customer database, and the name and address information was conveyed via a Leased Line to the PSAP. The solution has since been upgraded to a completely new platform and location information is now transferred via ISDN to PSAPs.

Recently and at the initiative of the Norwegian Post and Telecommunications Authority (NPT), Norwegian telecommunication network operators and representatives from emergency services formed a work group to develop common guidelines for the transfer of location information [4].

The guidelines establish directives for formatting of information and principles of transfer of such information. They define the interface between network operators and the PSAP and are operator as well as technology neutral.

In short terms the proposed solution states that the system, based on the incoming CLI of the emergency caller sends an electronic inquiry to the:

- (Voice) Service provider, resolving the name and civic address;

- Network provider, resolving the current location (applies to mobile telephony).

All relevant information is then returned in a standardized format and displayed at the PSAP dispatcher's workplace.

However, the guidelines were developed on the basis of traditional landline and mobile communication and there are still some unresolved issues regarding nomadic IP based voice communication.

3.8.2 Problems related to transfer of Location Information in IP-based networks

IP-based voice communication poses a lot of new challenges regarding the transfer of location information. The challenges are related to the nomadic nature of IP-based communication and the non-existent or unstructured binding between geographic/civic locations and IP addresses which identify the point of attachment to a network. Further complications arise of the fact that the roles involved in a communication service will typically be provided by different entities. Each in possession of different pieces of information needed to pinpoint the calls location or transfer of subscriber information. As an example the roles of the Application/Voice Service Provider and the Internet Attachment Provider can be provided by different entities. As a consequence, the Application/Voice Service Provider is typically unable to learn the physical location of the emergency caller [5].

In the absence of learning the correct physical location of the emergency caller, the Application/Voice Provider will also have problems converting the 3-digit emergency number to the correct 8-digit telephone number of the PSAP responsible for serving the specific location from where the emergency call is originating (ref. routing the emergency call to the correct PSAP).

Lacking a suitable technical solution regarding Location Information for nomadic VoIP services, NPT has given operators the possibility to apply for a temporary exemption from this specific obligation. However, the affected providers still have to provide PSAPs with the subscriber and civic information they possess in conjunction with an emergency call.

The stated issues concerning Emergency Communications and Location Information have recently received a lot of attention worldwide and are currently being addressed in a number of committees; within ETSI[4)] both EMTEL[5)] and TISPAN[6)] address emergency call handling. Other committees are IETF ECRIT[7)] and NENA[8)].

4 Market regulations

The telecommunication sector in European countries has been through a transition from monopoly to competition. It is a main objective within the EU to make this competition effective. It is recognised that in order to achieve this objective, sector specific regulations are needed in a transition period. When discussing different technical and commercial models for services based on open access networks the relevant regulatory framework should be taken into account. In this section we will describe the obligations which will apply for access to the fixed network in Norway in order to provide broadband services. We will focus on what is often called LLU ("Local Loop Unbundling"), although obligations related to

[4)] *European Telecommunications Standards Institute*

[5)] *Emergency Telecommunications*

[6)] *Telecoms & Internet converged Services & Protocols for Advanced Networks*

[7)] *Internet Engineering Task Force, Emergency Context Resolution with Internet Technologies*

[8)] *National Emergency Number Association* other services, e.g. wholesale broadband access (including "bitstream access") and access to mobile network(s) might have some implications in this context. NPT also has the power to impose specific obligations on undertakings with significant market power in the retail markets for fixed telephony. Recently, NPT designated Telenor (the incumbent operator in Norway) as the undertaking with significant market power in all the six relevant markets that are defined for public telephone service to end users provided at fixed locations. Some of the obligations pertain only to PSTN/ISDN telephony and not to voice over broadband (VoB).

4.1 Legal basis

Telenor is obliged to offer LLU as a result of the LLU Regulation adopted by the EU on 18 December 2000. The LLU Regulation was implemented in Norwegian law through amendments of the Public Telecommunications Networks and Services Regulations of 6 February 2001. The product launched by Telenor is offered together with a co-location product.

The new regulatory framework for electronic communication is based on five directives adopted by the European Union (EU) in 2002 [3]. The directive relevant for the LLU regulation is the Access directive. The directives came into force for Norway with effect as from 1 November 2004. The directives have been implemented in Norwegian law, inter alia through the Electronic Communications Act of 4 July 2003 and Regulations of 16 February 2004 on electronic communications networks and services (Ecom Regulations).

Under the Electronic Communications Act NPT is obliged to analyse the various markets for electronic communications and identify undertakings with significant market power. NPT has taken as a basis the 18 markets defined by the EU Commission and the EFTA Surveillance Authority (hereafter referred to as ESA) as relevant for sector-specific regulation.

ESA has defined the following related wholesale markets for the retail market for broadband access:

11 Wholesale unbundled access (including shared access) to metallic loops and sub-loops, for the purpose of providing broadband and voice services.

12 Wholesale Broadband Access.

Market 11 is a wholesale market that includes full and shared access to the fixed access network for supplying broadband and telephone services, and is often referred to as the LLU market (i.e. the market for "local loop unbundling").

In the Recommendation from EU/ESA, the market for LLU is specifically defined as a particular access technology: copper-based access. One of the reasons for this is that other access technologies are currently insufficiently developed or widespread.

Relevant obligations in the LLU market are:

- Access obligations, cf. Electronic Communications Act §§ 4-1, 4-2, 4-4 and 4-5;
- Obligation of non-discrimination, cf. Electronic Communications Act § 4-7;
- Obligation to publish a reference offer, cf. Electronic Communications Act § 4-6;
- Obligation of transparency, cf. Electronic Communications Act §§ 4-6 and 4-8;
- Price controls and obligation of cost accounting, cf. Electronic Communications Act § 4-9;
- Obligation of accounting separation, cf. Electronic Communications Act § 4-8.

4.2 The Norwegian Broadband Market

The LLU market and the relevant market for broadband access are two wholesale markets with the same associated retail market. Since the end of the 1990s the broadband market has grown rapidly. Figure 1 provides an overview of market share in the retail market for broadband access, based on volume (i.e. number of broadband accesses).

Figure 1 shows that Telenor has just over a 50 % market share in the retail market if the number of broadband accesses sold is used as the basis for the calculation of market share. The group "Others" consists of more than 110 operators, of which many have registered with the NPT in the last couple of years.

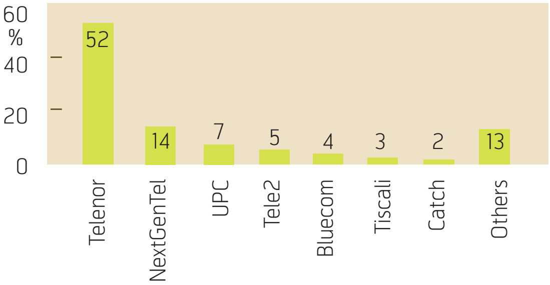


Figure 1 Market share in the retail market, based on volume (Source: NPT's telecom statistics based on reported figures for 2004 from the operators in the market)

ISSN 0085-7130 © Telenor ASA 2006

NPT's telecom statistics for the first half of 2005 show that Telenor's market share, based on volume, has risen to approximately 54 %. However, this share includes Tiscali, which is incorporated into Telenor's figures in 2005.

4.3 Regulation of LLU

In this section we will describe the regulation which is likely to apply for LLU in the near future and which must be assumed to be relevant for providers of OBAN services in general and Telenor in particular.

On 11 January 2006 NPT notified ESA, submitting draft decisions for market 11 (LLU) and market 12 (wholesale broadband access), which designate an undertaking with significant market power, impose new obligations and remove old ones. After having received comments from ESA, NPT made the decisions for these two markets on 20 February 2006. For the LLU market ESA had no comments.

Given the way in which market 11 is defined and delineated, Telenor has virtually a 100 % market share. Furthermore NPT has concluded that significant entry barriers exist in the LLU market. NextGenTel is by far the biggest operator on the demand side in the LLU market, accounting alone for more than 65 % of the unbundled loops that Telenor had sold by the close of 2004. Catch is an equally clear No. 2 operator in this market, measured by number of loops. The market analysis concludes that Telenor has significant market power in the LLU market.

After having assessed the appropriateness and proportionality of the remedies at its disposal as well as having evaluated the remarks of the commenting bodies and ESA, NPT has concluded that Telenor should be obliged to grant any reasonable request for access to the products wholesale unbundled access (including shared access) to metallic loops and sub-loops. Such access also includes access for co-location and information and support systems.

Telenor is also obliged to set the subscription charge for full and shared access in accordance with a price cap regulation that is to apply until 31 December 2007. These price controls involve a price cap of NOK 105 per month for full access with effect from 1 June 2006 and a price cap of NOK 95 per month with effect from 1 January 2007. This part of the decision has been appealed by Telenor. An obligation of cost accounting for full and shared access is also imposed on Telenor.

Furthermore, the access obligation is tied to non-discrimination, reference offer and transparency obligations.

5 Summary

The concept of open access networks present new regulatory challenges both to market actors and authorities. It is the responsibility of the providers to make sure they fulfil the regulatory requirements. The regulator's role is basically two-fold: On the one hand they usually act upon complaints and do not regulate unless considered necessary. On the other hand they analyse the various markets for electronic communications and may impose specific obligations on undertakings with significant market power.

To the concept of open access networks a regulator can help identify relevant regulatory issues and provide guiding input to the discussion of possible problem areas.

The main concerns are:

- To maintain secrecy on the content of electronic communications and others' use of electronic communications;

- And at the same time operate networks and services so that statutory access to information on end users and electronic communications is assured;

- Open access networks should not be introduced in conflict with local loop unbundling principle.

6 References

1 *The electronic communication act*. June 30, 2006 [online] – URL: http://www.npt.no/iKnowBase/FileServer/ekom_eng.pdf?documentID=7922

2 *The regulation on electronic communications*. June 30, 2006 [online] – URL: http://www.npt.no/iKnowBase/FileServer/ekomforskrift_eng.pdf?documentID=30917

3 *EC New regulatory framework directives* (starting with Framework directive). June 30, 2006 [online] – URL: http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm#reg

4 *Veiledning for tilbyderes overføring av opprinnelsesmarkering i forbindelse med nødanrop*, ver. 1.0. Post- og Teletilsynet, 1 desember 2005.

5 Schulzrinne, H, Marshall, R. IETF Draft: *Requirements for Emergency Context Resolution with Internet Technologies*, June 9, 2006. June 30, 2006 [online] – URL: http://www.ietf.org/internet-drafts/draft-ietf-ecrit-requirements-10.txt

Malin Tønseth graduated as a Master of Laws from the University of Copenhagen in January 1999. From 1999 to 2003 she worked as a lawyer in the law firm KromanReumert, Copenhagen. Malin Tønseth was awarded the Degree of Master of Laws in Information and Communication Technology Law from the University of Oslo in 2004 and following that she was associated with the University of Oslo, the Norwegian Research Center for Computers and Law as a Research Assistant and Guest Lecturer in IP-law. Since December 2004 Malin Tønseth has been working at the Norwegian Post and Telecommunications Authority as a Legal Advisor within the Department of Security and Preparedness in Networks.

email: mto@npt.no

Øystein Hoel received his Master of Business and Economics degree from the Norwegian School of Management (BI) in 1994. For the last ten years he has been working with regulatory issues in the telecom sector – both for Telenor ASA and the Norwegian Post and Telecommunciations Authority (NPT). He is currently with NPT, primarily dealing with issues related to the broadband market, regulatory accounts and other pricing issues.

email: oho@npt.no

Christian A. Nøkleby received his Siv.Ing. degree from the Norwegian University of Science and Technology (NTNU) in 2004. He was employed as a trainee in the Norwegian Post and Telecommunications Authority in September 2004 and is currently working in the Terminals and Networks Department. His main working areas are related to technical issues in public and private networks and services, including NGN, quality in public networks and services and emergency related issues.

email: chn@npt.no

Einar Meling is Senior Advisor at Norwegian Post and Telecommunications Authority (NPT). His work is mainly focused on development and implementation of the regulatory framework in both the postal and electronic communications areas. He received his law degree from the University of Oslo in 1991. Before joining NPT, Einar Meling was a lawyer at the Norwegian Civil Aviation Authority.

email: eim@npt.no

Runar Langnes has been Senior Advisor at Norwegian Post and Telecommunications authority since 2005. He received his Siv.Ing. degree from Agder University College in 1999. He has many years' experience from information and communication technology. In recent years his professional interests have been within communication security and mobile systems. His current field is security and preparedness in networks.

email: runar.langnes@npt.no

ISSN 0085-7130 © Telenor ASA 2006

Section 2 – Conceptual System Description

EINAR EDVARDSEN

Einar Edvardsen is Senior Adviser in Telenor R&I

We already see a number of commercial and non-commercial approaches to open access networks on the market. The most known example complying with our OAN definition is the Spanish FON[1] community initiative. Other examples are unsecured WLAN in general and a number of local community initiatives around the world.

In order to be able to understand the differences between the main categories of open access approaches this section addresses their architectures and explains their performance. The Unlicensed Mobile Access (UMA)-approach makes it possible for users with a dual-mode mobile phone handset (GSM and WLAN) to connect over WLAN instead of the GSM network. The UMA standard supports best effort voice communication and data communication restricted to the limitations given by the mobile network. Further details can be read in the paper *Using UMA to Realize the OBAN Vision* by John Charles Francis and Rico Schwendener.

The paper *The Open Access Network Architectural Paradigm Viewed Versus Peer Approaches* performs a comparison between a number of the best known OANs of today. An important aspect is to evaluate how these OANs deal with not only today's regulatory requirements, but also to see how future proof they are as regards potential new requirements.

The third article, *Architecture for Sharing Residential Access with Roaming WLAN Users*, gives an analysis of the architecture proposed by the OBAN project[2]. The OBAN approach differs fundamentally from the others since it focuses on solving a broader scope of challenges than any of the others. The main issue has been to design an architecture that provides mobile services with fast handover while maintaining agreed QoS and meeting all security related requirements from the regulator authority as well as users and other market players. A comparison between this approach and the others, however, is limping, because the OBAN approach is not yet commercial, while the others are available on the market.

[1] *http://en.fon.com*

[2] *http://www.ist-oban.org*

ISSN 0085-7130 © Telenor ASA 2006

Using UMA to Realize the OBAN Vision

JOHN CHARLES FRANCIS, RICO SCHWENDENER

John Charles Francis is Senior Project Leader at Swisscom Innovations

Rico Schwendener is Project Leader at Swisscom Innovations

Unlicensed Mobile Access (UMA) technology is potentially an alternative means to deliver OBAN-type services to the public over WLAN. The UMA effort was initiated in 2004 and is adopted by 3GPP, the main body responsible for enhancing cellular services. Connection to the fixed network occurs automatically when a mobile subscriber with a UMA-enabled, dual-mode mobile handset moves within range of an unlicensed wireless network such as WLAN to which the handset is allowed to connect. The technology was developed to offer a converged service for residential subscribers; however, in this article the possibility of extending the technology to offer the residential WLAN to public users is addressed.

The work reported in this paper was supported in part by the IST 6FP programme of the European Commission under contract OBAN, No. 001889 with the participation of Swisscom Innovations partially funded by the Swiss Bundesamt für Bildung und Wissenschaft.

1 Introduction

Unlicensed Mobile Access (UMA) [1] technology provides access to GSM and GPRS mobile services over unlicensed spectrum technologies, including Bluetooth and 802.11 (Wireless LAN). By deploying UMA technology, operators can enable subscribers to roam and handover between cellular networks and public and private unlicensed wireless networks using dual-mode mobile handsets. With UMA, subscribers receive a consistent user experience for their mobile voice and data services as they transition between networks. The UMA effort was initiated in January 2004 and is currently adopted by 3GPP, the main body responsible for enhancing cellular services. [2]

Connection to the fixed network occurs automatically when a mobile subscriber with a UMA-enabled, dual-mode mobile handset moves within range of an unlicensed wireless network to which the handset is allowed to connect. Upon connecting, the handset contacts the UMA Network Controller (UNC) over the broadband IP access network to be authenticated and authorized to access GSM voice and GPRS data services via the unlicensed wireless network. If approved, the subscriber's current location information stored in the core network is updated, and from that point on all mobile voice and data traffic is routed to the handset via the Unlicensed Mobile Access Network (UMAN) rather than the cellular radio access network (RAN).

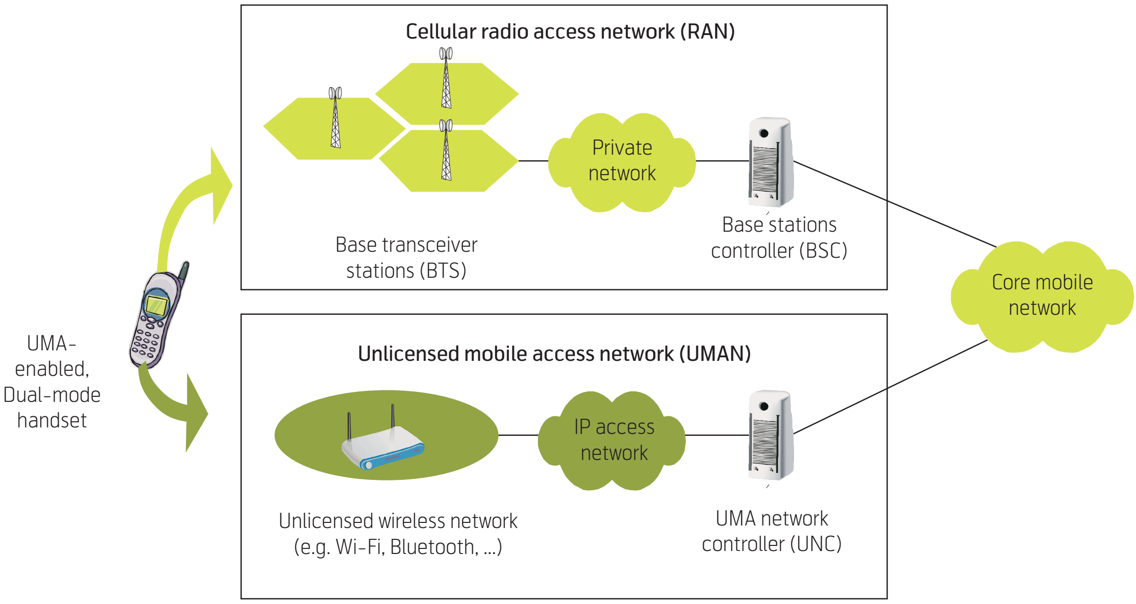

Cellular radio access network (RAN)
Private network
Base transceiver stations (BTS)
Base stations controller (BSC)
Core mobile network
UMA-enabled, Dual-mode handset
Unlicensed mobile access network (UMAN)
IP access network
Unlicensed wireless network (e.g. Wi-Fi, Bluetooth, ...)
UMA network controller (UNC)

Figure 1 UMA high-level architecture

ISSN 0085-7130 © Telenor ASA 2006

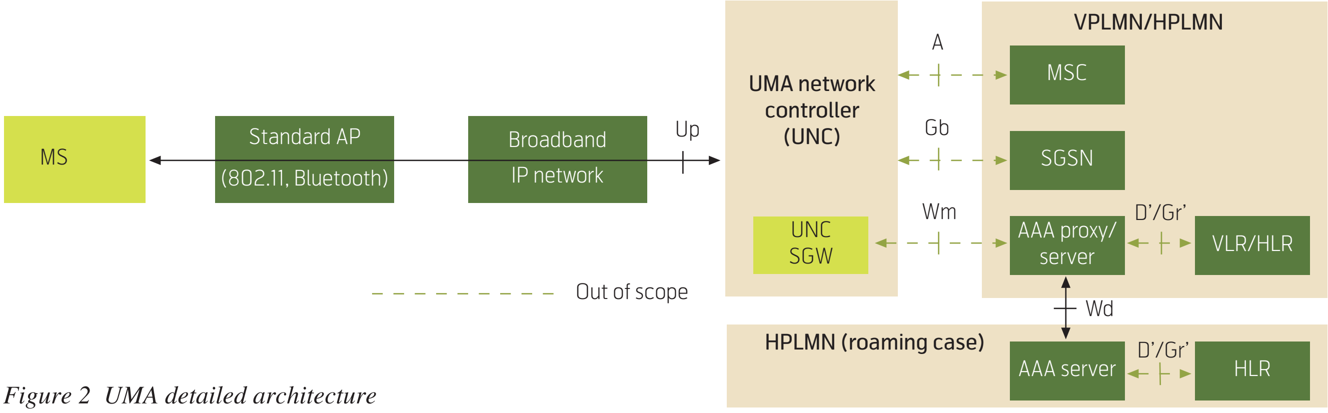


Figure 2 UMA detailed architecture

When a UMA-enabled subscriber moves outside the range of an unlicensed wireless network to which they are connected, the UNC and handset facilitate roaming back to the licensed outdoor network. This roaming process is completely transparent to the subscriber. If a subscriber is on an active GSM voice call or GPRS data session when they come within range (or out of range) of an unlicensed wireless network, that voice call or data session can automatically handover between access networks with no discernable service interruption. Handovers are completely transparent to the subscriber.

The high-level architecture of UMA is shown in Figure 1.

UMA is a possible way to realize an OBAN-like system that is tightly coupled with the cellular network. Accordingly, the scope of this article is to provide a high level description of this approach and to compare it with the mainstream approach of the OBAN project. We also attempt to identify the advantages and disadvantages of using UMA to realise the OBAN vision.

2 An OBAN architecture based on UMA

The UMA architecture is shown in more detail in Figure 2.

The following elements play a central role:

- A *Core Network* with cellular components including MSC, SGSN, VLR/HLR and AAA Proxy/ Server;

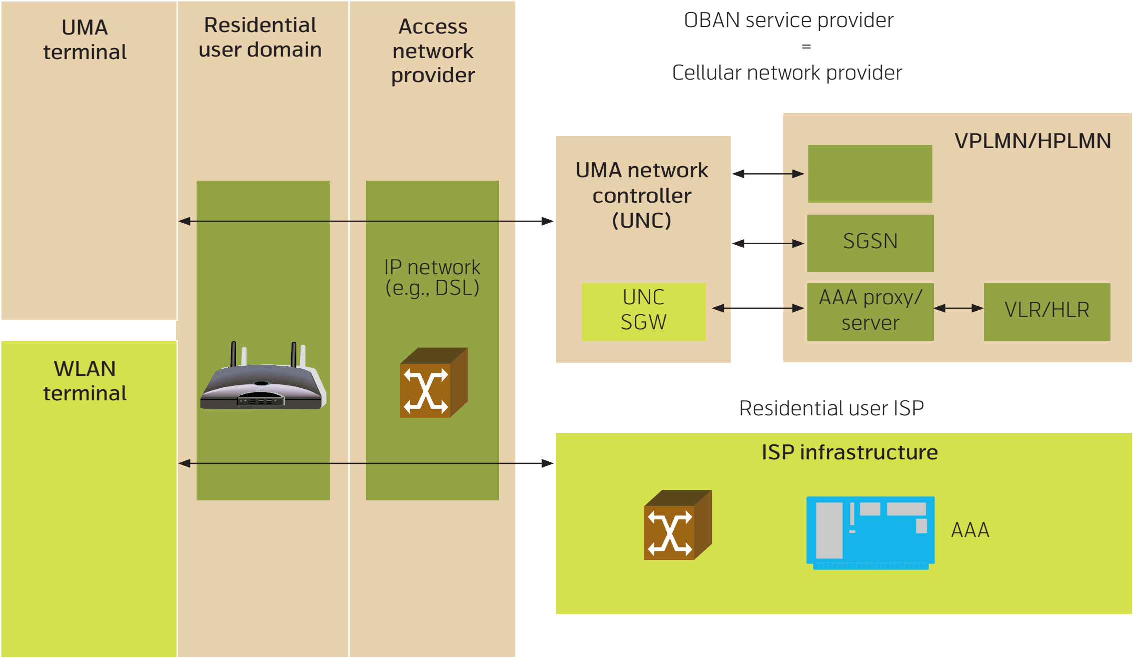


Figure 3 Allocation of technical functions to different roles for OBAN realisation with UMA

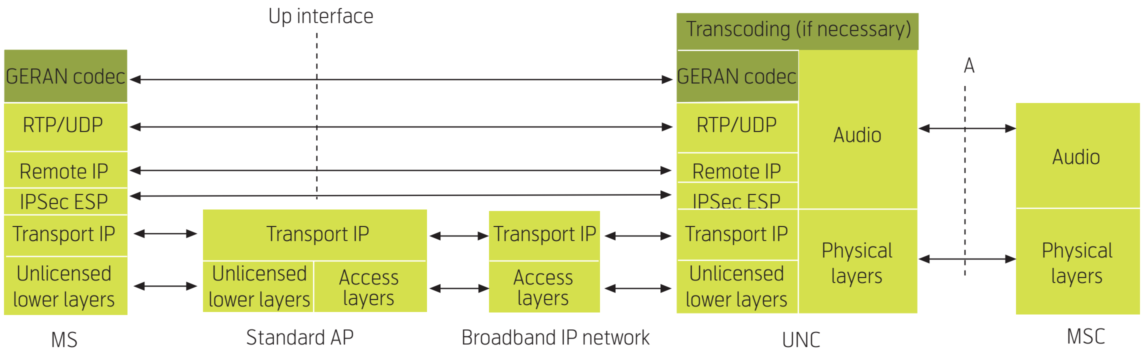


Figure 4 UMA CS domain voice bearer protocol architecture

- A fixed broadband *IP Network* that interconnects standard 802.11 Access Points;

- One or more *UMA Network Controllers (UNC)* that act as a "gateway" between the cellular core network and the broadband IP network, such that the UNC is at the same place in the architecture as a BSC in a traditional GSM network;

- *Terminals* that support the UMA protocol stack are required.

Subscriber authentication and billing with this solution is made using existing cellular components.

A possible allocation of the technical functions to the different business roles of OBAN (access network provider, residential ISP, OBAN service provider, etc.) is shown in Figure 3. In the residential and IP network, the OBAN traffic and the residential user traffic are transported by the same infrastructure. In the upstream direction, the IP layer (i.e. IP destination address) at the access network provider directs OBAN traffic to the cellular operator and residential traffic to the residential user ISP. In the downstream direction, the IP layer (i.e. IP destination address) in the Access Point directs OBAN traffic to the UMA terminal.

The OBAN traffic is secured on the IP link in the residential user domain and in the access provider domain by standard UMA methods, namely a second "Remote IP" layer is used above an "IPSec ESP" layer on top of the "Transport IP" layer, which is the IP layer supported in the Access Point and in the broadband IP access network. This layering is shown in Figure 4 for the CS (Circuit Switched) voice user plane.

Mobility and security aspects of UMA are performed using the procedures of cellular networks, complementing them with some specifications for unlicensed wireless access. The required procedures for mobility and security in the cellular network are implemented in the signalling plane on the core network side of the UNC. The interesting and relevant aspects are specified in layer 3 of the signalling plane. The signalling layer 3 for non-GPRS services in cellular networks is composed of three sub-layers comprising the Radio Resource Management (RR), Mobility Management (MM) functions and Connection Management (CM)

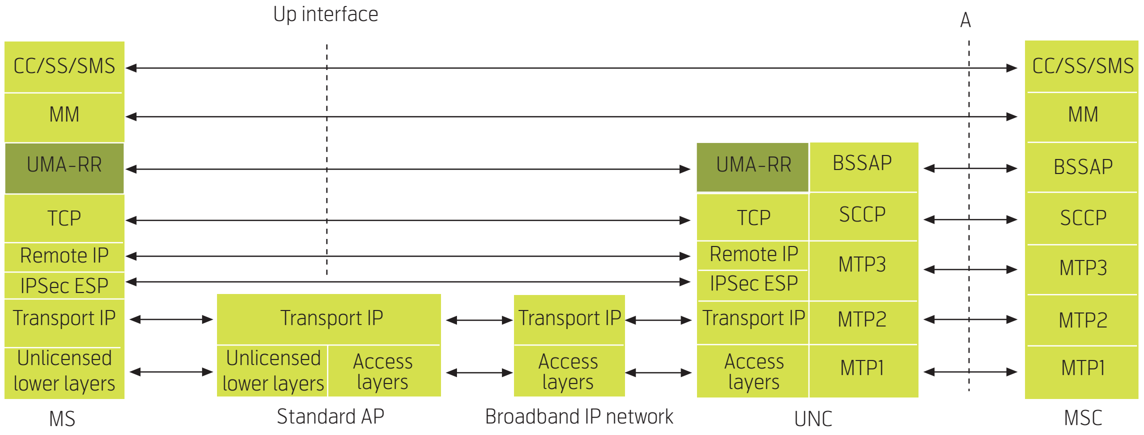


Figure 5 Up Signalling Protocol Architecture for CS Domain

ISSN 0085-7130 © Telenor ASA 2006

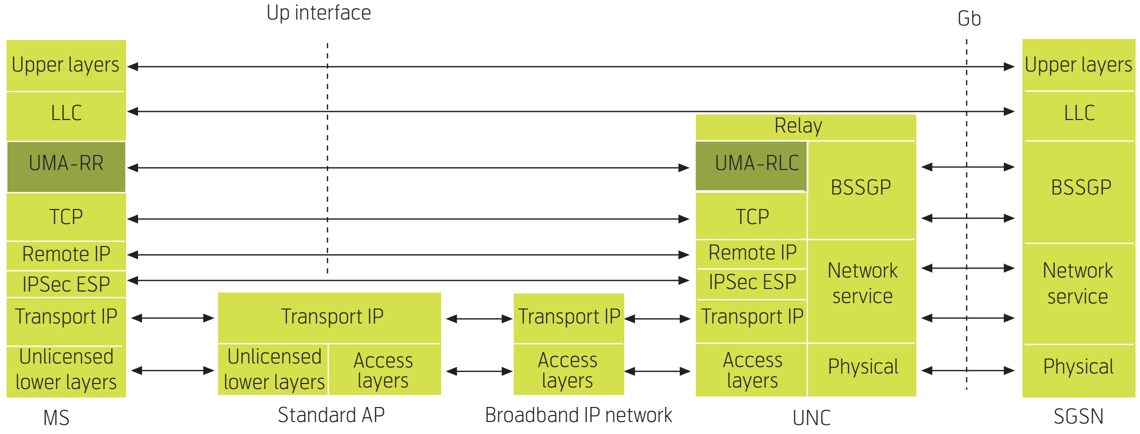


Figure 6 Up *GPRS Signalling Architecture*

functions. The latter contains functions for the control, provision, and support of services offered by the network and consists of Call Control, Supplementary Services Control and Short Message Service Control. UMA signalling reuses existing cellular specifications where possible. The *Up* protocol architecture in support of CS signalling (i.e. non-GPRS services), as well as UMA-specific signalling, is illustrated in Figure 5.

The salient features of this part of the *Up* interface with respect to the CS domain are as follows:

- The GSM protocols MM and above are carried transparently between the MS and MSC. This allows the MS to obtain through the UMAN all GSM services that it would normally receive through a GSM BSS.

- The GSM-RR protocol is replaced with a UMA-RR protocol. The unlicensed radio link presents different characteristics from that of the licensed GSM radio link, so the UMA-RR protocol is customized to take advantage of these characteristics. As in a GSM BSS, the UNC terminates the UMA-RR protocol and inter-works it to the A-interface using BSSAP messaging.

- Security of UMA traffic on the IP link is assured by a "Remote IP" layer above the "IPSec ESP" layer on top of the "Transport IP" layer.

For GPRS, the cellular protocols are again reused. The *Up* protocol architecture in support of GPRS signalling is illustrated in Figure 6.

The important features of the *Up* interface here are as follows:

- The GPRS LLC PDUs for signalling and higher layer protocols are carried transparently between the MS and SGSN. This allows the MS to obtain all GPRS services as if it were connected to a GERAN BSS.

- The GPRS-RLC protocol is replaced by an equivalent UMA-RLC protocol. As in a GERAN BSS, the UNC terminates the UMA-RLC protocol and inter-works it to the *Gb*-interface using BSSGP.

- Security of UMA traffic on the IP link is assured as in the CS domain.

3 Comparison of UMA with Conventional OBAN

The 'conventional' architecture for OBAN developed by the IST OBAN project is described elsewhere in this issue. A comparison of that approach with OBAN based on UMA is made in Table 1.

4 Conclusions

UMA technology can be reused to provide OBAN services. This would currently enable the following services to be provided to OBAN visitors[4)]:

- GSM 9.6 / 14.4 kb/s for voice.

- GPRS for data: 171 kb/s using 8 timeslots with 21.4 kb/s in theory, 30–40 kb/s downstream and 10 kb/s upstream in current practice. Services would include data link to Internet or Intranet, Email, MMS, chat, location-based information, community applications and WAP.

- EDGE ("enhanced GPRS"): would offer higher data rates of 150–200 kb/s

Feature	Conventional OBAN	OBAN via UMA
Basic architecture	Pure PS architecture for IP traffic. No separation of user traffic and signalling traffic specified so far.	Different architecture for CS and PS traffic. Separate user traffic (voice, data) and signalling traffic at core network side of UNC.
Architecture for user data	IP network based on routers. MIP encapsulation between Foreign Agent in RGW and Home Agent at OBAN service provider.	Different solution for CS and PS traffic. *Circuit Switched:* - "Traditional" 2G CS core network (MSCs). - IP Access: GERAN Codec from MS to UNC, transported using RTP/UDP/Remote IP/IPsec ESP on top of transport IP layer. Standard A interface protocols between UNC and MSC. *Packet Switched:* - "Traditional" 2G PS core network (SGSN, GGSN). - IP Access: Transparent transport of GPRS LLC PDUs (carrying data and higher layer protocols) between MS and SGSN. LLC is transported from MS to UNC over UMA-RLC[1] / UDP/ Remote IP / IP sec on top of the transport IP layer. Standard Gb interface protocols from UNC to SGSN. Note: Transparent transport of IP traffic between MS and GGSN.
Signalling architecture	Four types of signalling traffic are present: MIP signalling, Card signalling, authentication signalling, QoS signalling. *MIP signalling* (IP traffic) of MIP agents between RGW and OBAN service provider, passing through RGW, access network provider and residential user ISP. *Card signalling messages* are exchanged between terminal, Card proxy at RGW and the Mobility Broker. *Authentication signalling* between terminal and residential user ISP (EAPoL between terminal and RGW, IP traffic between RGW and residential ISP), passing through RGW and access network provider. *QoS signalling* between terminal, QoS broker in the RGW and AAA server at the OBAN service provider.	Different solution for CS and PS traffic. *Circuit Switched:* - "Traditional" 2G CS core network (MSCs) - IP access: Transparent transport of Mobility Management between MS and MSC. Mobility Management is transported from MS to UNC over UMA-RR[2] / TDP/ Remote IP/ IP sec ESP on top of the transport IP layer. Standard A interface protocols from UNC to MSC. *Packet Switched:* - Traditional" 2G PS core network (SGSN, GGSN). - IP access: Transparent transport of GPRS LLC PDUs (carrying GPRS Mobility Management between MS and SGSN. LLC is transported from MS to UNC over UMA-RLC[3] / TCP / Remote IP / IP sec ESP on top of the transport IP layer. Standard Gb interface protocols from UNC to SGSN.
Mobility	Mobile IP: Foreign Agent in RGW, Home Agent at OBAN service provider, Gateway Foreign Agent at residential user ISP.	Cellular mobile radio interface signalling layer 3 mechanisms (Mobility Management, Radio Resource Management, ...), complemented for unlicensed mobile access over IP with UMA-RR for CS and with UMA-RLC for PS traffic.
Authentication	Authentication Gateway with access control in RGW, AAA proxy at residential ISP, AAA server at OBAN service provider, Accounting tunnel from RGW to OBAN service provider. Client authentication based on EAP/802.1x, and Kerberos ticket based authentication after handovers.	EAP-SIM authentication for IP link from terminal to UNC. Standard cellular authentication procedure: SIM card (key Ki), VLR, HLR, AUC (key Ki). Authentication messages transported in separate signalling plane (at core network side of UNC). Traffic encryption (to secure wireless link).
QoS	Resource management: Resources are allocated on a terminal basis. A QoS broker at the RGW is responsible for maintaining QoS guarantees. Traffic prioritisation is based on priority queuing and WLAN QoS classes (802.11e).	QoS in core network guaranteed for CS services. However, no QoS solution specified in UMA for the IP access. As a consequence, the specification for an end-to-end QoS guarantee is missing.

Table 1 Comparison of conventional OBAN and UMA approach

[1] *UMA specific protocol*

[2] *UMA specific protocol*

[3] *UMA specific protocol*

[4] *Services requiring QoS only, if a suitable QoS mechanism is available on the IP network.*

In principle, the data services listed above may be provided at higher bandwidth. Enhancements of UMA technology are handled by 3GPP.

UMA has the advantage compared to the conventional OBAN approach that best-effort GSM and GPRS services can be provided without the need to develop additional specifications. In principle, conversational services such as voice can be provided by UMA under the assumption that the broadband access (fixed network and WLAN) has the needed QoS mechanisms. Accordingly, short term realization should not be an issue. Broadband services with bandwidths higher than GSM/GPRS/EDGE require sufficient capacity in the cellular core network, however. In consequence, a potentially expensive upgrade to the cellular core network components such as SGSN, GGSN may be required.

In conclusion, UMA is in principle a good solution to implement the OBAN vision, but for services at higher bandwidth the cost of a cellular core network upgrade may be a limiting factor. The loosely coupled solution envisaged by the OBAN project is likely the less expensive option for higher bandwidth services.

References

1 *Unlicensed Mobile Access (UMA)*. 2006, November 30 [online] – URL: http://www.umatechnology.org/

2 3GPP. *Radio Access Network. Generic access to the A/Gb interface*. June, 2006. (3GPP TS 43.318)

John Charles Francis is Senior Project Leader at Swisscom Innovations and holds a PhD in Electrical & Electronic Engineering. He has been active in the field of 3G mobile standardisation and his current research interests include systems beyond 3G. In addition to work for innovation projects, he has supported Swisscom UMTS and WLAN hotspot deployment and has coordinated Eurescom consortia in the mobile area. Within the OBAN project, he leads the work package for scenarios and requirements.

email: JohnCharles.Francis@swisscom.com

Rico Schwendener is Project Leader at Swisscom Innovations. He holds a PhD in Technical Science and a post-diploma degree in Information Technology. He has been active in the field of network modelling for carrier grade networks. His current research interests cover Open Broadband Access Networks, QoS in mobile networks, and cross-layer optimizations. In addition to work for innovation projects, he supports the Swisscom Triple Play architecture development.

email: Rico.Schwendener@swisscom.com

The Open Access Network Architectural Paradigm Viewed Versus Peer Approaches

MUSLIM ELKOTOB, HERBERT ALMUS, SAHIN ALBAYRAK, KLAUS REBENSBURG

Muslim Elkotob is Research Engineer and Doctoral Candidate at DAI-Labs, TU-Berlin

Herbert Almus is Deputy Head of Inter-departmental Research Center at TU-Berlin

Sahin Albayrak is Professor at DAI-Labs, TU-Berlin

Klaus Rebensburg is Director of Inter-departmental Research Center at TU-Berlin

Currently, the demand for wireless ubiquitous connectivity is increasing; moreover, as new types of applications and services emerge, the need for more bandwidth is steadily growing too. All of this promotes broadband deployment, integration with other access technologies, and additionally paves the way for new paradigms which solve the modern communication requirements of users. Among the paradigms currently successful and promising are Open Access Networks and Wireless Mesh Networks. OBAN (Open Broadband Access Network) [3] is the leading solution in the OAN trend. On the other hand, competing solutions are emerging especially 'quick-and-dirty' drafted models which are trying to penetrate the market. Among those solutions is FON [4], whose core idea is identical to that of OBAN, but which only focuses on establishing a circle-of-trust among private users so as to increase the number of coverage spots. OBAN on the other hand focuses on supporting seamless handover, quality of service awareness and a sufficient level of security for residential as well as roaming users. This article analyzes from an architectural as well as a functional perspective the different trends and points out pros and cons of peer approaches compared to OBAN.

1 Introduction

As the migration trend from wired towards wireless networks increases, and due to the improvements occurring in coverage range and capacity, in addition to the booming in the number of new network access technologies driven by user demand and the profit-quench of operators, new paradigms start to emerge to incorporate all of this. The main driving forces behind the 'Open Access Networks' paradigm are the need to have a generic scheme which is able to constantly incorporate upcoming network access technologies, the so-called Next Generation Networks (NGN) trend, and the growing demand for connectivity, bandwidth, as well as ubiquity support. Mobility and coverage on the other hand is a trade-off with capacity or data rate as shown in Figure 1.

The figure really paves the way for justifying the need for new paradigms such as Open Access Networks which in fact aim at providing sufficient capacity, close to broadband and also at the same time be able to support full user mobility, providing

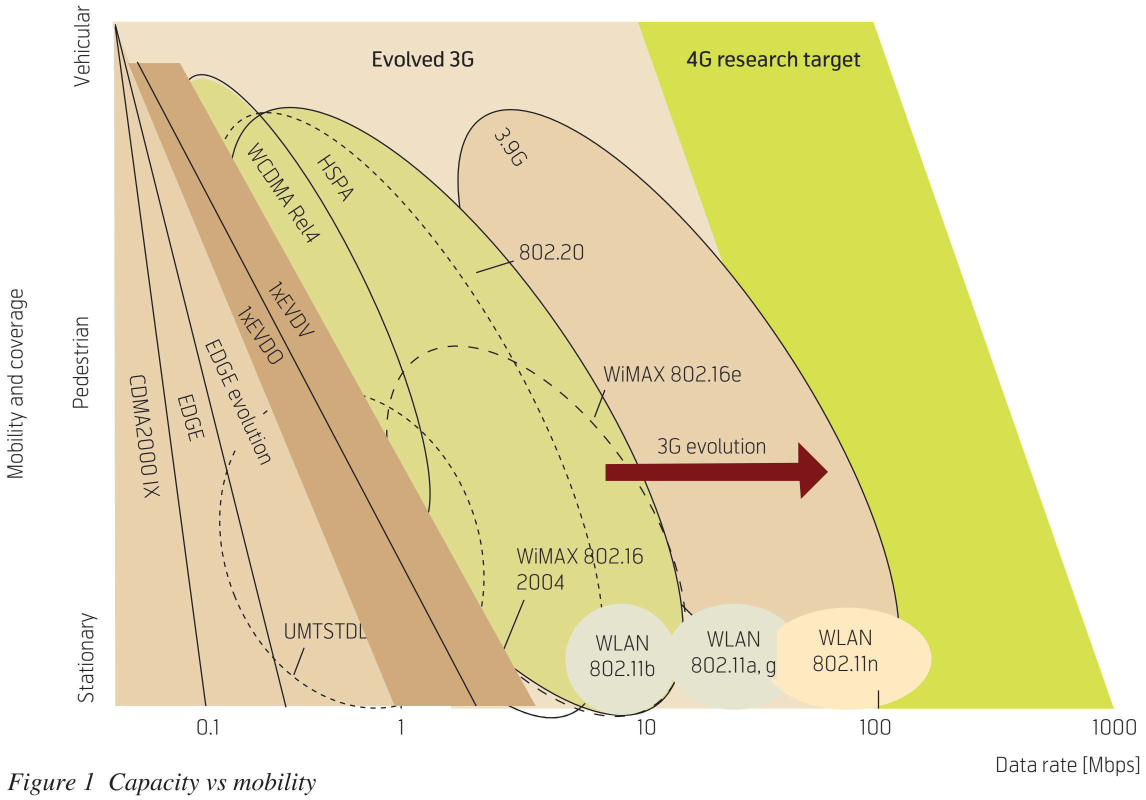


Figure 1 Capacity vs mobility

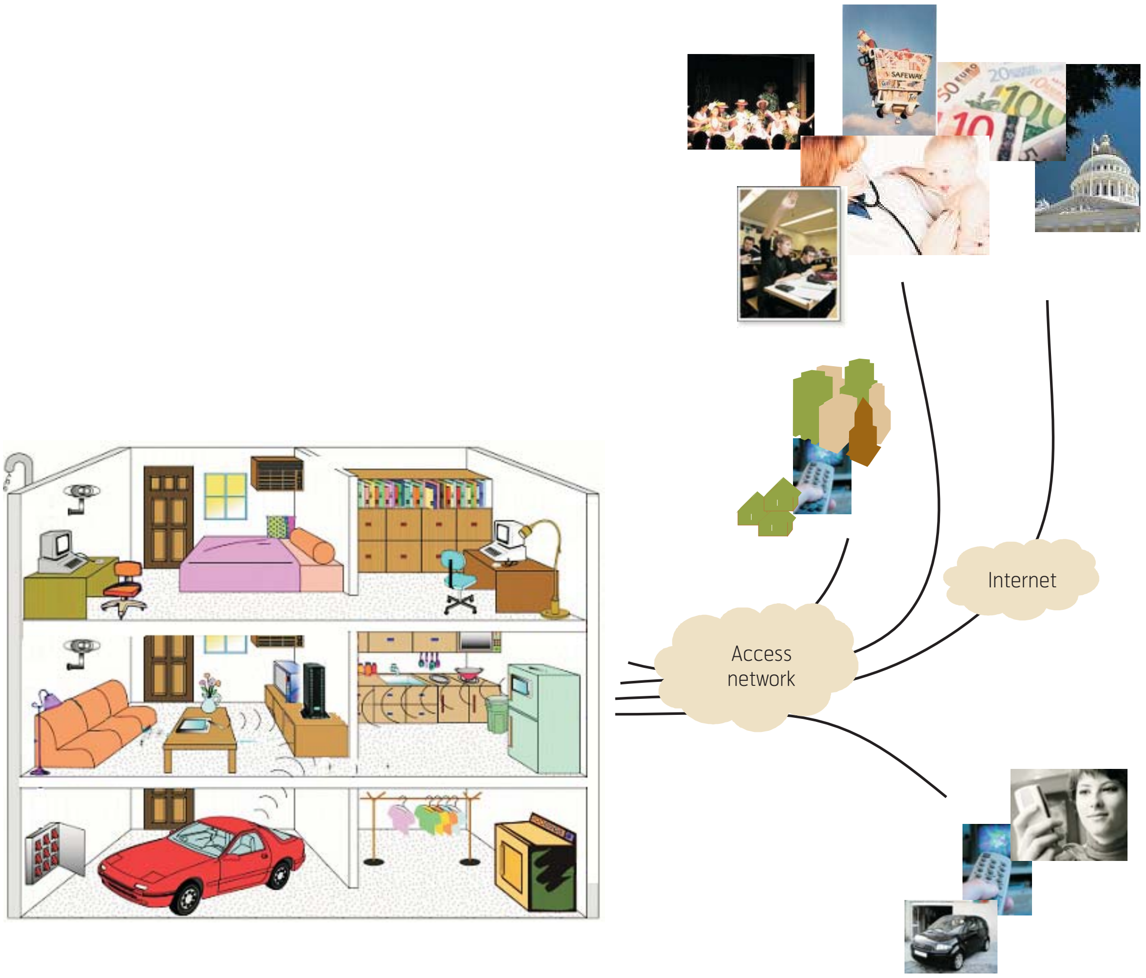


Figure 2 Broadband at home promotes ubiquity for mobile users

fast handover, session and service continuity on the move, and so on. Architectures therefore which make networks open, and then provide broadband connections to roaming users with sufficient QoS, Mobility and Security solidify in OBAN [3] as one of many efforts in this direction [4][10][15][20]. Other peer approaches aim at this as well, but they have very simplistic business models and are far from getting towards this particular vision. This article will provide insight into where each approach fails, what it focuses on, how well it serves its subscribers, and what it provides them with.

Building new specialized infrastructures for each upcoming technology is a challenge in itself, and it is starting to fail more and more over the long run. Moreover, even if such a thing succeeds, it is very hard to keep shifting customer bases from one technology to another, thus guaranteeing stable profits. As a result, operators have to turn to strategies which support evolution, reuse of infrastructure in an efficient and smart fashion, and also to making networks open. Due to the fact that internet has reached almost every home using mainly broadband lines, providing users with ubiquity can barely avoid using bandwidth from home networks. The global spread of the internet and the expansion of broadband deployment have led to using the home as a private connected spot as well as a ubiquity provider for roaming users. This is outlined in Figure 2.

After this introductory chapter, the next chapter will, from an architectural and functional point of view discuss the open access networks paradigm and also point out key services and look at the potential of this paradigm. Chapter 3 analyses in detail peer approaches which are in fact a sort of rivals because they aim at achieving the same vision, but fail at one point or another since they follow a pretty simplistic approach. Chapter 4 then compares aspects of different approaches and points out pros and cons. Finally Chapter 5 concludes this article.

2 Open Broadband Access Networks

2.1 Open Access Networks: Architectural Insight

With the promotion and expansion of broadband, it is pretty certain that the majority of private residences will soon have access to a broadband network over ADSL, VDSL, fibre, cable, or even radio, and that wireless technology will be the winning technology for in-house communication both for residential and business users. In urban areas, all these micro base stations will form continuous radio coverage allowing users to roam through the landscape while maintaining their communication sessions. Compared to conventional cellular mobile networks consisting of a limited number of optimally located outdoor base-stations and antenna masts, the OBAN network will consist of a much higher number of micro base stations randomly located. As Figure 3 shows, users can continuously roam in OBAN through a sufficiently dense metropolitan area and rely on other network access technologies as backup or umbrella cells. Suitable candidates are WiMax and UMTS to bridge WLAN coverage gaps. OBAN has already proposed architectural designs showing how WLAN-interconnected cells forming the core of OBAN can inter-work with peer technologies. This research issue is being analyzed within IEEE [21], 3GPP [22], and other bodies, but in a more generic fashion. OBAN on the other hand, proposes a concrete and specific solution in terms of WiMax and UMTS inter-working with the WLAN-based architecture [27]. This issue distinguishes clearly OBAN from its peer rivals such as FON or Boingo where integration or co-working with other systems and technologies is either out-of-the-question or totally decoupled from the logic or the architecture of the system.

The visitors and the stationary users will share the capacity of wireless LANs and access lines according to a general service agreement between all users and the network operator. This justifies the term ‘Open’ within the open access network paradigm. Promoting broadband, opening networks for access, enabling evolution and integration and inter-working with further access technologies are the driving forces behind all initiatives discussed in this article.

Now we will take an architectural look inside OBAN with its three key pillars: mobility, quality of service and security.

2.1.1 Mobility

OBAN uses a hybrid mobility approach combining SIP and Mobile IP underneath, and making use of strengths from both approaches. OBAN’s mobility architecture is highlighted below:

In contrast to hotspot architectures used by some operators for additional revenues today [6], [29], OBAN supports full mobility. hotspot architectures select some strategic sports where they place at very high prices certain access points with a pre-calculated capacity intended to serve users e.g. at a café, airport, hotel and so on. In addition, there are many well known operators offering UMTS or GPRS cards for ubiquitous mobility; this is nevertheless narrowband connectivity despite the fact that it is ubiquitous. OBAN focuses on combining broadband connectivity and mobility aspects with seamless handover, which is a challenge in itself. By deploying regional elements in the backend such as a mobility broker seen in Figure 4, it is possible to improve cooperation and coordination between neighbouring access points so that they can perform proactive measures to shorten handover times and improve resource utilization. With the help of the Candidate Access Router Discovery (CARD) [23] protocol, communication between clients and access points on residential gateways, gateways and the mobility broker (backend) is enabled.

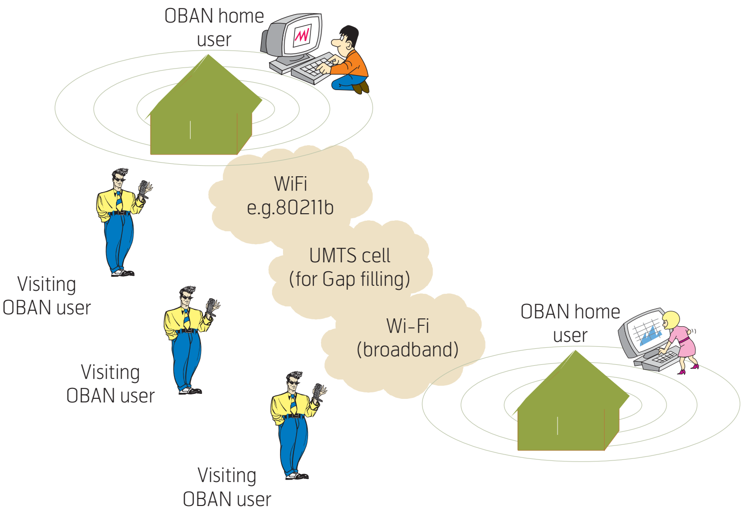


Figure 3 Roaming in Open Access Networks

Furthermore, due to the fact that today both IP-layer mobility using Mobile IP [24] and application-layer mobility using the Session Initiation Protocol (SIP) are well known, we decided to utilize an optimized combined or hybrid mobility scheme. This scheme runs using elements and components shown in Figure 4.

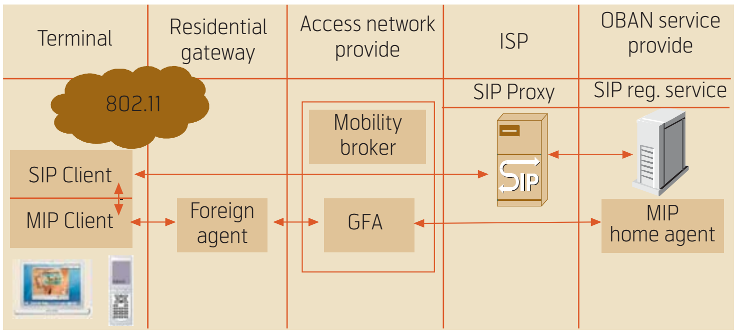
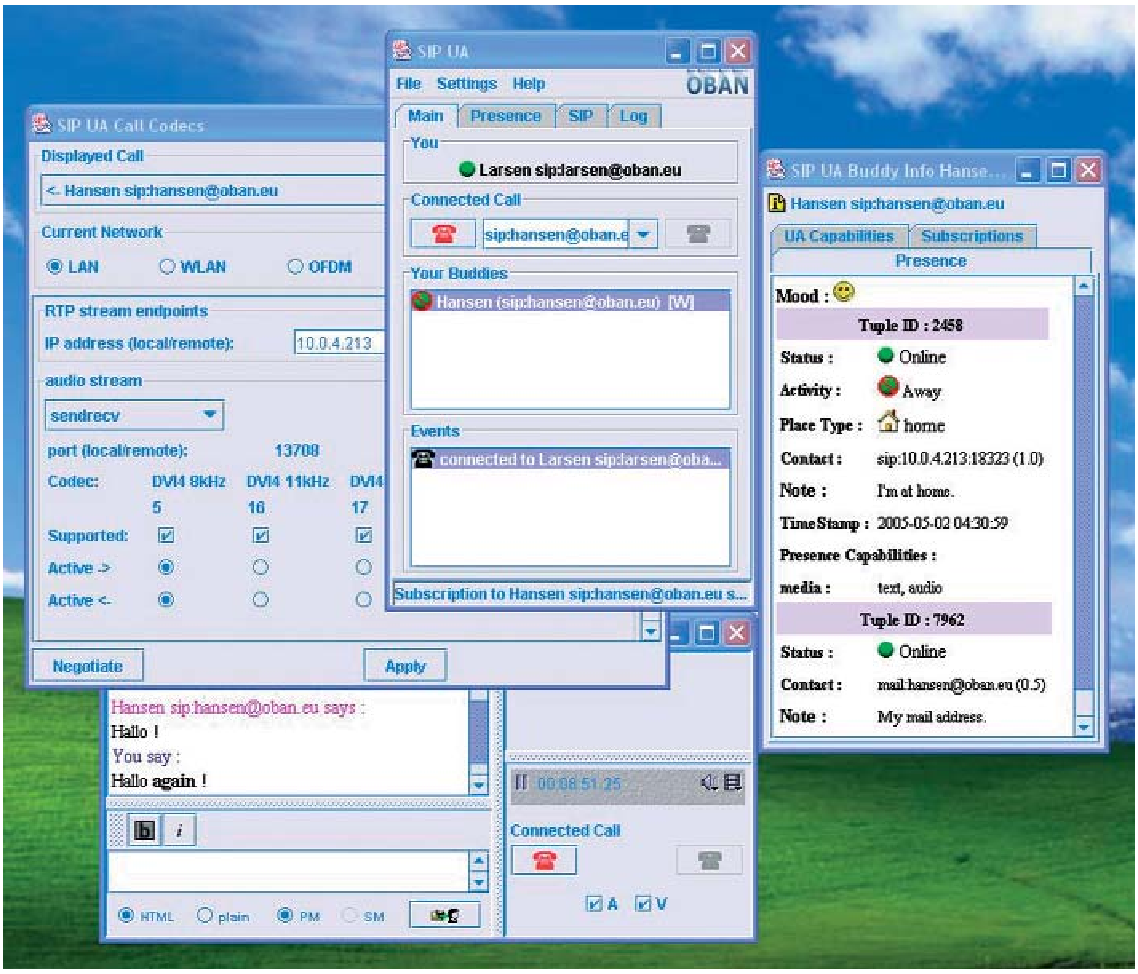


Figure 4 OBAN SIP MIP Mobility Architecture [7], [8], [28]

ISSN 0085-7130 © Telenor ASA 2006



<- Hansen sip:hansen@oban.eu

● LAN ○ WLAN ○ OFDM

IP address (local/remote): 10.0.4.213

sendrecv

port (local/remote): 13708

Codec:	DVI4 8kHz	DVI4 11kHz	DVI4
	5	16	17
Supported:	☑	☑	☑
Active ->	●	○	○
Active <-	●	○	○

● Larsen sip:larsen@oban.eu

sip:hansen@oban.e

Hansen (sip:hansen@oban.eu) [W]

connected to Larsen sip:larsen@oba...

Subscription to Hansen sip:hansen@oban.eu s...

Hansen sip:hansen@oban.eu

Mood :

Tuple ID : 2458

Status : Online

Activity : Away

Place Type : home

Contact : sip:10.0.4.213:18323 (1.0)

Note : I'm at home.

TimeStamp : 2005-05-02 04:30:59

Presence Capabilities :

media : text, audio

Tuple ID : 7962

Status : Online

Contact : mail:hansen@oban.eu (0.5)

Note : My mail address.

Hansen sip:hansen@oban.eu says :
Hallo !
You say :
Hallo again !

● HTML ○ plain ● PM ○ SM

00:08:51:25

Connected Call

☑ A ☑ V

Figure 5 OBAN Multimedia client for audio, video, text, with an OBAN-specific session adaptation mechanism

Fast handover and network selection decisions are made by Mobile IP in coordination with certain security components using tickets and in association with the Candidate Access Router Discovery protocol also mentioned in the section to follow. On the other hand, SIP has very powerful session adaptation capabilities especially for multimedia communication. Information such as used media types, formats, CODECs, compression rates, pixel stretch or multimedia playback frame rate can be adjusted in SIP. Due to the fact that we assume users will use Voice over IP as a basic telephony service, in addition to streaming media content whether music, video clips from news sites or whatever, OBAN provides an own developed multimedia client, namely a SIP client (depicted in Figure 5) which takes care of this for the end-device by talking to a SIP proxy which in turn communicates with the backend.

Access point coverage ranges are small, so mobile users switch quite frequently between different access points. For this reason, session re-adaptation is necessary to keep up the good user experience and preserve consistency of the service. The mobile IP client we use provides an API towards the application layer where we integrate our SIP client. In this way, the SIP client is able to receive regular updates on network condition parameters as well as on handover decisions so that it can act accordingly.

We distinguish between three significant cases:

- When mobile IP performs a handover, and from the network context it is known that very shortly another handover shall take place, then the SIP session is left intact (audio and video, VoIP), and upper layer traffic is simply tunnelled over Layer 3.

- When the duration of stay within a particular WLAN cell is moderate, then only location update is performed within the SIP re-invite for the upper layer traffic.

- In case the duration of stay in a particular cell is long enough, above 15 seconds for example, then even a SIP re-invite with multimedia session parameter update (complete SDP [14] update) can be done, adjusting the multimedia parameters to current network conditions and user preferences.

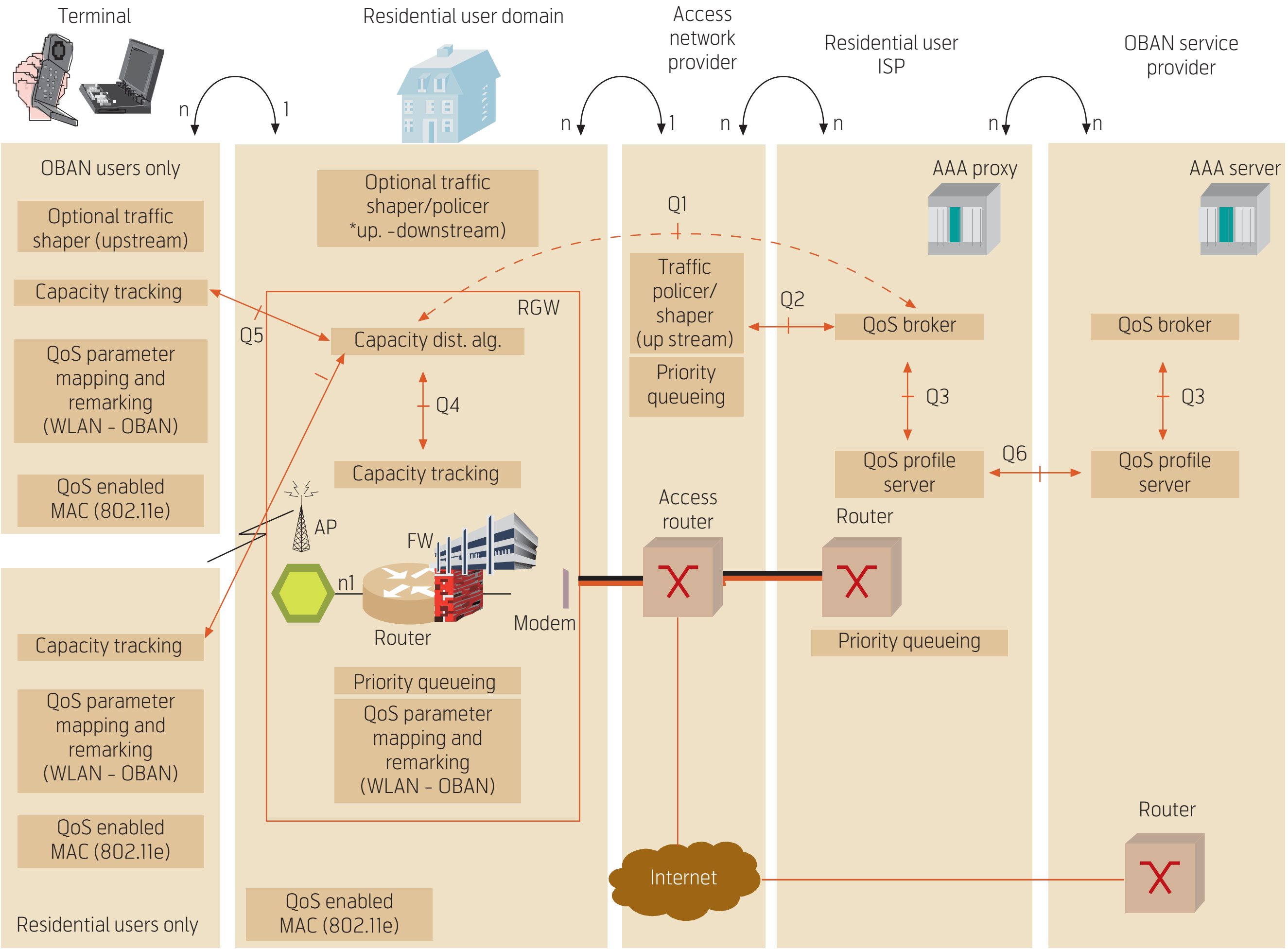


Figure 6 OBAN Quality of Service Architecture; source [7]

2.1.2 QoS Architecture

The Open Broadband Access Network has one of its key goals to provide an acceptable level of user-perceived QoS for various traffic types and services used by subscribers. Multimedia QoS management in wireless networks is a challenge in itself due to stringent requirements on delay, jitter, and throughput, all under complicated channel conditions and varying available resource profiles.

Despite the fact that OBAN makes use of existing telecommunication infrastructure, thus avoiding immense setup and hardware costs, it still offers a very solid mechanism for resource distribution and maintenance for wireless clients. One way in which OBAN pioneers at the moment is with its support for various traffic classes, customer classes with different profiles, different levels of QoS, in addition to various adaptation and optimization strategies as queuing, capacity redistribution, load balancing, and brokerage. Due to the fact that OBAN offers an integrated client environment, it is ensured that the components on the end device function in harmony and also interact when needed with network-side components mainly those on the residential gateway they are associated with.

Functions on the client include tracking of capacity, monitoring, mapping of parameters, remarking, and communication with the gateway for information and parameter exchange. The various functions are highlighted in Figure 6. The core QoS functionality within OBAN takes place at the residential gateway which is also offered to subscribers as an integrated box. The residential gateway maintains capacity balance or border-line between visiting or roaming users associated with the publicly broadcast SSID and the home subscribers which also have a residential gateway attached to their home internet connection and which use a private SSID.

As Figure 6 shows, just as in other typical Internet Service Providers (ISP), traffic shaping as well as user profiling, contract management, information storage, and brokerage at a high level are done partly in the backend. Moving closer to the front end, namely towards the Access Network Provider (ANP), OBAN starts to deal with traffic shaping and policing issues in order to efficiently use its network resources and also ensure consistency in service delivery and user differentiated treatment.

Due to the fact that the wireless medium is a shared one, a sufficient degree of fairness is required to have a consistent way of accommodating several users using various applications and having different customer classes. For this OBAN has developed a Capacity Distribution Algorithm (CDA) [25] which distributes the shared medium resources among clients. When clients join, and if capacity becomes a bottleneck as is mostly the case in wireless, then the CDA has to redistribute resources among already connected clients or in some cases perform admission control, reading the QoS requirements of a mobile station willing to join and deciding whether or not to grant it the permission to join. This is all done via interactive communication periodically performed between the CDA on the RGW and the attached clients. Dynamic maintenance and update of connection Service Level Agreements (SLA) is a feature where OBAN far outweighs its open access services offering rivals such as FON.

2.1.3 Security in OBAN

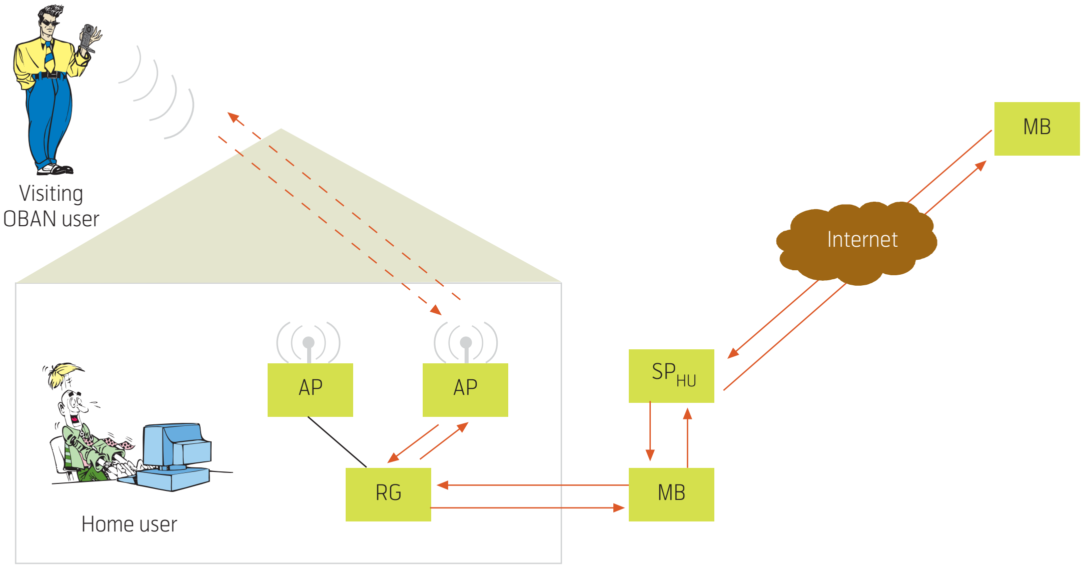
Security as well as data privacy is another requirement in open access networks. Especially when such access is offered as a commercial service, certain regulatory requirements have to be fulfilled. Regarding security and data privacy the EU directive on privacy and electronic communications defines rules for the protection of privacy and personal data in relation to communications over public communication networks (2002/58/EC).

To fulfil the security requirements an authentication of users is one of the essentials. In a stationary WLAN environment like a hotspot, this can be done based on different well-known and acceptable mechanisms, but OBAN supports mobility providing seamless connectivity while moving between WLAN access points. This does not only require the possibility to continue to use already established IP connections and VPN tunnels, in addition a (re-) authentication at the newly joined access point has to take place for security reasons.

A typical traditional authentication process requires that the user authenticates to his service provider (SP), since only his SP can verify his credentials. In a multi-ISP scenario like OBAN, the visiting users (VUs) are expected to authenticate with the OBAN service provider (OSP), but are connected via the residential network of the home user (HU) which normally will have network access based on a different service provider (SP_{HU}). Therefore the SP_{HU} must act as a proxy towards a AAA server in the domain of the SP of the visiting user (SP_{VU}). The multiple roundtrip delays introduced by the required communication between the several servers alone will lead to delay times exceeding the acceptable total handover delay of maximum 120 ms.

Because of this, OBAN invented a new approach, based on already existing trust relations, extended by a Kerberos-style ticket mechanism. Only when a terminal initially joins the OBAN network, a full authentication will be executed. In OBAN the method EAP-SIM [18] has been chosen as the method to be used. The full authentication is expected to take a substantial amount of time, but this is considered to be acceptable because it just takes place once. The shared secret, which is established during full authentication, is used as a basis to create Kerberos-style tickets used to authenticate during handover.

In addition, the ticked-based solution could have been realized based on typically existing infrastructure but uniquely in OBAN a Mobility Broker (MB) entity has been introduced for various reasons and it is heavily involved in the authentication mechanism.

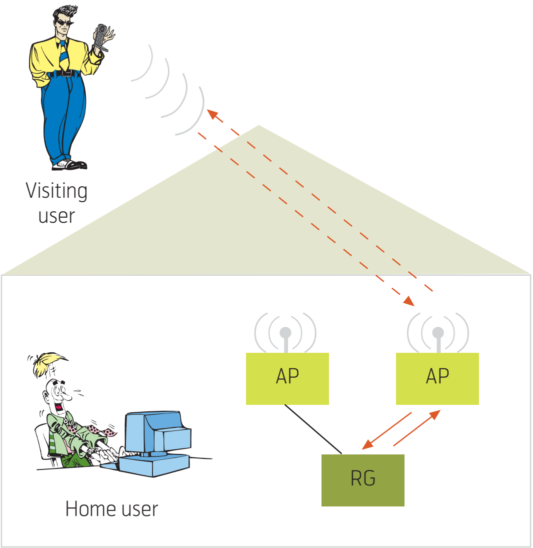


The MB has a direct trust relation with all Internet Service Providers, serves as a AAA proxy to the OSP, issues tickets and has detailed knowledge regarding geographical location.

Another essential component in OBAN is the Residential Gateway (RGW), which is located at the home user's site and contains a Radius proxy (acting as proxy towards the MB) as well as a module called "EAP-OBAN end point", responsible for verifying the Kerberos tickets.

2.2 Authentication in detail – but never less simplified

Upon completion of the initial full authentication, the terminal will issue a request to establish a shared secret between itself and the MB. The request is forwarded by the RG, which already has a trust relation to the MB. To establish the shared secret the terminal will initiate a new EAP-SIM authentication directly towards the MB. Next the MB will issue a Ticket-Granting-Ticket (TGT) to the OBAN user (terminal). The OBAN user will use the TGT to request an access ticket for an RGW (TRGW) considered switching to. The TRGW will be transmitted encrypted with the TGT access key and contain a new access key to be used to encrypt the air interface. The ticket itself is encrypted with the permanent shared secret between RGW and MB, allowing the RGW to verify the ticket on receipt later. After a handover, the terminal replies to the EAP-Request (Kerberos-OBAN) with a ticket. The (new) RGW verifies the ticket and grants access to the OBAN user. For the interested reader a detailed description is available in [19].



Because the solution above allows the authentication processing during handover to be a local matter between the terminal and the RGW, the delay caused by authentication is estimated to be in the range of 5 to 40 ms.

2.3 Overview of Services in OBAN

Table 1 outlines in detail the most prominent service types in OBAN, the challenges they are faced with, and the used traffic types. It is important to see the potential of a new paradigm, especially whether or not it is capable of reaching the full-blown status in offering a particular service such as e.g. voice over IP which is decisive for the market value and the stability of the subscriber base. Traffic types are important for planning, shaping in operators and also for QoS mechanisms. The Challenges highlighted express more or less where ongoing research work is taking place to tackle those barriers.

Service	Remarks	Support	Traffic Types	Challenges
VoIP Telephony	Soft-support, multimedia client integrated with OBAN; SIP infrastructure supported by OBAN	Full-blown	Realtime/Voice	High capacity consumption in WLAN (RTS/CTS); jitter over wireless medium to high
Personal Portal and Space	Globally accessible data space and web space, for unloading and loading data especially from devices with small storage, e.g. digi-cams, mp3 players, etc; retrieving important information also possible	One such space per user; payment according to size; it is an integral part of OBAN	FTP, Data transfer	Making it globally accessible, making both uplink and downlink efficient
Location-based Services	Enables better experience, supporting users, providing infotainment, and facilitating access to data	Partial	Background, data, in some cases real-time	Content providers necessary
Community-based Services	Increases customer base, brings people together, makes OBAN a service provider for all age groups	Partial	Real-time (interactive), background (email/forum)	Enablers for services are necessary

Table 1 OBAN Services Overview

ISSN 0085-7130 © Telenor ASA 2006

3 Peer Paradigms: FON, LinSpot, Boingo, The Cloud

3.1 FON

Similar to OBAN, FON is based on the idea of opening two Virtual LANs (VLANs) on a single WLAN access point, thus having two different SSIDs; one private for the equipment and connection owner, mostly a private resident, and one public broadcast for roaming users to be able to associate with the access point. The core logic of FON is also to establish a sort of a circle of trust whereby someone who buys the so-called "FON social router" would also have the chance to use other access points attached to FON routers belonging to other FON community members or "FONEROs".

How FON speaks of itself and what can be read in the media are outlined in the two paragraphs below.

The basic idea behind FON is to create a large community which is in a way self-sustaining and self-supporting. Their motto is 'Wi-Fi access for everyone'. According to sources, FON's stated objective is "to build a global Wi-Fi network bottom up, with one million hotspots by 2010." To do this, FON users connect to the Internet via Wi-Fi hotspots provided by other members of FON. FON claims to pose a business challenge for traditional network access providers by using broadband access to support what amounts to Wi-Fi access for everyone.

How broadband access providers respond to this challenge – whether they put up roadblocks or join the party – could be the next huge issue in multimedia communication and the net neutrality issue.

The company says the network will enable members "to connect to the Internet safely and securely all around the globe." The interest for Skype and Google is obvious: more ways to connect to their services and the potential to develop services specifically for FON members.

In other words, FON's message to the people is: buy our cheap router, put it in your home, deploy the necessary software and use your connection normally further on. Then, when you are on the move, check out some FON hotspot locator and find a nearby access point, go to that spot, sit down, and try to get some access. This is a more generalized version of the process where e.g. "T-Mobile" subscribers going particularly to the "Starbucks Cafe" since almost every "Starcbucks" Café operates a T-Mobile hotspot [6].

3.2 LinSpot

LinSpot was one of the earliest ideas to deploy privately owned and operated WLAN technology for providing Internet access to others, e.g. visiting users. LinSpot is marketed as a consumer-to-consumer solution. Similar to OBAN, the idea is to "turn all individual wireless Internets into a big network delivering Internet access anywhere" [10].

The software required to participate in LinSpot is available for free. To offer a LinSpot an Apple Mac system is required; software for Windows and Linux will be available later. The software packet to be installed is in principle an around 30 MB mini-Linux distribution. On the visiting user side any of today's operating systems will work because LinSpot works with standard IP protocols.

The billing concept of LinSpot is simple, but user-friendly. It is based on the use of PayPal [11], current prices start from 2.50 Euro for 2 hours up to 25 Euro for a month (flat rate). All billing relevant information is passed directly from the wireless LinSpot station to PayPal (SSL-encrypted). 15 % of the payment of the visiting users goes to LinSpot. But on the other hand, the LinSpot solution has severe deficiencies. Especially regarding security, LinSpot not only fails to provide any support to protect privacy or enhance security, the use of the LinSpot software even requires disabling any encryption on the radio layer. Regarding security the LinSpot web pages just advise you to properly secure all shares and to use firewall technologies. Another drawback of the LinSpot approach is that many ISPs do have clauses in their contracts which prohibit the resale of their internet access. The advice given on the LinSpot web clearly shows that LinSpot is well aware of those problems: "In that case you still might want to consider not putting your location information online to avoid potential problems".

Figure 7 FON Router and Access point in 1 box from LinkSys [30]

3.3 Boingo

In principle Boingo [15] acts as a Wi-Fi network aggregator. It offers convenient Wi-Fi hotspot connectivity to business travellers by aggregating hotspot locations throughout the world.

Boingo in between aggregates more than 45,000 hotspots but the regional distribution is quite different. There are more than 7,000 hotspot locations available in the US as well as in the United Kingdom and nearly 1,500 in Italy. But regarding some other European countries the numbers are really small; for Belgium only 51, for Norway 23 and for Luxembourg only 5 hotspots are registered.

Boingo offers a monthly service at USD 21.95 (flat rate) called *Boingo unlimited* and a service called *Boingo As-You-Go*, which offers connectivity to a single location for a single day. But *Boingo As-You-Go* does not include access to so-called "premier locations", those locations usually charge based on connection minutes. In addition to the usual Internet connectivity Boingo is partnering with Skype for Skype's VoIP service. *Skype Zones* offers unlimited use of Boingo hotspots for making phone calls with Skype (monthly charge USD 7.95). This service does not provide any other connectivity like web surfing, running email etc.

The software to use Boingo is available for free; supported operating systems are Windows, Mac OS X and the mobile Windows versions used on Microsoft Pocket PCs (PDAs). The software is convenient to use, a network sniffer, a location finder, WEP key management as well as Wi-Fi network profile management including preferred network priority are provided. Connecting to a Boingo hotspot just requires "one click". Besides aggregating the hotspots, the easy connection method developed by Boingo is the major benefit. Boingo worked out an authentication token methodology which handles each network's individual requirements, but hits it from the end-user. Boingo's software does not even require any proprietary software to be installed at the service provider. Boingo's interface to service provider can collaborate with many different kinds of login systems allowing the service provider to continue to use its existing authentication system.

The next big step Boingo started to focus on is twofold:

1 To extend the support to a significant larger number of different mobile devices;

2 To make sure that the public Wi-Fi hotspots do play a role in the fixed-mobile convergence.

Boingo offers the "Boingo Embedded Wi-Fi Toolkit" [16] as an open source software package to enable developers of small devices (dual mode phones, VoIP handsets and other portable devices) to integrate Wi-Fi connection management to any Wi-Fi hotspot. The toolkit consists of three sub-modules. The authentication sub-module facilitates the transmission of user credentials allowing a device to seamlessly connect to Wi-Fi networks. The so-called Wi-Fi engine sub-module communicates with the device's Wi-Fi chipset and operating system. It even includes power-saving logic for recognizing known signals to minimize unnecessary connections that waste battery power. The third sub-module is the configuration engine, which provides the functions needed to maintain user profiles and manage connection control scripts for public hotspots. For the communication to the application layer an open *Wi-Fi Application Interface* (WAI) is provided. The toolkit communicates with the lower layers by a so-called Platform Abstraction Interface (PAI), which is also open to the public. This may be a simple "glue" layer but if functionalities are missed it provides augmented routines to ensure proper operation of the toolkit.

In addition to supporting the development of "Boingo-ready" small-factor devices Boingo partnered with Birdstep to enforce the integration of cellular/Wi-Fi handoff. As the availability of cellular data services is growing, Boingo plans to use Birdstep's *WAN Access Connection Engine* SDK to integrate GPRS, EDGE, UMTS, 1xRTT and EV-DO network connection capabilities into the Boingo software [17].

3.4 The Cloud

The Cloud [20] is Europe's leading Wi-Fi network aggregator and – in Europe – the strongest competitor to Boingo. It was founded in 2003. The Cloud started with Wi-Fi only services but extended its focus already in 2004 to the integration of WLAN and 3G services. In 2005 The Cloud teamed up with Skype to integrate Skype Zones-based phone calls via their Wi-Fi hotspots.

The Cloud provides a service called *Cloud PayGo* to end-users but in contrast to Boingo it does not seem to be the most important focus. The Cloud is mainly partnering with Internet service providers and providers of hotspot, including Boingo. RoamPoint, an independent division of The Cloud supports service providers to realize consistent roaming with multiple Wi-Fi network operators.

The Cloud seems to be aware that security is becoming more and more important. The Cloud's hotspots are connected to private network connections to The

Cloud's core network, VPN technology is used to secure data transmission from the hotspots to The Cloud's core. In addition, The Cloud supports a variety of VPN client types to allow especially enterprise users to establish secure, encrypted connections to their corporate network.

From a technical point of view the security activities and pilots are the most exciting developments within The Cloud's operation. The *GuestBridge* platform enables third parties visiting an enterprise to get online, based on a combination of the enterprise WLAN network infrastructure and a managed network service and authentication platform operated by The Cloud. VLAN technologies, as well as 802.1x and associated methods are used to achieve this. An overlay network carries all third-party traffic directly to The Cloud, while enterprise users are connected in the normal manner. Peer-to-peer traffic between third-party and enterprise users is prohibited. Another interesting pilot deployment was done together with RoamPoint and Inte Solution Services. The consortium developed a solution supporting the co-existence of 802.1x security based access methods and Universal Access Methods (UMA). The solution employs VLAN technology to create two logically separated networks inside, one network for 802.1x traffic and one for the open UAM network. The access network support of 802.1x with IPsec in addition allow secure transmission of credentials and data over the air interface to The Cloud's network RADIUS platform and is forwarded to the enterprise RADIUS server where authentication is performed. The solution was successfully installed and tested in 2005 at the Stockholm Railway Station.

4 Pros and Cons of OBAN Compared to other Approaches

We outline below the various features and aspects where OBAN either outperforms other peer approaches or does worse. This is explained in point form.

- OBAN is currently developing community based services, a concept also strongly supported in the popular IP Multimedia Subsystem (IMS) [2] from 3GPP [22]. Forming different communities with different social interests and activities enlarges the customer base which would otherwise be limited to a number of connectivity freaks. For instance, elderly people in Europe are a growing community, and services for the elderly with selected services with particular content and style would encourage more people from this age group to subscribe to OBAN. Likewise, interest groups are formed based on activities and categories such as art, gaming e.g. chess clubs, etc. Being part of a community in an OBAN context means having access to specialized/adapted content, services, as well as community members' contact details. This feature puts OBAN way ahead of FON, Boingo and The Cloud whereby the latter three offer nothing beyond connectivity and global services such as Skype VoIP telephony. LinSpot just offers pure connectivity.

- Within the business and service model of OBAN the concept of ubiquity with continuously roaming users is supported. Connectionless as well as connection-oriented services are both highly important revenue sources. Every OBAN subscriber gets a globally reachable web space so that one can have access to personal data as well as use this web space as a buffer and repository where audio content, video content, and documents can be retrieved. This is especially useful for small devices such as digital cameras, PDAs with memory sticks and portable players. When on the move for some time, users can then unload their digital photos from their memory sticks or cards and also reload new playlists from time to time. For connectivity, users would either use a laptop connected via USB, Infrared or Bluetooth or the devices would connect directly via wireless interfaces if the OBAN residential gateways support this.

- Seen from a legal point of view, OBAN is being investigated by a regulatory body which is also a partner in the project. The business idea and the process of launching OBAN will be regulated and legalized in advance based on European regulations. This includes security aspects, keeping data and records, privacy protection, revenue division, granting access to third parties, roaming agreements and so on. FON as well as LinSpot face the severe problem of regulation in the sense that the "Wi-Fi for everyone" approach has immediate drawbacks, particularly for those providing access using their cable modem or DSL connections. Many cable companies and some DSL service agreements prohibit "unauthorized reuse" of broadband services, such as sharing a connection with neighbours. Cable companies have been particularly concerned with this issue.

- OBAN offers a broad range of services; not just connectivity, but also storage, location-based infotainment, multi-media, IP telephony (also intended to be achieved in FON using Skype, in OBAN we have our own SIP client). In OBAN, we have less dependence on off-the-shelf products than FON; this makes our solution more flexible, personalisable and better scalable in some cases. In OBAN we used a modified version of our mobile IP client (Birdstep) adapted to the OBAN context. Moreover, we used a self developed SIP stack (Technical University of Berlin) as a multimedia client for Voice-over-IP telephony, video streaming, video conferencing, text chatting/instant messaging, and other call and session management functionality. Using a hybrid mobility approach as mentioned in [26], we coordinate MIP and SIP in a mobility-optimized way. In other words, handover decisions when made, mostly from one access point to the other are first executed by Mobile IP. Mobility is one of the key goals of OBAN with focus on seamless handover and proactive network selection procedures. This is absolutely absent in FON, LinSpot, Boing and The Cloud, which do not allow user mobility. Reconnection to every spot is necessary in all of those being unacceptable for certain applications.

- In terms of security, the FON software includes a level of access control that could be beneficial to service providers. This is also the case for Boingo and The Cloud. Boingo offers a unique user interface for authentication and maps it to the used carrier's approach. The Cloud supports the approach of the actual carrier the user chooses. On the other hand, OBAN provides complete security architecture as described in the previous chapters. Moreover, security in OBAN is tightly coupled at functional and component level with mobility, quality of service and other features. OBAN handles various security aspects such as home user protection from roaming users, and vice-versa, protection of roaming users' private data and location information.

Feature	Approach			
	OBAN	FON	Boingo, The Cloud	LinSpot
Security	Integrated scheme, authentication	Single virtual layer	Simple encryption	No encryption allowed
Range of Services	Large	Connectivity only	Connectivity only	Connectivity only
Mobility and Handover Support	Fast handover, seamless mobility, proactive mobility, service and session continuity during motion	None; full re-authentication necessary; no continuous coverage	The Cloud: weak roaming support, hotspot like architecture; Boingo: none	None
Continuous Coverage	Yes	No	Clustered/spotty topologies (The Cloud)	Coverage very limited
Regulation	Conform to European regulations; Regulation autority within project consortium	Big problem: violates US ISP laws, no solution for regulatory issues within Europe found yet	N.A.	Solution illegal if ISP does not allow access sharing (often the case in Europe)
Pricing, Market Attractivity	Price-worthy, requires little	Very cheap	Questionable (a little below regular market prices)	Questionable (a little below regular market prices)
Business Model	Sophisticated, flexible, evolvable	Extremely simple/trivial	Straightforward, oversimplified	Straightforward, oversimplified
Ease of Management/ Maintenance	Yes	Single point of failure per router, no collective system coordination, detection or replacement capabilities	Medium	Medium
3rd Party Interaction	Possible, various application support (VPN, Email, etc)	High dependence on 3rd party products; black-box relationship	No	No
Flexibility/ Scalability	High	Medium	Low	Low
Full-blown VoIP	Integrated within OBAN (SIP client, proxy, single sign on, built-in telephony, video, chat in OBAN multimedia client)	Indirect support; planned via Skype (requires additional account and credit)	No	No
Interoperability/ Portability	Yes	N.A.	OS dependent, restricted	OS dependent, restricted
Incentives from operator to subscribers	Yes, for opening connection to OBAN visiting users	Connectivity offer; open connection so as to access other APs	None	None

Table 2 Summary of features of different approaches

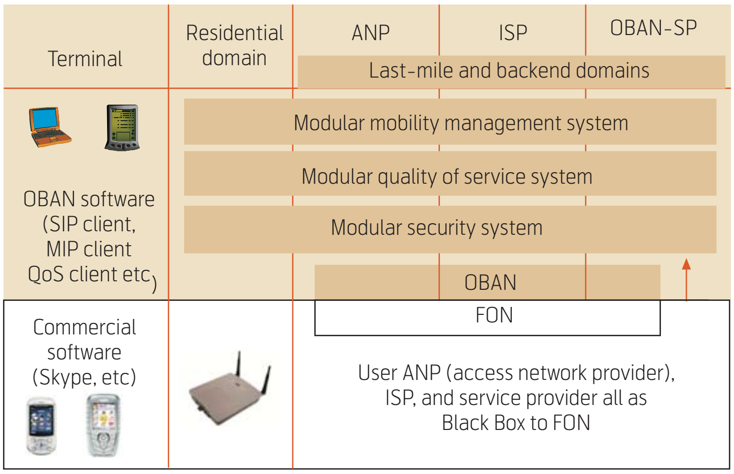

Terminal
Residential domain
ANP
ISP
OBAN-SP
Last-mile and backend domains
Modular mobility management system
Modular quality of service system
Modular security system
OBAN software (SIP client, MIP client QoS client etc)
OBAN
FON
Commercial software (Skype, etc)
User ANP (access network provider), ISP, and service provider all as Black Box to FON

Figure 8 FON versus OBAN Architectural Level Comparison

- Concerning deployment, both OBAN and FON require additional components, the 'social router' in the former and the 'residential gateway' in the latter. OBAN is deployed mostly however as a virtual operator over existing infrastructures. The crucial difference is however that OBAN has a flexible business model adaptable to different cases whereas FON has a simplified and very rigid business model with three user classes.

4.1 Similarities with OBAN

FON is not an Internet service provider. As a matter of fact, in order for someone to become a member of the FON Community, they must first have a broadband connection contracted through a provider. For this very reason, FON actively encourages and drives broadband adoption. This is the basic idea behind OBAN which was developed even before FON was launched. OBAN profits from the idea of meshing privately owned access points into a virtual network and letting mobile users profit from the unused part of the privately owned capacity.

In FON, the router will have two completely separate environments; one private, one public; the same concept is used in OBAN with a private SSID for home users and a broadcast one for public roaming users. Protection and separation of the environments is already done with special adapters. OBAN builds a more reliable, sophisticated and adaptable broadband access network, promoting not only broadband but also services which are the main revenue source for operators.

Compared to OBAN, Boingo and The Cloud act as aggregator, but does not provide new use of technologies as OBAN does. Both are focussing on mobile users, but usage on a fixed location. Mobile use with location changing and fast handover to keep established connections and data flows is not supported by Boingo, The Cloud and LinSpot and does not seem to be on the agenda for the near future. Especially regarding LinSpot the security limitations as well as the legal concerns are the reasons that this approach, besides starting already in 2004, has limited success regarding coverage and acceptance. On 1 July the LinSpot locator just delivered a single hotspot location for Norway, and only 21 for California (USA).

4.2 Comparison on an Architectural Level

Figure 8 depicts the various functional aspects Quality of Service, Mobility Management, and Security, and how they are spanned in each approach (OBAN and FON) over the logical and physical domains comprising a network serving customers, namely: the residential domain, the access network provider, the internet service provider, and the core service provider (e.g. OBAN SP or FON SP).

After the graphical presentation of the architectural comparison of OBAN versus FON as in Figure 8, we move on to Table 3 which outlines the individual modular elements (components in hardware and soft-

	Domain or Level			
Functional Aspect	Residential Domain	Access Network Provider	Internet Service Provider	Core Service Provider
OBAN Mobility	Foreign Agent	Mobility Broker, Gateway Foreign Agent	SIP Proxy	Home Agent, SIP Registrar Server
OBAN Security	Inter-domain trust mobility broker	Inter-domain trust ISP-RU	Inter-domain trust OSP	Inter-domain trust ISP-RU
OBAN QoS	Capacity Distribution, shaping and Policing, Tracking, Priority Queuing, Mapping, Marking	Traffic Shaping, Policing	Priority queuing	QoS Profiling and Brokerage
FON	Proprietary Router-Access Point single box	Black Box	Black Box	Black Box

Table 3 Tabular comparison for functional aspects over different domains OBAN versus FON

ware) which reside on each domain or level to fulfil the core functional aspects: mobility, security, and QoS.

5 Conclusion and Outlook to the Future

As we can see throughout this document, there are several approaches all attempting to fulfil a certain vision, namely, to cope with the evolution in networking and with increasing user demands for bandwidth, service quality, and ubiquity. This is done by following new paradigms which mainly open networks, try to cluster services together or build new ones, and invent certain business models or billing techniques for making such approaches attractive and increasing the customer base. This article has analyzed differences and similarities of the best known approaches, namely OBAN, FON, LinSpot, Boingo, and The Cloud. We pointed out pros and cons. Our prediction is that only approaches such as OBAN, which is more totalitarian in its philosophy can survive in the long run. In other words, OBAN made a vision whereby three key pillars were named as design goals and have been investigated and implemented in parallel with lots of interactions; those pillars are mobility, quality of service and security. A very tightly integrated solution has been realized on component level. Moreover, due to the fact that services are the main revenue source for operators, architectures which support a broader range of services are the more attractive ones. The future will bring along developments in each of the aforementioned approaches, but interestingly enough, each development of each particular approach will take a totally different direction. For instance, FON will evolve by making further deals with product-service providers to extend their pool of possibilities for subscribers. After Skype, other products would become partners of FON, and thus be offered as services within one environment. Still connectivity in a hotspot-like environment is the main thing FON offers. However, OBAN in particular, and Open Access Network approaches in general pursue ongoing research efforts in the three key pillar areas: mobility, security, and quality of service. The whole control logic as well as the palette of components with the OBAN functionality in the three areas will keep evolving to profit from new standards and advances which improve user experience and smoothen the whole service execution process.

References

1 *3rd Generation Partnership Project (3GPP)*. 25 July 2006 [online] – URL: www.3gpp.org

2 *IP Multimedia Subsystem (IMS); Ericsson Whitepaper*. 25 July 2006 [online] – URL: http://www.ericsson.com/mobilityworld/sub/open/technologies/ims_poc/docs/ims_wp

3 *Open Broadband Access Network (OBAN) website.* 25 July 2006 [online] – URL: www.ist-oban.org

4 *FON website*. 25 July 2006 [online] – URL: http://en.fon.com

5 Magedanz, T. IMS – IP Multimedia Subsystem. Towards a unified platform for multimedia service. *Eurescom Mess@ge*, 1/2006. (URL: http://www.eurescom.de/message/messageMar2006/IMS_%20IP_Multimedia_Subsystem.asp)

6 *T-Mobile Hotspot Architecture*. 25 July 2006, [online] – URL: http://hotspot.t-mobile.com

7 Panken, F (ed) et al. *Crucial properties of a wireless LAN-based open access network*. OBAN Deliverable D10. IST FP6 Project No 001889. 6 January 2006.

8 Panken, F (ed) et al. *Open Access Environment Architecture*. OBAN Deliverable D5. IST FP6 Project No 001889. 3 February 2005.

9 BBC News. *Wi-Fi pioneers offer cheap router*. 25 July 2006 [online] – URL: http://news.bbc.co.uk/2/hi/technology/5116960.stm

10 *LinSpot website*. 25 July 2006 [online] – URL: www.linspot.com

11 *PayPal website*. 25 July 2006 [online] – URL: www.paypal.com

12 *LinSpot Frequently Asked Quetsions 7.2: Can I resell my Internet Connection?* 25 July 2006 [online] – URL: http://www.linspot.com/faq.html#7.2

13 Internet Engineering Task Force (IETF). *SIP: Session Initiation Protocol*. RFC 3261, by Rosenberg, Schulzrinne, Camarillo, Johnston, Peterson, Sparks, Handley, and Schooler. June 2002

14 Internet Engineering Task Force (IETF). *SDP: Session Description Protocol*. RFC 2327, by Handley and Jacobson. April 1998. IETF Drafts

15 *Boingo Wireless*. 25 July 2006 [online] – URL: http://www.boingo.com

16 *Boingo Embedded*. 25 July 2006 [online] – URL: http://www.boingo.com/embedded/

17 Boingo Wireless Press Release: *Boingo Wireless and Birdstep Technology Partner to Bring Integrated Cellular Data and Wi-Fi to Operators Worldwide.* 25 July 2006 [online] – URL: http://www.boingo.com/pr/pr113.html

18 Haverinen, H, Salowey, J. *Extensible Authentication Protocol Method for Global System for Mobile Subscriber Identity Modules (EAP-SIM).* RFC 4186, January 2006.

19 Jaatun, M G, Tøndel, I A, Paint, F, Johannessen, T H, Francis, J C, Duranton, C. Secure Fast Handover in an Open Broadband Access Network using Kerberos-style Tickets. *Proceedings of the 21st IFIP TC-11 International Information Security Conference (IFIP/SEC 2006) on Security and Privacy in Dynamic Environments*, Karlstad, Sweden, 22–24 May 2006.

20 *The Cloud: Your Wi-Fi route to the Internet.* 25 July 2006 [online] – URL: http://www.thecloud.net/

21 *Institute of Electrical and Electronic Engineers (IEEE) web site*. 25 July 2006 [online] – URL: http://www.ieee.org

22 *3rd Generation Partnership Project (3GPP) website*. 25 July 2006 [online] – URL: http://www.3gpp.org

23 Internet Engineering Task Force (IETF). *Candidate Access Router Discovery (CARD)*. RFC 4066, by Liebsch, M and Singh, A (eds), Chaskar, H, Funato, D, Shim, E. July 2005.

24 Internet Engineering Task Force (IETF). *IP Mobility Support for IPv4*. RFC 3344, by Perkins, C (ed). August 2002. (Obsoletes RFC3220) (Status: PROPOSED STANDARD)

25 *OBAN QoS Architecture*. Lucent Netherlands; OBAN-WP2-LUC-208-u.doc; OBAN Internal Project Document, IST FP6 Project No 001889. May 2006.

26 Elkotob, M, Martini, S, Marx, S. *Session Based Mobility*. OBAN Deliverable D19.3, OBAN Internal Project Report, August 2005.

27 Panken, F (ed) et al. *Architecture for Interaction of OANs with Cellular Networks*. OBAN Deliverable D11, IST FP6 Project No 001889, July 2006.

28 Panken, F (ed) et al. *OBAN Architecture*. OBAN Deliverable D27, IST FP6 Project No 001889. 25 October 2005.

29 *Swisscom Hotspot Public WLAN Access*. 25 July 2006 [online] – URL: http://www.swisscom-mobile.ch/scm/gek_pwlan_en.aspx?c.scn=pwlan

30 *LinkSys website*. 25 July 2006 [online] – URL: http://www.linksys.com

Muslim Elkotob is Research Engineer and Doctoral Candidate at DAI-Labs, Technische Universität Berlin, Germany. He received his BSc in Computer Engineering in 2000 and his MSc in Electrical and Communications Engineering from the Technische Universität München in 2003. He has contributed with research as well as project management to several ICT projects financed by the EU as well as by the German Federal Ministry of Research (BMBF) and the Deutsche Telekom AG (DTAG). His research interests include Quality of Service in wireless networks, autonomic communications, cross-layer optimization, and next generation network architectures (open access networks, mesh networks, extensions to standard 3GPP architectures).

email: muslim.elkotob@dai-labor.de

Herbert Almus is Deputy Head of the Inter-departmental Research Center for Networking and Multimedia Technology at the Technical University of Berlin. His experience with networking started in 1978. Since 1989 he has been working on high-speed networking, since 1992 on ATM. He has been involved in the evaluation of ATM for the German Research Network as well as in several trials on the Pan-European ATM network. His main focus in research lies in the fields of Traffic Management and Quality of Service in communication networks as well as in the development of test suites for network protocols and services. Herbert Almus regularly conducts ATM, MPLS, QoS and Traffic Management courses for industrial and academic participants.

email: herbert.almus@tu-berlin.de

Prof. Dr.-Ing. Sahin Albayrak studied computer science at Berlin Technical University and received his PhD in 1992. Sahin Albayrak qualified as a professor in 2002 with the topic "Open Platforms for the Development of Distributed Systems and Online Services" and received the call to the chair "Agent Technologies in Business Applications and Telecommunications" at the Technische Universität Berlin in 2003. In 1992, Professor Albayrak founded the DAI Laboratory as an integral part of the chair "Agent Technologies in Business Applications and Telecommunications" and took on academic management. With more than 100 highly qualified researchers, the DAI Laboratory is one of the world's leading research institutes in the area of agent technology. Sahin's research interests include mobility management, next generation networks, and clean-slate internet design.

email: sahin.albayrak@dai-labor.de

Klaus Rebensburg is Director of the Interdepartmental Research and Service Centre for Network Technologies and Multimedia Applications (FSP-PV) of Technische Universität Berlin. His institute is involved in research and service activities on real-time and multimedia systems, intranet/internets, office automation, (mobile) broadband communications and distributed telecommunication services and network security services. Prof. Rebensburg is also teaching computer science at University of Potsdam (MultiMedia Engineering, Nonlinear Media, Tele-services, Multimedia Production and Network Technologies). His institute has been partner in the European Community's RACE and ESPRIT programme. Human Factors Evaluation activity has been set up around the technology projects as well as an internet security initiative.

email: klaus@prz.tu-berlin.de

Architecture for Sharing Residential Access with Roaming WLAN Users

FRANS PANKEN, HAAKON BRYHNI, PAAL E. ENGELSTAD, LEIF HANSSON, GERARD HOEKSTRA, MARTIN GILJE JAATUN, TOR HJALMAR JOHANNESSEN

Frans Panken is a senior member of the technical staff at Lucent Technologies

Many countries have relatively densely populated areas where the population concentrates around urban centres. The access capacity used to connect these homes to the Internet is often not fully consumed, either because of the low-range subscription selection or because the user is not on-line. If the residential equipment within these urban areas is used to provide access to casually passing users, a contiguous radio coverage landscape of WLAN access points is potentially obtained. This paper describes the challenges and the solutions when the surplus capacity available in the residential broadband access connection is used to offer WLAN access to users who casually pass a residential area. The focus is on the architecture that functions as a framework to solve the technical challenges that arise when using unlicensed bands for public network access.

Haakon Bryhni is CTO of Birdstep Technology ASA

Paal E. Engelstad is Research Scientist in Telenor R&I

Leif Hansson is Research Project Manager in Birdstep Technology ASA

Gerard Hoekstra is a member of the technical staff at Lucent Technologies

1 Introduction

The convergence of the various access networks forms a crucial aspect in the next generation networks. Telecom operators have concentrated on 2G and 3G public networks that operate in licensed frequency bands. On the other hand, the unlicensed frequencies in wireless local area networks (WLANs) have been applied successfully as home and last mile technology in the increasingly pervasive computing environments where mobile users access Internet services. The integration of WLAN in 3G devices and the convergence of various access network technologies indicate that WLAN is no competitor for 3G and that the unlicensed WLAN spectra may become an important and cost effective supplement to offer network access.

In residential areas, WLAN is often positioned as the primary means of broadband access, widely deployed in many countries by access lines based on Digital Subscriber Line (DSL), fibre, and cable. When considering the limited capacity usage of for instance the popular Asynchronous DSL (ADSL) technology, it becomes clear that an enormous network access potential is currently wasted. In [1] this waste of capacity is metaphorically compared to a not very lucrative airline company that flies with an average of 97 out of 100 unoccupied seats. The broadband modems are often equipped with WLAN and when the device or antenna is placed optimally in a home, signal attenuation to reach the public domain is equivalent to a 40 m distance (real distance + walls / windows, see [2]) which may be sufficient for offering supplement capacity to realize public access via residential equipment.

Many countries have relatively densely populated areas where the population tends to concentrate around urban centres. It is envisaged that in the urban areas the residential WLANs offer near-contiguous radio coverage, potentially allowing casually passing users to roam seamlessly through a landscape of WLAN access points. This paper studies this situation and distinguishes two kinds of users, namely the residential users (RUs) and visiting users (VUs). Residential users own (or store) the broadband modem or wireless access point (AP) and offer this equipment to the casually passing users, referred to as visiting users. Note that the term visiting user refers to the visiting of the AP located in a house and not to visiting a person living in the house where the AP is located. In general, the visiting user will be a complete stranger to the person who opens the residential equipment to visiting users, who casually pass (or are close) to the WLAN equipped home. The communication in the fixed access broadband network required by the visiting users should not jeopardise the access or the availability of the residential equipment, but can utilize surplus capacity offered by the physical feeder lines terminating the fixed broadband access network.

Exploiting the residential network for public access has challenges. One of the primary challenges is to realize it without replacing existing residential equipment, fully exploiting the installed residential infrastructure. Initiatives as FON (see [3]) and LinSpot apply this idea, sometimes including the offering of firmware upgrades of popular WLAN equipment to improve security or to separate residential traffic from visiting traffic. The drawbacks of their solution arises from excluding the access network provider and the Internet service provider of the residential user, resulting in a stand-alone solution and hence lacking the potential integration offered by the integration with 2G/3G networks and/or WiMax. In addition, neither QoS nor fast handover are solved in these initiatives. Security mechanisms are needed to prevent visiting users to gain access to peripherals and/or data of residential users. Quality of service

ISSN 0085-7130 © Telenor ASA 2006

Martin Gilje Jaatun is Research Scientist at SINTEF ICT

Tor Hjalmar Johannessen is Research Scientist at Telenor R&I

mechanisms need to enforce that visiting users keep airtime consumption within limits and do not dominate the wireless access network. Network coverage planning should ensure that the unlicensed WLAN spectrum is used efficiently and without the need for manual optimization. Mobility issues such as network discovery and seamless handovers between neighbouring located access points need to be solved. The tree topology of access networks introduces an extra challenge for fast mobility, as neighbouring access points are not directly interconnected. In addition, neighbouring households may have selected different access networks or Internet service providers, increasing the physical network distance between neighbouring APs and increasing the challenge to realize handoffs seamlessly. Finally, legal and regulatory issues as well as social and economic aspects may arise, where simple and effective charging solutions need to be applied to make the solution profitable.

This paper describes the WLAN system architecture to use residential network for public access. It first describes the challenges and requirements and subsequently sketches the solution that allows resource sharing and prediction and to realize handoff between neighbouring access points fast and securely.

2 Challenges and requirements

Figure 1 depicts a simplified topology of the various network elements in the access network that are relevant for sharing residential access with roaming users. The access network basically consists of IEEE 802.11 stations that may belong to visiting or residential users, one or more WLAN access points and a residential gateway (RGW) connected to the fixed broadband access network and equipped with several queues to distinguish and give priority to various traffic classes.

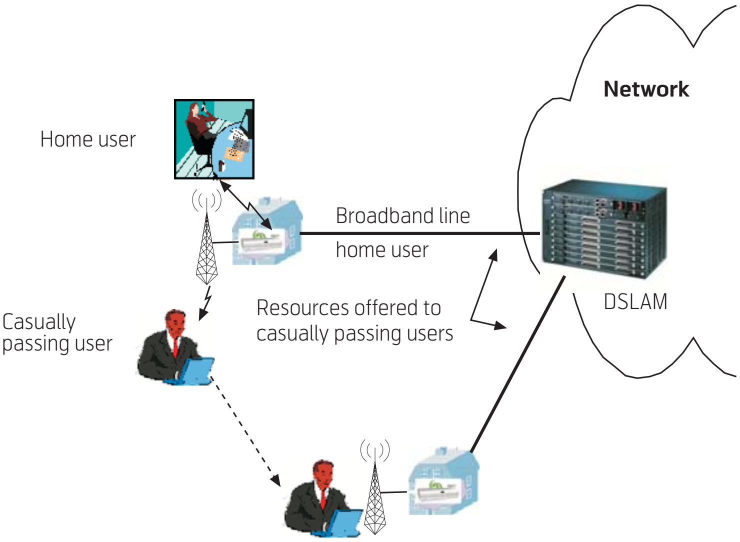


Figure 1 Exploiting surplus capacity of the broadband home network connection to WLAN broadband mobile access to casually passing users

2.1 Mobility

The mobility objective is to provide a user experience that is comparable with mobile phone networks, where handover, even between different operators, is virtually unnoticeable. The key challenge is to provide an application session for the user, with undiminished quality of service, even when the mobile terminal moves between different residential gateways, potentially operated by different network operators. If these operators provide the sharing of residential access functionality, a mechanism to ensure both mobility and quality of service for the mobile user must be installed.

A mobile VU terminal will move from WLAN access point to access point. In existing technology, the handover preparations and decisions are exclusively handled by the mobile client without pre-processing assistance and help from the network. In contrast to 2G/3G types of networks, WLAN does not provide ‘make before break’ handover facilities between APs, so delays are possible, especially if the APs and visiting user all belong to different domains and home-ISPs.

The main challenge is that of speed; network detection, handover decisions and authentication must be effective enough to support rapid handovers. Traffic paths must also be kept as short as possible, both for control messages and for data payload.

During a handover the following tasks must be performed:

- Find convenient and neighbouring APs/RGWs with sufficient spare resources to fulfil the QoS requirements of the VU
- Make a handover decision based on information about neighbouring APs, user preferences and current signal quality
- Re-authenticate to the new AP, so that the associated RGW will open a port to the Internet
- Handle the AAA/accounting functions
- Establish a secure, encrypted channel over the new wireless link with dedicated keying material
- Re-direct all ongoing traffic to and from the visiting client via the new AP
- Notify and report the location data for the actual AP for an ongoing session (e.g. as a requirement from regulatory authorities in case of an emergency call).

ISSN 0085-7130 © Telenor ASA 2006

In principle, most of the above requirements can be handled by existing standards and distributed functions. The major problem is simply the amount of time consumed before handover is completed and an existing session is continued.

To sum up, the following mobility requirements must be fulfilled:

- The terminal must be able to find neighbouring APs/RGWs regardless of the domain they belong to.
- The handover decision should be based on a combination of information about the neighbouring APs, user preferences and current signal quality.
- AAA/accounting functions must be handled in a multi domain environment.
- The application session must be preserved during handover with undiminished quality of service.
- Handover must be fast enough to permit real time traffic such as Voice over IP without compromising security.
- Network latency should be kept to a minimum.
- Possible regulatory requirements regarding access to location information must be met.

2.2 Quality of service

The Quality of Service objective is to solve QoS issues in realizing efficient network utilisation and user assurance at the same time. The residential user's QoS can easily be affected by visiting users if insufficient measures are taken. Resources of the fixed access network as well as in the WLAN must be allocated such that all involved parties benefit the most. Especially when offered in a commercial public context, the WLAN will have to meet user expectations regarding throughput, delays, jitter and availability of the network. The shared nature of the medium in an unlicensed spectrum poses several challenges, including:

- Available resources should be shared among all stations in an efficient manner that is based on a user's subscription.
- Resource consumption in the (wireless) access network should be predictable. This requires proper assignment of resources to each station.
- The admittance of visiting users should be limited so that an acceptable and configurable level for residential users can be reached. This also means that access to stations may be denied if this is expected to jeopardize point 2.
- Data originating from and destined to visiting users should be separated from residential traffic.
- The solution should fit within the current QoS solutions offered by the IEEE 802.11e standard.

In order to make QoS guarantees, WLAN access networks require a resource allocation mechanism to provide QoS guarantees similar to 3G networks.

2.3 Security

The security objective is to develop a secure solution for public access to private wireless LANs and private broadband access lines. The goal is to ensure privacy for all users and optimal usage of the network resources, but at the same time make sure that the residential users do not experience any degradation in security and privacy level. All users must experience the same level of security. For the Visiting User this means that the same security level as experienced at home is reached, whereas residential users should experience the same level of security as prior to sharing access resources. Relevant security services include authentication of users to the network, access control, as well as confidentiality and integrity protection of the data flow through the shared wireless LAN and the shared broadband access lines. It must not be possible to eavesdrop on wireless users, and hence mechanisms that ensure the confidentiality of information sent over the air interface are needed.

When associating with an access point, users must have a way to make sure that the access point is indeed part of the network operated by their provider. Given the low-cost ubiquitous availability of WLAN technology, it is relatively easy for a malicious party to impersonate the network.

The mobility requirements also have implications for security, since the former place a restriction on how much time the authentication and other security mechanisms can be allowed to take in connection with a handover.

To sum up, this gives us the following security requirements:

- User authentication
- Anonymity of visiting users
- Separation of residential user and visiting user
- Confidentiality of wireless traffic

- Authentication of access points

- Fast authentication for handover.

2.4 Radio coverage

The WLAN standard distinguishes between various versions of 802.11a/b/g that mainly differ on the physical medium aspects used. The 802.11g variant has increased in popularity, but there are still many stations that only support the 802.11b variant. The new 802.11n standard will be released soon and the solution should support all variants, potentially impacting the service coverage as well as the QoS solutions.

The maximum communication distance for any radio technology is limited by factors such as transmission power, receiver sensitivity, noise environment, interference, antenna characteristics, etc. This means that offering public access by exploiting residential equipment is restricted to a certain area around each wireless access point. Ranges covered by antennas have increased during the past decade and amplifiers could be used to strengthen the business case as long as interference with neighbouring access points is at an acceptable level. The theoretical boundary for the range that can be serviced by WLAN technology is 3 km, as the propagation delay then exceeds 10 microseconds, the maximum delay prescribed by the IEEE 802.11 standard. Solutions for the MAC protocol on how to deal with outside WLAN with even larger ranges are presented in [4]. Radio coverage is outside the scope of the system architecture and more details for potential solutions to maximize coverage can be found in e.g. [5].

3 System architecture

This chapter describes how the challenges enumerated in the previous chapter can be solved and how the solutions together form the system architecture.

3.1 Mobility

The mobility challenges presented in section 2.1 are solved by a combination of features in the Terminal, the Residential Gateway, a Mobile IP Home agent in the Home ISP of the Visiting User and a new component called the “Mobility Broker”. An optional Gateway Foreign Agent provides reduced latency, when the Home Agent is located far away from the current ISP. The overall architecture is shown in Figure 2 and a detailed view of all architectural components is found in Section 3.3.

WLAN networks lack pre-processing abilities to support “make before break” assistance in handover cases. This introduces potential delays. In the normal case re-authentication requires what is called a full AAA round-trip between the client, the Access Point and the home-ISP/AAA server for that client. Furthermore, if SIM is involved in the authentication, the AAA server must contact the mobile home operator’s HLR (Home Location Registry) for the client (as in 2G/3G roaming).

Since the WLAN cells are small, re-authentication is expected to occur frequently, potentially introducing annoying interruptions each time. This indicates a requirement for a new regional node; the Mobility Broker (MB), which integrates functions such as supervision of QoS and location of the APs, and re-authentication of the VU to achieve more efficient handover. The MB is intended as a regional trusted supervisory and controlling resource that can also handle cross-domain handovers for a VU. It facilitates the fast authentication scheme, which is a prerequisite for the fast handovers needed by interactive streaming services.

The requirement for fast handover combined with security is solved by a two-phased authentication scheme, where the first phase (initial authentication) is a full-cycle EAP/SIM authentication in which the identity of the Visiting User is established using well known SIM-based authentication. This first authentication will be relatively slow, since it relies on communication all the way from the SIM card to the HLR server connected to the Home ISP. This authentication step is enhanced by the Mobility Broker, which acts as an AAA proxy. Because the authentication is proxied through the Mobility Broker, the broker can

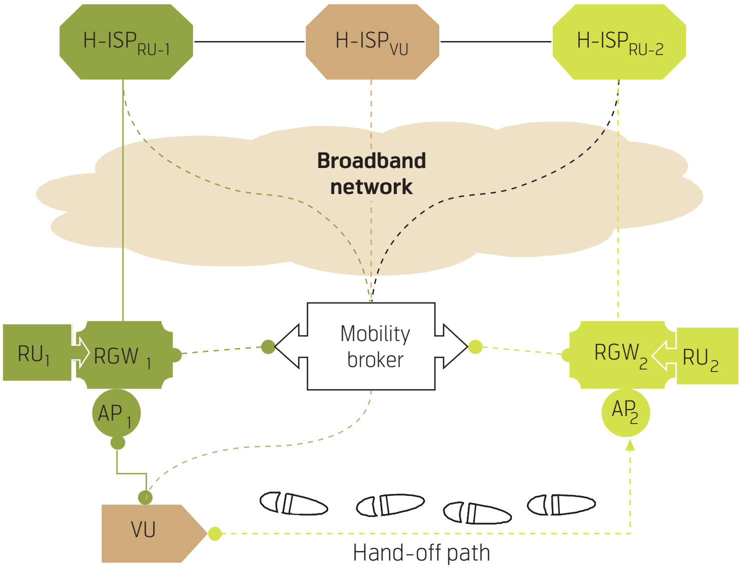


Figure 2 Multi-domain WLAN roaming, where H-ISP stands for: Home Internet Service Provider, RU: Residential User, RGW: Residential Gateway, AP: Access Point, VU: Visiting User

react upon successful authentication and start advance preparation for subsequent authentications.

The second authentication step realizes mobility between neighbouring RGWs[1]. The stringent requirements for handover speeds of streaming services such as Voice over IP force a solution of this within tight time constraints. A new authentication protocol that uses pre-calculated Kerberos-style tickets to facilitate local decision in the Residential Gateways realizes this. See Section 3.3 for more detail.

The process of moving from one access point to another can be divided into three different phases; information gathering, network selection, and handover.

During the information gathering phase, the Connection Manager scans available WLAN networks to determine local connectivity options. The protocol used to obtain relevant network information on scanned WLAN access point is CARD, see [6]. The CARD Client in the terminal then issues a request to the CARD Server in the Mobility Broker, asking for information about local participating RGWs. The MB will maintain dynamically updated information about the AP/RGWs in its region (which may comprise several domains). For each AP/RGW this will include QoS capacity, location information (own and neighbouring APs), and not least the VUs that are currently connected to each AP. The MB must also know the home-ISP (H-ISP) of the VUs. The broker acquires QoS information by QoS information exchange with the QoS_{RGW} in the RGWs, while location data is collected through the IETF CARD (Candidate Access Router Discovery) protocol. During this phase the terminal also makes preparations for fast handover, which is described in detail in Section 3.3.

In the network selection phase, the Connection Manager utilises the collected information to make the correct decision. Access point selection may be based on several conditions, e.g. signal strength, available QoS, user preferences, etc.

Once the new AP has been selected, the Connection Manager disassociates from the current AP and associates with the new one. The actual handover of the traffic is then carried out using Mobile IP, initiated by the Mobile IP Client. For Mobile IP, handover is carried out for all IP-based applications. Alternatively, the Connection Manager can inform the SIP Client about the handover, if a SIP mobility solution is desired. Prior to the handover, the EAP/OBAN authentication must have been performed.

Note that the information gathering phase is normally not time-critical and is a continuous process. The critical timing is in the physical handover and authentication process. Also note that there are several aspects influencing the timing of the fast handover. Some aspects we can control, such as the processing time in the terminal, the time taken to retrieve and control authentication parameters, perform the actual network switch etc. However, many timing factors are outside our control, for example, the network latency and the response time from critical servers such as AAA, Mobility Broker, Foreign Agent in the Residential Gateway, Gateway Foreign Agent, etc. It is the objective of the fast handover design to minimize these latencies by using a combined approach where fast authentication is combined with fast handover.

3.2 Quality of Service

One aspect of QoS guarantees is to distinguish various priority classes. In [7] a possible priority mapping scheme was proposed for accommodating residential and visiting users where packet treatment (e.g. transmission, queuing) depends on the assigned priority level. If the traffic ingress volume of a network exceeds the amount that can be processed, these mechanisms are not sufficient and QoS degradation is inevitable. This is why – besides priority – QoS solutions must include indications about volumes, specified in a traffic contract or a Service Level Agreement (SLA). The SLA determines how much traffic the parties can send on a network. When combining traffic differentiation with SLA agreements, parties are free to operate, each within the given contract space, without affecting others and may prioritize their most valued traffic accordingly.

In WLAN systems, the terminology *load* requires special attention, as the overhead depends on the station's transmission speed as well as the WLAN variants (802.11b/g) stations associated to the access point. The load on a WLAN medium cannot be uniquely determined by the data rate only and hence *QoS traffic profiles* are introduced to overcome this. A QoS profile describes the traffic service level contract defined by the average number of packets per second (PPS) sent in the upstream and downstream directions, combined with the average number of bytes of these packets (BPP). Note that the data rate is obtained by multiplying PPS with BPP. The set of QoS profiles describes the traffic subscription of a user and this set is retrieved from the network as part of the authentication process. The QoS profiles are subsequently used as a base for performing user/terminal admission control and network resource plan-

[1] *In the current design, fast handover is limited to AP/RGWs connected to the same Mobility Broker.*

ning. Based on a combination of the QoS profiles and the current resource planning status the conclusion can be drawn whether a user can be granted access or not. If access can be granted, two QoS profiles from the set are assigned to the user, namely *committed profile* and *peak profile*. The committed profile is guaranteed, on statistical grounds. This selection process requires a capacity distribution algorithm, described in more detail in [8].

Additional requirements to the resource planning in WLAN networks are imposed as stations may perform rate adaptation and thereby affect the medium capacity and thus the available resources of all users associated. To counteract on these and other unforeseen events (e.g. SLA contract violations by users), the QoS solution monitors the channel conditions and the user traffic to take measures when QoS guarantees may be jeopardized. A total of three QoS entities are defined, located in the terminal (QoS_T), the residential gateway (QoS_{RGW}) and in the AAA server (QoS_{AAA}). These QoS entities communicate to guarantee the desired QoS level of the users in the network. Before users gain network access, their QoS profiles must be obtained. For residential users, these QoS profiles may be stored locally and for visiting users these profiles are obtained as part of the authentication process, realised by internal communication. If the RADIUS protocol is used for authentication, vendor specific attributes are intercepted by the QoS_{RGW} to obtain the set of QoS profiles information sent from QoS_{AAA}. From this set of QoS profiles, the QoS_{RGW} will select the one profile to be guaranteed and derives the minimum WLAN data rate needed for using this profile. The QoS_{RGW} maintains its QoS guarantee to the user as long as the user operates at least at this minimum WLAN data rate. For more details on how a QoS profile is selected, how the minimum WLAN data rate is calculated and how guarantees are maintained under varying channel conditions we refer to [8].

The selected QoS profiles selected by QoS_{RGW} are communicated to the QoS element QoS_T on the terminal. The communication between the QoS element on the terminal, QoS_T, and QoS_{RGW} can be realized in various ways (e.g. RSVP; Intserv).

Consequently, the terminal is held accountable for not exceeding the selected QoS profile and is policed upon this limit. Traffic shaping in the terminal prevents packets being deleted. In turn, the QoS_{RGW} entity will try to meet the QoS profile committed to QoS_T by monitoring the channel conditions and the individual user's data rate and traffic consumption. If a user drops below the minimum data rate or if a medium overload occurs, the QoS_{RGW} will redistribute the network resources and may update the affected QoS_T of their newly assigned profiles and rates.

3.3 Security

Security must meet the challenges identified in Chapter 2, namely user authentication, anonymity, separation of users, authentication of access points, confidentiality and fast handovers.

User Authentication

To ease GSM/UMTS integration, EAP-SIM [9] has been chosen as the primary authentication mechanism for Visiting Users. As can be seen from Figure 3, an hierarchic authentication structure is used, where the VU exchanges EAP-SIM messages with the RGW (1); the latter forwards these messages using RADIUS ([10]) to the Mobility Broker (2), which forwards them to the ISP of the Residential User (3), which finally forwards them to the ISP of the Visiting User (4). This effectively re-uses a AAA infrastructure that would be present in any enterprise network (i.e. the components under ISP_{RU-1} in Figure 3), but introduces a few extra hops.

Authentication relies on existing long-term trust relationships[2)] between the Mobility Broker and all Residential Gateways in its cell, between the Mobility Broker and all ISPs in its cell, and unilaterally between all participating ISPs (this latter relationship

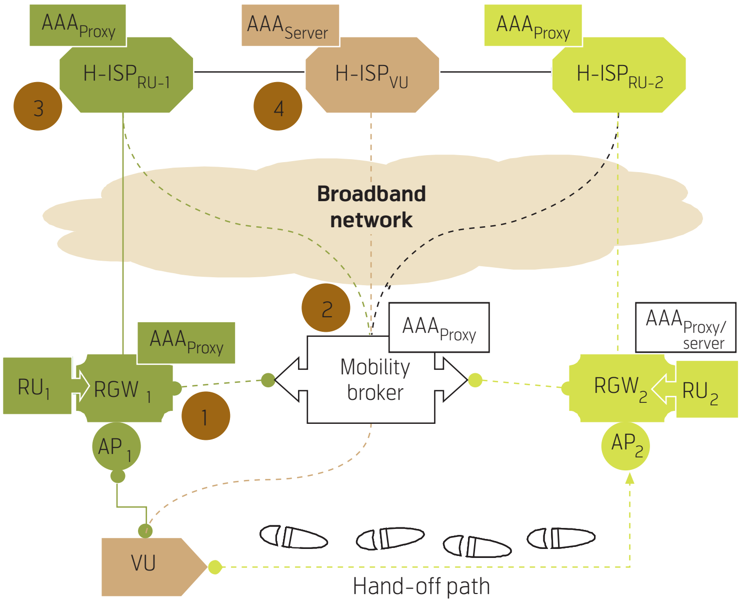


Figure 3 Authentication path for full authentication

[2)] *For our purposes, a "trust relationship" can be read as a "shared secret", i.e. both parties that have a trust relationship have access to a secret value that no other parties know or can determine.*

ISSN 0085-7130 © Telenor ASA 2006

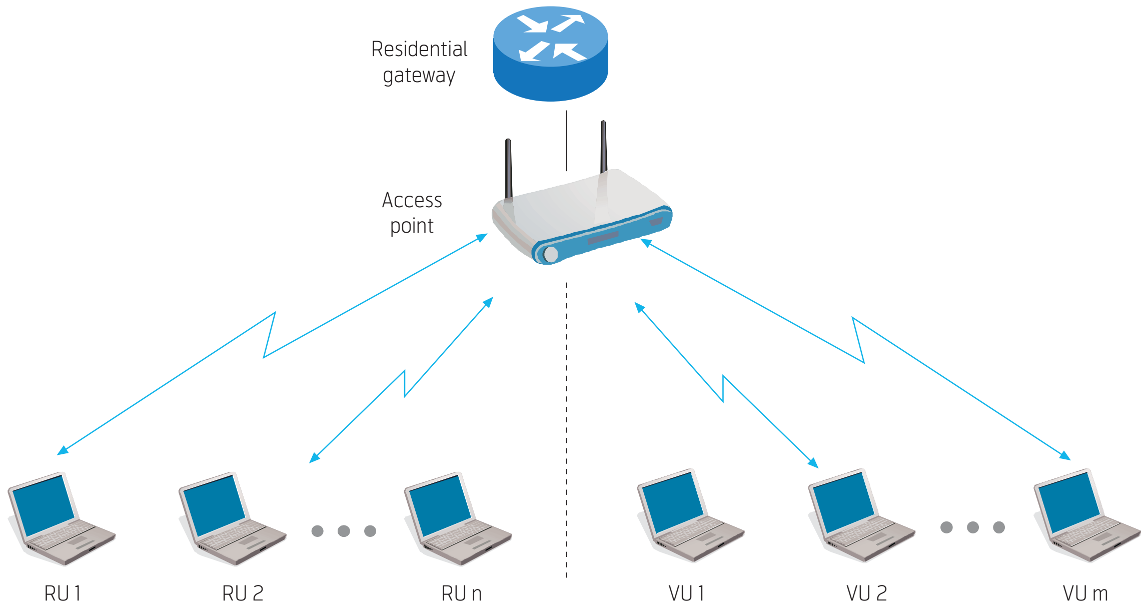


Figure 4 Residential Users (RUs) and Visiting Users (VUs) are separated, and access two different virtual WLANs of the same Access Point (AP) and Residential Gateway (RGW)

is orthogonal to current roaming agreements between e.g. GSM operators).

When a terminal first joins the network (i.e. when it is turned on), it must perform a full EAP-SIM authentication involving all the parties mentioned above. As we shall see, subsequent handovers are much more efficient.

Anonymity of Visiting User

The use of EAP-SIM grants the Visiting User the same level of anonymity as with the use of a GSM telephone, and will make it very difficult for e.g. an RGW operator (i.e. residential user) to track VUs. The handover solution described below can make it impossible for RGWs that are not part of the initial authentication to do any kind of tracking of Visiting Users.

Separation of residential and visiting users

A principle of the sharing concept is to protect the traffic of the residential user (i.e. the owner of the access point) from excessive traffic from visiting users. Apart from perhaps getting some reduced bandwidth, the residential user should to a large extent be unaffected by the fact that there might be visiting users accessing the residential gateway/ access point belonging to the residential user.

To accommodate separation between the residential user traffic and the visiting user channel, QoS features are necessary. In addition, the IEEE 802.11 WLAN access is split into two different logical parts, resulting in two separate virtual WLANs. This is realized by letting the WLAN access point transmit two different versions of beacon / probe response frames, resulting in a set of 802.11 management messages for each of the virtual WLANs.

Figure 4 illustrates the separation between *n* number of residential user devices and *m* number of visiting user devices separated in two different virtual WLANs.

The RU may only use the Pre-Shared Key (PSK) functionality of e.g. WPA; RADIUS is only used for Visiting Users. This implies that the Residential Users are not aware that they are part of the network that allows sharing residential access facilities; this satisfies the “same as before” requirement with respect to user perception.

Confidentiality of Wireless Traffic

One of the features of EAP-SIM that makes it suitable for sharing residential access is that it as a by-product of the authentication process generates a shared secret between the Visiting User and the Visiting User’s home ISP. This shared secret is then “passed down the line” from ISP_{VU} to ISP_{RU} to MB (and finally) to RGW. Again we exploit the fact that each link in the authentication path is protected by a (long-term) shared secret; this enables the secure transmission of the dynamic shared secret.

Once the dynamic shared secret reaches the RGW, it represents a dynamic trust relationship between the terminal and the RGW. On the practical side, it also means that the terminal and the RGW now have a (dynamic) shared symmetric encryption key, which is used to encrypt the wireless traffic.

Authentication of Access Points

Since the terminal and access point (RGW) do not have a pre-existing trust relationship (and thus no long-term shared secret), the terminal has to rely on the chain of trust based on the pairwise shared secrets described above. Once the dynamic shared secret has trickled down to the RGW, the terminal can ascertain that the access point is legitimate when the RGW proves that it does indeed possesses this secret. The fact that transmitted data from the RGW is intelligible once decrypted (by the terminal) with the dynamic shared secret, represents implicit proof of such possession.

Fast authentication for handover

If the mobility requirement regarding maximum handover latency is to be fulfilled, it is clear that a full EAP-SIM multi-actor roundtrip takes too long time. Thus, a separate authentication technique specifically for fast handovers is required.

When the terminal has a list of access points from CARD as described in Section 3.1, it will contact the Mobility Broker for a Kerberos-style ticket to the most likely access point(s) (see [11] and [12] for more details). The Mobility Broker is able to create such a ticket since it shares a secret with every RGW; the ticket itself can only be decoded by the recipient RGW. Once in possession of a ticket, the terminal may perform the handover directly to the corresponding access point and once Layer-2 connectivity is established, the terminal will offer the ticket to the RGW. The ticket can be verified locally on the RGW, without involving any other actors; this implies that the handover authentication will be dramatically faster than a full EAP-SIM authentication. Once the ticket has been verified on the RGW, the terminal will be granted Layer-3 connectivity, and can proceed to update Mobile IP information in the network. It can be noted that this solution allows the terminal to start transmitting IP traffic almost immediately after associating with the new access point, but it will not be able to receive Mobile IP traffic before the Home Agent (or Gateway Foreign Agent) is updated.

Authentication with Kerberos tickets is also a good choice with respect to the other security requirements:

- *User authentication*
  (Implicit)

- *Anonymity of Visiting Users*
  Kerberos could re-use EAP-SIM identifiers, or even create new pseudonyms for each ticket.

- *Separation of Home User and Visiting User*
  Only Visiting Users get tickets.

- *Confidentiality of wireless traffic*
  The secret in the ticket can be used as a basis for creating a shared encryption key.

- *Authentication of access points*
  Only valid access points (RGWs) are able to decode the ticket and extract the embedded key for decryption of encrypted traffic from the client. Additionally, explicit mutual authentication can be offered as an option.

3.4 Overall system architecture

Figure 5 gives an overview of the architectural building blocks mentioned before. As the functionality of the modules is described in other places in the document this section elucidates the interfaces between the modules. One module that has not been mentioned before, however, is the IP Zone server (IPZ). It is the base platform for the residential gateway and contains core functions such as firewall (IP tables rules) and traffic control.

Table 2 describes the inter-node interfaces, labels refer to Figure 5.

3.5 Integration with 3G networks

The integration of WLAN with 3G infrastructures is an on-going topic for research and standardization within ETSI and 3GPP, see [14],[15],[16]. Open challenges that require solutions to provide a seamless user experience in an integrated 3G and WLAN network infrastructure include session continuity, intercarrier roaming and integrated billing and authentication. Various levels of integration (coupling) are proposed to solve some of these challenges in different ways. The couplings vary from open (where the networks are completely separated) to very tight, where the WLAN equipment becomes integrated elements within the 3G infrastructure and are connected with a Serving GPRS Support Node (SGSN). The residential infrastructure makes a tight coupling difficult, as the access point is connected to the RGW that in turn is connected to the fixed broadband access network and not to the 3G infrastructure. A tunnel from each RGW to the SGSN can realize the tight integration in the case where the service provider offering the sharing of residential access for roaming WLAN users is the same as the 3G operator. In the case where the 3G operator and the service provider offering the residential sharing for roaming WLAN users are not the same, the level of integration is likely to be limited to *loose coupling*, a common authentication phase where the user does not see significant difference in the way access is granted and the mobility broker

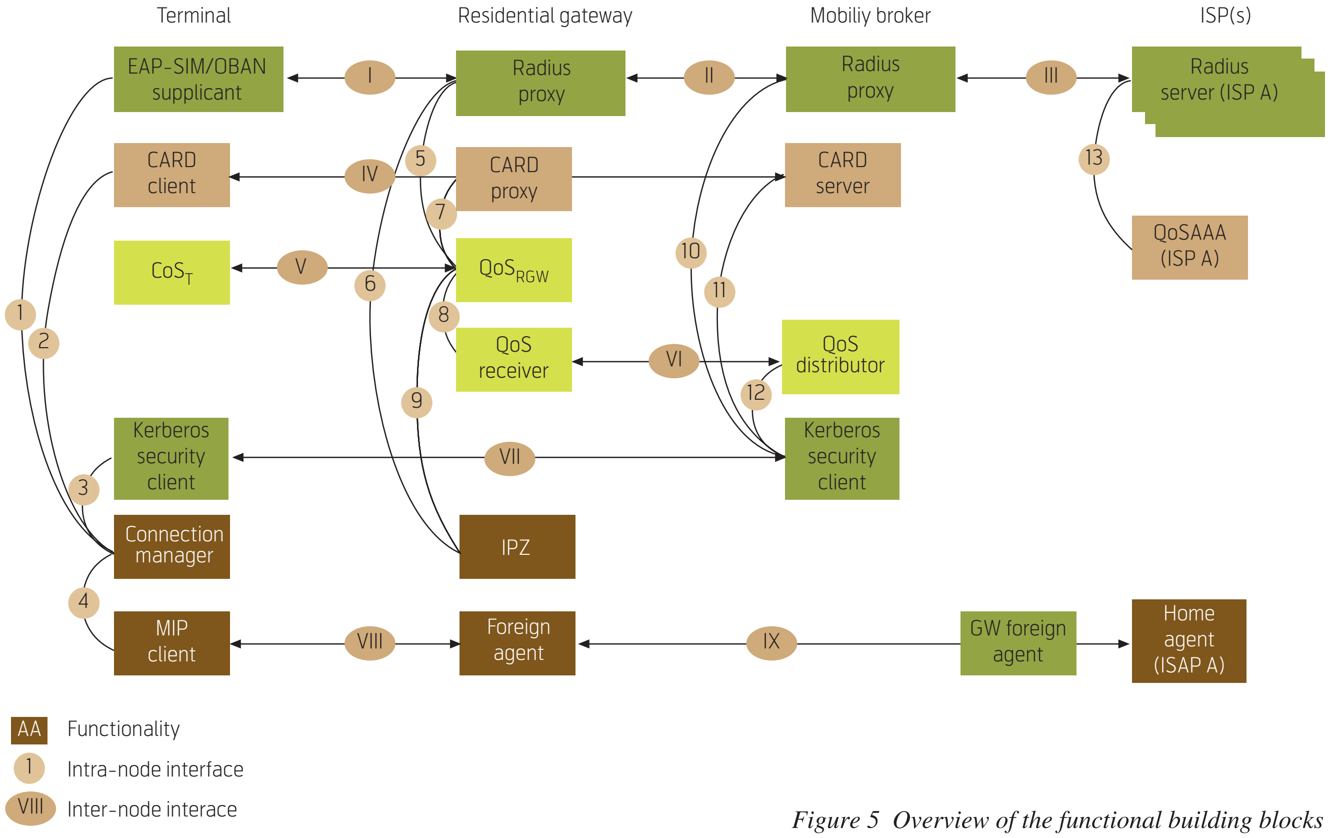


Figure 5 Overview of the functional building blocks

Intra-node interfaces used in Figure 5

1	Exchange of the Kerberos-style tickets used in the EAP-OBAN authentication and shared secrets used to derive encryption keys for the wireless link
2	CARD requests for information about neighbouring APs and requests for Kerberos-style tickets for handover candidate RGWs
3	Initial establishment of shared secret between the Terminal and the Mobility Broker
4	Control and status messages between the Connection Manager and the Mobile IP Client
5	VUs QoS profiles extracted from Radius Vendor Specific Attributes in the EAP-SIM authentication reply intercepted by the Radius proxy
6	Upon successful authentication of VU the Radius proxy sends a request to the IP Zone to open the firewall for the VUs terminal
7	When extending the QoS solution scope from one AP to an entire residential sharing network, the mobility of visiting users is an important aspect that must be considered to assure service continuity when roaming through the network. Preferably, a previously assigned QoS level (profile) should be guaranteed again by the next RGW. Before initiating a hand-off a terminal needs to discover the available network resources at other RGWs. Based on the MAC addresses of the observed APs, the terminal will query its local RGW about the network resource availability on the observed RGWs. As soon as the terminal roams to the next RGW, the authentication process is performed in the non-critical path. Again, the QoS_{RGW} will intercept the set of QoS profiles and subsequently assign and guarantee the selected QoS profile to the concerned user, as discussed earlier
8	See Inter-node interface VI below
9	Up- and downstream limits for the VU. The IPZ sets IP tables and Traffic Control parameters in accordance with this information
10	EAP-SIM authentication requests from the Kerberos Security Server to the AAA server during establishment of a shared secret between the Terminal and the Mobility Broker
11	The Kerberos Security Server listens for ticket requests from the CARD Server, originating from the visiting user's terminal. When a request is received, a ticket is generated and returned to the client via the CARD Server
12	See Inter-node interface VI below
13	QoS profiles which are added as Vendor Specific Attributes to the authentication reply

Table 1 Intra-node interfaces as shown in Figure 5 and the information exchanged between them

Inter-node interfaces	
I	The EAP-SIM/OBAN protocol is an authentication protocol consisting of an EAP-SIM and an EAP-OBAN authentication path. In the absence of a valid fast handover ticket for the RGW in question, EAP-SIM authentication will be used.
II	Radius requests to the AAA server and replies containing QoS profiles for the authenticated user as Vendor Specific Attributes.
III	Same as inter-node interface II
IV	Modified IETF CARD protocol used by the terminal to collect information from the Mobility Broker about neighbouring AP/RGWs, and request fast handover tickets. Also used to exchange location and QoS information between MB and RGWs.
V	QoS protocol used to update the QoS_T with current QoS constraints.
VI	QoS protocol used to prepare an RGW for a potential handover by distributing QoS profiles for potentially new VUs, i.e. users that have requested a Kerberos style ticket for that RGW. These profiles are extracted from the Radius replies received by the Radius proxy on the MB and distributed to the RGW by the Kerberos Security Server when it issues a ticket for the same RGW.
VII	Tunneled EAP-SIM protocol used to establish a shared secret between the Terminal and the Mobility Broker.
VIII	Mobile IP protocol, see [13]
IX	Same as inter-node interface VIII

Table 2 Inter-node interfaces as shown in Figure 5 and the information exchanged between them

communicates with the 3G operator via the GGSN for checking credentials. The network of the service provider who offers access to the residential gateway is then functioning as an equivalent of a 3G visiting network. The mobility broker may also function as a packet data gateway and establish a tunnel to the GGSN which is architecturally the same as introducing a mobile IP gateway foreign agent in the mobility broker that in turn has tunnels with home agents, that may either reside in a GGSN or somewhere else.

4 Conclusions

Exploiting the residential network for public access is an interesting business case and is technically feasible, but has challenges. In this paper, architecture and solutions to solve the challenges developed in the IST OBAN project have been shown. Forcing visiting users to authenticate before granting network access allows associating traffic profiles with each user, which in turn can be used to enforce and predict the resource consumption of the residential access facility and also allows charging the visiting user for the consumed network access. By separating residential and visiting users in separate virtual WLANs, the situation can be prevented that visiting users gain access to peripherals and/or data of residential users. In order to solve fast and secure handoff within time constraints, the concept of a mobility broker was introduced. This component, located in the access network, has a service contract with the various service providers who offer broadband residential access. By involving the mobility broker in resolving multiple disjoint Kerberos realms, the security bottleneck that prevents fast handovers between neighbouring residential access facilities can be removed. The mobility broker is involved in two out of three handover phases: the phase where information needs to be gathered to select the best residential access point for each visiting user and the phase where the visiting user performs the actual handover. The period that bridges these two phases is called network selection and is used by the WLAN station to make a decision which network to select to perform the handover.

5 Acknowledgments

The work reported in this paper was supported in part by the IST 6FP programme of the European Commission under contract OBAN, No 001889.

6 References

1 Francis, J C, Zurkinden, A. Deterministic Handover in Open Broadband Access Networks. *Proc. Int. Workshop on Broadband Wireless Access for Ubiquitous Networking*, Alghero, Sardinia, September 2006.

2 CISCO white paper. *Capacity, Coverage, and Deployment Considerations for IEEE 802.11g*. 12 June 2006 [online] – URL: http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_white_paper09186a00801d61a3.shtml.

3 Shaw, R. *And we'll have FON, FON, FON : Skype, Google to help fund global WiFi network*, ZDNET blogs. 5 February 2006 [online] – URL: http://blogs.zdnet.com/ip-telephony/?p=890.

4 Leung, K K, McNair, B, Cimini, L J Jr., Winters, J H. Outdoor IEEE 802.11 Cellular Networks: MAC Protocol Design and Performance. *IEEE ICC 2002 Communications on Broadway*, New York, USA, 28 April – 2 May 2002.

5 Kuzminskiy, A M. EIRP-restricted downlink beamforming in WLAN OFDM systems. *Proc. IEEE Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Cannes, July 2006.

6 Liebsch, M, Singh, A (Eds.), Chaskar, H, Funato, D, Shim, E. *Candidate Access Router Discovery (CARD)*. (IETF RFC 4066)

7 Hoekstra, G J, Østerbø, O, Schwendener, R, Schneider, J, Panken, F J M, van Bemmel, J. QoS solutions for open wireless access networks. *IST Mobile Summit*, Dresden, June 2005.

8 Panken, F, Hoekstra, G, van der Gaast, S. Resource allocation and guarantees for real-time applications in WLANs. *Telektronikk*, 102 (3/4), 125–134, 2006. (This issue)

9 Haverinen, H, Salowey, J. *Extensible Authentication Protocol Method for Global System for Mobile Subscriber Identity Modules (EAP-SIM)*. January 2006. (RFC 4186)

10 Rigney, C, Willens, S, Rubens, A, Simpson, W. *Remote Authentication Dial In User Service (RADIUS)*. June 2000. (IETF RFC 2865)

11 Jaatun, M G, Tøndel, I A, Johannessen, T H. Security in Fast Handovers. *Telektronikk*, 102 (3/4), 111–124, 2006. (This issue)

12 Jaatun, M G et al. Secure Fast Handover in an Open Broadband Access Network using Kerberos-style Tickets. *IFIP SEC2006*, Karlstad, Sweden, 22–24 May 2006, 389–400.

13 Perkins, C (Ed). *IP Mobility Support for IPv4*. August 2002. (IETF RFC 3344)

14 3GPP. *Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 6)*. September 2003. (3GPP TR 22.934 V6.2.0)

15 3GPP. *Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking*. December 2004. (3GPP TR 22.234 v 6.2.0)

16 3GPP. *3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3*. 2004. (3GPP TS 29.234)

Frans Panken received his MSc degree in applied mathematics from the University of Twente and the PhD degree in computing science and mathematics from the University of Nijmegen in 1992 and 1997, respectively. In 1997 Frans joined Lucent Technologies where he currently works as senior member of technical staff in the Bell Labs Europe department located in Hilversum, the Netherlands. Dr. Panken has been involved in various research projects funded in part by the EC and the Dutch government and was work package leader within the FP6 project OBAN. His research interests range from stochastic modelling and performance analysis of communication networks to specifying open and application programmable interfaces.

email: frans@lucent.com

Haakon Bryhni is Dr. Scient (PhD) from the University of Oslo, where he served as Associate Professor II. He also holds a Master in Engineering from the Norwegian University of Science and Technology. Dr. Bryhni is CTO of Birdstep Technology Norway.

email: haakon.bryhni@birdstep.com

Paal E. Engelstad completed his PhD on resource discovery in Mobile Ad hoc and Personal Area Networks in 2005. He has also a Bachelor and Masters degree (Honours with Distinction) in Applied Physics from NTNU, Norway, and a Bachelor degree in Computer Science from University of Oslo, Norway. After working five years in industry, he joined Telenor R&I where he focuses on IETF and IP technology (e.g. IP mobility, IPv6, QoS, MANET and AAA-issues) and IEEE wireless technologies (e.g. 802.11, 802.15 and 802.16). Paal Engelstad has published 36 refereed papers in journals and proceedings and holds three patents (two pending).

email: Paal.Engelstad@telenor.com

Leif Hansson holds a BSc in System Analysis and System Design and has also graduated from the Military Academy as a Technical Officer specializing in communication technology. After leaving the Defence Material Administration he worked for eight years as a professional in the telecom industry. He now works in Birdstep Technology ASA as Research Project Manager.

email: leif.hansson@birdstep.com

Gerard Hoekstra received his BSc and MSc (cum laude) degrees in electrical engineering in 1996 and 1999, respectively, from the Hanzehogeschool Groningen and the University of Twente, both in the Netherlands. After working for Alcatel's Corporate Research Centre in Antwerp, Belgium, he joined Lucent Technologies in 1999 and is currently a member of technical staff in the Bell Labs Europe department, located in Hilversum, the Netherlands. Gerard has been involved in various research projects funded by the EC and the Dutch government. His research interests range from network modelling and simulations, performance analysis, packet resequencing algorithms, to importance sampling techniques.

Martin Gilje Jaatun received his MSc degree from the Norwegian Institute of Technology (NTH), University of Trondheim in 1992. From 1993 to 1997 he worked for the security consultancy firm System Sikkerhet AS (now: Secode Norway), and then as scientist at the Norwegian Defence Research Establishment (FFI) from 1997 to 2002. He then served as Senior Lecturer in Information Security at the Bodø Graduate School of Business (HHB) until 2004, after which he has finally settled down as research scientist at SINTEF ICT. His research interests cover (too) much of the IT security field, possibly with special emphasis on communication security.

email: Martin.G.Jaatun@sintef.no

Tor Hjalmar Johannessen is Senior Adviser at Telenor R&I. He graduated from the University of Oslo in 1975 as Cand.Real. After working with military crypto systems at Alcatel Telecom since 1989, he joined Telenor R&I Security Group in 2000. His main interest and occupation has been security in general and deployment of PKI systems in particular, which includes several engagements for ZebSign and Telenor Mobil mCommerce. He participates regularly in ETSI ESI and CEN/ISSS WS on Electronic Signatures. He has been co-writer of EURESCOM P1001 deliverables, and also given several lectures on PKI and security topics.

email: Tor-Hjalmar.Johannessen@telenor.com

ISSN 0085-7130 © Telenor ASA 2006

Section 3 – Service and Business Opportunities

EINAR EDVARDSEN

Einar Edvardsen is Senior Adviser in Telenor R&I

Section 3 contains a selection of papers addressing services and business opportunities. Up to the present time the fixed broadband network has been almost inaccessible to people. The only location where the network could be accessed has been at each user's home or office since the subscription agreement is not valid outside the four walls of their home. This situation has changed with the introduction of the OAN concept. In an OAN users are able to authenticate themselves at many places, i.e. wireless via other people's WLAN to the fixed broadband access network. This feature of an OAN opens a number of new opportunities as regards services that may be offered over such a network, but it may also create a room for new market players and force changes to the relation between existing market players. Thus, the three papers in the third section address some of the most important aspects related to how these new opportunities can be commercially exploited and how they also give value for people by offering increased network availability and improved services.

The paper called *Services and Applications in Future Wireless Networks* by Josef Noll gives a glimpse of the future application of broadband, both as regards how people may connect to a ubiquitous network and also how future terminals, services and applications will develop and make life easier for people. Simplicity to connect and simplicity to use are key features that are about to be available to people. Adaptable terminals that can be used in different networks like mobile networks, WLANs and fixed networks are already on the market. Such terminals can be considered as steps towards a future where people do not need to bother about what network they want to connect to, the terminals make their own decision dependent on the services that are actually run.

The popularity of WLANs has been the enabler for companies like FON[1], Boingo[2], LinSpot[3], The Cloud[4] and also for some other initiatives based upon WLAN technologies. The paper *Actors, Activities and Business Opportunities in Open Broadband Access Markets Today* by Thor Gunnar Eskedal and Tor Hjalmar Johannessen gives an introduction to these initiatives and explains their business models.

OAN networks can be realised and operated by a number of constellations between existing as well as newcomers on the market. We may see a rise of community operators like the one of FON, but the traditional telecom operators may also take the leading role. At the present time it is impossible to predict how it will develop. There is, however, a number of reasons pointing towards increased roles for the existing network and service providers. The paper *Business Scenarios for Open Broadband Radio Access* by Thor Gunnar Eskedal et al. contains a comprehensive analysis of a selected number of scenarios.

Charging for access and use of broadband services is a critical premise for any business model. Fixed subscription fees and volume based charging have been the dominant ways to create income, but with the appearance of new service providers on the market, this is about to change. Other ways of creating income are being tested and applied. The paper *Charging Models in the Open Broadband Access Market – Theory and Practice* by Andrea Amelio presents an evaluation of some of the best known charging models.

[1] *http://en.fon.com*

[2] *http://www.boingo.com*

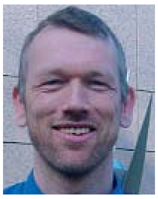
[3] *http://www.linspot.com*

[4] *http://www.thecloud.net*

ISSN 0085-7130 © Telenor ASA 2006

Services and Applications in Future Wireless Networks

JOSEF NOLL



Josef Noll is Prof.stip. at the University Graduate Centre at Kjeller (UniK), Norway

This *Telektronikk* contribution will provide a view on the future wireless service landscape, with a special focus on seamless service access to wireless services. Authentication for mobile network access is performed through the SIM card. In wireless networks such as the IEEE802.11 family authentication might be provided through SIM related protocols being the Extensible Authentication Protocol for Subscriber Identity (EAP-SIM) and the EAP for UMTS Authentication and Key Agreement (EAP-AKA). With the help of the Bluetooth SIM access profile (SAP), the SIM credentials can be transferred from one device (typically the mobile phone) to a second device (a laptop) for seamless WLAN network access for the user. Near field communication (NFC) has the potential of providing contactless authentication services, including identification to home devices. A critical issue is NFC2SIM, the interface from NFC to the SIM card. The contribution concludes with an overview over upcoming personalised broadband wireless services, including home data access and community services.

1 Introduction

Third generation (3G) mobile systems have entered the market, providing enhanced functionality to deliver multimedia communication to the mobile user. Network costs and limited cell capacity [1] have opened discussions on how to extend the public cellular network using other access networks, e.g. WLAN access or using UMTS as a return channel for a personalised DVB system. Such integration also requires additional network functionality for interworking and interoperation. The resulting system clearly represents an advanced stage of 3G, or even beyond 3G (B3G) depending on the definition. Work is ongoing in standardisation, specifically within ITU in the special study group on IMT-2000 and beyond IMT-2000 [2]. The Wireless World Research Forum and 3G.IP are other organisations heavily involved in B3G [3][4].

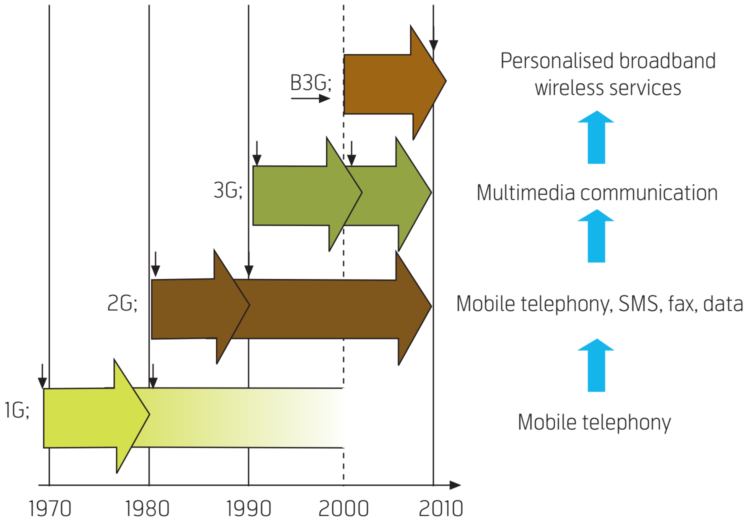


Figure 1 Service evolution from mobile telephony to personalized broadband wireless services

The major conclusions from the ongoing work state the need for addressing the relationship between User preferences, Services, and Technologies [5]. Access is expected to be provided through all kinds of wireless access networks, ranging from broadcast to wireless/mobile access systems. The main focus will be on providing personalised wireless services to the user.

This paper will in Section 2 provide an introduction to systems beyond 3G, address the communication challenges in Section 3, and introduce identity management in Section 4. It provides an overview over future community services in Section 5. The paper finally provides examples of services in the digital world in Section 6, and conclusions in Section 7.

2 "Beyond 3G"

Mobile telecommunication systems were previously defined in *generations* (see Figure 1). In the analogue system, mobile telephony was the first telecom communication service. One of the main reasons for introducing GSM was mobile telephony service provision in European countries, including SMS and data services. 3G was introduced to provide roaming on a world-wide base, and compatible standards such as UMTS currently provide multimedia communication in the whole world. "Systems beyond 3G" will provide personalized wireless broadband access and will incorporate mobile and wireless access methods including e.g. Wi-Fi, WiMAX [5].

Standardization of the system B3G started in 2000, and consists of the three major elements:

- *Wireless services:* Users prefer to receive their services wireless, either through the mobile network or a wireless (Wi-Fi) connection. This statement is

ISSN 0085-7130 © Telenor ASA 2006

underlined by the sales numbers of mobile phones and laptops: There are 1.5 billion cell phones in the world today, more than three times the number of PCs [6]. In June 2005 the number of laptops sold bypassed the number of fixed PCs [7].

- *Broadband services:* Market expectations for fixed broadband services estimate that 60 % of households will have broadband in 2007 [8]. Mobile broadband services like TV and video telephony are available in most 3G markets.

- *Personalised Services:* The wide distribution of mobile phones has increased the need for adapting the content to both user preferences, terminal and network capabilities.

2.1 Wireless services

The major challenge of wireless service provision is the variation in radio quality. Radio is a shared resource, and the quality of the radio link is affected by:

- User mobility,
- Radio environment (user speed and coverage radius),
- Application topology, and
- User terminal requirements.

Service delivery to a wireless terminal should take into account the Quality of Service (QoS) measures on the radio interface, e.g. propagation delay, variation of delay, bit error rate, error free seconds, distortion, signal to noise ratio, duration of interruption, interruption probability, time between interruption, bit rate, and throughput. These parameters will depend on the user and terminal environment, and underline that an optimum access will have to use all available wireless and mobile connections.

2.2 Broadband services

Gordon Moore's prediction, popularly known as Moore's Law, states that the number of transistors on a chip doubles about every two years (Figure 2) [9]. Since the start of the digital age the amount of information created is tripled approximately every 12 months. Comparing these growth rates with the increase of modem speed and air interface capacity shows that modem speed has a similar growth rate to the number of transistors, while air interface capacity has not increased substantially from GSM to 3G/Wi-Fi. The experienced increase in air capacity is due to increased bandwidth B of the communication channel, from B_{GSM} = 200 kHz in GSM to B_{UMTS} = 3.8 MHz in UMTS, and $B_{802.11}$ = 25 MHz for 802.11b.

Claude E. Shannon defined the capacity C of a system as being proportional to the bandwidth B

$$C = B \log_2 (1 + P / N_0 B), \qquad (1)$$

with B the bandwidth of the carrier, P the signal power and N_0 the noise level of the system. For a given bandwidth B, the maximum range R_{max} is a log-function of the signal to noise ratio

$$R_{max} = \log_2 (1 + P / N_0) \qquad (2)$$

Propagation attenuation (free space loss) is proportional to the carrier frequency, thus carriers such as Wi-Fi have shorter ranges than GSM, but provide higher throughput. These indications support the usage of specific access networks for applications, e.g. broadcast for video, Wi-Fi for email and ftp services, and GSM/UMTS for mobile services. It can be assumed that services are available through all access networks, but will have their preferred network for operations.

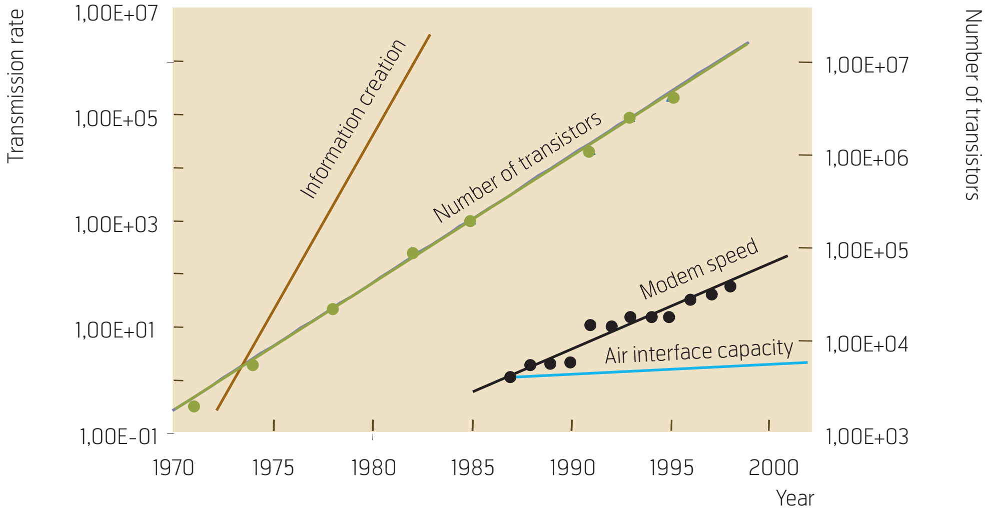


Figure 2 Moore's Law in transmission capacity and information creation

2.3 Personalised services

In order to design and develop innovative and successful services one has to understand the user and be able to "guess" his needs. This is the area of market researchers and service designers who have to sense and test the usability and social impacts of new service concepts, while looking for the added value that could make a service offer a success. To that end a phased methodology is recommended addressing the following topics [5]:

1 Understanding the users by understanding their culture and lifestyle;

2 Creating potential service concepts that satisfy particular user needs described by technical details and likely usage;

3 Validating the service concept against potential users by means of prototypes and models.

To build these types of personalised services is a challenge to the system design as well as the user interface. The system should be flexible and allow the definition of personal preferences, and these should be carried seamlessly with the user as he moves geographically or between access networks. The user interface should be such that personalisation is easy and intuitive. Personalisation might be supported by "learning" profiles handling the preferences of the user, the "presence" (where is the user, what is he doing), and the social/community characteristic of a user.

The next section will provide an overview of existing developments in order to overcome the borders between wireless and mobile networks.

3 Communication challenges

This section addresses the communication challenges of a mobile user, analysing trends in radio communication development, the position of the mobile phone and authentication as key issue for user acceptance.

3.1 Radio communications

Section 2 has concluded that optimum access networks will have to be used for the specific applications. This section will look into existing standardisation and market trends for wireless network access, e.g. UMA, IMS, and Bluephone.

3.1.1 Unlicensed Mobile Access (UMA)

The UMA Technology specification will allow the usage of mobile phones in unlicensed bands, typically using Wi-Fi or Bluetooth as radio interface. Typical applications cover the home and office environment, where WLAN subnets exist, but usage of mobile phones in those networks is not yet supported. Submitted in February 2005 to the 3rd generation partnership project (3GPP), UMA specifications are adopted as Generic Access Network (GAN) within the GERAN (GSM/EDGE Radio Access Network) TSG (Technical Specifications Group).

UMA has thus become the standard for fixed-mobile convergence (FMC). UMA technology enables access to mobile voice, data and IMS services over IP broadband access and unlicensed spectrum technologies. By deploying UMA technology, service providers can enable subscribers to roam and handover between cellular networks and public and private unlicensed wireless networks using dual-mode mobile handsets. With UMA, subscribers receive a consistent user experience for their mobile voice, data and IMS services as they transition between networks [10].

3.1.2 British Telecom – Bluephone/Fusion

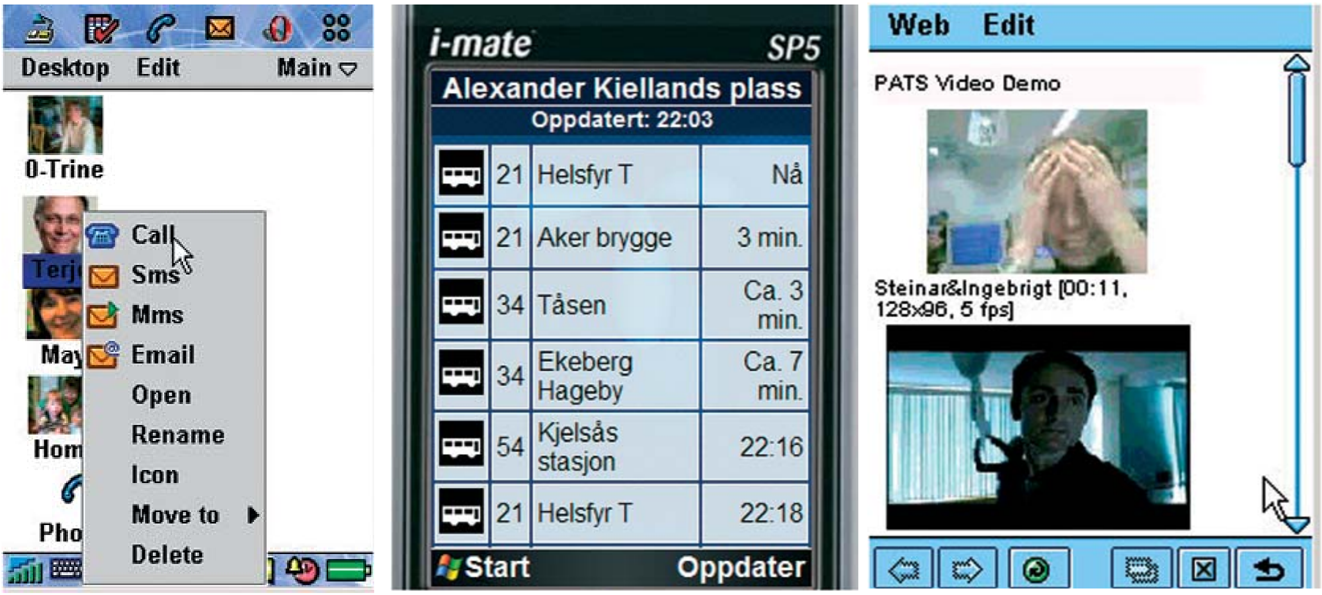
While Eurescom launched a study called "Public Bluetooth Access" in 2001 [11], parallel developments started at British Telecom (BT) to enable Bluetooth based mobile services. Technical problems such as interference, especially in the voice channel, and missing standardisation delayed the launch of the *Bluephone* product until mid June 2005 [12]. After successful customer testing in 2005, BT runs the service as a conventional FMC package called *Fusion*, offering a Wi-Fi/Bluetooth combined router, which users can plug into BT's Broadband ADSL at home. Currently two mobile phones are supported, Motorola's RAZR V3 and V560.

The main difference between *Fusion* and UMA is the focus of the network operator. *Fusion* is based on SIP and IMS standards, thus promoting the developments in the direction of next generation networks, while UMA brings the home area into the mobile network, using mobile network core technologies.

3.2 My future terminal

While the access network development will follow the main position of the operator, i.e. mobile operators will tend to promote UMA, while fixed network operators will promote *Fusion*-like approaches, the developments on the terminal side are more widespread.

We see two major trends, on the one hand following the PC and making applications available for the mobile user, and on the other hand the development of specific mobile services, promoting lifestyle and community services. The mobile phone has the major advantage as it is available 24 hours / 7 days a week, as compared to about 4 h average usage of a PC.



Alexander Kiellands plass
Oppdatert: 22:03

21	Helsfyr T	Nå
21	Aker brygge	3 min.
34	Tåsen	Ca. 3 min.
34	Ekeberg Hageby	Ca. 7 min.
54	Kjelsås stasjon	22:16
21	Helsfyr T	22:18

Figure 3 Functionality of mobile terminals, e.g. communication portal (left), public transport information (middle, from [13]), video/surveillance (right)

Thus, the mobile phone provides the *always online* functionality with availability, email and Internet access (see Figure 3). While this trend is visible in the enterprise market, the consumer market is dominated by lifestyle trends. Decisions to buy a certain phone are rather based on attitude, e.g. the tough phone for the outdoor person, and the city phone for the urban person.

What is common in both trends is that service availability has reached all phones. Communication and interaction is provided, connectivity to my community (Figure 3, left), local services such as public transport information (Figure 3, middle) and video/TV (Figure 3, right) show some of the potential services.

The mobile phone has several service enablers inbuilt, i.e. positioning information, potential for seamless and personalised service access, mobile commerce, and adaptation of content to personal preferences. However, these advantages are not yet properly addressed by the operators. The following section will provide examples of personalised service access, indicating the potential of mobile services, but also addressing the current deficits.

3.3 Device, network and service authentication

Authentication is the key for a customer relation, and the entry for value-added services. Telecom customers are used to hassle-free access (GSM works everywhere), and will expect the same functionality for access to other networks and services. The customer is used to having the mobile phone around, and the SIM card opens for authentication and encryption in every wireless network (Bluetooth, WLAN, WiMAX) in addition to GSM and UMTS.

Service authentication has to satisfy the security requirements of the application, e.g. *nice to know* security for network access, *need to know* security for email and intranet access and *have to know* security for VPN and *m*Commerce services. We suggest the following the mechanisms from the Initiative for open authentication (OATH[1]):

- SIM authentication (SIM)
- Public Key Infrastructure (PKI)
- One-Time-Password (OTP).

These mechanisms fulfil the requirements of the Norwegian Government and other European countries for an *e*Signature. The mobile phone has the capabilities of providing all of them: SIM, PKI and OTP, and thus may provide the security requirements for various applications in the virtual world.

The security requirements might be satisfied through SIM authentication and can be enhanced through a password/pin mechanism. The highest security requirements are required for *have to know* services, such as admin access to home content or electronic transactions. We recommend a PKI based authentication, which most European Operators have on their SIM cards [14].

[1] *http://www. www.openauthentication.org/*

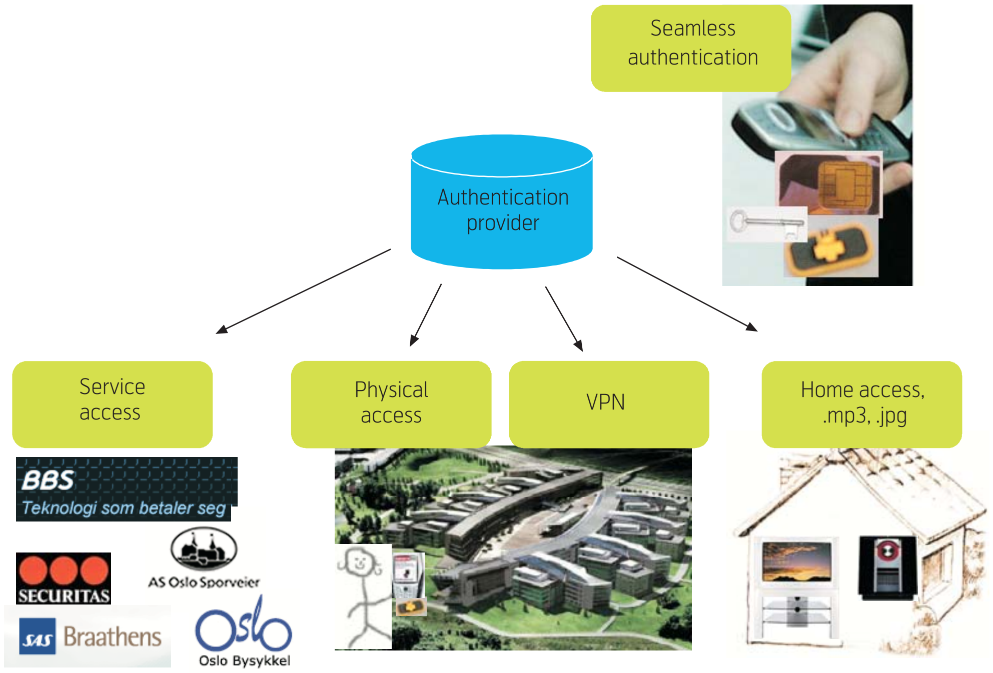


Figure 4 The mobile phone as authentication device for admittance, network and service access

4 My identity in the digital world

This section postulates the need for identity in the virtual world. It will identify the threats of using biometric identification, and suggests the mobile phone as an identifier. In the virtual world identity is verified through an authentication mechanism. The Web community has defined Laws of Identity, providing a unifying identity meta-system that can offer the Internet the identity layer it needs [15]. One of the conclusions is to provide the user with the capabilities of providing exactly the information required to receive the service, and not his complete identity.

4.1 Biometrics versus SIM card

Biometrics, especially the fingerprint is used nowadays for identification to systems and services. Fingerprint authentication is used by Lufthansa to speed up check-in procedures and the hand's palm vein pattern by the Tokyo-Mitsubishi banks to increase security in ATM money withdrawal. Avivah Litan, an analyst with Gartner, argues that biometrics is the most secure form of authentication because it is the hardest to imitate and duplicate [16].

Current discussion is ongoing on how a safe storage of biometric information can be performed. Once biometrical information is stolen, it cannot be revealed. The fear of permanently losing your ability to use a biometric trait has caused European Legislators to deny usage of biometrical information. Measures are taken as e.g. a two-factor protection of the biometric information to protect the information, but the missing revocation is the most critical issue when it comes to biometrics.

Section 3.3 introduced the security mechanisms needed for different kinds of applications and has a two-factor authentication for the *has to know* security level. The SIM card in the mobile phone has the capability of providing all levels of authentication and supports mechanisms for revocation of credentials stored in the SIM card. A SIM card is only active if authenticated by the network operator. If the SIM card gets stolen, the operator can disable the card. The main challenge is on how SIM information can be securely distributed to other devices and services.

4.2 Supporting technologies

SIM authentication is used for GSM/UMTS network access and also as transaction receipts for content download, e.g. ring tones. Including authentication methods through Bluetooth and Near Field Communications (NFC), SIM-based authentication opens for all types of service access (see Figure 4). The NFC forum has introduced RFID technologies in mobile phones, and thus allows the mobile phone to replace contactless credit cards and admittance cards [17].

With the introduction of the NFC technology into the mobile phones, the SIM card takes a more important role for payment, ticketing and SIM card providers. When NFC functions as a contactless card, it requires a place to store critical information such as ticket numbers, credit card accounts or ID information. This storage place could basically be anywhere in the mobile phone (RAM), but since the SIM card has storage capacity and already offers a high level of security, it is the obvious place for storage of critical and sensitive information (Figure 5).

ISSN 0085-7130 © Telenor ASA 2006

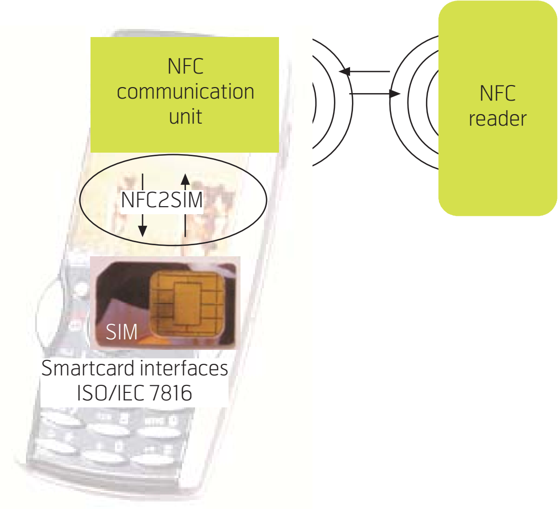


Figure 5 Mobile authentication based on near field communications (NFC)

Communication between the NFC chip and the SIM card, called NFC2SIM, has to be developed and standardized. This is one of the main reasons why NFC mobile phones are still in the demonstration phase. The communication between the SIM card and the NFC chip requires a high-speed transaction in order to offer a real alternative to today's ticketing and payment systems. Users would not accept a new ticketing solution that is not easier or faster than the already available solutions offered by contactless plastic cards.

Authentication for network access is performed in the mobile network through the SIM card. In wireless networks such as the IEEE802.11 family authentication might be provided through various protocols, with the two SIM related protocols being the Extensible Authentication Protocol for Subscriber Identity (EAP-SIM) and the EAP for UMTS Authentication and Key Agreement (EAP-AKA). If a mobile phone supports EAP-SIM, it can seamlessly connect to WLAN networks using the SIM card. With the help of the Bluetooth SIM access profile (SAP), the SIM credentials can be transferred from one device (typically the mobile phone) to a second device (a laptop) for seamless WLAN network access of the user. The EAP-SIM and Bluetooth SAP profile interworking has been demonstrated on several occasions, but is currently only available for a limited number of mobile phones [18].

SIM-based service authentication in mobile networks is known from premium SMS services, e.g. ring tone and logo download. Operators have introduced the SIM authentication also for WAP services, allowing e.g. a seamless access to the personal email account through the WAP portal. The WAP gateway adds an information string to the http header, which is forwarded to the content server. The string contains both information on the user and the device requesting the service. The user (x-nokia-alias) is represented through an md5 hash of the mobile ID (MSISDN), and the device is represented through a device identifier (mobile phone type) [19].

The following section will provide examples of services based on seamless authentication.

5 Community services

Having addressed security requirements and mobile phone/SIM-based authentication as a major service enabler, this section will address upcoming services. It will first address community services and then position the mobile phone as integrator for mobile and broadband services.

5.1 Communities, groups and roles

The digital services trend has reached everyday life. Information is spread by Internet, email and SMS, rather than by plain paper. Youngsters use micro coordination, using the mobile phone to communicate with their community at every minute of the day [20]. Depending on the context, these communities are changing, ranging from working colleagues to friends, to members of classes, school, or sporting clubs. Figure 6 indicates a location based service for a friend community, indicating at all times where your friends are, and even introducing an alert when a friend comes nearby. The mobile phone is the preferred device to keep control of your communities, providing availability, location and communication.

Community services will become more dominant in the future, addressing contact, location and availability as well as exchange of pictures, music and other digital content.

5.2 Digital content: picture, video, music

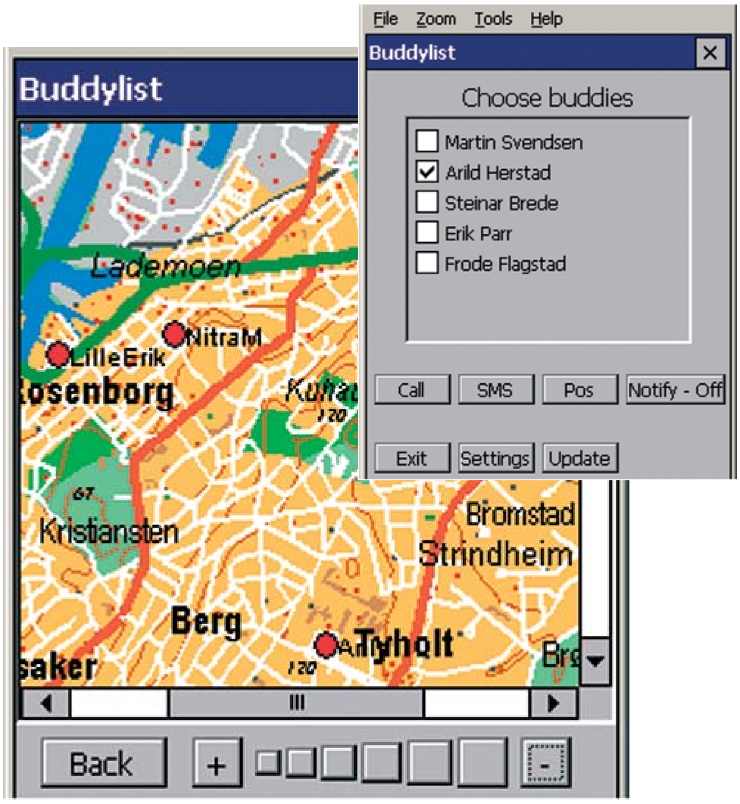
The digital home has turned into reality. As predicted by the Eurescom study P1401, flat screen and high-definition TV (HD-TV), broadband recording either on DVD or on hard-disk recorders, and the transformation from analogue to digital video and photography are the dominant events in 2006 [8]. The home broadband connection (e.g. ADSL) supports always online and enables on-demand services. Residential gateways are getting more mature, cheap, and offer innovative services in addition to communication. The social drives of a broadband, always-on connection are on-demand video and multimedia social connectivity. The home portal becomes the centre for communication, making people's content available in and outside the home and allowing for the control of the home infrastructure.

Even though video and TV recording are the current drivers, photo and music exchange are mature market services. Current upload/download network access rates support file exchanges (typical 1–3 Mb) and audio streaming (typically 128 kbit/s), while video exchange is still cumbersome. More advanced personal data recorders will support the streaming of video content in a mobile format, providing reasonable mobile video quality at data rates up to 384 kbit/s.

P1401 suggests to subdivide broadband home services into four categories; Entertainment, Home automation, Personal Enrichment and Social Inclusion [8]. This paper will concentrate on entertainment, providing electronic content like music, video and data while being on the move.

5.3 Mobile and broadband – a synergy

Section 3 has provided evidence for the fixed mobile integration, based on IMS or SIP standards. This paper goes beyond network access, and suggests the mobile phone becoming the identifier for home broadband services (see Figure 7).



Choose buddies

□ Martin Svendsen
☑ Arild Herstad
□ Steinar Brede
□ Erik Parr
□ Frode Flagstad

Figure 6 Community service, location of friends

Digital content in broadcasting is usually secured through a conditional access module (CAM), which requires a Smartcard to decrypt the incoming video streams. These systems, even though registered to a person, are used anonymously, as they stay in the set-top box. The mobile phone has the potential to allow a personalised access to broadband content by providing user information and preferences to the set-top box. This user information can either be provided through Near Field Communication (NFC), see Section 4, or through personal area network access based on e.g. Bluetooth or WLAN. Having established con-

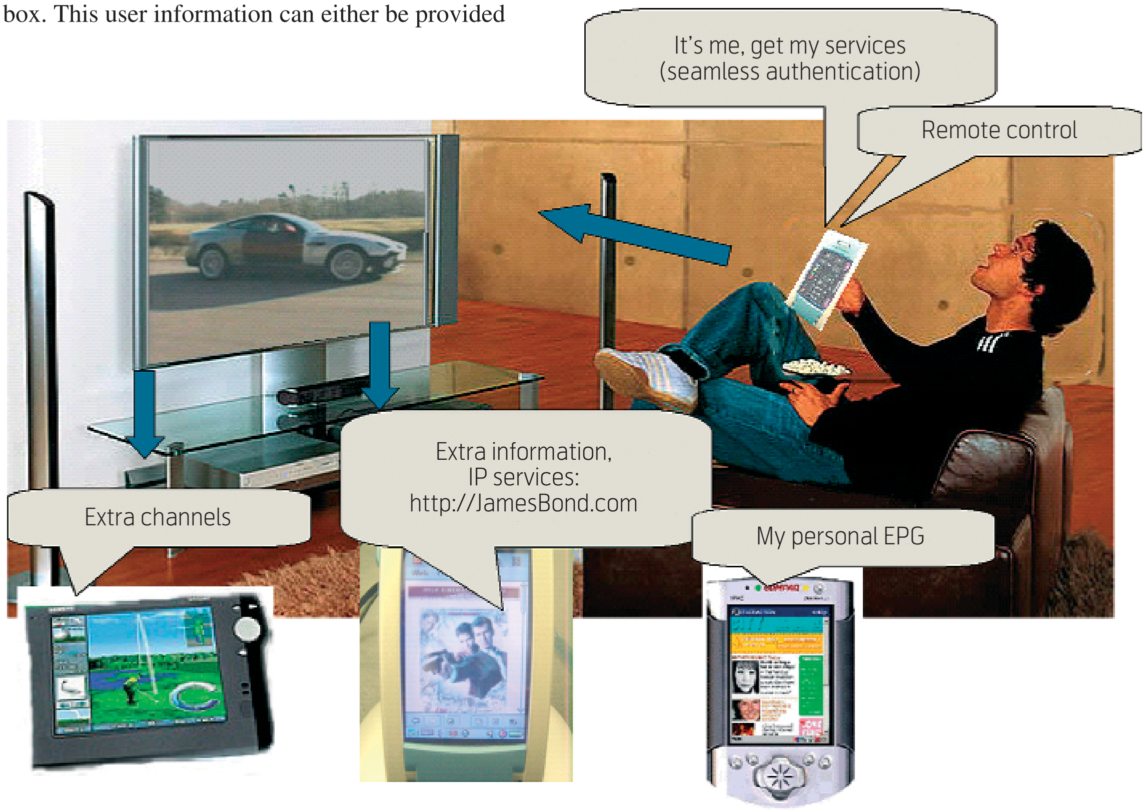


Figure 7 Using the mobile to control and receive broadband services

ISSN 0085-7130 © Telenor ASA 2006

nectivity and authentication, the user would be able to receive a personalised electronic programme guide (EPG), additional services through a locally forwarded channel or might even watch another channel or camera viewpoint on his personal device.

To provide a detailed overview of ongoing developments would exceed the scope of this paper. Lohse et al. provide a state-of-the-art discussion and suggest a network middleware solution, allowing mobile phones to control the digital video recorder, playing music stored in the home device, or chatting with visitors over the home located web cam [21]. The main challenge is to combine the broadcast and IP-world by introducing standards for interworking of authentication and DRM mechanisms in the virtual world.

6 Entering the digital world

Section 4 introduced seamless network and service access based on NFC, Bluetooth/WLAN, GSM/UMTS and WAP gateway authentication. Somogyi extended the seamless authentication to personalization of services for a picture gallery, using both user identity and device identity information [19]. Further work at UniK included access to various types of home content, including music download, web cam based surveillance and community address book.

6.1 Service examples

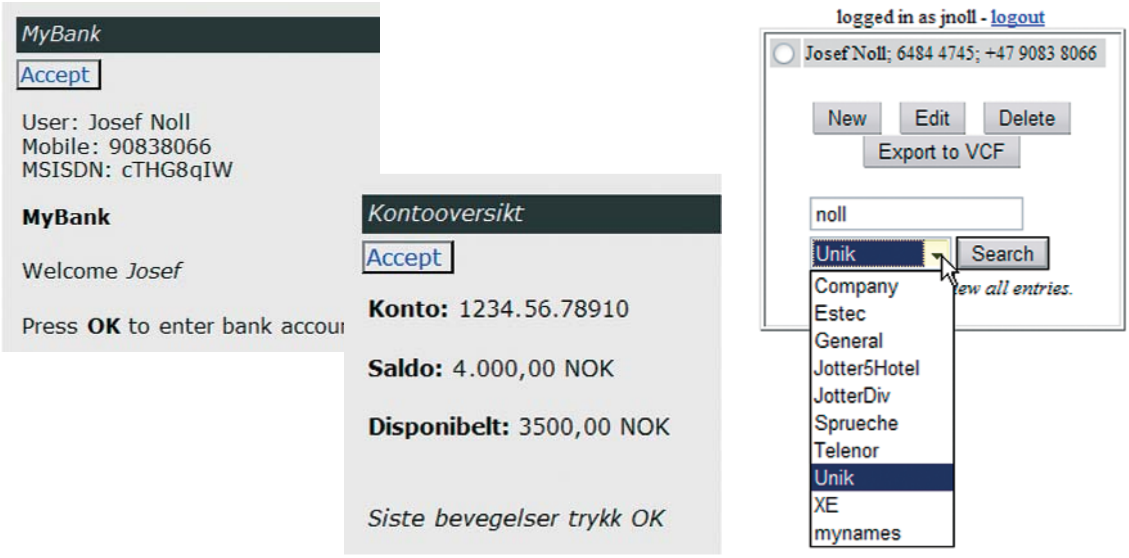
Internet services provide access to personal information through username/password authentication. On a mobile phone or a personal data assistant such a login procedure is not accepted by the customers, as input of text strings and passwords is too cumbersome. This section provides two examples of service access: Internet banking and access to a community data base (Figure 8). Both examples are based on WAP gateway authentication addressed in Section 5. The user is identified through his mobile number, and a provider specific md5 hash of the user id (MSISDN) is delivered to the service provider, here the bank. With this information the *nice to have* service account status and last transactions are provided to the user. For mobile transactions, a *need to have* service has to be provided in the form of a level 2 security, either through one time password or through PKI based authentication.

The second example provides access to a community database, where contact info is stored in specific databases, here a *Company* address list for companies the user has contact with a UniK list for all members at UniK. As compared to a public available database, such a community oriented database allows adding personal information which is only shared by members of the group.

6.2 Challenges/ongoing research

This paper concludes with access to encrypted home content from outside of the home, a typical OBAN case. The functional requirements are based on the following assumptions:

- Content will be available in a digital form, and content storage devices will be networked.
- The user will have a variety of devices which he can use for content access.
- A ubiquitous network allows content access wherever the user is.



User: Josef Noll
Mobile: 90838066
MSISDN: cTHG8qIW

MyBank

Welcome *Josef*

Press **OK** to enter bank accou

Konto: 1234.56.78910

Saldo: 4.000,00 NOK

Disponibelt: 3500,00 NOK

Siste bevegelser trykk OK

logged in as jnoll - logout

○ Josef Noll; 6484 4745; +47 9083 8066

noll

...iew all entries.

Figure 8 Seamless authentication, used for bank access (left) and community address book (right)

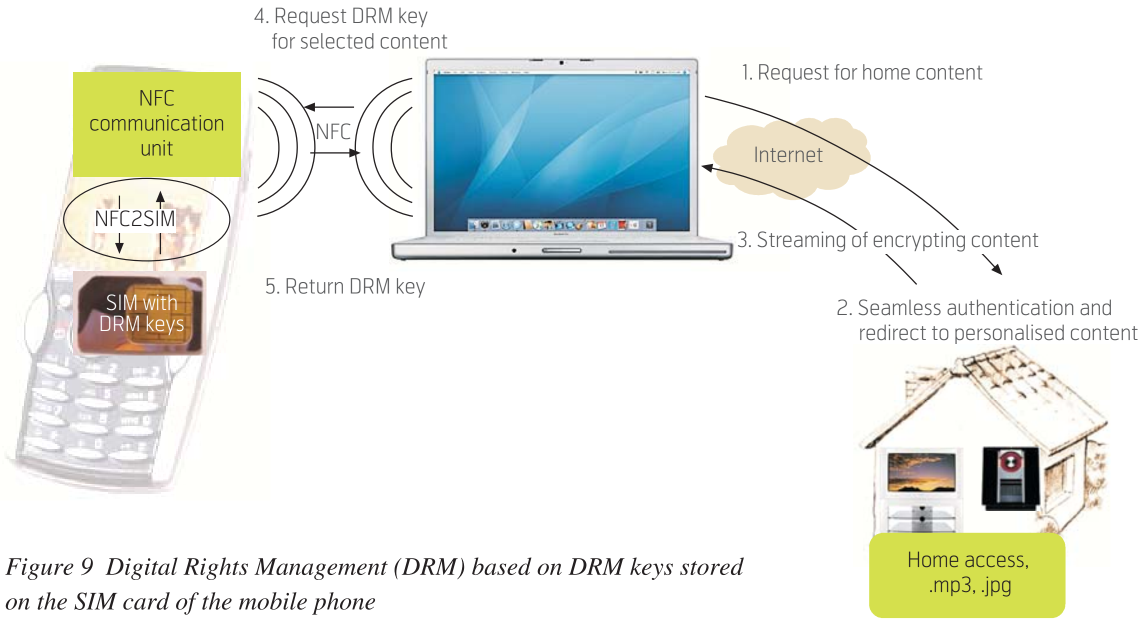


Figure 9 Digital Rights Management (DRM) based on DRM keys stored on the SIM card of the mobile phone

- The SIM card is the secure place to store identities and access rights.
- The user owns the SIM, and allows access/content providers to install access keys to the SIM. The SIM might be administered centrally, allowing for backup/update/restore functionality.
- Rights Management is delegated to the SIM. Content will be streamed to the device, and rights management checked against the access rights on the SIM.

Figure 9 represents the steps for content access fulfilling the functional requirements stated earlier. We have selected access to home content as example, following the argumentation provided by Noll et al. [8]. They claim that users will have a preference of having their content (music, video, pictures) at home, rather than storing them in the network.

The access to home content contains the following elements: The home content storage, the media player, the personal device and the network elements interconnecting the devices. The access is performed in the following steps [14]:

1 The user requests home content by addressing his home content storage.

2 The user device is authenticated in a seamless manner, and access to content is provided. Terminal capabilities are also transferred to the home content storage.

3 The content is adapted to the capabilities of the media player and network capacity, and streamed to the media player.

4 The media player asks for an authentication from the personal device, here indicated through an NFC interface.

5 The personal device returns an authentication, allowing for decryption of content in the media player.

Steps 1–3 are realised in prototypical implementations. Steps 4 and 5 are challenging, as they include NFC as communication medium, NFC2SIM as protocol for exchange of information between the NFC and the SIM card, and handling of DRM keys on the device in general.

The suggested NFC2SIM protocol has to secure the communication between the NFC module and the smartcard. Application keys like access or licensing keys are stored on the SIM, and are accessed through the NFC radio.

7 Conclusions

Service authentication has to satisfy the security requirements of the application, e.g. *nice to know* security for network access, *need to know* security for email and intranet access and *have to know* security for VPN and *m*Commerce services. Including authentication methods through Bluetooth and Near Field Communications (NFC), SIM-based authentication opens for all types of service access, providing admittance (keys, access cards, and tickets), payment (wal-

ISSN 0085-7130 © Telenor ASA 2006

let) and content access (home). Examples of such services are mobile service access for banking, or ticket ordering, physical access based on proximity card functionality, VPN access based on *have to know* authentication, and *need to know* access to private home content. The SIM card in the mobile phone has the capability to provide a two-factor authentication, and supports mechanisms for revocation of credentials stored on the SIM card.

Authentication for network access is performed in the mobile network through the SIM card. In wireless networks such as the IEEE802.11 family authentication might be provided through various protocols, with the two SIM related protocols being the Extensible Authentication Protocol for Subscriber Identity (EAP-SIM) and the EAP for UMTS Authentication and Key Agreement (EAP-AKA). If a mobile phone supports EAP-SIM, it can seamlessly connect to WLAN networks using the SIM card. With the help of the Bluetooth SIM access profile (SAP), the SIM credentials can be transferred from one device (typically the mobile phone) to a second device (a laptop) for seamless WLAN network access of the user.

References

1 Annunziato, A, Jankovic, M, Odadzic, B, Noll, J, Buracchini, E, Melis, B, Harris, J. Guidelines for the Design of the UMTS Radio Access. *Proc. EURESCOM Summit 2001*, Heidelberg, Germany, 13–15 Nov 2001.

2 ITU-T Special Study Group: *IMT-2000 and beyond*. 10 August 2006 [online] – URL: http://www.itu.int/ITU-T/studygroups/ssg/

3 *The Wireless World Research Forum*. 10 August 2006 [online] – URL: http://www.wireless-world-research.org/

4 ITU-R Working Party 8F: *IMT-2000 and systems beyond IMT-2000*. http://www.itu.int/ITU-R/index.asp?category=study-groups&link=rwp8f&lang=en

5 Noll, J, Svaet, S (eds) et al. *4G – the next frontier: Perspectives for Research on Next Generation Mobile Systems*. Heidelberg, Eurescom, Sep 2001. (Project Report Eurescom P1145 study)

6 Stone, B. Your next computer. *Newsweek*, 7 June 2006. URL: http://www.msnbc.msn.com/id/5092826/site/newsweek/

7 Associated Press. *Era of mobile computing arrives – Notebooks have outsold desktops for first time*. 10 August 2006 [online] – URL: http://www.msnbc.msn.com/id/8090448

8 Noll, J, Ribeiro, V, Thorsteinsson, S E. Telecom perspective on Scenarios and Business in Home Services. *Proc. Eurescom Summit 2005*, Heidelberg, Germany, 27–29 April 2005, 249–257.

9 *A Prediction Made Real Improves Billions of Lives*. 10 August 2006 [online] – URL: http://www.intel.com/technology/silicon/mooreslaw/

10 *Nokia and Kineto Announce Collaboration in UMA technology*. 10 August 2006 [online] – URL: http://www.kinetowireless.com/news/press_releases/nokia.html

11 *Public Bluetooth Access – an opportunity for operators*. Eurescom P1118, Project deliverable D1, Nov 2001. (www.eurescom.de)

12 Kewney, G. BT 'BluePhone' is better than Skype because ...? *The Register*, 15 June 2005. (http://www.theregister.co.uk/2005/06/15/btfusion_launch/)

13 Valmot, O R. Finn veien med mobilen. *Teknisk Ukeblad*, 2 May 2006. (http://www.tu.no/nyheter/ikt/article52133.ece)

14 Noll, J, Carlsen, U, Kálmán, G. License transfer mechanisms through seamless SIM authentication. *Intern. Conf on Wireless Information Systems, Winsys 2006*, Setubal, Portugal, 7–10 August 2006.

15 Cameron, K. *The Laws of Identity*. http://www.identityblog.com/stories/2005/07/25/thelaws.txt

16 Kerstein, P L. *Biometrics ID devices are gaining popularity*. 10 August 2006 [online] – URL: http://www.csoonline.com/talkback/102505.html

17 Noll, J, Lopez Calvet, J C, Myksvoll, K. Admittance Services through Mobile Phone Short Messages. *Proceedings of the International Conference on Wireless and Mobile Communications ICWMC'06*, Bucharest, 29–31 July 2006.

18 Derenale, C, Martini, S. EAP-SIM based authentication mechanisms to open access networks. *Telektronikk*, 102 (3/4), 135–144, 2006. (This issue)

19 Somogyi, E. *Seamless access to structured home content*. Budapest University of Technology, January 2006. (Master thesis)

20 Ling, R, Yttri, B. Hyper-coordination via mobile phones in Norway. In: Katz, J, Aakhus, M. (eds.) *Perpetual contact: Mobile communication, private talk, public performance*. Cambridge, Cambridge University Press, 1999.

21 Lohse, M, Repplinger, M, Slusallek, P. Dynamic Media Routing in Multi-User Home Entertainment Systems. In: *Proceedings of The Eleventh International Conference on Distributed Multimedia Systems DMS'2005*, Banff, Canada, 5–7 September 2005.

Dr. Josef Noll is Prof.stip. at the University Graduate Centre at Kjeller (UniK), Norway, in the area of Mobile Systems. He is also Senior Advisor at Movation and at Telenor R&I. He received his PhD from the University of Bochum, Germany. He worked for the European Space Agency at ESTEC from 1991 to 1997, and from 1997 to 2005 at Telenor R&I. His working areas include mobile authentication, wireless broadband access, personalised services, mobile-fixed integration, and the evolution to 4G systems. Further information at http://jnoll.net.

email: Josef.Noll@unik.no

ISSN 0085-7130 © Telenor ASA 2006

Actors, Activities and Business Opportunities in Open Broadband Access Markets Today

THOR GUNNAR ESKEDAL, TOR HJALMAR JOHANNESSEN

Thor Gunnar Eskedal is Researcher at Telenor R&I

Tor Hjalmar Johannessen is Research Scientist at Telenor R&I

The telecom business has gone through a tremendous change the last 20 years. From the POTS system implemented and run by a national telecom operator in the 1970s, we now see a growing myriad of operators and service providers for telecom services. The value chain for offering a telecom service to users has moved from being provided by one, often monopolistic national actor, to several competing actors, each specializing in supporting only a single or a few roles in the value chain. The division between tele- and data communication is also getting more and more blurred since all services may now be transported by the IP protocol family with enhancements to guarantee a minimum quality of service, reliable security and recently also full-fledged mobility across heterogeneous network technologies. This article looks into some of the new actors who have gone into telecom business by deploying WLAN technology. The new actors include hotspot actors, actors offering community network products, actors offering large-scale WLANs covering whole cities or countries, and several specialized actors operating as brokers, aggregators, wireless service providers etc. The common denominator for these actors is that they offer products related to enabling open access possibilities for public users.

Introduction

The market for Wireless Local Area Networks (WLAN) has had an extremely high growth rate the last couple of years. Today laptops are shipped with WLAN cards, and emerging PDAs, palm pilots and small handheld devices are equipped with WLAN radio transceivers. The family of different standards from the IEEE 802.11 Working Group [1] is increasingly incorporating new functionality such as QoS, security, multi antenna facilities etc. The conformance specification (so-called "Wi-Fi certified") of the Wi-Fi Alliance [2] has made use of equipment from different vendors problem free. Finally the increased mobility of people and need for high capacity connectivity has lead to an increasing demand for out-of-home and office deployment. In a global perspective the number of public WLAN hotspots is exceeding 100,000 (Jan2006) [3], and estimated to reach about 200,000 at the end of 2007. Based on this development, one can surely understand that WLAN already has a major impact on wireless communication and will have an even greater impact in the years to come.

While 2G and 3G cellular systems are designed for roaming and include the necessary AAA tools to handle mobile subscribers' consumption and billing of cell-phone services, WLAN based systems do not. With the increased number of WLAN access points (AP), and potentially cheap bandwidth, new business initiatives arise in order to include roaming. The basic idea is to provide centralized subscriber or membership systems as an add-on value to a group or 'cluster' of APs or 'hotspots'. A single hotspot has a limited amount of resources to manage a large customer base and a small coverage zone. Typically a public Wi-Fi zone has a coverage radius of about 30–40 metres. To really make the public WLANs profitable wide coverage is one of the most essential aspects. Later in this article we will look at some initiatives that have made commercial business on WLAN by playing the role of a broker or aggregator. However, the number and distribution of APs as well as the number of subscribers are, together with pricing, essential for this idea to be attractive. Features such as security and quality of service may also play a major role in the potential business profitability of Wi-Fi networks.

This article aims at giving a short overview of various WLAN operations and actors in the existing communication market. Most of these actors use the concept of an open access network where customers can use the WLAN communication facilities either for free or for a specific subscription fee e.g. per month. These WLAN initiatives constitute a new era of communication deploying a new wireless technology for public use rather similar to an existing mobile network such as GSM and UMTS. For the incumbent mobile and fixed operators the use of WLAN may pose new opportunities. On the other hand, the WLAN evolution also shows many new actors emerging and entering the communication business creating competition to the traditional incumbent operators. Many incumbent operators are thus struggling with how to deal with this development and to positioning themselves in the WLAN value chain.

The article starts out by giving a short background overview of the WLAN standard followed by a defi-

ISSN 0085-7130 © Telenor ASA 2006

nition of the term ‘open access’. All WLAN actors described in the next two chapters deploy WLAN quite similar to the given definition of an open access network. Their business models are however different. Each of them are trying to distinguish themselves from the others by creating a unique service offering to their target customers. The article rounds up with a discussion of potential impacts of the WLAN initiatives on the incumbent telecom operator’s communication business.

Short overview of the WLAN developments

A vast majority of deployed WLANs (Wireless Local area network) are based on the standards developed by the IEEE 802.11 working group [1]. The first 802.11 standard was ready in 1997, and since then several amendments have been published. The WLAN products currently found in the market are based on one of three physical layer specifications: 802.11b, 802.11g, or 802.11a. The first popular WLAN standard for residential and business users was 802.11b. 802.11b-based products provided a data rate of up to 11 Mb/s and operated in the 2.4 GHz unlicensed band. Today 802.11g products are the most sold WLAN standard and use the same frequency band as 802.11b providing data rates of 54 Mb/s. 802.11a-based products operate in the 5 GHz frequency bands and provide data rates similar to the 802.11g[1]. The upcoming amendment 802.11n will provide data rates up to five times the rate of the currently existing standards by deploying multiple antennas (MIMO) for the data stream to a specific user. In order to ensure equipment from different manufacturers operating together, several manufacturers and operators have joined in the Wi-Fi Alliance [2]. A conformance specification is drawn up and equipment is tested according to this to get the label “Wi-Fi certified”. Often the terms WLAN and Wi-Fi are used for the same purpose. In this article, WLAN is mostly used to denote the technology, however not strictly consistently.

Currently, WLANs are mostly used with laptops as the primary end-user terminal. WLANs may however also influence the mobile services market, as radios are integrated into mobile handsets. Major handset vendors, including Nokia and Motorola have already launched a number of WLAN-enabled terminals. The Nokia N80 and N91 cellular phones are examples of phones that can access GSM, UMTS and Wi-Fi networks.

Figure 1 shows the development of WLAN capable terminals sold on a yearly basis in Western Europe from 2004 to 2008. This trend of integrating WLAN in various communication devices is anticipated to continue in the future years.

These terminals, combined with low-cost access points installed in offices, homes, and public hotspots might lead to substitution of traffic from mobile networks like 2G & 3G to WLAN. With the emerging VoIP services and messaging services like SMS over IP networks, the substitution may be large if the users favor the quality, capacity and price of the WLAN services compared to e.g. 2G/3G-mobile voice and messaging services.

How to make WLAN business fly

To make public WLAN business fly, however, the weaknesses of the WLAN technology need to be overcome. Many people experience:

- Limited coverage
- Cumbersome login and password procedure
- Low compatibility and roaming between WLAN hotspot actors
- Generally hard to use offered services
- Cumbersome payment procedure with scrap cards
- Poor marketing
- Prohibitive pricing regimes
- Feeling of insecure access

These obstacles need to be tackled and more aligned with the experience from mobile networks such as GSM and UMTS. Wider coverage is thus a prerequisite, likewise easier pricing regimes and payment. Global WLAN access with roaming facilities and

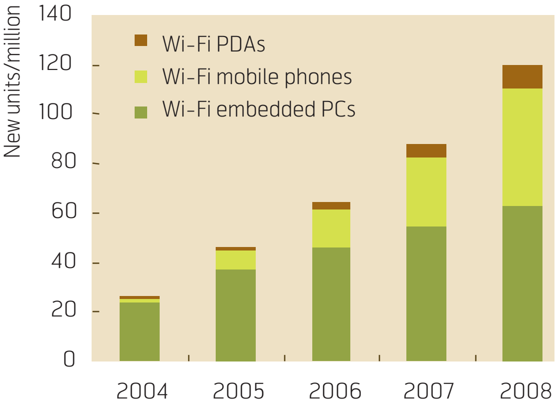


Figure 1 Forecast of Wi-Fi (WLAN) embedded terminal markets (source: Strategy Analytics)

[1] *The data rates usually referred to for WLAN and Wi-Fi standards are the physical layer (air-) data rates. The actual data rate available for the application is usually between 30 and 50 % of this.*

ISSN 0085-7130 © Telenor ASA 2006

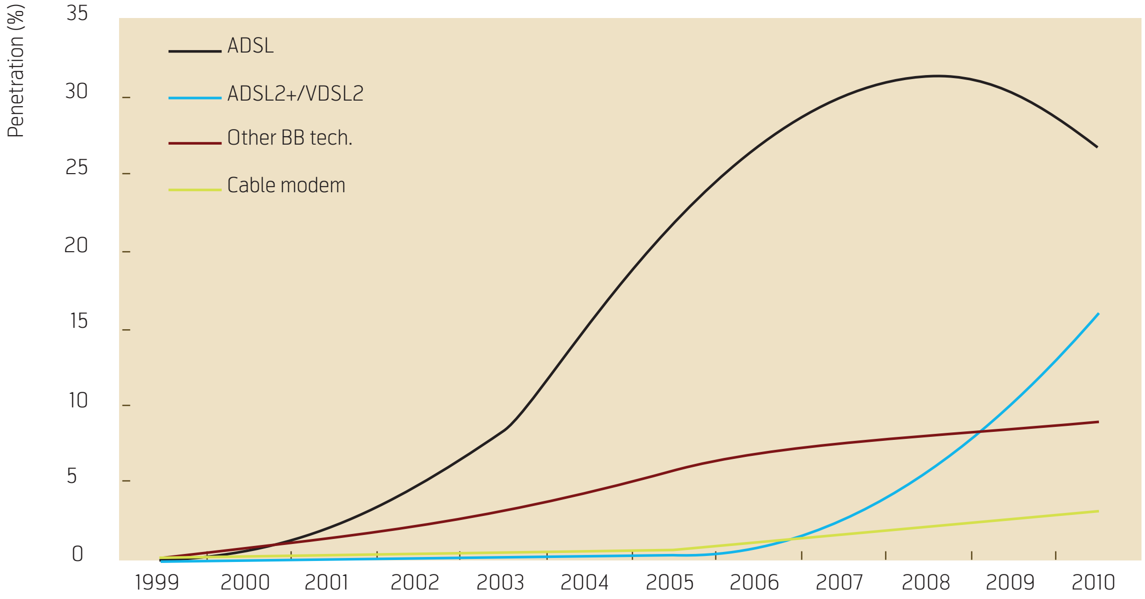


Figure 2 Broadband penetration forecast. Source ref [16]

ease of use are essential. The WLAN terminals must also be affordable for the public and handheld devices must be small and handy at a reasonable price with good battery capacity. To boost the uptake of public WLAN usage bundling the service with existing service offerings such as GSM/UMTS subscriptions would be beneficial. This latter issue guarantees that the user will always be connected to another wireless network if leaving a WLAN zone. Bundling of WLAN access and GSM/UMTS may however be impacted by regulatory intervention if it impacts the competition situation in the region.

To increase the WLAN coverage many new actors specialised as aggregators, brokers, clearing houses etc. have entered the market. These players have a business idea of merging the dispersed WLAN hotspots into a united global network with a common look and feel for the customers. For the customers this development is very beneficial and prompts people to use WLAN. The larger the coverage area the better it will be for the customers and customers tend to make agreements with the actors that have the largest footprint in the area of interest, locally, nationally or globally.

Another prerequisite to deploy WLAN commercially is the broadband coverage or the possibility to get access to broadband infrastructure. WLAN is deployed in residential as well as in enterprise environments today, so the residential broadband coverage is an important parameter for the roll out of WLAN. Figure 2 shows a forecast of various broadband technologies that may be used as fixed access to WLAN access points. This is first and foremost applicable to residential and the SOHO (Small Office, Home Office) (typically 1–12 employees) market. As Figure 2 depicts, ADSL is forecast to become the dominant broadband technology in use in Western Europe the next four years. Thereafter, ADSL2+ and VDSL2 will gradually take over the broadband residential market. As also seen ADSL2+ and VDSL are just starting to be rolled out in the market today increasing the capacity to 20 Mb/s downstream.

Usage of Wi-Fi

In office locations and in targeted hotspots such as airports, hotels, libraries, cafés etc, WLAN has been a part of the internal data communication network for some years already. The new boom of bringing WLAN into the residential environment however opens up for new business possibilities in that segment. The private end-user is now communicating through a wireless network, which is directly connected to the fixed broadband access.

In the residential market the primary reason for buying and setting up a WLAN hotspot is the micro mobility it supports. It has been installed only for own comfort without any commercial aspects behind it.

However, installing WLAN in private homes also opens up the possibility for visitors, or people in the near vicinity to access the fixed network through this WLAN access point. If the access point is open, i.e. no need for user authentication, all users with WLAN cards in their laptops or handheld devices can easily connect to the fixed access line and send and receive data across the network. The owner of the access point is usually unaware of these “free riders”. If many users are simultaneously connected to the Wi-Fi network the capacity is shared and the owner of the network will experience a reduced capacity and quality of the connection. In addition to experiencing poorer capacity the owner is not aware of the content sent across the WLAN connection from visiting users. If this is illegal content such as child porn, the owner of the access point, although not aware of it, may be prosecuted since the owner is responsible for the usage of the fixed connection. Due to these issues more and more private WLANs are now being encrypted and closed to the public. In Norway the majority of the new WLAN access points installed are encrypted. The number of open private WLANs are, however, still quite high. The fact that there are still many open access points also creates problems for commercial WLAN actors; why should anyone pay to have a commercial WLAN access point installed if free WLAN access is available from your neighbour? Due to the small WLAN cell size, this possibility is mostly available in urban areas, however.

For the commercial hotspot actors the situation is different. The Wi-Fi hotspots are used as open access channels to the Internet, where the user pays per minute or per volume of content transported. A user and password authorization is demanded to support the billing. This is the case in most hotspots today where e.g. the mobile telephone number is used as credentials for billing the user. The user is typically locked to a ‘sticky page’ until his credentials are verified. Some operators offer the user free access for a minute or two, just to test the access quality and service.

The focus of these hotspot actors has been to serve WLAN enabled laptop users connectivity to Internet. This would typically be to access data applications such as web browsing, e-mail, Virtual Private Network (VPN) access to the corporate networks etc. For travelling users – both “business” and “private” – access to e-mail comprises the largest use of WLAN access. This is followed by access to corporate networks, Internet access and entertainment services. WLANs are thus used for many types of applications while on the move and are thus seen as mobile connectivity networks although without the seamless mobility of 2G and 3G networks.

There are many reasons for WLAN hotspot actors to enter the mobile market. Some of them are:

- Price of 2G/3G mobile communication, especially when roaming
- Increase in demand for capacity
- Support better indoor wireless coverage
- Penetration of broadband
- Emerging VoIP applications and suppliers
- Penetration of WLAN in consumer and business.

All these issues are driving forces for independent actors and operators to look into the possibilities of using WLAN as a mobile network. Several actors have already built out large city areas with continuous public WLAN access and offer the network as a substitute for the mobile networks in the area. Later in this article we will describe some of the actors that have built out large city areas with WLAN coverage. These networks are open to the public. However in most of these city wide coverage cases the network has been built as a standalone public network very similar to the GSM network; i.e. it is built with new feeder lines and is located at sites such as street light poles. The situation is different for many of the hotspot initiatives where the network behind the access point has been the private broadband access line which was earlier only used by the owner of the site. It is in this context the term open access comes into play. Before looking into the hotspot operator’s value chain we will thus first explain the meaning behind the term open access used in this article. The reason is to put the initiatives from the hotspots operators described later in this article into the context of an open access implementation.

Definition of open access

The definition of open access can be manifold. However, as a new concept it is a prerequisite in this article that the access was earlier experienced as closed to public users. In this manner the concept introduces enabling technology of functions that change this former closed access into an open access by enabling public users to acquire access, e.g. to the Internet. One example of an open access may be to change the usage of the privately fixed access line to a residential home into an open fixed access line that also offers public users access.

The concept of an open access may be viewed in relation to a layered network defining openness on several functional layers. For example, the physical access line is open if any service provider can rent it to reach the customer. This falls under the regulatory requirement for operator access or Local Loop UnBundling (LLUB). The access to the Internet services is open if anybody can access the Internet, e.g. through an open WLAN access point. If the access point is configured with authentication keys, then it is open to all users with the right authentication key. In this article the term ‘open access’ is defined as including authentication. This means that a WLAN AP is open according to specific authentication keys. The reason for including authentication as

Content provider

Clearing house/broker/aggregator

Virtual Wireless internet service provider

WLAN operator

WLAN site owner/property owner

Fixed network operator

Figure 3 Roles in the WLAN market chain

a prerequisite in the definition is to make sure to stay within both legal and commercial constraints. This may for instance be to avoid unauthenticated access as well as reselling of capacity, which may be illegal in some countries. However, as mentioned earlier the intention here is not to define the term open access strictly but give a short description of the meaning of the term in this article.

Value chain considerations in the WLAN market

Figure 3 shows the main roles involved in the WLAN market. Note: The roles can participate in both hierarchical and non-hierarchical structures. A role is here defined as a group of functions enabling an entity taking on the role to provide a set of services to its environment. A role is thus a separate legal entity that may have its own commercial interfaces and its own business obligations regarding financial statements. An actor like Telenor may be defined as an organisation that takes on one or more roles. In Figure 3 the various levels may be broken down into even more granularity. In this article the depicted levels represent separate entities. The figure depicts the relation between the roles; e.g. a WISP may have relations to many network operators, an aggregator may in turn have agreements with many WISPS, and so forth. It is a kind of hierarchy where a content provider may support customers connected to many network operators.

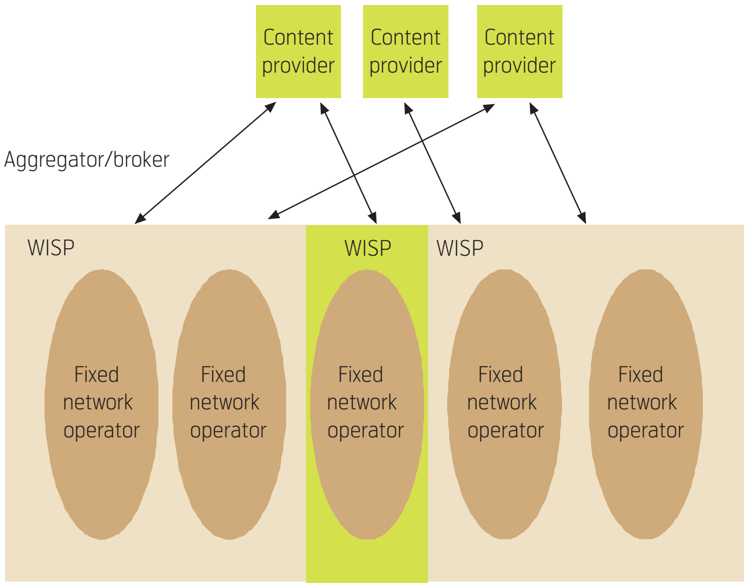


Figure 4 Possible hierarchic structure of the WLAN value chain

Access network owner

The fixed access network owner is very often the incumbent operator in a country. In Norway, Telenor is the major infrastructure owner with the biggest share of ownership of the fixed broadband access network (about 40 %). The incumbent fixed access owner is in most western countries obliged by the national regulatory authorities to open the access resources to independent service providers, at the wish of the customers.

Property owner / site owner

The property owner / site owner is in Figure 3 depicted as the next level. This is where the WLAN AP is located. This may be a coffee shop owner, a public airport owner or a residential user. The business model for the site owner could be to attract customers, increase customer retention at their location or they could introduce WLAN access as a revenue generating service in itself. Hence, there may be many incentives for a site owner to install an open access enabled WLAN AP in its own location. The placing of the site owner in offering public wireless services is therefore very important.

For a network owner acquiring the right strategic sites for installing WLAN AP may be of vital importance. Since WLAN uses an unlicensed frequency band, access points within range of each other may interfere. The first actor entering a strategic location and getting an agreement with the site owner may effectively block other actors entering the same location. Partnerships through roaming agreements will then be the only way to offer services to customers of different WLAN operators at the given location. Due to the limited radius and indoor coverage challenges the site acquisition is thus a more vital role compared to implementing mobile networks such as 2G and 3G.

WLAN operator

The WLAN operator may be the property owner, incumbent access operator, or an independent service provider. WLAN operators go into the business believing there is profit in deploying WLAN access services. This may be for data access only, or also for real time applications such as voice or video/streaming services. To maintain a good voice service it is very important to support continuous session coverage with handover support between the WLAN AP. Providing continuous coverage with WLAN with an acceptably high capacity is not easy to achieve technically, however. This is mainly due to the small cell radius and the interference levels. Small cells may result in frequent handovers for the user while moving. If the handover is not seamless this will be noticed by the user as frequent small interruptions in the communication. The degree of coverage is thus one important strategic aspect the WLAN operator need to take into account to be attractive to the wireless service providers and the users.

The WLAN operator does not usually have a direct customer relation. The customer relation is the task of wireless service providers.

Virtual Wireless Internet Service Provider (WISP)

The wireless service provider supports its customers with services associated with contractual customer relationships like subscription, where accounting of consumed resources and customer billing are important elements. Simplified billing from one common provider instead of from a multitude of WLAN AP owners is a step towards a customer-friendly approach. Another important aspect for the customer when choosing a WLAN service provider is, as mentioned earlier wide coverage. Hence, service providers enter a clustered cooperation with several WLAN operators to cover the targeted market area as best possible.

Clearing house/brokers/aggregators

Above the level of independent WLAN operators and service providers there are different constellations of brokers, clearing houses and aggregators. All these actors work on behalf of the WLAN operators and/or wireless service providers to ease the work of roaming, billing, authentication etc. Often service providers will use the networks of several WLAN operators to cover a larger area and support roaming. The brokers/aggregators then take care of all service level agreements between the service provider and many independent WLAN operators.

Content providers

Since many of the same services may be carried by WLANs, mobile networks and fixed networks, the content providers may be the same actors as content providers on mobile networks. The content may be videos, newspapers, news programs, internet search etc.

Several actors within the telecom and WLAN market may take on several of the described roles and thereby position themselves in the WLAN value network. This positioning is based on different business models where each actor makes the best use of their main assets, knowledge and business strategy. Cooperation and alliances between actors are here an important point to form a cost-effective and efficient network roll-out.

In the following we will take a closer look into some actors operating WLAN hotspots that have a business model utilizing the open access concept. Actors like FON, The Cloud and Boingo are described. We then describe citywide actors, which operate according to a different business model not directly following our definition of an open access network. Here actors like Ottawa Wireless, Google and On.Net in Macedonia are examples that we briefly describe.

Current hotspot initiatives

The business models of the following hotspot operators/brokers range from community networks to charged public access models. The benefit of the community model is to be a member of the Wi-Fi community and thereby take advantage of each other's WLAN for free. The business models including charging of the wireless access are open to all users, but each user must pay to acquire access to the network. These models also often imply a revenue split between the site owner and an aggregator. The common denominator for all is however that the fixed access is 'open' in the sense that the total capacity is not exclusive to one user but is shared between the site owner and other people. For all the hotspot initiatives there is an authentication regime for access control and charging/billing.

The Cloud

The Cloud®
Your WiFi route to the Internet

The Cloud [4] launched its Wi-Fi service mid 2003. The business idea is to build WLAN hotspots and sell the access capacity on a wholesale basis to service providers that have the direct customer relation. O2, BT, Vodafone D2, Skype, Ericsson and Intel, among others, have taken actively part in the network development of The Cloud to facilitate the growth of wireless broadband services across Europe. By May 2006 The Cloud offered national WLAN coverage in hotspots and hot zones locations throughout the UK (over 7000 hotspots, May 2006), Sweden and Germany. The Cloud's infrastructure is a multi-service provider platform, which allows providers such as ISPs, mobile operators and cable companies to offer a fully branded WLAN experience to their customers nationwide. The Cloud also supports roaming agreements between WLAN operators. This provides a simple way for operators and service providers to ensure that their customers have a designated user experience on all the included WLAN operators' networks.

The Cloud's technology adds security to the access so it is possible to separate home users or site owners from visiting/public users. The Cloud also offers management functionality to support visiting users.

This management functionality may be used to support different business models.

The service offerings of The Cloud recently launched an unlimited data offering based on a flat rate package, called UltraWi-Fi, which was available from 1 July 2006 at a price of £11.99 a month. This is with a 12 month subscription and £11.99 a week on a pay-as-you-go basis.

FON

FON [5] is an initiative financed by Skype, Google and two venture capitalists; Sequoia Capital and Index Ventures. It is a global community of and for people who will share their WLAN AP capacity and fixed access resources. By purchasing a compatible Wi-Fi router ($25 in the US or 25 Euro in Europe) and registering to the community, the members allow other members to share their home/work connection and are entitled to enjoy free access to all the other members' wireless access points. The charging scheme is very simple given that the only cost for the member is a router bundled to the membership. By bundling the router with the membership (which should be subsidized to encourage participation) value has been created and it is possible to set a positive price. Bundling has solved the problem of subsidization to induce participation with a safer implementation than giving money away.

Non-members (named "aliens") are expected to be charged 5 Euro per day for connecting to the FON network. Members can also be remunerated (named "bill") by keeping part of the revenue generated by an access of an "alien". This means that the member actually resells the access capacity of the broadband access line. It would also be possible for a member to pay a fixed fee to be upgraded to a "bill".

LinSpot

LinSpot [6] is a Virtual WISP located in 38 countries. LinSpot has recognized the growing residential usage of WLAN and the density of WLAN coverage in dense areas and seen it as a potential market for their software product. The software is given to WLAN AP owners free of charge. It makes it possible for the AP owner to charge other people for offering access to Internet through their WLAN connection. LinSpot authenticates the users and bills them. The WLAN AP owner in essence resells the fixed access capacity to other users for a share of 85 % of the connection fee that LinSpot charges. This is a typical consumer-2-consumer business model where the private residences make up a network for public use. If the residents are living close enough to each other they may together form a continuous WLAN coverage zone. 15 % of the payment from the public usage goes to LinSpot. This shall cover for the development of new versions of the software, operating the LinSpot servers where the customers are registered, marketing of the network and profit to LinSpot. The prices of the service are dependent upon the duration of the connection ('pay per minute').

Through the LinSpot offer the private fixed broadband access line is made open to the public. Users only have to register to the Wi-Fi access point through the LinSpot software.

Boingo

As the first and largest hotspot roaming aggregator, Boingo's mission is to unite Wi-Fi hotspots into a seamless network. Boingo [7] has roaming agreements with dozens of operators, representing over 5,000 public hotspots. The company has built the technology and systems necessary to turn these diverse public hotspot networks into a single unified network that can be offered to end users. In this way Boingo enables major brands to rapidly offer a powerful hotspot service.

To support this hotspot service, Boingo has created Boingo Platform Services. This is a system that includes agreements between the leading roaming networks of hotspot owners and advanced WLAN client software. The system is offered to the WLAN operators and is customized and delivered under the carrier's or Internet service provider's brand. The user thus sees the brand name of their own carrier or WLAN operator at all WLAN hotspots deploying Boingos Platform Services.

Boingo also offers the product "HotSpot-in-a-Box", which allows any WLAN access point to become a commercial hotspot. With HotSpot-in-a-Box, every one of these broadband endpoints would have the ability to be a commercial hotspot. A person living in an apartment over a busy street corner already having a DSL or cable broadband connection could opt to become a wireless Internet provider just by flipping a switch on his HotSpot-in-a-Box enabled home access point. He would receive settlement at the end of the month for all the users who connected to his network.

Boingo's client software makes finding and connecting to both private Wi-Fi networks (in the home and office) and commercial public hotspots easy, all under one brand (the brand of the carrier that owns the end-user relationship). The user may use every hotspot that is part of the Boingo aggregated network. The user sees a familiar entry window where he can submit his username and password. Boingo takes care of authentication and accomplishes the procedures so the user gets fully connected.

In addition to WLAN, Boingo supports agreements with carriers of wireless wide area network (WWAN) technologies such as 2G and 3G technologies. The end-users are then able to move between WLAN hotspots and wide area networks through a single service.

Boingo pays its partner hotspot operators a wholesale fee for each connection generated through Boingo's distribution channels, which include laptop and WLAN manufacturers, Internet service providers and major carriers. This wholesale fee typically ranges between $1 and $2 per connect day (up to 24 hours for one user in one location). In addition, Boingo provides a marketing bounty of $20 – $50 for new customers who use the Boingo software to sign up in one of the hotspot operators' locations. Revenue from connectivity and sign-up bounties can make a hotspot profitable, but hotspots also deliver significant indirect benefits. They foster loyalty, increase the amount of time that customers spend at the venue and create the opportunity to sell additional goods and services.

Others

There are many other hotspot initiatives whose operation is very similar to the ones mentioned above. Some of these are iPass [17], FatPORT [18], SURF [19] and SIP [19]. All these exist today and have made commercial business the last years.

WLAN is first and foremost suited for micro mobility within limited areas. However, some actors have taken the technology further and constructed city wide networks based on WLAN. In the following some of these actors will be briefly described.

City wide Wi-Fi actors

Ottawa Wireless

Ottawa Wireless [8] was one of the first operators that built out a whole community with WLAN technology. The wireless coverage was completed in 2004 and covered an area size of about 10 km^2. The Grand Haven community with a population of about 12,000 got a public Wi-Fi service based on 802.11a/b/g for laptops, PDAs and other similar equipment which have a Wi-Fi compliant radio.

Security of the Grand Haven WLAN network is based on Virtual Private Networks, WPA and 802.11i encryption, firewalls filtering, RADIUS authentication and Virtual LANs (VLANs).

The coverage has been achieved by installing WLAN antennas on existing outdoor light poles. Ottawa Wireless and the Board of Light and Power company cooperate to make the deployment possible. The wireless network thus covers streets, parking lots, parks, and up to the front door of houses. Inside the houses people have to put up their own repeaters to access the public service.

The business idea of Ottawa Wireless was to offer a low cost high bandwidth public wireless service for the public of Grand Haven. Services such as video-on-demand and Internet telephony (using VoIP) are offered together with video surveillance. Both the City of Grand Haven and the power company reserve the right to purchase the network from Ottawa Wireless in the future. The network would then become a community-owned utility service.

Google

Google [9], which is by far the largest Internet search company in the world, will together with Earthlink [10] cover San Francisco with continuous WLAN connectivity [11]. This is an example of a software company that goes into the area as a wireless service provider. The two actors will cover the whole city with WLAN and compete for the customers based on different business models. Google will cover its network expenses on advertising revenue, so that subscribers get free access. Earthlink on the other hand will charge the customers about 20$ a month for the service. To defend their charging scheme compared to Google's free access, they claim that the speed of their network will be four to five times higher than Google's free service. The two companies will take on the expense of building the entire network, which is expected to cost at least $15 million.

Google officials say [20] that San Francisco residents (and visitors) will enjoy a free 300 kb/s "always on" connection anywhere in the city. As part of its proposal, the company says it will be offering wholesale access to other service providers, who will offer high throughput connections to their customers. Google Secure Access service allows a user to establish a secure connection by using Google Secure Access, which is their own authentication service, the internet traffic will be encrypted, thus preventing others from viewing the information transmitted. Google Secure Access connects to Google's VPN (Virtual Private Network) server provided for this service. Google Secure Access is a downloadable client to the customer's device. The company is going to use San Diego-based WFI, which is a cellular network [21] builder company, to deploy the wireless network.

Google will thus act as a Wi-Fi service provider buying capacity on San Diegos infrastructure.

The company in San Diego will install about 400 access points on light poles throughout the city, which will mean about 50 to 75 per square kilometre. Google will then rent the city's light poles for about $12,600 a year to place the needed WLAN access points. Google may also roll out its own last mile feeder network to the streetlamps and there capture another asset in the value chain. Technologies like WiMAX have also been discussed as feeder access technology to the streetlamps.

Macedonia

Macedonia claims to be the first country of its size (24,856 sq km) to have a broadband wireless network covering 95 % of its population (estimated 2.0 mill, 2005). A project called *Macedonia Connects* [12] funded by the United States Agency for International Development (USAID) is in charge of this aggressive Wi-Fi roll out.

A local ISP, On.Net [13], which is part of the Macedonia Connects project, intends to blanket the country using wireless broadband based on WLAN technology. On.Net is deploying a transport network solution from Motorola as the backbone network to distribute broadband connectivity throughout the country. The WLAN network will also be based on Motorola's technology, to bring high-speed Internet access to schools and villages. Mesh technology is used to fill in coverage gaps in urban areas.

By using mesh technology, Macedonia Connects is creating hot zones which stretch 15 kilometres across a city. In addition, they will deploy a mesh wireless solution in the six most populated cities in Macedonia. This mesh solution is WLAN compliant and will provide nearly 100 % wireless coverage in these six cities. In addition, a WLAN repeater will be installed at each of the 531 locations that include primary and secondary schools, universities and local government offices as part of the main delivery of services within the Macedonia Connects project.

0
20
40 km
0
20
40 mi
22
23
SERBIA AND MONTENEGRO
Kumanovo
BULGARIA
Tetovo
SKOPJE
42
42
Golem Korab
Gostivar
Štip
Veles
Vardar
Kičevo
Strumica
Prilep
Lake Doiran
Lake Ohrid
Lake Prespa
Bitola
41
41
ALBANIA
GREECE
Aegean Sea
21
22
23

On.net is free to sell capacity to additional corporate or consumer subscribers throughout the country. Furthermore, in metropolitan areas they are deploying mesh based network providing pervasive hotspot connectivity in the country's population centers.

Others

There are many other city wide WLAN actors. In the US over 50 cities are covered with either region or city wide networks. In addition over 120 other cities are in a deployment phase or have ongoing negotiations with actors to build region or city wide WLAN coverage.

WLAN initiative under study

OBAN

The former two sections have looked into existing WLAN initiatives. In this section we will briefly describe another initiative which is under development through an IST project named OBAN (Open Broadband Access Network) [14]. The business idea behind OBAN is to utilize the unused broadband capacity in the existing privately owned fixed access network for public use. Traffic logging tools connected to the fixed access line have shown that on average less than 10 % of the broadband capacity is used by the household. This unused capacity can be used for public users by separating the access line into two segments, one for the home user or site owner and another segment for public or visited user.

The WLAN access point is enhanced with Virtual LAN functionality so as to separate the resources between the home and visited users. The enhanced WLAN node also implements QoS classes to be able to prioritize real time traffic and also prioritize the traffic from the home user in front of the visiting user. All users are thus authenticated either by IEEE 802.1x (RADIUS) in combination with EAP-SIM, or simple log on with pin code or password authentication. The entity that contains all this functionality is denoted an OBAN Residential Gateway (RGW).

The network behind the OBAN RGW is further enhanced with a mobility broker that supports fast authentication, fast handover between OBAN access points and optionally act as an interceding point for regulatory authorities. The terminal devices are also

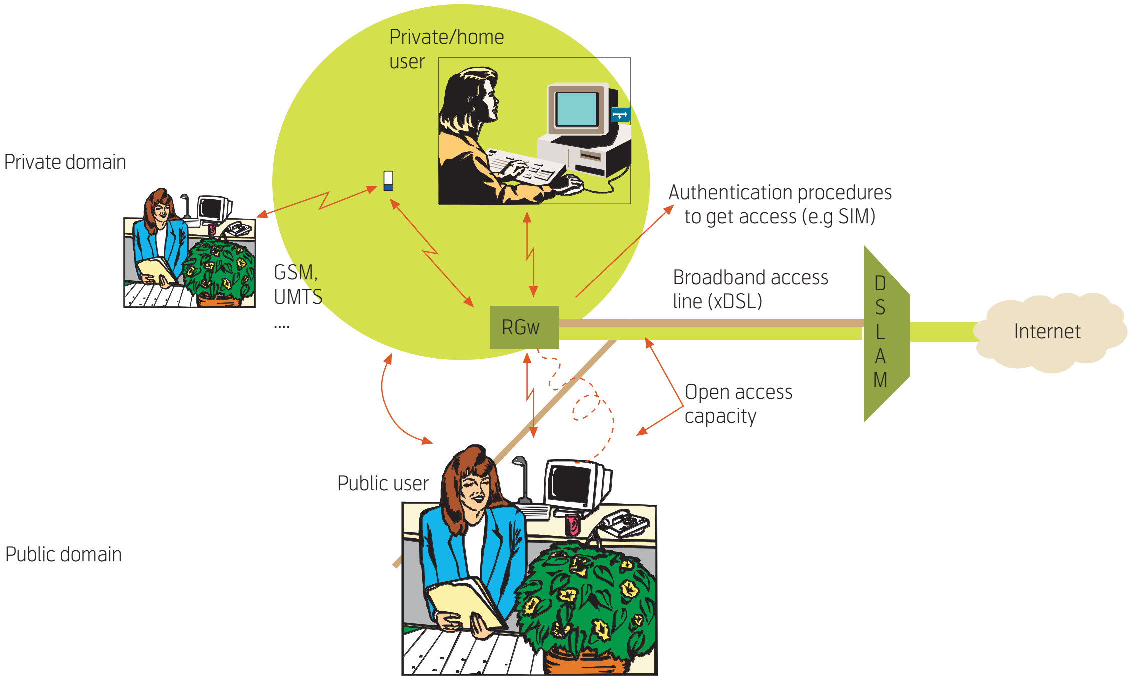


Figure 5 Open access network supporting private and public users

enhanced with special software such as SIP client, Mobile IP and security client and network selection functionality to choose the best OBAN WLAN to connect to.

There may be many potential business models for the utilisation of the OBAN concept. Some of these are described in [15].

Wi-Fi actor considerations

All the actors described above deploy WLAN as their main technology to reach the customers. Hence they all see the potential of the technology and have taken on roles and established business models to acquire a piece of the growing revenue from the tele- and data communication market. It is estimated that the ARPU[2] from the Wi-Fi business will steadily grow and become one major source of revenue within telecommunication in the future. This is both within the home zone of the public market and within the enterprise market. The actors described have recognized this and positioned themselves in this growing market.

However, some actors deploy WLAN as an enabler to acquire revenue from other sources than communication. Google is an example of such an actor that use marketing on its web portal as the source of income from the WLAN business. Some are focusing on the hotspot market, some are building a seamless network based on WLAN and others are offering software so every WLAN AP owner can actually enter the tele- and data communication business themselves. The ways of making business connected to WLAN usage is manifold and the number of actors is growing. Since wide coverage and roaming possibility are such important features, the small hotspot operators enter into larger cooperative partnerships. One also sees that network operators such as BT and Vodafone have gone into partnership with the WLAN operators bundling their fixed and cellular communication offering to the customers.

Many of the initiatives offer software and install WLAN AP in locations where only a fixed private access line was installed. This is the case for FON, The Cloud and Boingo. What was former a private fixed access line, is enhanced by various functionality and equipment to become a public connectivity access. A common denominator for all these initiatives is that the customer authenticates himself to the network which is seen as a prerequisite for a sustainable business model.

It is important to note that some of these initiatives support reselling of capacity to the public users in a commercial manner: in some countries this may be illegal. If the fixed access provider has stated that the capacity is only provided for the household the LinSpot software may support illegal activity. It may also raise governmental taxation issues (for private persons now becoming enterprises) that have to be solved.

[2] *Average Revenue Per User*

ISSN 0085-7130 © Telenor ASA 2006

System	Roaming	IdM / AAA Properties	Billing	Handover	Authentication means*)	Communications Security	Reflections on Regulatory Authority Security Issues	Number of Hotspots
The Cloud Enterprise Guestbridge™	Yes	Enterprise oriented IdM & AAA for visiting users	No	No	Home User: Strong & mutual Visitor: weak (?)	Home User: Strong Radio Link Sec. (802.1X/WPA2) Visitor?	None	Not available
The Cloud Public Hotspot Wi-Fi Access	Yes	RADIUS, EAP Methods supported	Applicable but not provided by The Cloud	No	Weak (password) Single sided?	SSL/VPN	None?	50-60,000 (June 06)
Boingo 'HotSpot in-a-box' 'Wisp in-a-box'	Yes	User subscription system by Boingo offered to retailed hotspot operators	Boingo subscription	No	Weak? Single sided?	Strong Radio Link Sec. (802.1X/WPA2) + VPN	None?	45,000 (June 06)
LinSpot	Yes	Yes (no details given)	LinSpot subscription	No	Weak Single sided?	? (even WEP disabled)	None?	Not available
FON	Yes	Membership alliance	Membership fee • Free surf for members • Billing of others	No	Weak Single sided?	?	None?	30,000 (Feb 06)
OBAN	Yes	RADIUS EAP-SIM/ EAP-AKA EAP-KERBEROS, IdM by HLR	Potentially by mobile (OBAN) operator	Yes (fast)	Strong and mutual	Strong Radio Link Sec. (802.1X/WPA2)	Reflected in architecture	None (yet to be implemented)

*) *Mutual (Client-Server/AP) or Single-sided. Strong: 2-factor, Weak: 1-factor (e.g. password only).*

Figure 6 Comparison of Wi-Fi hotspot initiatives

Wireless networks based on WLAN technology, either as stand-alone hotspots or mesh networks can be built relatively inexpensively. However, when going into building city wide continuous coverage many challenges of providing reliable services come to the surface.

One of the most important technical issues that actors face in deploying city wide WLAN coverage is that it can suffer interference from other wireless devices trying to utilize the same radio channel. Because WLANs use unregulated spectrum, many devices can interfere with the transmission. For example, microwave ovens, hand-held phones, garage door openers and Bluetooth devices all use the same 2.4 GHz. This makes it extremely difficult to build a robust network since the interference sources are many and totally out of control from the Wi-Fi operator. Other problems, which also impact hotspots, concern the handling of network abusers, such as spammers, illegal file-swappers and people launching virus attacks. These may harm the network's service provisioning and in severe cases block the network totally. Dealing with all these potential problems can increase the cost of the network considerably.

The table in Figure 6 sums up some characteristics of the hotspot initiatives mentioned.

Some reflections for incumbent mobile and fixed operators

For fixed operators it is evident that the WLAN technology has come as a life buoy. This is not only to combat the fixed mobile substitution of voice but also to make the home zone more user friendly in terms of micro mobility to access the fixed broadband line.

For mobile operators the situation is different. There has been much debate about whether WLAN shall be regarded as a substitute or a complement to 2G/3G networks such as GSM and UMTS. For mobile operators WLAN may be seen as both. It is a substitute in the sense of the higher bandwidth, and the perfect fit to data-centric applications mostly run on laptops. It is often also cheaper to use. As some of the initiatives described earlier, WLANs may be used for free as in community networks and Google's initiative in San Francisco. Mobile network operators realize this threat from WLAN operators and the demand for cheaper and higher bandwidth. New developments for the mobile networks are thus intensively studied in 3GPP; e.g. High Speed Packet Access (HSPA). For HSPA the capacity will be increased from 2 Mb/s, which the UMTS network may run today, and up to about 12 Mb/s for the downlink direction (HSDPA)[3]. So WLAN, ranging up to 54 Mb/s, may clearly be seen as a substitute. Mobile operators also see the need for high bandwidth to increase the indoor coverage and capacity. For these aspects WLAN may be a complement to the 2G/3G networks if the mobile operator gets into the WLAN business. The initiatives around Fixed-Mobile Convergence (FMC) are steps where mobile operators can enter into the WLAN business in a cost optimal way. By deploying a common network infrastructure as far as possible, and a common service and call control platforms, mobile and fixed operators are well positioned to be able to get the best out of the WLAN technology.

Conclusion

This article has given a brief overview of the emerging WLAN business in the context of an open access network. With the increasing deployment of both Wi-Fi APs as well as broadband network capacity a number of new actors, activities and business ideas have emerged. Enterprises that offer identity management combined with AAA and billing capabilities for roaming WLAN clients constitute one typical segment which, furthermore, can be split into several roles. Since critical mass of users and access points is a profit clue, various hierarchical and non-hierarchical clustering models also apply. The business models range from free WLAN access for users (local advertisers will pay the bill) to profiting from different levels in the communication path's value chain like site-owners' participation in hotspot clusters. Some of these actors are described above. The offered technology varies with respect to both security and quality of service measures. Security is typically a matter for the local AP to install as a recommendation. Fast hand-off between access points is still at the R&D-stage; hence local mobility is not offered in the market. A car, for example will have problems staying connected even at low speed due to the short radio range of a Wi-Fi AP.

Although the number of actors today is increasing, it may decrease in the future since small actors can accumulate into larger alliances. Who the 'winning' actors will be is also hard to fore-tell. Telecom operators, from both the fixed and mobile segments should be included in the forecast; WLAN becoming a part of the communications infrastructure may be a driving force to converge mobile and fixed network operators. But also other service providers with identity management and/or billing capabilities like credit card companies or *e*Commerce service providers are likely to take roles in agreement with Wi-Fi AP site-owners. The future constellations and prospects will, needless to say also depend on constraints set up by regulatory authorities. For example, free-surf abilities due to private Wi-Fi APs without activated security is bad for business: will non-secured APs be allowed in the future? No one knows. Nobody will pay for services that can be achieved freely from an unaware neighbor. Such parasitic behavior can become impossible if legislation mandates access control, or if the site-owners themselves are given incitements to activate access control by participating in business groups.

Since the business wheel only relatively recently has started to spin, it is far too early to conclude much today on what the future business scenario map will look like. The profit potential is large however, so many new ideas and models will doubtless be observed in the years to come, both of the prosperous and not-so-prosperous kind.

References

1 *IEEE 802.11 Wireless Local Area Network (WLAN) Working Group*. 4 July 2006 [online] – URL: http://www.ieee802.org/11

2 *Wi-Fi Alliance*. 4 July 2006 [online] – URL: http://www.wifialliance.org

3 *JiWire: Worldwide Wi-Fi Hotspots Hits the 100,000 Mark*. 5 July 2006 [online] – URL: http://www.jiwire.com/press-100k-hotspots.htm. Posted: San Francisco, CA, 24 Jan 2006.

4 *The Cloud – Your Wi-Fi route to the Internet*. 5 July 2006 [online] – URL: http://thecloud.net/

5 *FON*. 4 July 2006 [online] – URL: http://en.fon.com/

6 *LinSpot – Sell your Air!* 5 July 2006 [online] – URL: http://www.linspot.com/

7 *Wireless Service at Boingo: Wireless Internet, Wi-Fi, Wireless Access, hotspot*. 5 July 2006 [online] – URL: http://www.boingo.com/

8 *Ottawawireless.com*. 5 July 2006 [online] – URL: http://www.ottawawireless.com/

9 *Google*. 5 July 2006 [online] – URL: http://www.google.com/

[3] *The data rates for 3G and HSPA are theoretically obtainable values, practical values are 384 kb/s and 2.5 Mb/s, respectively.*

10 *Earthlink Wi-Fi*. 5 July 2006 [online] – URL: http://www.earthlink.net/wifi/

11 *Earthlink Press Room: Earhtlink & Google submit joint RFP for city of San Francisco wireless broadband network*. 5 July 2006 [online] – URL: http://www.earthlink.net/about/press/pr_san_francisco_network/. Posted: Atlanta, GA, 21 Feb 2006.

12 *USA Today: From warfare to wireless in Macedonia*. 5 July 2006 [online] – URL: http://www.usatoday.com/tech/wireless/2006-03-27-macedonia-wireless_x.htm?POE=TECISVA. Posted 27 March 2006.

13 *On.net*. 5 July 2006 [online] – URL: http://www.on.net.mk

14 *OBAN – Open Broadband Access Network*. 5 July 2006 – URL: [online]. http://www.ist-oban.org

15 Eskedal, T G, et al. *OBAN viability study*. Brussels, December 2005. IST project 001889 – OBAN, Deliverable D25.

16 Stordahl, K et al. *Overview of demand forecasts for the fixed and mobile networks and services in Europe*. CELTIC project ECOSYS, Helsinki, October 2004.

17 *iPass*. 15 August 2006 [online] – URL: http://www.ipass.com

18 *FatPort – Secure Broadband Wireless*. 15 August 2006 [online] – URL: http://www.fatport.com

19 S*URF and SIP network – High Speed Wireless Internet Access*. 15 August 2006 [online] – URL: http://www.surfandsip.com

20 Malik, O. Google confirms free San Fransisco Wi-Fi plans. *GigaOM*, 30 September 2005. (http://gigaom.com/2005/09/30/google-confirms-san-francisco-wifi-plans/)

21 *Wi-Fi – Next generation networks*. 15 August 2006 [online] – URL: http://www.wfinet.com/

Thor Gunnar Eskedal received his MSc degree in physics from the University of Oslo in 1990. After graduating he started working as research assistant at the Norwegian Institute of Technology (NTH) in Trondheim. In 1991 he received his business economist degree from BI Norwegian School of Management and joined Telenor R&I. At Telenor he started working with system architecture, broadband technologies and IP network performance. Since 1998 he has been following the standardisation and uptake of various wireless networks such as 2G/3G and Wi-Fi. From 2000 his main focus has been on business modelling, techno-economic analysis and network development.

email: thor-gunnar.eskedal@telenor.com

For a presentation of Tor Hjalmar Johannessen, please turn to page 59.

Business Scenarios for Open Broadband Radio Access

RAGNAR ANDREASSEN, THOR GUNNAR ESKEDAL, RIMA VENTURIN

Ragnar Ø. Andreassen is Research Scientist in Telenor R&D

Thor G. Eskedal is Research Scientist in Telenor R&D

Rima Venturin is Research Scientist in Telenor R&D

It is possible to exploit Wi-Fi technology also to provide publicly available broadband radio access services. This requires a fine-grained backhaul for access points. We propose to use existing copper infrastructure here. Such a development represents a specific case of fixed mobile convergence, and it is unclear how the commercial environment will be. This paper describes several possible business scenarios associated with the proposed technical development, and discusses their relative merits with particular emphasis on the situation for incumbent fixed and mobile operators, and emerging hotspot operators.

I Introduction

The last years' trends show a pronounced growth within Wi-Fi technology. Public WLANs in terms of Wi-Fi hotspots are already widely deployed. More that 100,000 public hotspots are up and running, and this number is increasing rapidly. The increase is seen both in the business and residential spheres. In addition, we observe that several communities in different parts of the world attempt to offer WLAN coverage as a public utility in competition with commercial services offered by existing cellular networks. Another trend is the increase in functionality associated with the WLAN 802.16 protocols, and the technical effort that is taking place in order to integrate mobility handling traditionally associated with cellular networks into the WLAN domain (e.g. Universal Mobile Access (UMA) initiative [1]). A third important trend already observed, is the integration of WLAN components, not only in portable PCs, but also in handheld devices (e.g. gaming consoles) as well as in some mobile terminals. These factors indicate a convergence in functionality and services between WLAN and the telecom-driven 3G wireless systems.

The development raises several interesting questions with respect to how and by whom the mobile broadband services will be offered to the public. New technology may enable new actors to become mobile access providers and compete with existing cellular operators. In this paper, we analyse a novel concept, utilizing the existing copper based local loop infrastructure combined with WLAN technology in offering public broadband radio access coverage. We denote the architecture the Open Broadband Access Network (OBAN) concept [3]. The aim of the paper is to describe some relevant business scenarios that are made possible based on the technology developed to implement the concept, and to discuss their relative merits.

In the following sections we will firstly motivate the open broadband access approach. Then the OBAN concept itself is described, with focus on the shared access and the possibility to create a broadband mobile network. We then describe a stepwise approach for launching the concepts in the market. Then follows a presentation of business scenarios based on the new technology using a role model method for the presentation. An overall discussion around the proposed business models sums up the article, highlighting the value proposition of the various models as seen from the different market players.

II Rationale for Open Broadband Access Networks

The main motivation behind OBAN is to explore the possibility to utilise the spare capacity of the privately owned fixed broadband access line to form a public broadband wireless network based on Wi-Fi. As described, there is already a strong focus on Wi-Fi both in the private sphere as a mobile add-on to the fixed broadband line, as well as a broadband public wireless alternative to 2G and 3G mobile networks. Wi-Fi has a strong momentum especially due to its use of the free frequency band, low cost equipment, easy and cheap installation and IP centric radio characteristics. All these aspects have led to a large-scale installation of Wi-Fi access points, producing an interest in the industry to explore the potential of the technology as a complement and/or substitute to 2G/3G networks. Especially for indoor coverage, Wi-Fi is a strong competitor to the cellular mobile networks. This is due both to the increasing capacity demands for data applications and to its better indoor radio coverage.

The penetration of broadband accesses is currently large in most European countries. xDSL is the most widely used broadband technology to private and public locations besides cable and fibre access. The bandwidth of these technologies is steadily increasing. A large part of the capacity of the fixed broadband access line is unused. At the same time, it is

ISSN 0085-7130 © Telenor ASA 2006

foreseen that the mobile networks will not be able to deal with the increasing capacity demands of the future. If the many broadband access lines could be enhanced with a public Wi-Fi access, this would relieve the load on the mobile networks and give the users a high-speed data centric wireless access network.

The OBAN concept may be used in both public and private environments. In dense areas there will also be high traffic load outdoors. To cope with this high traffic load, the 2G and 3G networks need to be built with a correspondingly high density of base stations. Due to interference and bearer channel structure there is however a practical upper limit of the capacity of these mobile networks. The cost per bit will increase as the interference levels increase. With public Wi-Fi based on the privately owned broadband access network and with outdoor reach a low cost broadband wireless network would be sought without extra external feeder lines and radio masts. This evolution of Wi-Fi and broadband fixed access together with the need for a high capacity cheap IP centric wireless technology have led to the formation of commercial Wi-Fi hotspots and Wi-Fi community networks. By bringing the hotspot business models into the private domain one obtains the OBAN vision of sharing the privately owned fixed broadband access line with public users.

Fixed mobile convergence is another driver towards the use of public Wi-Fi access and the integration of Wi-Fi and mobile networks. Terminals are becoming multi-radio enabled and most services are IP based and able to run over IP networks. This IP service and IP transport are seen as a requirement for the future market, which demands a seamless service experience regardless of the underlying network technology. The service should not be broken or disturbed in any way when moving between networks. This requires fast mobility and authentication procedures when moving between heterogeneous networks as well as between Wi-Fi APs. Being able to support real time applications like interactive gaming and multimedia conferencing is one of the main study items in the OBAN project. In the following is given a description of the technical realisation of OBAN.

III OBAN key technical concepts

The OBAN concept is based upon a technological solution that enables public nomadic users to use the capacity of the already installed fixed broadband accesses. This is made possible by introducing a Residential Gateway (RGw) at private or public spaces with functionality to split the WLAN capacity into two separate Virtual LANs (V-LANs), e.g. by means of different Service Set IDentifiers (SSIDs). The traffic on the wireless segment is grouped into different Quality of Service (QoS) classes to support time sensitive traffic. Traffic on the fixed access line is also split in accordance with e.g. QoS classes with priority mechanisms. In that way, priority can be given to the owner of the fixed access line. Public users may also use time-sensitive applications on the other V-LAN. Everywhere where an OBAN RGw is installed this splitting of the fixed access line will be possible.

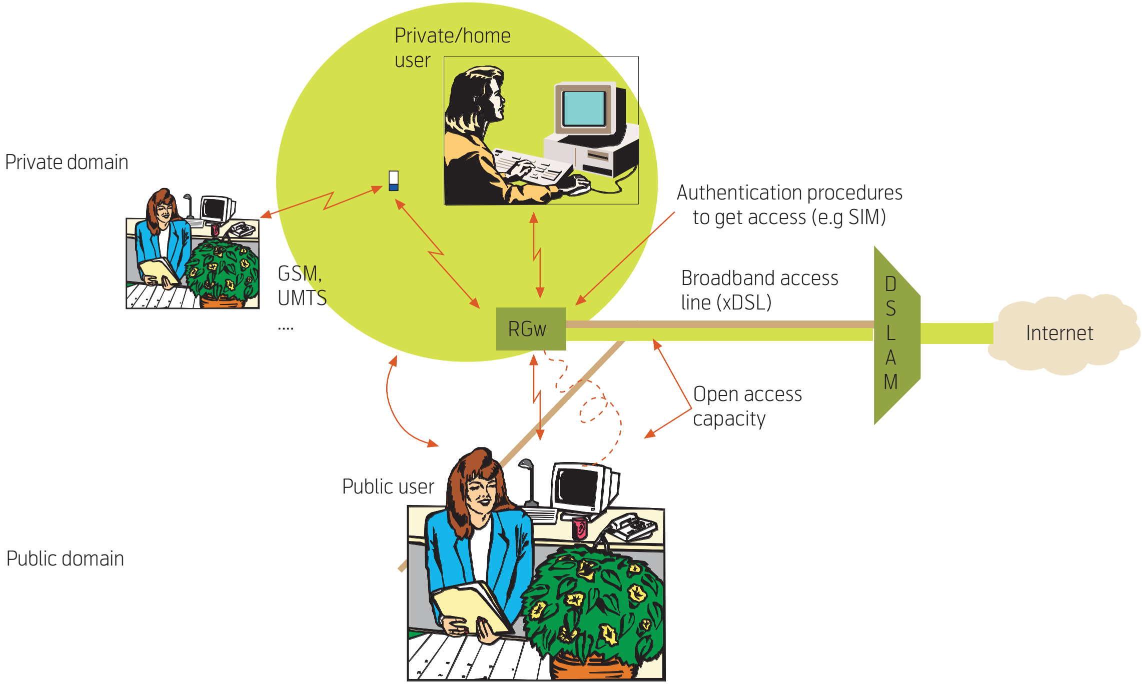


Figure 1 Open access network supporting private and public users

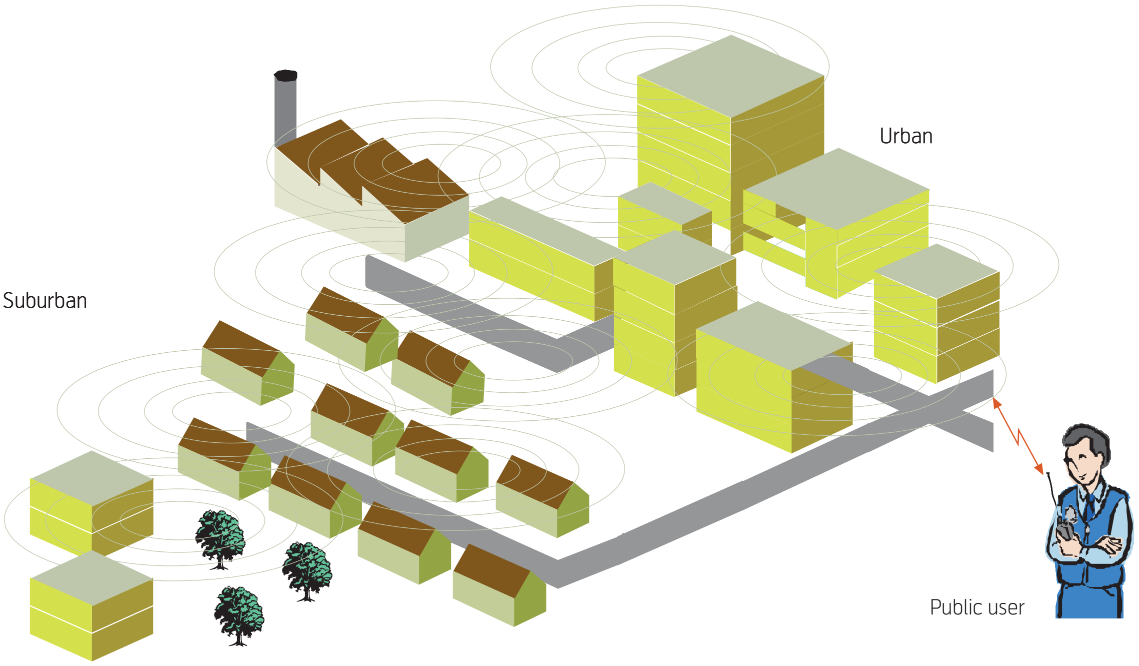


Figure 2 City wide Wi-Fi coverage based on the OBAN concept

As Figure 1 shows the access line to a residential or public environment is divided into two domains; one for the home user or private domain and one for the public domain. The access line may be divided in several ways. It may be a static separation with fixed capacity for the home user and the public users. This static separation does not efficiently use the capacity of the access line but it ensures that the home user gets the capacity paid for. Alternatively, the access line capacity may be divided dynamically. The home user may still have priority to use a fixed share of the capacity but if not used the public users may use the unused capacity. This multiplexing may benefit both the home and the visiting user. The home user may pay for less capacity that he can use if there are few public users on the network. On the other hand, the public users may have the opportunity to use high bandwidth if the home user is not using the access line for the moment. Each domain is allocated separate SSIDs as security access codes.

By extending the reach of the residential or business WLANs to also cover outdoor environments, the OBAN concept may be used to build citywide Wi-Fi coverage enabling seamless mobility throughout the whole coverage area. Mobility mechanisms, authentication, authorisation and accounting (AAA) functionality, subscription repositories etc. are needed in the fixed access core network very similarly to cellular networks today. In dense areas where the buildings are close together, the open access concept may be a cost efficient way to enable public broadband radio access. The open access concept will also support vertical handover to cellular networks and other wideband technologies such as WiMAX, enabling continuous coverage also in areas where gaps in the Wi-Fi coverage may exist (e.g. parking lots, parks).

There are various options when it comes to integrating the RGw functionality with the functionality associated with residential usage. A minimum integration scenario is where the access resource is split at the physical level, and the RGw offering public services is realized in a separate unit. In that case the residential user owns and operates a WLAN router more or less in the same way as today. A maximum integration scenario is the replacement of the original private WLAN router with an operator operated RGw. This will require a much tighter relation between the involved operators, e.g. mobile operators and fixed operators, with respect to service provisioning for the residential user.

IV OBAN business models

This section presents the strategic implications of the OBAN concept with respect to both incumbents and emerging players in the telecom market. Strategic issues are covered through a role model, discussing the roles and values different players can take applying the OBAN concept. The considered OBAN role model includes the following roles:

- RGw operator: Controls the configuration and operation of the residential gateway.

- Site owner: In addition to providing housing of the RG, the site owner may be a traditional broadband fixed access subscriber.

- Visiting user: A user different from the site owner that accesses services available at the residential gateway.

- Mobile service provider: Offers publicly available mobile services (e.g. speech, messaging, multimedia, Internet access).

- Internet service provider: Offers Internet services available over fixed or dial up access.

- Mobile access operator: Operator of wireless access networks that can be used for providing mobile services.

- Fixed access operator: Operator of fixed access (e.g. DSL) networks.

Several players may want to control the residential gateway (RGw). Therefore, RGw-operation is separated into a role that can be performed by several players. The basic function of the RGw will be to provide local WLAN-based radio access, separation of domestic (for the site owner) versus external use, and resource management and usage metering. Depending on who actually performs the role, RG-functionality can be further tailored.

The RGw must be located somewhere, namely at the premises of the site owner. In anticipation that the RGw may be an evolution of a domestic WLAN router, the site owner is given special status as user compared to other occasional users. Other users are here named visiting end users.

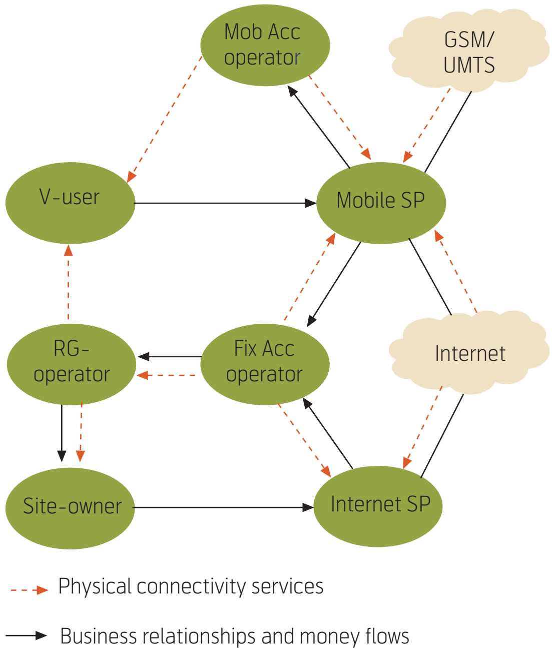


Figure 3 Roles and their interrelations in terms of connectivity services and business relationships

Mobile service provider is the unit offering traditional and emerging mobile services to end-users. It offers two-way reachability by operating a location register. The mobile service provider also offers mobile Internet access. In order to offer its services, the mobile service provider needs to use the network and services of a Mobile access operator. The Mobile access operator has the radio nodes providing regional (usually country-wide) mobile services. It also handles access control, usage metering and mobility handling.

Internet service provider is the unit offering traditional end emerging Internet services, such as Internet access, e-mail etc. In particular, the Internet service provider will offer VoIP services. The ISP handles the interconnect agreements towards other parts of the global Internet. In our context, the Internet service provider offers its services through a fixed access network such as DSL or cable. This access network is operated by a fixed access operator, which conceptually offers a bitpipe with certain characteristics (service classes, etc.) between access points at the user premises and the Internet service provider premises.

Several parties are left out of the discussion, such as application service providers, content providers, equipment vendors and backbone network operators. Even though these may deliver important premises, we consider that they will not have important strategic roles with respect to the particular aspects discussed here.

Figure 3 represents the base role configuration with no players yet defined. Note the difference between a role and a player; a player is an economically responsible business unit that may take one or more roles. We can use the above figure to define various player scenarios as illustrated in the following. In the figure, the dotted (red) arrows denote the physical connectivity services. The directions of the arrows denote who provides a service to whom. The solid arrows indicate potential business relationships, and the directions of arrows here indicate the likely direction of money flows.

The reasoning behind the figure is: The V-user has a subscription at an MSP. The MSP buys access services from mobile access operators and/or fixed access operators/RG-operators. The RG-operator compensates the SO for use of physical premises, electrical power etc. The site owner is a customer with an ISP, which again provides access via a fixed access operator. It is possible to break up the roles into still finer units. We could for example in the model have differentiated the fixed access operator on whether it provides a bare copper access service or a version of bitstream access. We propose however to use the above as a compromise between simplicity and accuracy.

We omit the arrows indicating service relationships in the remaining figures describing business scenarios.

V Some relevant OBAN business alternatives

Players considered in this section are fixed network operators, mobile network operators (both new and incumbent), service providers (Internet and Mobile service provider), WLAN hotspot operators and aggregators. All these players want to manoeuvre into a position that can be considered as advantageous and profitable. This means that each participant is considering its main interests and strategic assets relative to specific roles.

a) Fixed access operator manages the RGw

In the scenario illustrated in Figure 4 the fixed access operator sees a business opportunity in enhancing its access network functionality to provide wireless access as well.

In effect the fixed access operator then walks into the traditional domain of the mobile access provider. It may need to perform many of the tasks associated with the role of being a mobile access operator such as mobility. Such an actor will however still also provide fixed access services in residential and corporate markets. The RGw can in this case be seen as an integral part of the access network, and can be operated and maintained as such. This enhanced fixed network is rented to service providers, both fixed Internet service providers and/or mobile service providers, on a wholesale basis. The customer relation is always with the Internet service provider or the mobile service provider. These players charge the customer for the OBAN service and pay the fixed access operator for the transport and additional functionality as quality of service support and mobility. In essence the fixed access operator operates the Wi-Fi network as a mobile access operator operates a 2G/3G network by renting the radio capacity to MVNOs and SPs. The fixed access operator gets traffic charges and management charges from the SPs.

b) Internet Service Provider manages the RGw

The next considered alternative, where the Internet Service Provider (ISP) takes on the role of operating the RGw, is illustrated in Figure 5. This is a natural deployment scenario considering that ISP is often today in charge of the broadband modem and thereby has the customer relation directly.

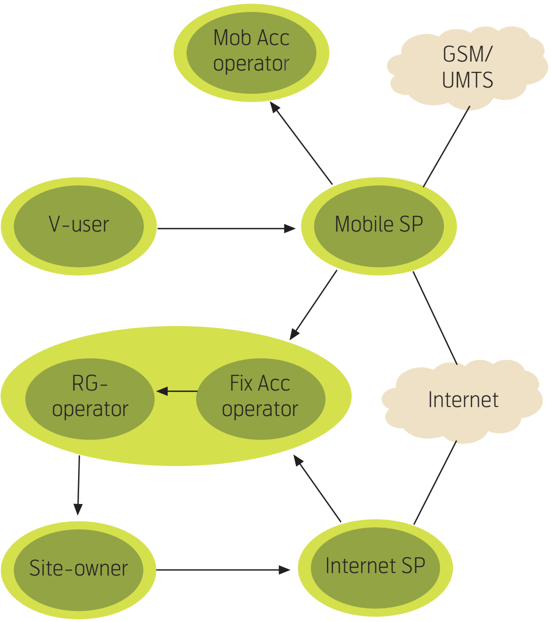


Figure 4 Fixed access operator manages the RG

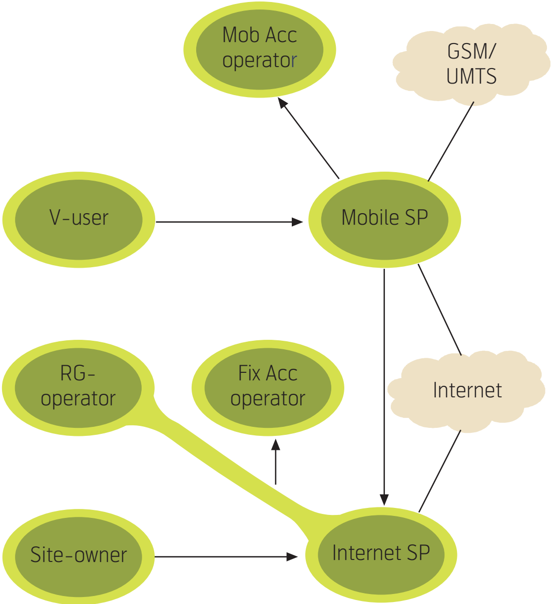


Figure 5 ISP manages the RGw

The difference from this case to today's situation is that the ISP also needs to take on functionality to support visiting mobile users. To support inbound roamers the ISP needs to invest in AAA servers with radius functionality, home agent functionality supporting mobility and roaming agreements. The foreign agent client and radius client is located in the RGw and there is a direct relation between the authentication and the routing of the traffic to the correct Internet service provider of the customer.

The value proposition for the internet service provider may be to take back the lost voice traffic to

ISSN 0085-7130 © Telenor ASA 2006

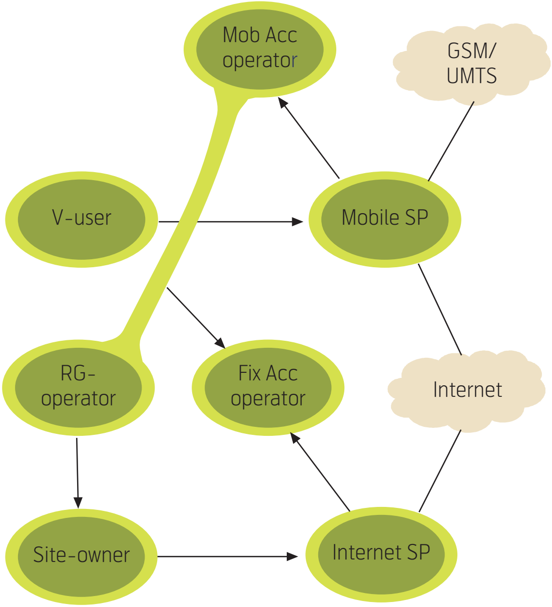


Figure 6 Mobile access operator manages the RGw

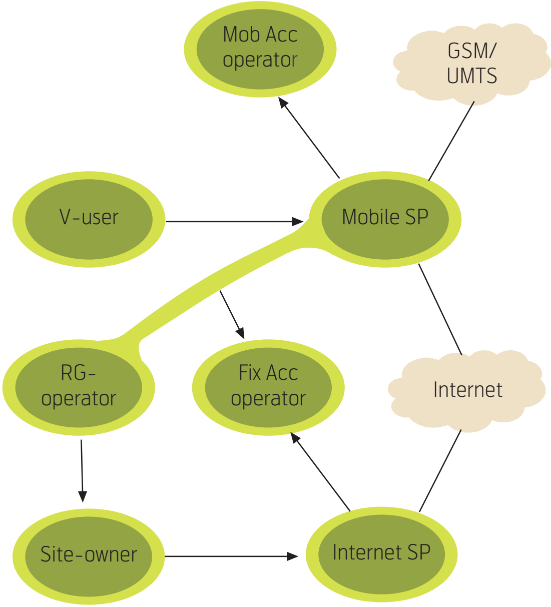


Figure 7 Mobile service provider manages the RG

mobile networks by offering a Wi-Fi based broadband offering with VoIP services. If the Wi-Fi coverage is large including seamless outdoor coverage the ISP is actually becoming a mobile service provider.

c) Mobile access operator manages the RGw

As illustrated in Figure 6 the incumbent mobile access operator is a natural candidate for operating an RGw in order to offer public mobile wireless services based on Wi-Fi. In this manner the Mobile access operator acquires another high bandwidth wireless technology. The coverage reach is short but due to the higher bandwidth the Wi-Fi network may be rolled out in dense traffic areas and share the load with the 2G/3G networks. The operator may adjust the traffic volumes to the different networks to optimize the various network usage and build out cost.

The Wi-Fi network may be operated in the same manner as 2G and 3G networks meaning that other market players may take on roles as MVNO and SP similar to today's regime. The mobile access operator gets traffic charges as well as charges due to good indoor coverage with a high capacity wireless alternative to 2G/3G networks.

d) Mobile Service Provider manages the RGw

Figure 7 illustrates the fourth alternative where the mobile service provider takes on the role of managing the RGw. This scenario is not very different from alternative 2 where the ISP operates the RGw. The mobile service provider is thus in a better situation than the ISP since the mobile service provider's main business has been to support mobility and roaming. The mobile service provider has special knowledge to support authentication, mobility, charging in terms of mobility and roaming and will have the right equipment and skills to take on the role of an RGw manager. The mobile service provider will also be in a very good position to give the customers a converged service experience while camping on fixed and mobile networks and offer the same service portfolio across network boarders.

Since Wi-Fi is typically short reach and high bandwidth, it would be especially suited as a complement and load reliever to the 2G and 3G networks for indoor installations, e.g. in shopping malls, train stations, and coffee shops.

e) RGw Operator – Disintegration scenario

The next alternative, illustrated in Figure 8, is a disintegration scenario where the barriers for establishing RGw-operation are very low. In this alternative a large number of independent RGw-operators can be seen. These RGw operators may be the residential users themselves or companies specializing in RGw-operations. If the user operates the RGw themselves and charge customers for access, they are actually taking on a business role. By taking on such a role business obligations will follow, e.g. taxation, producing financial statements, etc. With a large number of independent RGw-operators, there will be a need for an aggregation function that can act as an interconnect central. This will relieve the visiting user of the need to have agreements with all the many OBAN hotspot operators. If such an aggregator exists, each mobile service provider would go to the aggregator and sign up a contract to grant all authorised customers to the mobile service provider access to the RGws. All users would then also have one entity to contact to get access to all the RGws that are under the domain of the aggregator. If the aggregator has agreements with many RGw operators, the users that connect via the aggregator will have a larger coverage zone.

Many existing and upcoming Wi-Fi operators, such as Boingo, The Cloud, FON, Iport, has gone into the business of supporting independent Wi-Fi AP owners to enlarge their coverage zone. Their business models are different and their customer base of Wi-Fi owners is based on different incentive strategies. The models are not based on OBAN but they are quite similar all the same. All of them have entered Wi-Fi business supporting a business model where the site owner can share the access network with other people.

FON, as an example, has implemented a business model of creating a community network for registered FON users. Access point owners can join the FON community either as roaming members ("Linuses") or non-roaming members ("Bills"). The Linuses get access to free roaming by admitting other FON members to roam into their access points. Bills join FON on a revenue share basis, and do not have access to free roaming. The revenues in the system are generated by "Aliens", i.e. non-FON members that pay for Wi-Fi access. FON members either download special access control software to their routers, or buy pre-configured routers from FON. FON as such plays the aggregator and service provider roles in relation to the OBAN role model.

The business model of Boingo is different from FON. Boingo supports site owners with software to their Wi-Fi access points that supports authentication of public users. Boingo acts as an aggregator and supports the authentication and billing of users that use the Boingo customers' Wi-Fi access point. The user gets 75 % of the payment from the public user and Boingo gets 25 %. This is similar to the "Bill"-part of FON and provides the incentive for RGw owners to open their Wi-Fi access points to visiting users. As for FON, Boingo here acts as an aggregator which a public user can sign an agreement with, and thereby get access to all Boingo access points.

The aggregator can be a new player, or an incumbent mobile access operator. This latter case is not unnatural, as an aggregator can perform several of the tasks usually associated with mobile access operation such as access control, mobility handling and roaming. The incumbents may on the other hand consider the emerging aggregators as competitors in their core business.

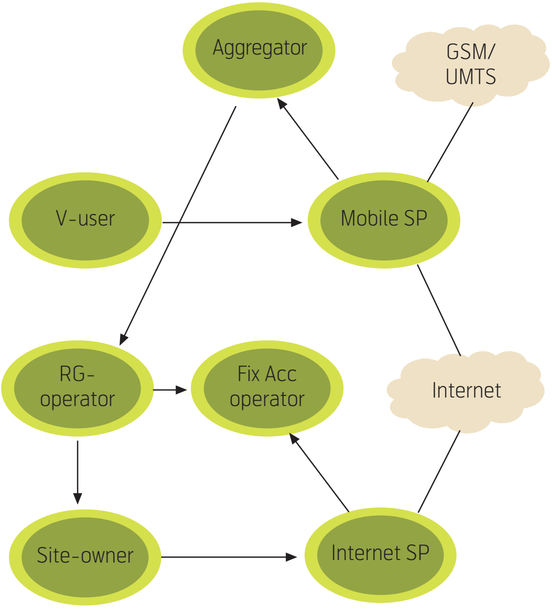


Figure 8 Separate RGOs & Aggregator

f) Integrated business models

Since different operators have different internal company structure, the models presented above may be partly integrated. The fixed access operator and the Internet service provider may for example be the same business unit and will cooperate very closely to implement an OBAN solution. Also operators with a total integration of the fixed and mobile department will utilize their common assets to create a converged network based on OBAN. With such tight integration the operator may benefit from the different characteristics of the different wireless technologies to optimize traffic handling. Incumbent cellular operators and fixed operators may also enter into cooperation with independent hotspot operators such as Boingo or similar to broaden their portfolio of wireless networks.

With all integration it is however important to be aware of potential regulatory constraints. Such constraints may affect bundling strategies, pricing and other factors that are relevant for competition.

OBAN was mentioned earlier as a way to achieve fixed-mobile convergence (FMC). Since the OBAN RGw has incorporated functionality to authenticate users, e.g. based on SIM, it may be used for public FMC access. Customers who are connected to a mobile 2G/3G network and who reach the coverage area of an OBAN RGw, may be automatically switched over to the Wi-Fi network. Functionality such as network selection in the handset, common SIM authentication and SIP signalling as a common call control protocol are enablers to support FMC. The upcoming standard for voice call continuity (VCC) can be deployed to achieve seamless handover across heterogeneous access networks.

VI Discussion

We shall limit the discussion to focus on the following stakeholders: incumbent fixed operators, incumbent mobile operators and the emerging hotspot operators. A more extensive discussion is carried out in [4].

The incumbent fixed network operator has traditionally had a substantial part of its income from sale of PSTN services. This is an inheritance from old, where telecom business was monolithic and not horizontally and vertically segmented as we see it today. Indeed, in later years the access network operation has become a more independent business, a development much urged by public regulation. A typical incumbent player is still a combined fixed transport and access network operator that may sell services on a wholesale basis to service providers. Many of these operators are in the midst of a more or less aggressive xDSL roll-out phase, meaning that the copper access network is a most valuable strategic resource. Therefore, they will probably see a possibility for increasing the value of that resource through the OBAN concept by extending their control to also incorporate the Wi-Fi access point. As many of these players are facing considerable PSTN revenue decreases, they have a motivation for pursuing this possibility aggressively. Technically, the inclusion of RGw operation can be seen as a natural extension to the service provisioning already being undertaken in the access. Some fixed access operators are already implementing quality differentiation at the access level, which is a major and complicated service upgrade. They are in a prime position to also include and extend these services to the air-interface of the RGw and open the access for public usage. By opening the access for public users the operator may in fact sell capacity on the same access line to several service providers simultaneously and increase the revenue from the sale of access resources.

Other incumbent players that surely will consider the RGw operation are mobile network operators. These operators already operate wireless access networks on which they produce mobile access services either for internal use or offered externally on a wholesale basis. As mobile terminals imminently are equipped with WLAN capabilities, and coordination bodies like UMA [1] and 3GPP [2] make available specifications for seamless interoperation between WLAN and cellular, it will be natural for them to consider the capabilities open access offers as an extension of their core business using yet another wireless access technology. Many mobile operators are in the midst of a 3G network upgrade phase, e.g. with High-Speed Downlink Packet Access (HSDPA), that will make available several of the services that might have been offered also on an OBAN platform. For this reason, they may be less eager than the fixed access operator to promote the technology. Still, if they choose to do so, they have extensive expertise in the handling and operation of mobile service. They also partake in a commercial environment where interconnect and roaming are everyday practice, and are thus supremely positioned to enter the RGw operation role.

Another possible scenario is that hotspot operators develop their service portfolios from simple Internet access to more advanced mobility based services such as VoWLAN, and that they organize. In that case, a scenario like the one presented in Figure 8 may develop. In particular, if person-to-person communication becomes an important service for hotspot operators, the motivation to organize and interconnect through an intermediary aggregator will be stronger. This is due to the network property of person-to-person services, increasing the value of networks in proportion to the square of the subscriber base. Wi-Fi hotspot operators are typically simpler companies with moderate capital bases compared to incumbent fixed and mobile operators. The main assets for some of the hotspot operators are agreements with interesting site owners such as hotels and airports. Still, if operation of RGws becomes inexpensive and simple enough, these actors may venture into the market of providing more general connectivity, possibly also cooperating with mobile operators. Cooperation with mobile operators will be a major asset for hotspot operators since the hotspot operator/aggregator will then be able to market wide area mobility for their customers through the agreement with a mobile operator.

When considering OBAN and hotspot operations, it is important to keep in mind the potential regulatory requirements and obligations. Wi-Fi wireless access use unregulated frequencies. As Wi-Fi is being deployed commercially this may result in problems due to interference, radiation and disturbances for/from other electronic devices. Regulation may therefore be enforced on the usage of Wi-Fi. One should also be aware of irregular usage of Wi-Fi, where opening the access point for public usage conflicts with Internet service provider agreements.

Summing up this discussion, there are currently large uncertainties with respect to the commercial environments in which the open access technology will be operated. We have here pointed out some factors that may influence the development and the potential impact the open access concept could have, especially for incumbent fixed and mobile access and service providers.

Acknowlegdements

The authors would like to thank the participants in the IST OBAN project for valuable technical information, and all the work package 5 participant especially for co-working with us on the business models[1].

References

1 *UMA Technology*. 8 August 2006 [online] – URL: http://www.umatechnology.org/

2 *3GPP*. 8 August 2006 [online] – URL: http://www.3gpp.org/

3 *Market and environmental aspects of OBAN*. Brussels, IST project OBAN, Jan 2005 (Deliverable D6)

4 *Business viability study*. Brussels, IST project OBAN, Jan 2006 (Deliverable D24)

5 *Open Broadband Access Network – OBAN*. 8 August 2006 [online] – URL: http://www.ist-oban.org

Ragnar Ø. Andreassen received his MSc degree in Physics from the University of Oslo in 1988, and his PhD from the Norwegian University of Science and Technology, Trondheim, in 1997. Since 1988 Andreassen has been with Telenor R&D, where he has worked in various fields associated with telecommunication services, network technologies and business aspects. His current research interests include network architectures, network traffic and dependability performance, and charging and pricing of telecommunication services.

email: ragnar-oivind.andreassen@telenor.com

For a presentation of Thor Gunnar Eskedal, please turn to page 84.

Rima Venturin received her BSc and MSc degrees in the field of Electrical Engineering, area of Telecommunications, from the Faculty of Electrical Engineering and Computing at the University of Zagreb, Croatia, in 1992 and 1995, respectively. She has been employed by Telenor R&D as Research Scientist since 1996 and has been working with techno-economic analysis, business modelling and network planning since 1998. She has been involved in numerous international projects (IST, EURESCOM) and is the author/co-author of several publications. At the moment she is Research Manager for the Business Assessment group.

email: rima.venturin@telenor.com

[1] *The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability and other partners are not committed under any circumstances by the content.*

Charging Models in the Open Broadband Access Market – Theory and Practice

ANDREA AMELIO

Andrea Amelio is a special consultant at LECG and ISMB and research assistant at GREMAQ

Due to the massive development of WLAN, users can now access Internet through a WLAN Access Point. The total price that users pay is determined by a set of rules that is commonly known as a charging scheme. This article aims to address theoretical relevant aspects that must be taken into account when designing a charging model for open broadband access and gives practical evidences of their recent implementation providing real cases.

Introduction

Due to the massive development of WLAN, users can now access Internet through a WLAN Access Point. All they require is purchasing a subscription, an authentication key and paying the usage fee.

The total price that users pay is determined by a set of rules that is commonly known as a charging scheme. Such a charging scheme is a mathematical relation that describes how a charge is calculated based on a set of attributes pertaining to the service.

A well-designed charging model is the one that guarantees the sustainability, growth and development of a service. Therefore, understanding how to optimally charge consumers for a service they make use of is a fundamental business activity. A good choice of the charging strategy determines the adoption of the service by consumers and its success.

This article aims to address the theoretical relevant aspects that must be taken into account in designing a charging model for the open broadband access and gives practical evidences of their implementation providing real cases. Section 1 highlights ten relevant aspects to account for in the definition of a charging scheme in the open broadband network context. Section 2 provides empirical evidences on the actual implementation. Section 3 concludes.

1 Relevant elements in the charging decision

Based on the vast literature on charging schemes and on the specificity of the open broadband access market, we identify ten main issues that a provider should be aware of when designing a charging scheme for open broadband access.

1.1 Maturity of the product

A brand new product is not known in the market and needs to be tried by consumers. Consumers have to be stimulated to adopt this new good. To build the attraction and to gain loyalty, an intuitive and easy-to-understand charging scheme (that makes clear how consumers are charged) is desirable. It may be difficult to induce sceptical consumers to try a new service. In this phase, the costs of supplying the product should not be the focus. Likewise, it is crucial that the consumer does not abandon the service after having tried it. The possibility to engage in long-term agreements with the consumers would be valuable for a new service in order to ensure its sustainability.

1.2 Consumer preferences

The perception of a service across consumers is heterogeneous and consequently the willingness to pay is also different. In such environments a profit maximizing service provider can increase its revenues by engaging in some sort of price discrimination. Targeting different classes of consumers on the basis of some verifiable characteristics or letting the consumers choose from a basket of options are well-known methods to achieve this aim. Therefore, a charging method should account for heterogeneity in the consumers and provide different selling options for the same products. However, the reaction of the consumers is not always positive to price discrimination. When the tariff basket gets more and more complicated, the fear of making the wrong choice or the burden of high screening costs could keep consumers away from the service. Simplicity seems also to have a strong impact on the consumers' preferences. As noted by the US Federal Communications Commission: "Customers have shown a strong preference for simple pricing systems" [1]. A trade-off between price discrimination and simplicity is therefore desirable.

Uncertainty is another relevant dimension in consumer preferences. Consumers are risk averse and face a limited ability in estimating their consumption due to uncertainty on the future. This could induce them to prefer paying a fixed amount (being insured) rather than some variable amount conditioned on their future uncertain consumption.

ISSN 0085-7130 © Telenor ASA 2006

Consumers also have different perceptions and different abilities of forecasting service usage depending on the time or the volume (i.e. kbit). For some services (e.g. telephony and web browsing) customers easily understand how long they are connected, but may have a harder time getting a handle on their data usage, so they have a "temporal perception" of their connection. On the other hand, for other services, such as information download, the volume is known while the download duration may depend on factors outside user control.

1.3 Network effects and market conditions

In all the communications services, consumers are affected by the size and the type of the community of people using the service. For some services, users benefit from a direct interaction with users within the same community. For other services, the benefit passes through a "platform" which connects the different communities of people. We call this direct and indirect network effects, respectively. In both cases, the larger the number of people using the service, the better it is for each individual consumer.

Firms in the telecom market are more and more realizing their real nature of platforms that put callers and receivers in contact. More generally, platforms match groups (two or more communities) of people that have an interest in meeting each others[1]. These groups are interested in joining the platform and using the offered services only if they are able to meet a sufficiently large number of participants belonging to other groups. In this context indirect externalities arise and platforms' success (and profit) depends on the ability to attract people from all the groups (participation) and on the total use of the service (transaction volume) made by the participants (usage). In this context, a charging model entails participation fees (to join the platform) and usage fee (to use the service). These are the two instruments that platforms dispose to design a charging model whic must overcome different issues.

Convincing people to participate is the most difficult problem for platforms. People's willingness to participate depends on the participation of others. Therefore, a consumer will participate only if he believes that others will do the same. A coordination problem could arise: in a condition where users do not know what the others will do, the rational consumer does not join, and so the others, causing the failure of the platform. A solution to overcome this failure is to give some subsidies (money back to subscribers or through special discounts) [2].

In these particular "matching" markets (like telecom), a symmetric tariff structure with respect to the different groups of participants may no longer be the optimal one with respect to maximisation of transaction volume (and profits). A more general rule says that the group with more elastic demand compared to the other groups' demands is the one to charge less, or stated differently; the user group that sees the most value in the participation of the other group should be charged more. In many real cases, like voice calls service, platforms charge only one group. This is what mostly happens in telecom markets where only the caller is charged and the receiver does not pay.

1.4 Degree of market power

The relation between the charging model and the market power is a complicated field with no general results. However, it seems to be well understood in practice that the market position held by a firm is a key factor to define the charging strategy. Some observations seem to indicate that when firms face a very competitive market, the main objective is to steal customers from rivals, which calls for a simple charging strategy to facilitate the tariff comparison. On the other hand, a firm with strong dominance position can engage in discrimination, presenting a more complex tariff basket with less risk of losing customers.

1.5 The selection of the attributes

Attributes are intrinsic characteristics of a service which can be used to meter its usage. The selection of attributes is a crucial point in the charging strategy. The set of attributes is vast and consequently also the mathematical rules implemented for each charging scheme. However, in the telecom industry only a subset of them is commonly used. Time based, flat and volume based are the most common charging schemes.[2]

[1] *Examples of "platforms" are videogame platforms like Nintendo, Sony (game developers and players) or credit card (merchants and shoppers), dating agencies (male and female), portals, TV, newpapers (audience and advertisers) and also telecommunication networks (caller and receivers).*

[2] *Many other charging models can be implemented. We mention briefly contents based charging models where users are charged according to the type of contents they consume. More complicated charging models are based on expected capacity. Under these models, the users are charged based on their expected capacity and not on the peak capacity of the network.*

Another charging scheme uses the concept of "edge" of the network. This model, called edge pricing, charges for usage at the "edge" of the network scope for the subscriber rather than along the expected path of the source and destination. Finally, the Paris metro pricing uses the concept of travel classes on transport systems. The higher priced service classes will be less congested and thus have the higher quality.

In time based charging, the user pays based on the time. Time based charging requires the notion of service sessions. On the consumers' side, users have a precise perception of the time passing. Therefore they can monitor the costs they are bearing. During voice communications, they can also estimate the connection time with fair precision and consequently forecast in advance the cost of the connection. Regarding Internet users, the ability to forecast the connection time seems a lot lower, possibly leading to a decrease in usage.

Flat rate is one of the most widely used charging models by Internet Service Providers. In this model, the network provider will charge users a fixed rate for using their network. The rate is therefore independent of how much network resources the user occupies. The advantage of this charging model is that there is no need for the service provider to implement complicated systems to gather usage information in order to charge the users. This enables the service provider to save on billing systems and mediation systems infrastructure. The disadvantage of this model is that the service provider will be unable to reap the economic benefits of the heavy user. The light user would be subsidizing the heavy user. This model could also lead to congestion in the network especially during peak hours due to the lack of usage incentive mechanisms.

Volume based charging is a charging model used by many Internet service providers. Volume typically means the amount of bytes transferred, but volume charging can be implemented in a simplified way by counting the number of IP packets passing. In both cases, the user is charged based on the amount of data the user sends or receives through the network. The advantage of the model is that users are charged based on their usage of the network. On the other hand, the disadvantages are that the service provider will have to implement counters within the system leading to higher implementation costs and consumers have a limited perception of the volume of data exchanged. The consequence may be a decrease in usage. Only consumers who prefer "always on" usage may appreciate this type of charging.

1.6 Option tariff

An option tariff is constructed by combining usage based tariffs with flat rate elements. These tariffs are normally called two or three part tariff. A two-part tariff is thus a flat rate plus a usage a part. A three-part tariff is usually a flat rate with a usage based fee and an additional usage based fee for excess usage. Several two- or three-part tariffs form a basket of tariff options offered at the same time, providing a mechanism for consumers' self-selection (and thus price discrimination). Perfect discrimination can be a viable way to raise profits. However, it can imply very complex tariff baskets. Complication is not always desirable and sometimes profit gains from implementing a complex option tariff strategy decreases rapidly with the number of tariff options offered. A study done by Miravete [3] on the US mobile industry tries to evaluate the optimal number of tariff options. This is determined when the level of foregone incremental profits becomes comparable to reasonable costs of product development and commercialization. The results question the idea that offering many tariff options to screen consumers is beneficial and show that cost and benefit become comparable when offering two or three options. Therefore, two- or three-part tariff options are generally the best compromise for a tariff basket.

1.7 Bundling

Bundling is the practice of selling two or more products together. This practice does not relate directly with a charging model; however, it could be an instrument to implement some charging decision in a more effective way. In the context of platforms, if the charging decision entails subsidies to one group, the cost of subsidization might be large. The platform may have to pay a large population to attract a small one. Instead of actually paying out cash, the platform can sometimes tie some goods or services with the registration so as to create a value to registration. Concerning this, studies have been performed in which the emergence of bundles arises from the need to get people [4][5]. This is particularly true when the cost of making a bundle is relatively low and the bundling helps to enlarge the mass of people interested in the offer. Bundling has the function of solving the coordination problem by boosting the number of subscriptions. Selling the bundle can also be a way of guaranteeing a certain level of service usage. By tying the subscription with goods that are directly related to the usage of the platform, not only subscription but also usage can be boosted.

Bundling can also have the positive effect of screening people according to their willingness to pay. Bundling can be an effective way to price discriminate and to target offers to specific segments of the population.

1.8 Giveaways

Giveaways are presents to consumers. In the telecom markets these are generally services or additional options of one service. Giveaways are a decision not to charge consumers, which seems to be very common in recent business models.[3)] To the extent that business models can be defined as the artful mix of "what companies profitably charge for" versus "what they give away free", successful innovators are branding and bundling ever-cleverer subsidies into their market offerings.

1.9 Pre-paid or subscription

The contract type imposes different commitment on the consumers. Generally, contract types depend upon the maturity of the service and consequently the consumers' awareness and knowledge about it. The consumers perceive the subscription as a long term relationship given the transaction cost involved when opening and closing this contract. Pre-paid contract is typically a temporary deal with a clear value but with complete absence of consumers' commitment. It is used to invite consumers to try the service, lowering the uncertainty on the expected monetary loss in case of no appreciation.

1.10 Randomization

Randomized charging strategy is a widely recognized means to enhance profits. As noted by Baye and Beil [6] the strategy works "by increasing the uncertainty about where the best deal exists, (thereby reducing) consumers' incentive to shop for price information (...) it (also) precludes rivals from knowing precisely what price to charge to undercut a given firm's price". Periodical offers can be seen as a tool to achieve randomized price by making the price more volatile.

2 Open broadband access charging models

In this section we provide three examples of open broadband access charging schemes. All the examples are charging schemes of business activities that aim to implement open broadband networks.

2.1 The FON

FON is a project whose aim is to build a global community of people who are willing to share their fixed access (capacity) to the Internet.

To be part of the community people must subscribe to the FON platform and be willing to share their Internet broadband access by means of a Wi-Fi router and the installation of software.

The subscription is conditionally to the purchase of a specific router which costs 25 €/$ (now offered for 5 €/$) if bought on the FON website. The commercial price is around 53 €/$. Therefore subscription and router are tied. No customer would subscribe to FON and buy the router independently. The subscription fee is subsidized by means of bundling.

Once the subscription and the router purchase have been realized, the user, in the community called FONero, can decide to be a "Linus" or a "Bill". The two statuses give different benefits. A "Linus" shares his Wi-Fi connection in exchange for free access to all other Wi-Fi Hotspots within the FON Community. On the other hand, a "Bill" user shares his Wi-Fi connection in exchange for getting 50 % of the net revenues from those who purchase daily access FON passes to the FON Community through the Bill's FON Hotspot. The people who can purchase daily access FON passes can be "Bill" users or people outside the FON community called "Aliens". The standard rate for these FON passes is currently 3 € for a 24 hour connection period. FON passes are similar to pre-paid cards.

2.2 LinSpot

Likewise FON, LinSpot is a community of people willing to share their fixed Internet access by means of a Wi-Fi router. The organization of this community is simpler than the FON community. The subscription is free and the installation of the software that guarantees the authentication and the billing is downloadable for free from the website. The software works with all Wi-Fi routers, base stations, NAT and network configurations. Therefore, the purchase of the Wi-Fi router is totally independent from the subscription. Each user shares his Wi-Fi connection in exchange for getting the 85 % of the traffic made by the visitors leaving the remaining 15 % to LinSpot to cover the costs for the development of new software versions, the LinSpot servers, marketing of the network.

The end user who purchases the access (generally by credit card using a Pay-Pal system) is charged depending on the length of the connection without subscription fee or activation fees. Prices are 2.5 €/$ for 2 hours, 5 €/$ a day, 12 €/$ a week and 25 €/$ for a month.

2.3 Boingo

Boingo is the most important hotspot aggregator. Its aim is to create a Wi-Fi seamless hotspot network. The intermediation between location owners or hotspot owners and end users is crucial in its business model and the charging strategy reflects its nature of a platform that deals with two different groups of agents.

3) Google charges users nothing to search the Internet; neither does Yahoo nor Microsoft MSN. E-mail, instant messaging, blogging are all free services. Skype, the Luxembourg-based company division of eBay, offers free VoIP – Voice over Internet Protocols – telephone calls worldwide. San Francisco-based Craigslist provides free online classified advertising around the world.

On the side of end-users, Boingo proposes two tariff schemes; "Boingo Unlimited" and "Boingo AsYou-Go". The first offer is a flat rate tariff and it consists of a $21.95 monthly membership fee where no contract is required. The second one is a pay-as-you-go tariff and consists of $9.95 per "Connect Day" with no monthly fee where the "Connect Day" includes unlimited access in a *single* Boingo location for up to 24 hours.

On the side of location owner or hotspot owner, Boingo offers two solutions; "WISP in a box" and "Boingo in a box". The first offer is a way to set up a hotspot location under an own brand name, allowing to offer customized services to property owners. The price of a Boingo-Ready Hotspot is $799. The end user pricing strategy is decentralized and the hotspot owner can offer free-trial coupons and pre-paid cards, and determine end user pricing. If the hotspot owner signs up his own users, he determines his own end user pricing (minimum end user pricing is as follows: $12 monthly rate, $6 daily rate and $3 hourly rate) and receives 75 % of end user revenue. If he signs up Boingo end users, he receives $1 per connect day plus a $20 one-time bounty fee for monthly Boingo subscribers that remain customers for 60 days. If he does both – sign up his own and Boingo subscribers (which is what Boingo recommends) – he will receive both revenue streams.

The second offer is a way to give access to the private Internet broadband connection to Boingo end users and be rewarded by Boingo according to the utilization of the hotspot by end users. The membership fee is free conditional to the purchase of a Wi-Fi router whose price ranges from $117 to $230 that allows giving access to end-users. The hotspot owner is rewarded by Boingo, which pays every time a customer connects at owner's Hot Spot. If the customer has a membership to a Boingo retail monthly subscription plan, or if they are a user of Boingo's roaming system, the owner gets $1.00 per Connect Day. If the customer is using a single "As You Go" day-connect, the owner gets $4.00 per Connect Day (each Connect Day is good for up to a 24-hour period in a given location). Boingo also pays a sign up bonus of $20.00 every time a new customer signs up for a monthly retail Boingo subscription plan at the hotspot owner's location and has been a paying subscriber for at least 60 days.

3 Conclusions

The charging scheme is a strategic and relevant choice in a business activity and it determines the adoption and the usage of the service.

In this article we have presented several relevant issues that a charging scheme for the open broadband access should account for. We have also provided three examples of charging scheme implementation.

It emerges that the existing competition for this type of services and the recent development of this new service play in favour of simple charging schemes, intuitive and not very diversified, where there is almost an absence of discrimination and the relevant metering characteristics are time or flat rate. The need to make people free to try the service without any additional constraints also biases the charging schemes towards the absence of long-term contracts. Due to the presence of network externalities the end users' subscription fees are generally null or subsidized by means of bundling.

References

1 Federal Communications Commission. *Review of Customer Premises Equipment and Enhanced Services Unbundling Rules in the Interexchange, Exchange Access and Local Exchange Markets*. 1998. Further Notice of Proposed Rulemaking, available at http://www.fcc.gov/Bureaus/Common_Carrier/Notices/1998/fcc98258.txt

2 Caillaud, B, Jullien, B. *Competing in Network Industries: Divide and Conquer*. Toulouse, IDEI, 2005. (Working paper, 112)

3 Miravete, E. *Are all those calling plans really necessary? The limited gains from complex tariff*. SSRN eLibrary, 2005. (Working paper)

4 Jullien, B. Two sided markets and electronic intermediation. *CESifo Economic Studies*, 51 (2-3), 233–260, 2005.

5 Tirole, J. The Analysis of Tying Cases: A Primer. *Competition Policy International*, 1 (1), 2005.

6 Baye, M R, Beil, R O. *Managerial economics and business strategy*. Sydney, Irwin, 1994.

Andrea Amelio is a special consultant at LECG and ISMB and research assistant at GREMAQ. He is an expert in the area of telecoms and focuses his research on competition policy and two-sided markets. He holds a PhD in economics from Toulouse University.

email: andrea.amelio@inwind.it

Section 4 – Functionalities

EINAR EDVARDSEN

Einar Edvardsen is Senior Adviser in Telenor R&I

An Open Access Network means that anybody may connect over the present subscribers' lines and wireless home networks, thus the approach challenges many inherited conceptions of today's telecommunication. Not because the challenges are particularly difficult to overcome, but because we are used to looking at the physical access line and the home network as a private domain which belongs to the subscriber and where nobody else can interfere. In OAN we convert these resources into public resources, which can be used by any casual by-passer. This implies that the operator possibly must take control over the residential gateway, which normally is installed at the subscriber's premises. This section contains a selection of papers that address the most evident problems that must be solved in order to establish a public OAN service in a legally correct and commercially viable way.

The basic WLAN protocol IEEE802.11b/g does not provide Quality of Service (QoS) comparable to what is common in traditional telecommunications. The new standard, IEEE802.11e, is an attempt to mend this situation.

The paper *The Main Benefits of Applying IEEE802.11e in Access Networks with Possible Roaming Users* by Paal Engelstad and Olav Østerbø gives an overview of how the standard performs and also proposes a method to even improve its performance.

If OANs shall support mobile real-time services like telephony, disruptions during handover must be kept to a minimum. This is a challenge to be dealt with in OAN networks because the Wi-Fi standards do not support handover to the same extent as the 2G/3G standards do. A major problem is that the WLAN access points may be operated by different service and access providers, thus handover will happen in multiple ISP domains. The paper *Security in Fast Handovers* by Martin G. Jaatun, Inger A. Tøndel and Tor Hjalmar Johannessen presents the problems connected to such handovers and how they are solved in the OBAN project.

How to provide QoS in OAN environments is a demanding issue to solve. The problems are not only located to the wireless section where WLAN only provides limited QoS support, but also to the fact that the bitrate offered by WLAN depends upon the distance between access points. Interference from neighbouring access points also severely impacts on the available capacity experienced by the users. Then finally, when users move from one access point to another, nobody knows whether the next access point has enough available capacity for a new user. In summary, to guarantee QoS in OAN environments requires complex algorithms and traffic monitoring functionalities. The paper *Resource Allocation and Guarantees for Real-Time Applications in WLANs* by Frans Panken, Gerhard Hoekstra and Sietse van der Gaast presents a proposal for how QoS can be guaranteed in OANs.

The last paper in this section presents a solution for how users automatically (hands-free) can authenticate themselves via their mobile phones. The mobile phone transfers authentication data to the connecting terminal and towards the mobile network. The paper *An EAP-SIM Based Authentication Mechanism to Open Access Networks* by Corrado Derenale and Simone Martini describes the method.

ISSN 0085-7130 © Telenor ASA 2006

The Main Benefits of Applying IEEE802.11e in Access Networks with Possible Roaming Users

PAAL E. ENGELSTAD, OLAV N. ØSTERBØ

Paal E. Engelstad is Research Scientist in Telenor R&I

Olav N Østerbø is Senior Research Scientist in Telenor R&I

This paper discusses the possible benefits of deploying IEEE 802.11e in relation to scenarios where residential WLANs are used for public access. Three main features are discussed:

- *The Direct Link Protocol*, which makes it possible to communicate directly between STAs for internal communications (without going through the AP);
- EDCA, which makes it possible to differentiate between Access Categories;
- TXOP limits for fair utilization of the channel.

The actual benefits are discussed for a scenario where both residential and roaming user-traffic competes for the WLAN capacity. The example shows a large improvement in WLAN performance by deploying IEEE 802.11e in such an environment.

Introduction

This paper addresses some of the potential benefits IEEE 802.11e may have (compared to legacy IEEE 802.11) when deploying WLAN as an open access network that may also be applied for roaming users, like e.g. the concept studied in the IST OBAN project [1][2]. The main intension is to try to quantify the benefits of applying the features of the IEEE 802.11e when it comes to the possibility of differentiation among user classes and different traffic types.

In a series of papers [3]–[9], we have addressed different aspects of the performance of the wireless LAN based on IEEE 802.11e analysis protocol under non-saturation condition. This is different from most other work published where saturation conditions are employed. By analytical modelling we have analysed the following important key performance parameters:

- Starvation effects seen in the lower priority classes in IEEE 802.11e;
- Throughput per priority class as a function of the offered input traffic;
- Delays including MAC delay, waiting times in queues and total delay for higher layer protocols where both mean delay and delay distributions are given.

The actual analytical models are suitable tools for evaluating the benefit of IEEE 802.11e when using residential WLANs for public access; however, the actual benefits depend on the scenario. A set of scenarios are selected for discussion. It should be noted that when the channel resources are abundant, the benefits of IEEE 802.11e are less dominant. It is mostly in cases where there is scarcity of channel resources that IEEE 802.11e is of the highest interest, and where its features really come into play.

A brief overview of IEEE 802.11e

During recent years the IEEE 802.11 WLAN standard has been widely deployed as the most preferred wireless access technology in office environments, in public hotspots and in the homes. The IEEE 802.11 medium access control (MAC) comprises the mandatory Distributed Coordination Function (DCF) as a contention-based access scheme, and the optional Point Coordination Function (PCF) as a centrally controlled polling scheme. However, PCF is hardly implemented in any products, and DCF represents the commonly used MAC mechanism of 802.11. DCF adopts carrier sense multiple access ("listen-before-talk") with collision avoidance (CSMA/CA) and uses binary exponential backoff. A station not only goes into backoff upon collision. It also carries out a "post-backoff" after having transmitted a packet, to allow other stations to access the channel before it transmits the next packet.

Due to the inherent capacity limitations of wireless technologies, the 802.11 WLAN easily becomes a bottleneck for communication. In these cases, the QoS features of the 802.11e standard will be beneficial to prioritize for example voice and video traffic over more elastic data traffic.

The IEEE 802.11e standard works as an extension to the 802.11 standard, and the Hybrid Coordination Function (HCF) is used for medium access control. HCF comprises the contention-based Enhanced Distributed Channel Access (EDCA) as an extension for DCF, and the centrally controlled Hybrid Coordinated Channel Access (HCCA) as a replacement for PCF.

EDCA has received most attention recently. The reason is that the Wi-Fi Alliance has already "standardized" a subset of the 802.11e standard, called Wi-Fi MultiMedia (WMM). EDCA is the major part of

ISSN 0085-7130 © Telenor ASA 2006

WMM, while HCCA is not included. Furthermore, WMM has been available off-the-shelf, and various Access Points and interface cards support EDCA through WMM.

Since this document focuses on what is possible to implement now or within the next year, EDCA is of primary interest here. However, although HCCA will not be discussed any further in this document, one should bear in mind that it will provide additional features that might prove valuable in the OBAN context as soon as these features are available in off-the-shelf products.

EDCA enhances DCF by allowing four different access categories (ACs) at each station and a transmission queue associated with each AC. Each AC at a station has a conceptual module responsible for channel access for each AC and in this paper the module is referred to as an Enhanced Distributed Channel Access Function (EDCAF). Hence each of the four transmission queues (and the associated ACs) on a station is represented by one backoff instance. The channel access between different backoff instances on a station is not completely independent due to the virtual collision handling between the queues on the station. If two or more backoff instances on the same station try to access the channel in the same timeslot, the station attempts to transmit the frame of the highest priority AC, while the lower priority frames will go through backoff.

The traffic class differentiation of EDCA is based on assigning different access parameters to different ACs. First and foremost, a high-priority AC, i, is assigned a minimum contention window, $W_{0,i}$, that is lower than (or at worst equal to) that of a lower-priority AC. At a highly loaded (or "saturated") medium, the post-backoff of the high-priority AC will normally be smaller than the post-backoff of a low-priority AC. This results in an average higher share of the channel capacity, because the high-priority AC will on average have to refrain from the channel for a shorter period of time than the low priority AC. Furthermore, each AC is assigned a maximum contention window, $W_{m,i}$, so that a higher priority AC has a lower or equal maximum contention window compared to an AC of a lower priority.

Another important differentiating parameter is the Arbitration Inter-Frame Space (AIFS) value, measured as a Short Interframe Space (SIFS) pluss an AIFSN number of timeslots. A high-priority AC is assigned an AIFSN that is lower than (or at worst equal to) the AIFSN of a lower-priority AC. The most important effect of the AIFSN setting is that the high-priority AC normally will be able to start earlier than a low priority AC to decrement the backoff counter after having been interrupted by a transmission on the channel. At a highly loaded channel where the decrementing of the backoff counter will be interrupted by packet transmissions a large number of times, the backoff countdown of the high-priority AC will occur at a higher average speed than that of the lower-priority AC. As the wireless medium gets more and more congested, the average number of empty timeslots between the frames transmitted by the higher-priority ACs might be lower than the AIFSN value of the low-priority AC. At this point, the AC will not be able to decrement its backoff counter, and all packets will finally be dropped instead of being transmitted. This is referred to as "starvation".

Finally, another differentiation parameter that may be adjusted in 802.11e is the Transmission Opportunity (TXOP)-limit of each AC, i. This means that an AC may hold the channel only for a time interval determined by the TXOP-limit.

Selecting a scenario with roaming users

Assumptions

There are three major assumptions behind the selected scenario:

1 The access is divided between devices of the home user (HU) and devices of visiting (Roaming) users (VU).

2 The home user wants a soft guarantee that its sessions are not undermined by a sudden peak usage by the visiting users.

3 There is an ongoing trend that home users deploy the "Residential Gateway", i.e. the Access Point, as a hub for a wireless infrastructure in the home. (Figure 1)

An example of a vendor applying the 802.11 technology for wireless infrastructure in the home is Philips "Streamium" products. A large number of products are already available (see Figure 2). Philips focuses mainly on using the wireless infrastructure for streaming of music, video (e.g. DVD), entertainment and gaming.

Bit rates and 802.11 physical layer

There are three possible 802.11 PHYs that are natural to explore:

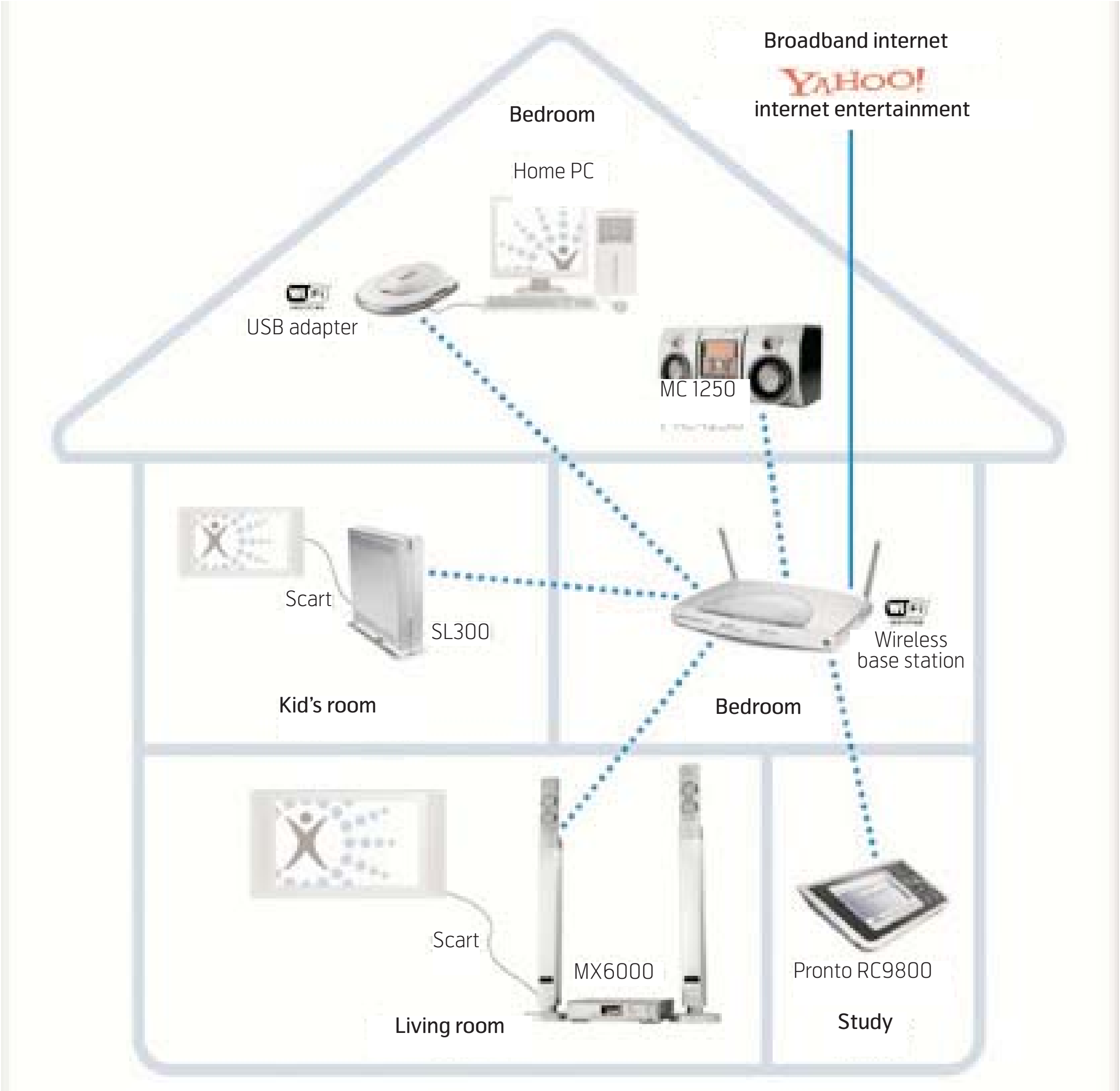
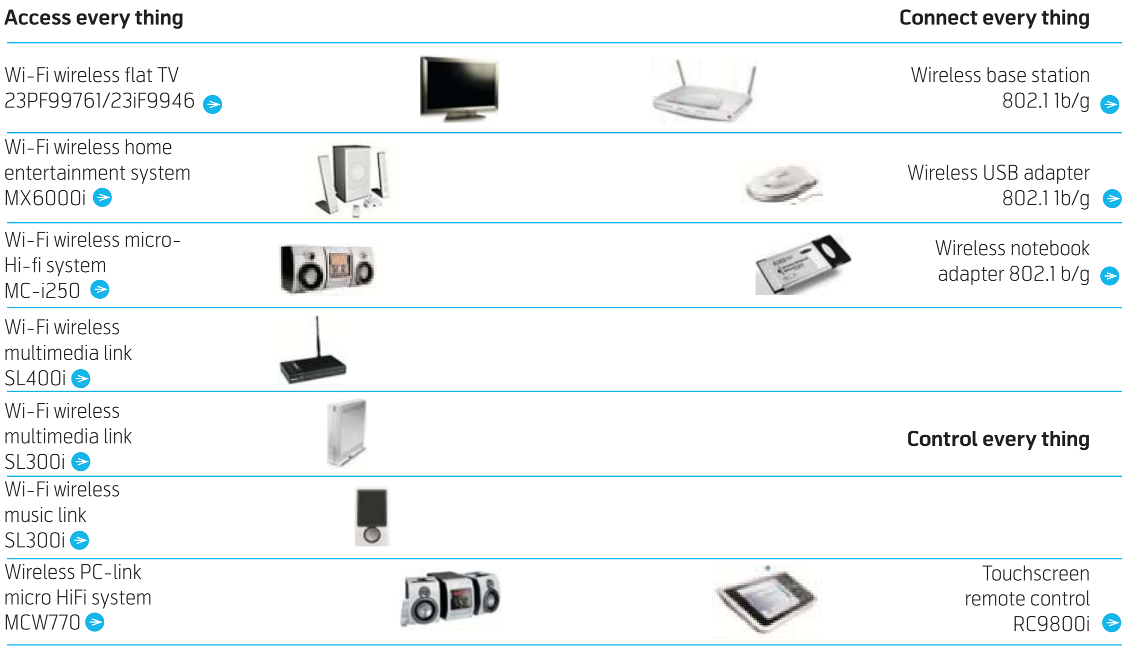


Figure 1 The Residential Gateway (i.e. Access Point) forms a hub for a wireless communication in the home



Access every thing	Connect every thing
Wi-Fi wireless flat TV 23PF99761/23iF9946	Wireless base station 802.1 1b/g
Wi-Fi wireless home entertainment system MX6000i	Wireless USB adapter 802.1 1b/g
Wi-Fi wireless micro- Hi-fi system MC-i250	Wireless notebook adapter 802.1 b/g
Wi-Fi wireless multimedia link SL400i	
Wi-Fi wireless multimedia link SL300i	**Control every thing**
Wi-Fi wireless music link SL300i	
Wireless PC-link micro HiFi system MCW770	Touchscreen remote control RC9800i

Figure 2 A large number of Streamium products are already available

1 802.11b:
- Max nominal rate: 11 Mb/s
- Are found in new and old products, i.e. most useful today

2 802.11g: Are found in all new products
- Max nominal rate: 54 Mb/s
- Are found in new and old products, i.e. most useful today.

Note that the nominal bandwidth does not give the total throughput. Typically, one will only get maximum 6 Mb/s (or most probably less) when using 802.11, despite the nominal bandwidth of 11 Mb/s.

In this document we use 802.11b as an example. The reason is that the 802.11b and its performances are well known. However, all the analyses in this document are applicable to 802.11g and 802.11n, simply by scaling up the generated traffic load as compared to the nominal bandwidth offered by the technology.

Unless explicitly stated otherwise, we assume that all stations have perfect radio conditions. The reason is that this document does not want to discuss details of radio effects or get into radio range discussions.

It should be noted that it is easy to find usage scenarios where the home user experiences the wireless medium as a bottleneck for communication, no matter which of the PHYs that are studied. It has been shown that 802.11g is a bottleneck for the widespread use of products like e.g. Streamium from Philips, and one would hope that 802.11n will provide sufficient bandwidth for a normal usage of such products.

A Basic Scenario

Let us assume that the father in the home is sitting in the living room watching a movie, where a DVD is streamed from a PC (PC1) in the house to the set-top box that is connected to the TV. The daughter is sitting in her room watching a music video that is located on her brother's PC (PC2). For simplicity we assume that the streaming is undertaken at a constant bit-rate. Figure 3 illustrates the example.

At the same time, there are a number of Visiting Users. To this end, we consider three different scenarios:

1 4 visiting users: This is probably the most common scenario.

2 10 visiting users: This can be a probable scenario, e.g. for a house located close to a bus station.

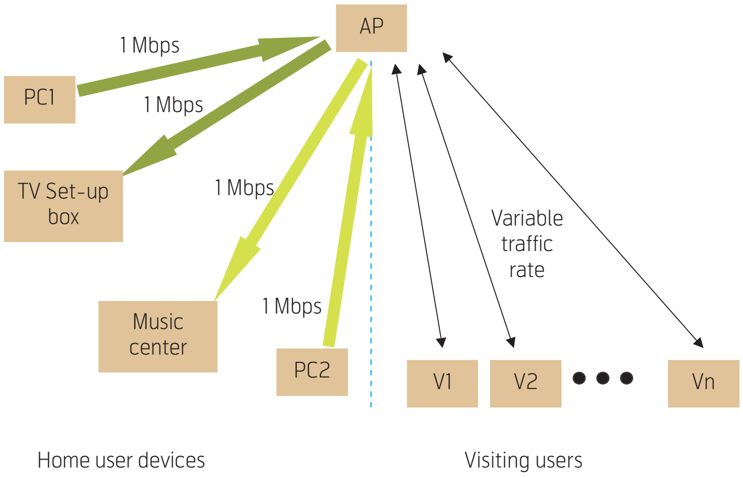


Figure 3 A basic scenario to exemplify possible benefits of using 802.11e

3 25 visiting user: This will be a typical "hotspot" scenario.

The visiting users are sending and reading e-mail, using an e-mail web-account (e.g. yahoo-mail or google-mail). They use best effort http communication at a variable traffic rate.

Potential Benefits of 802.11e

The Direct Link Protocol

Consider a scenario where two stations are associated with the same AP, for example the "TV Setup Box" and the "PC1" in Figure 3. With legacy 802.11, communication between the stations is always relayed via the AP, as illustrated in the figure.

However, 802.11e provides a feature called the Direct Link Protocol (DLP). With DLP, the two stations can use the AP to negotiate a direct link between them (Figure 4). When DLP has been used to set up the link, all subsequent data traffic between the two stations is sent directly between the two stations without having to be relayed via the AP (Figure 5).

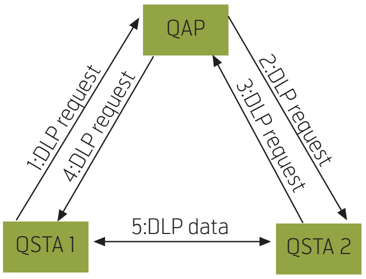


Figure 4 Using DLP to set up a direct link

ISSN 0085-7130 © Telenor ASA 2006

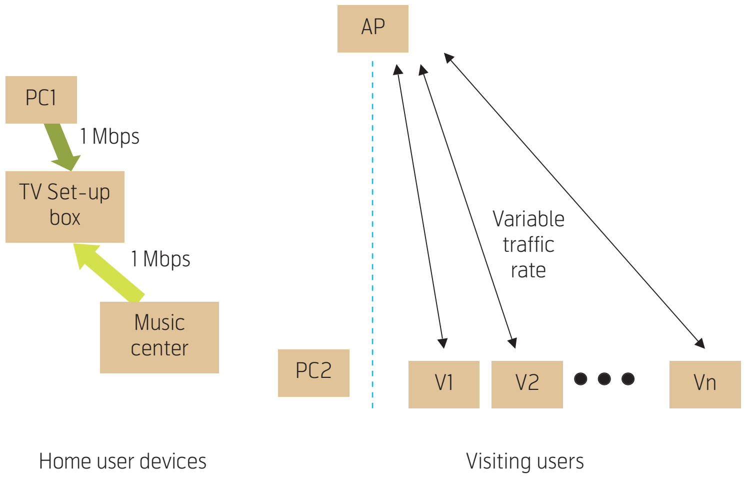


Figure 5 The benefit of using DLP of 802.11e

As seen from Figure 5, approximately only half of the channel capacity is required for the direct communication with DLP as compared to not using DLP.

This feature is particularly useful for the home user devices, because there will probably be communication between these devices. It is not very useful for the visiting users, because they will probably rarely communicate with other visiting users located at the same AP. (An exception is if two Visiting Users meet face-to-face and want to exchange some files, but this is not anticipated to be very common.) The benefits of DLP for the visiting users will therefore be neglected here.

Without 802.11e

Let us assume that 802.11 gives approximately 6 Mb/s user traffic. Without DLP, the home user spends approximately 4 Mb/s of the channel bandwidth, leaving only 2 Mb/s for the visiting users and *only 200 kb/s per visiting users* in the scenario with 10 visiting users per AP.

With 802.11e

If DLP is being used, the home user device needs only 2 Mb/s and leaves 4 Mb/s to be used by the visiting users. This gives *400 kb/s per visiting user* in this example.

EDCA differentiation between Access Categories

Another feature of 802.11e is that EDCA provides differentiation between different traffic classes. This means that it is possible to set access parameters of the AC in such a way that one AC is protected against an excessive traffic rate of the other AC. The benefit of this protection is that admission control will not often be required to implement such protection, and the lower priority AC can maximize the channel use without having to care about not stealing capacity from the higher priority AC.

In order to exemplify this, we will use the analytical model for 802.11e EDCA, which we have developed in the OBAN project. Another option would be to use simulations. However, we have demonstrated through a number of presentations that the analytical model is fairly accurate, and minor inaccuracies will not have impact on the main conclusions.

In order to study the basic scenario, we make some simplifying assumptions. We assume that there are four home user devices, each sending traffic at a constant bit rate of 1 Mb/s. At the same time, we assume that there are four visiting users, sending at a variable bit rate.

Figure 6 shows this scenario, where the total throughput of the home user and the visiting users is plotted as a function of the traffic rate generated by the visiting users. It is observed that the throughput of the home user is being gradually reduced as the throughput of the visiting users is increasing. Hence, without

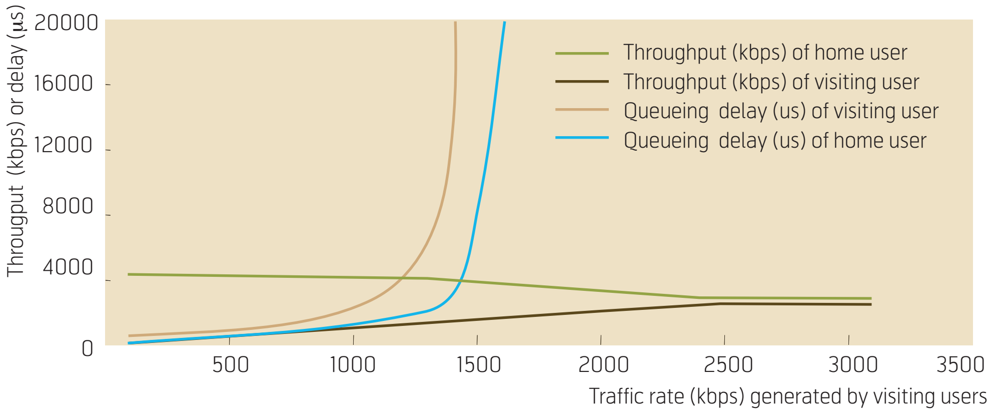


Figure 6 Total throughput and queueing delay of the home user and the visiting user is plotted as a function of the traffic rate generated by the visiting users

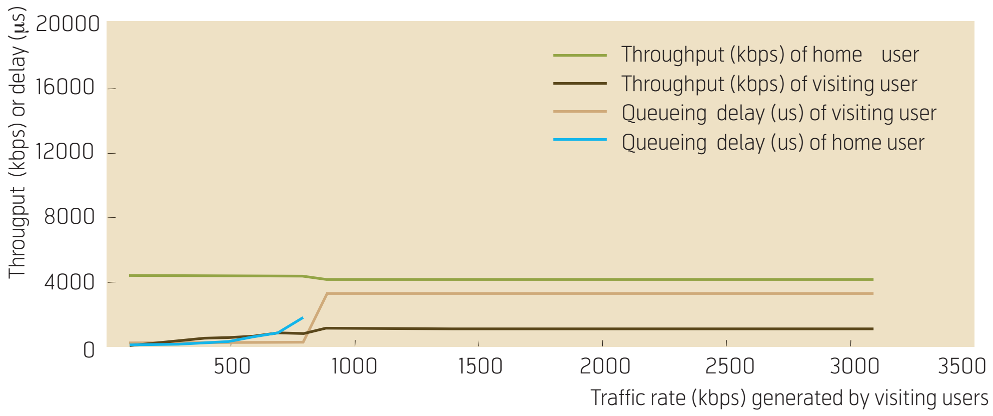


Figure 7 Example with 802.11e

802.11e there is no protection between the home and visiting users.

Figure 6 also shows the queuing delay of the home user's traffic and the queueing delay of the visiting users' traffic. It is observed that the queueing delay of the home user's traffic goes to infinity before the queueing delay of the visiting users' traffic. That means that it is the home user's communication that will primarily suffer when the traffic rate of the visiting user increases. When the visiting users send at a traffic rate of 1600 kb/s, for example, the queueing delay of the visiting users' traffic will be around 18 ms, while the queueing delay of the home user's traffic will be infinite. This means that the visiting users will be able to communicate without problems, while the traffic generated by the home user will be stacked on transmission queues or dropped due to buffer overflow.

To avoid a too high level of jitter, it is probably wise to restrict the visiting user's traffic to approximately 1300 kb/s. In this case, the home user is guaranteed the required bandwidth at a controllable level of jitter.

Figure 7, on the other hand, shows the same scenario but with the EDCA being used to differentiate between the home user's and the visiting users' traffic. Here the home user uses the default parameter settings of 802.11e for AC_VO (priority voice / real time) traffic, while the visiting users use the default parameter settings for AC_BE (best effort) traffic. It is observed that the throughput of the home user does not decrease considerably (except for some minor inaccuracies of the model) when the traffic of the visiting users is increasing. The traffic of the visiting user increases up to a certain point where it will not get any more traffic. Hence, the traffic differentiation mechanism of 802.11e can provide protection between the home user's and visiting users' traffic.

Figure 7 also shows the queuing delay of the home user's traffic and the queueing delay of the visiting user's traffic. Here it is observed that the queueing delay of the visiting user's traffic goes to infinity before the queueing delay of the home user traffic. That means that it is the visiting users' communication that will primarily suffer when the traffic rate of the visiting users increases. When the visiting users send at a traffic rate of 900 kb/s, for example, the queueing delay of the visiting users' traffic will be infinite, while the home user will be able to communicate without problems with a queueing delay of less than 4 ms.

The advantage in this example is that the visiting users can communicate as much as they want without having to consider the communication of the other nodes. The visiting users' traffic will not even result in any considerable jitter for the home user, since the maximum queueing delay that the visiting users can cause to the traffic of the home user is less than 4 ms. Since the visiting users will be using TCP for communication, TCP will sense the queueing delay and reduce the traffic when the bandwidth roof is hit. Hence, the visiting user can communicate freely and let TCP handle the bandwidth constraints.

Without 802.11e

If 802.11e is not being used, some kind of admission control is needed. The visiting users must share a bandwidth of 1300 kb/s, *leaving each of the four visiting users with only 325 kb/s*.

With 802.11e

If 802.11e is being used, *each visiting user can normally spend all available 900 kb/s*. With the packet bursting of typical http traffic, the visiting users will seldom experience a situation where many stations access the channel at the same time. Thus, most often the visiting user will have all the 900 kb/s available for its own use. On some occasions, two of the visiting users will retrieve and send an e-mail at exactly the same time, and will each receive a bandwidth of only 450 kb/s. And so forth.

Needless to say, if there are more than four visiting users the benefits of 802.11e will be bigger, because of the inefficiency of static bandwidth sharing per station of the OBAN admission control procedure when 802.11e is not used.

Using TXOP limits for fair utilization of the channel

A very OBAN-relevant feature of 802.11 is that the wireless channel is accessed on a per-packet basis, and each station holds the channel until the packet is sent, independent of the length of the packet.

An important problem with this feature in this context is that the visiting users are often outside the house at the border of the coverage area of the access point and with degraded radio conditions. Often the interface may adapt and send traffic at a more robust modulation, e.g. sending the data traffic at 1 Mb/s instead of at 11 Mb/s. The result is that a 1024 byte packet sent at 1 Mb/s will take almost seven times as much time on the channel asa packet sent at 11 Mb/s.

The following shows that channel time consumed by a 1024-byte packet sent at different maximum nominal rates:

- 11.0 Mb/s: 1.321 ms
- 5.5 Mb/s: 2.065 ms
- 2.0 Mb/s: 4.672 ms
- 1.0 Mb/s: 8.768 ms

A big question is – is this fair? Is this a reasonable way of utilizing the channel resources? How to protect the home user from the inefficient bandwidth utilization of the visiting users? A key point is that the visiting users will not only receive low bandwidth. In receiving this bandwidth it is anticipated that they will at the same time consume an unreasonable amount of the bandwidth of the home user. Let us explore this in detail and show that this intuitive fact is correct.

The curves for the given visitor rate of 11 Mb/s in Figure 8 are the same as the ones shown in Figure 6; i.e. in the scenario where 802.11e is not used. In this scenario it was assumed that both the home user's devices and the visiting users' devices had perfect radio conditions and could all communicate at a maximum nominal radio rate of 11 Mb/s.

We now assume, however, that the visiting users have bad radio conditions and can only communicate at 1 Mb/s. This situation is illustrated by the brown and blue curves in Figure 8.

Figure 8 shows that the visiting user obtains a theoretical maximum throughput of only 46 kb/s, i.e. 12.5 kb/s per visiting user, since the nominal bit rate is reduced to only 1 Mb/s. (This is also illustrated in Figure 9.) In doing so, the visiting users consume a big share of the channel bandwidth so that the theoretical maximum throughput of the home user is reduced to less than 2 Mb/s (Figure 8).

Figure 9 shows how the visiting users' throughput changes at a smaller scale. It is seen that the throughput evolves more or less along the input = output line. That means that most of the traffic gets through and is not stacked on queues. In Figure 8, on the contrary, we observe that the home user, on the contrary, reduces its throughput almost immediately. Since only a small fraction of the traffic are dropped due to exceeded retry counters, most of the traffic that are not sent here, are stacked on queues. It is seen that the queueing delay occurs at a very low throughput value of the visiting users.

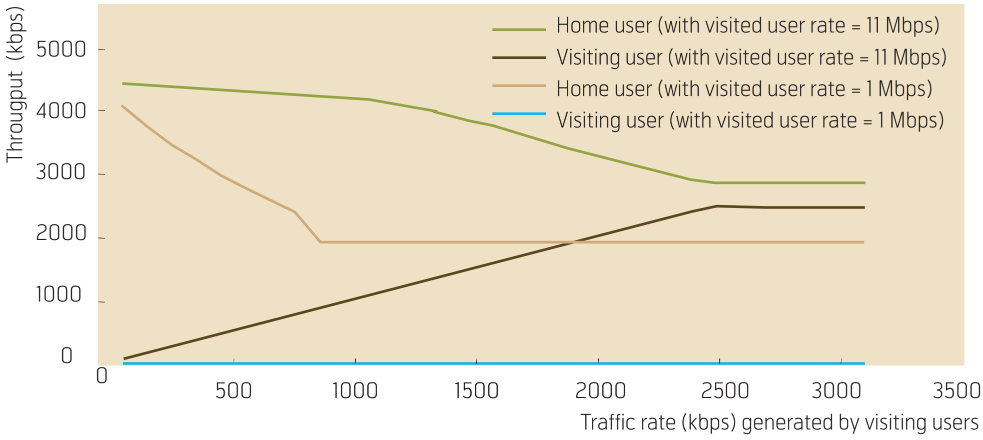


Figure 8 Effect of the lack of the TXOP limit when the Visiting users communicate at 1 Mb/s (without 802.11e)

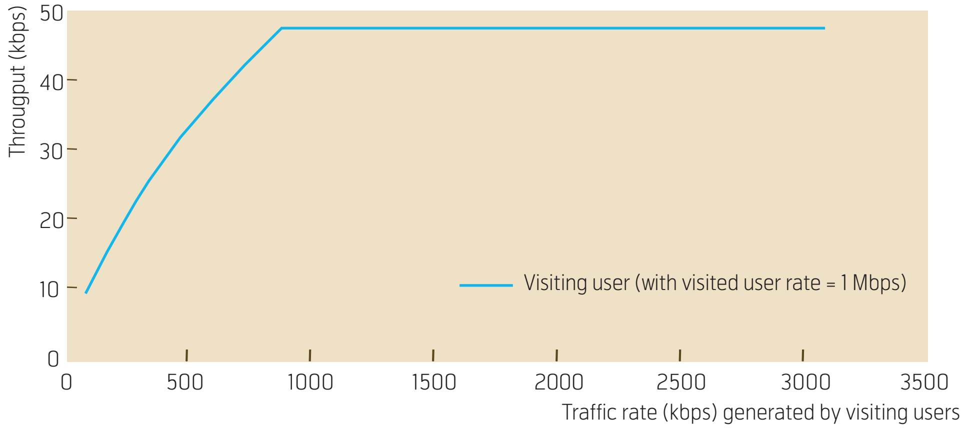


Figure 9 The throughput of the visiting users shown at a smaller scale (same data as in Figure 8)

Hence, another and considerably more alarming consequence of this effect is that the queueing delay of the home user will reach the upper limit very soon as the visiting users start to send a few kilobits per second. In other words, the visiting users will easily destroy the possibility for the home user to communicate, as soon as the visiting users start communication.

Let us also compare the effects of the lack of TXOP limit when 802.11e is used. The curves for the case of visiting users given 11 Mb/s in Figure 10 are the same as the ones shown in Figure 7; i.e. in the scenario where 802.11e is used. In this scenario it was assumed that both the home user's devices and the visiting users' devices had perfect radio conditions and could all communicate at a maximum nominal radio rate of 11 Mb/s. Two upper curves in Figure 8 (showing the throughput for home users with visited user-rate of either 1 or 11 Mb/s), on the contrary, illustrate a situation where the vsiting users have bad radio conditions and can only communicate at 1 Mb/s. Indeed, Figure 10 shows that the problem is the same also with 802.11e differentiation.

It should be noted that our analytical model needs to be adopted to study the queueing delay with different nominal bit rates when TXOP limits are not used. Our experience is that development of the model requires considerable resources.

The TXOP-limit feature of 802.11e provides a solution to the problem presented until this point in this subsection, as shown in Figure 8 – Figure 10. Let us now explain the feature and then explore the potential benefits of this feature.

802.11 states that an EDCAF cannot hold the channel more than the channel time given by the TXOP limit. Assume that the TXOP limit is set to 1.5 ms, which is a reasonable setting in 802.11e. The result is that the home user will be able to send all its packets as before, because each packet (with a duration of 1.3 ms) is below the TXOP limit.

The visiting users, on the contrary, will need a number of TXOPs in order to get the 1024 byte packet sent. In fact, at 1 Mb/s, the visiting users are able to

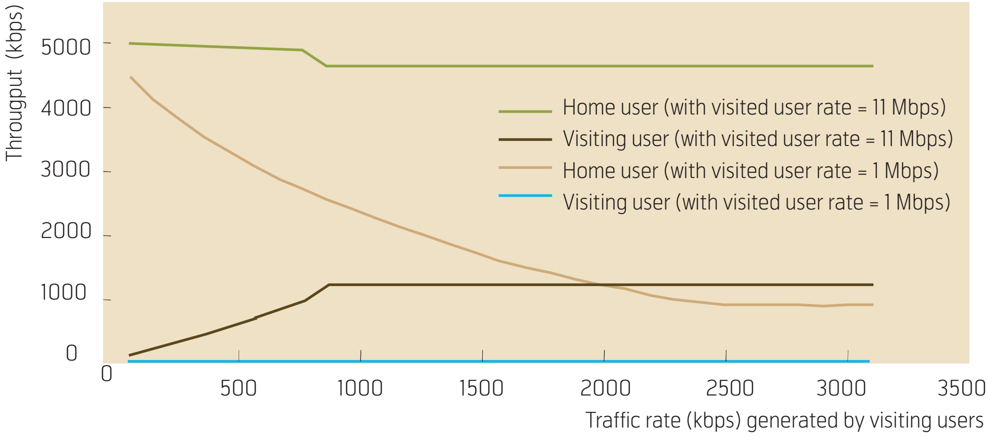


Figure 10 Effect of the lack of the TXOP limit when the visiting users communicate at 1 Mb/s (with 802.11e differentiation)

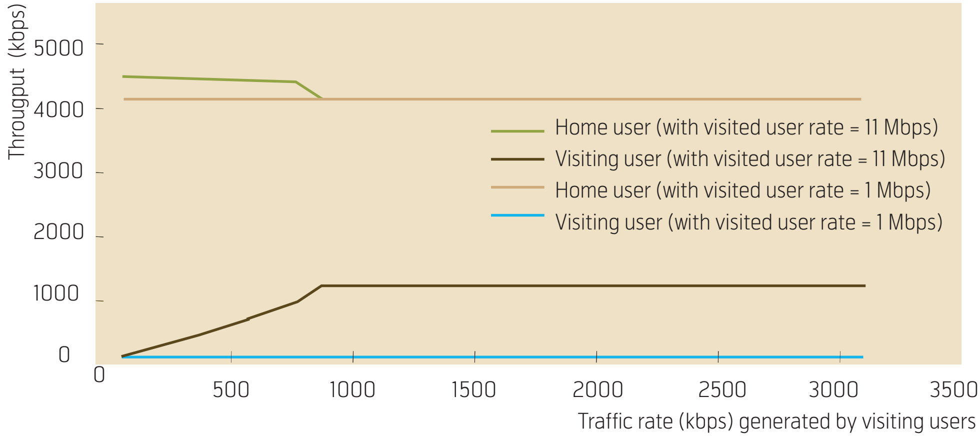


Figure 11 Effect of using TXOP limit when the visiting users communicate at 1 Mb/s (with 802.11e differentiation)

send approximately 115 bytes of data within the time limit of 1.5 ms. This means that the visiting user need to fragment each packet into nine fragments that are sent independently in separate TXOPs. Since 802.11 channel access works on a per-packet basis, it is now mostly the visiting users that will suffer, while the home user will not experience any major changes. However, the home user will notice that the traffic intensity – in terms of number of packets sent by the visiting users – increases, since the number of packet fragments sent on the channel increases.

Figure 11 shows the effect of using TXOP limits of 802.11e, when 802.11e differentiation is used. It is observed that the use of the TXOP limit fully protects the traffic of the home user. The fact that the visiting users are located far away from the AP with poor radio conditions puts the burden on these visiting users. Thus, it is no more a situation of the visiting users being able to obtain a few kb/s more bandwidth at a tremendous cost of the home user's bandwidth.

Figure 11 shows that the visiting users hits the capacity limitation before they try to transmit more than 100 kb/s. In order to study what really happens at traffic rates below 100 kb/s, we need to see Figure 11 on a smaller scale. This is shown in Figure 12.

Figure 12 shows that the home user is more or less unaffected by the fact that the visiting users are communicating at 1 Mb/s. It also shows that the queueing delay of the visiting user goes to infinity at a traffic rate of approximately 98 kb/s. Figure 12 reveals a remarkable result compared to Figure 8; it shows that the TXOP feature provides the visiting users with at least twice the available bandwidth without destroying for the home user. In Figure 8, on the contrary, we saw that the visiting users got less than 46 kb/s at a tremendous expense of the home user's ability to communicate.

Similar to our previous summaries, we may conclude this subsection with the following:

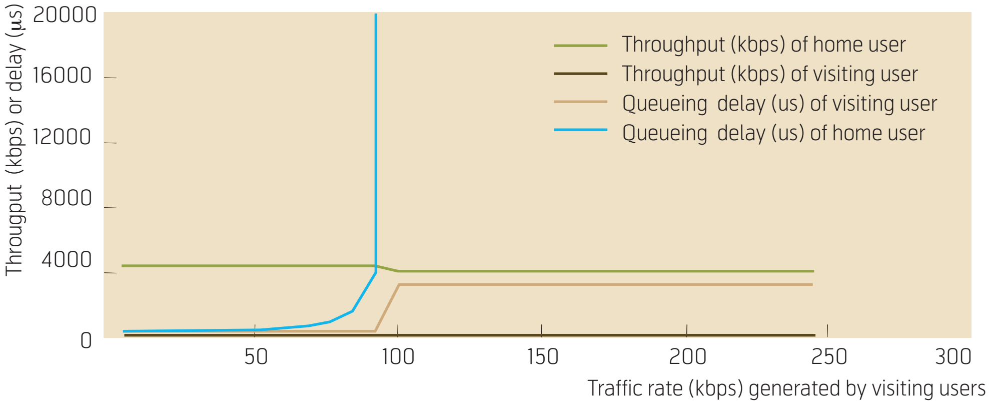


Figure 12 Effect of using TXOP limit when the visiting users communicate at 1 Mb/s (with 802.11e differentiation) seen on a small scale

Without 802.11e without TXOP_limits

If 802.11e is not being used, some kind of admission control is needed. The visiting users must share a bandwidth of 46 kb/s, *leaving each of the four visiting users with only 12.5 kb/s*. The home user gets very little through, typically *in the order of 100 kb/s or so*. [In order to estimate the limit for the home user, we need to enhance the analytical model, so that the queueing delay can be found.]

With 802.11e and TXOP-limits

If 802.11e is being used, each *visiting user can normally spend all the available 98 kb/s*. With the packet bursting of typical http traffic, the visiting users will seldom experience a situation where many stations access the channel at the same time. Thus, most often the visiting user will have all the 98 kb/s available to their own use. On some occasions, two of the visiting users will retrieve and send an e-mail at exactly the same time, and will each receive a bandwidth of only 46 kb/s. And so forth. On the other hand, *the home user can continue to spend approximately 4 Mb/s*, because the TXOP-limits protect it from the fact that the visiting users are communicating at 1 Mb/s nominal bit rate.

Downlink Fairness

802.11 works on a per-station (or per-EDCAF) basis. Thus, the downlink traffic will easily be subject to unfair treatment compared to uplink traffic.

Work is going on within the framework of EDCA and we hope to explore the benefits of 802.11e for such fairness, as it will indirectly influence on the capacity benefits that 802.11e will provide compared to a solution based only on legacy 802.11.

Other Potential Benefits

802.11e Admission Control

802.11e provides a feature for dynamic admission control at the link layer. This gives much closer operation with the actual link layer and thus offers an opportunity for more efficient exploitation of the radio resources.

HCCA

HCCA provides an additional channel access mechanism. We believe that HCCA will be particularly important in the downlink scenario, because 802.11 works on a per-station (or per EDCAF) basis. Thus, the downlink traffic will easily be subject to unfair treatment compared to uplink traffic. This can be solved within the framework of EDCA, however; HCCA provides an additional mechanism that might prove to be very useful.

Conclusions

It is shown that the following features of 802.11e might be of particular importance in an access network allowing for roaming users:

- Direct Link Protocol
- EDCA differentiation between Access Categories
- TXOP-limits

A scenario was presented as a starting point for the analysis, and the quantitative benefits of the various 802.11e features have been presented based on the scenario.

For simplicity, we have used 802.11b as the physical layer technology for our scenario, because the technology and its capabilities are well known in terms of for example bandwidth capacity. It is however straightforward to scale up the analysis to a scenario for a situation using the 802.11g PHY or the 802.11n PHY. In fact, we have already used very conservative throughput values so that the analysis should be more applicable to higher capacity PHYs. For example, for the streaming traffic of the home user, we have assumed a traffic rate of only 1 Mb/s. However, DVD, for example, typically runs at a traffic rate of 4–9 Mb/s. Thus, a simple upscale of our analysis would require a PHY that lies in the borderline between 802.11g and 802.11n. It is not the scope of this document to get into a detailed discussion about what are realistic traffic rates of the scenarios.

References

1 *Open Broadband Access Network (OBAN)* website. 13 June 2006 [online] – URL: http://www.ist-oban.org/

2 Panken, F et al. Arcitecture for sharing residential access with roaming WLAN users. *Telektronikk*, 102 (3/4), 48–59, 2006 (This issue)

3 Engelstad, P E, Østerbø, O N. An Analytical Model of the Virtual Collision Handler of 802.11e. *Proceedings of the Eighth ACM International Symposium on Modeling, Analysis & Simulation of Wireless and Mobile Systems (ACM MSWiM 2005)*, Montreal, Canada, 10–13 Oct 2005.

4 Engelstad, P E, Østerbø, O N. Non-Saturation and Saturation Analysis of IEEE 802.11e EDCA with Starvation Prediction. *Proceedings of the Eighth ACM International Symposium on Modeling, Analysis & Simulation of Wireless and Mobile Systems (ACM MSWiM 2005)*, Montreal, Canada, 10–13 Oct 2005.

5 Engelstad, P E, Østerbø, O N. Differentiation of Downlink 802.11e EDCA Traffic in the Virtual Collision Handler. *Proceedings of the 30th Annual IEEE Conf. on Local Computer Networks (LNC '05)*, Sydney, Australia, 15–17 Nov 2005.

6 Engelstad, P E, Østerbø, O N. Delay and Throughput Analysis of IEEE 802.11e EDCA with AIFS Differentiation under Varying Traffic Loads. *Proceedings of the 30th Annual IEEE Conf. on Local Computer Networks (LNC '05)*, Sydney, Australia, 15–17 Nov 2005.

7 Engelstad, P E, Østerbø, O N. Queueing Delay Analysis of 802.11e EDCA. *Proceedings of The Third Annual Conference on Wireless On demand Network Systems and Services (WONS 2006)*, Les Menuires, France, 18–20 Jan 2006.

8 Engelstad, P E, Østerbø, O N. The Delay Distribution of IEEE 802.11e EDCA. *Proceedings of the 25th IEEE International Performance Computing and Communications Conference (IPCCC'06)*, Phoenix, Arizona, 10–12 April 2006. (See also: www.unik.no/~paalee/PhD.htm)

9 Engelstad, P E, Østerbø, O N. Analysis of the Total Delay of IEEE 802.11e EDCA. *Proceedings of IEEE International Conference on Communication (ICC'2006)*, Istanbul, 11–15 June 2006. (See also: www.unik.no/~paalee/research.htm.)

For a presentation of Paal E. Engelstad, please turn to page 59.

Olav N. Østerbø received his MSc in Applied Mathematics from the University of Bergen 1980 and his PhD from the Norwegian University of Science and Technology in 2004. He joined Telenor R&D in 1980. His main interests include teletraffic modelling and performance analysis of various aspects of telecom networks. Activities in recent years have been related to dimensioning and performance analysis of IP networks, where the main focus is on modelling and control of different parts of next generation IP-based networks.

email: olav-norvald.osterbo@telenor.com

Security in Fast Handovers

MARTIN GILJE JAATUN, INGER ANNE TØNDEL, TOR HJALMAR JOHANNESSEN

Martin Gilje Jaatun is Research Scientist at SINTEF ICT

If an open access network is to support on-going real time services like voice, disruptions must be kept to a minimum. This can be a challenge to achieve with Wi-Fi access points, since Wi-Fi standards do not support handovers to the same extent as for instance 3G standards. Most of the delay time comes from re-authentication. Re-authentication cannot however be omitted since it, among other things, yields the baseline for accounting. Several techniques can be used to minimize the experienced disruption delays for a mobile user in handover situations. One option is to allow mobile users free access to network services only for a limited amount of time while the authentication functions are accomplished in the background (delayed authentication). Another option is to improve current security standards when it comes to speed. Still another option is to find ways to authenticate in advance. In this document we focus on two different solutions for reducing re-authentication delay; namely *delayed authentication* and *Kerberos-style tickets*.

Inger Anne Tøndel is Research Scientist at SINTEF ICT

Tor Hjalmar Johannessen is Research Scientist at Telenor R&D

1 Introduction

In an Open Broadband Access Network (OBAN), anyone with a broadband connection can offer Internet access to passers-by. Individuals and companies can make money on their Internet connection, while neighbours and people on the move get access to a high quality access network. Systems that offer such functionality are available today with different names; from traditional hotspots via the Boingo network [12] to the Linspot [13] and FON [14] concepts. The services offered are however simple, with limited support for mobility, Quality of Service (QoS) and security.

The OBAN project [19] takes the idea of sharing broadband connections several steps further. The OBAN architecture [20] offers defined QoS mechanisms for both visiting and residential users. When using OBAN, seamless handovers is a main requirement, and so is security. Users of OBAN should be able to roam while using real time services. At the same time security requirements of both users and operators should be met also during handover. Authentication is one of the basic security services that must be ensured. Operators are concerned with AAA services (Authentication Authorization Accounting) to ensure correct billing, while users need to feel confident that nobody can use their identity with the result that they have to pay for other users' service consumption.

In an OBAN setting, fast handovers between different wireless access points will in many cases also include handovers between different Internet Service Providers (ISPs), since there should be no monopoly on access point operation. Authentication can therefore involve many actors, something that limits the chances of fulfilling the requirement of seamless handovers. In this article the focus is on how to achieve fast authentication in an OBAN setting with many operators, to facilitate fast handovers.

Since OBAN's basic idea is to exploit the growth and increasing density of mobile access facilities like wireless access points, Wi-Fi technologies is the main focus; but the OBAN scope also covers other technologies like 3G and WiMAX among other things, in order to increase coverage. The range of Wi-Fi access points is much less than the size of 2G, 3G and WiMAX cells. Handover speed is therefore of higher importance in Wi-Fi networks, since handovers will happen more frequently. Fast handovers between Wi-Fi access points will therefore be given most attention in this article.

The article starts with an introduction to handovers in OBAN. In this introduction the different players involved are described, together with the handover authentication solutions in the underlying access technologies. Then different possibilities for speeding up authentication are described with a focus on two main alternatives; delayed authentication and pre-authentication using Kerberos-style tickets. Finally, we explain why the Kerberos-style ticket solution has been chosen for OBAN.

2 Handovers in OBAN

OBAN handover aims to fulfil security and QoS requirements in a multi-domain environment covering hybrid access technologies.

2.1 Requirements

OBAN aims at seamless handovers to be able to support real time services. For voice conversations, ITU-T considers delays of more than 150 ms to be unsatis-

ISSN 0085-7130 © Telenor ASA 2006

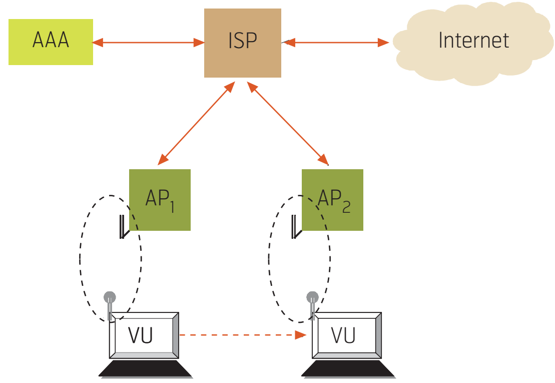


Figure 1 Handover within a single domain

factory [15]. Repeated disruptions during a voice conversation are also considered very annoying. Hence, the OBAN project has considered that at most 120 ms disruption if a real-time service like full duplex voice shall be offered. This formulates the limit for the fast handover working target.

Reaching the goal of maximum 120 ms handover delay should not result in insufficient security for any OBAN player. The overall security requirements for OBAN are stated in [7]. These requirements should be met also in the case of fast handovers. This means for instance that satisfactory authentication shall be achieved, and requirements regarding anonymity and encryption shall be met.

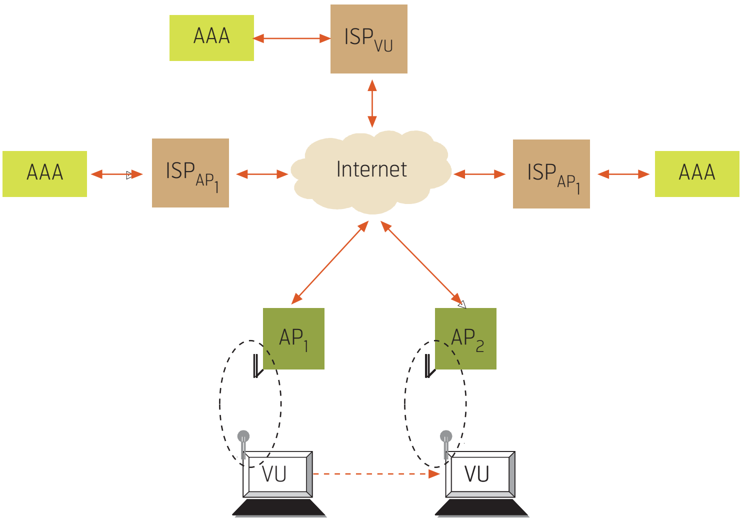


Figure 2 Multiple domain handover

2.2 Multi-domain aspects

An OBAN involves many players, and possibly several operators and business domains. Still, to understand the main ideas it often helps to look at a simplified model of a system; for us this means an OBAN with only one operator, as shown in Figure 1. In many ways, the heart of OBAN is the equipment placed in the individual homes. In this figure this equipment is named access points because the Wi-Fi access point is a main part of this equipment, but it is also a gateway (in OBAN called Residential Gateway (RGW)) that handles the connection to the outside world. In Figure 1 a visiting user (VU) is currently using Access Point 1 (AP1) but is moving towards Access Point 2 (AP2). A handover should thus be performed from AP1 to AP2. In this simplified figure both access points are served by the same Internet Service Provider (ISP). This is also the ISP of which the VU is an OBAN customer (ISP_{VU}). The VU is therefore already authenticated towards this ISP and a full authentication may therefore not be necessary. This ISP is also in a position to know which access points are present in a given area, something that makes it easier to predict what access points are candidates for handover at an earlier point in time, and prepare for the handover if this is desired.

Figure 2 shows a more complicated and probably more realistic OBAN environment with more players involved. The VU is still moving from AP1 to AP2, but this time the two access points are served by different ISPs. A VU that has been authenticated via the ISP of AP1 will not be known to the ISP of AP2 before a handover takes place. In the figure the ISP of which the VU is a customer (the ISP_{VU}) is also not the same as any of the ISPs of the access points. To authenticate a Visiting User, an ISP_{VU} and an ISP, together with an access point and the VU himself need to be involved. It is also harder to predict which access points are candidates for the next handover, since no entity has an overview of all access points within a given area. In this solution where preparations for handover may be more important, to compensate for all the actors that need to be involved in authentication, this is therefore also harder to accomplish.

The complexity, especially when it comes to all the involved ISPs motivates the introduction of an entity that can create order in this chaos of players, as shown in Figure 3. The Mobility Broker (MB) is in charge of keeping an overview of its geographical zone; i.e. to have necessary information on all access points in this zone. The MB needs to have a relationship with all relevant ISPs. Thus the MB eases the contact between ISPs and access points and can be used to facilitate handovers within a geographical zone. Handovers between geographical zones will involve two MBs, as shown in Figure 4, and will therefore be more time-consuming. Such handovers will however be infrequent.

2.3 Handover in the different access technologies

In OBAN, handover may not only involve several players and business domains, but also several technologies like Wi-Fi, 3G and WiMAX. These technologies do not necessarily have the same support for handovers, as will be described in the following.

2.3.1 WLAN

Within WLAN technologies, terminals must themselves discover that a handover is necessary, and perform a shift to the new access point. The network offers no help. This means that the terminal must undergo a full re-authentication process, something that will be time consuming; normally it includes a full round-trip RADIUS [17] protocol with the VU's ISP via the MB and the ISP of the access point before the IEEE 802.1X [16] port control grants access to continue the session. Taking this into account, it will be difficult to achieve the OBAN design target of maximum 120 ms handover delay. The problem of meeting the handover delay requirements is serious since handover between Wi-Fi access points is believed to be frequent. As shown in Figure 5, the range of an access point is limited, and VUs do not have to move at a high speed to experience a high number of handovers.

Since the terminals themselves are in charge of handover, one could think of a speed-up solution where the terminals are connected simultaneously to neighboring access points. VUs could then finish authentication at the new access point before disconnecting from the old access point. Current standards for wireless networks do not however allow for simultaneous connections to several access points. This means one less option to reduce the handover delay.

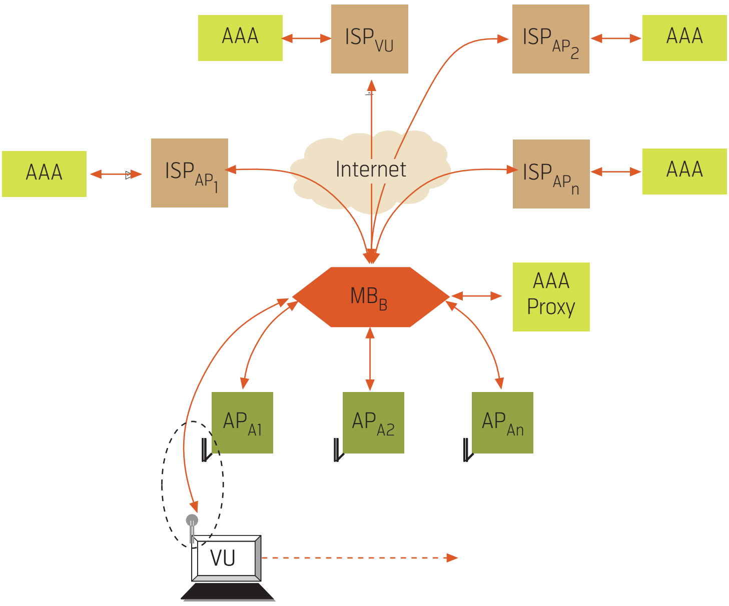


Figure 3 Mobility Broker: Regional grouping of access points

2.3.2 2G (GSM – GPRS) and 3G (UMTS)

Within 2G and 3G technologies, handover is an important feature, and effective handovers are an integral part of the design. The first logon to an access operator can be rather time-consum-

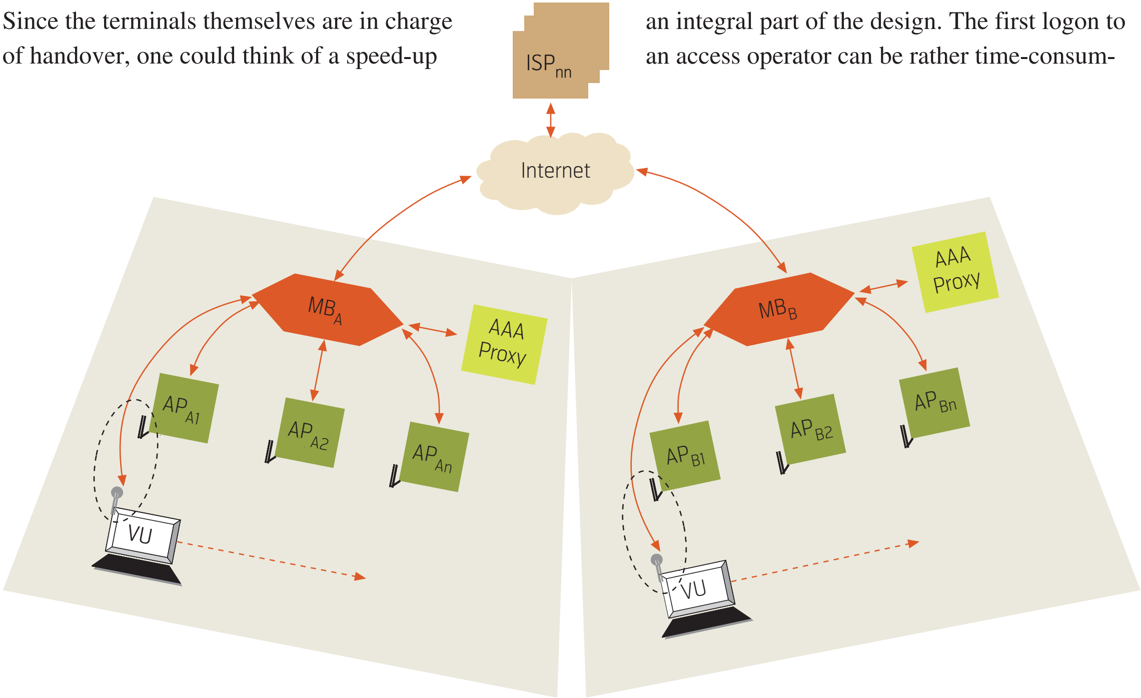


Figure 4 OBAN network with multiple Mobility Brokers

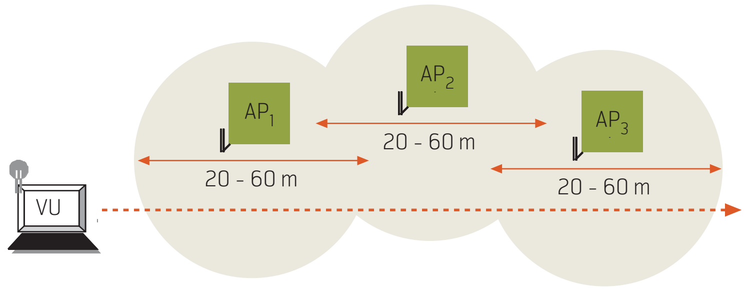


Figure 5 Scenario with typical density and ranges of Wi-Fi access points

ing, involving the Home Location Register of the mobile user, but later handovers between access points belonging to the same operator are handled locally and seamless. This will be the case for nearly all handovers, since handovers between different operators will be very infrequent, typically only when moving to a new country.

In 2G and 3G networks, the network itself initiates handover and is in control of the whole process. This also means that necessary session and authentication information is distributed to the new base station prior to handover. The handover itself is therefore well prepared and can be executed in a very short time, resulting in limited handover delay.

The cell sizes for 2G networks can vary from some hundred metres (in urban areas) to several kilometres (rural). Large cell sizes implies less frequent handover, and thus less experienced annoyance if temporary disruptions should take place in such cases.

2.3.3 WiMAX

WiMAX is defined in the IEEE 802.16 [18] standard published in 2002. Since then several amendments have been made, the latest being IEEE 802.16e which defines additional mechanisms to support mobile subscribers. The description of WiMAX handover below is based on [9] and [10].

WiMAX handovers take place as a cooperative effort between terminals and the network. Both terminals (Mobile Service Stations (MSS) in WiMAX) and WiMAX base stations can initiate handovers. A WiMAX handover consists of two phases; pre-registration and the real handover. During pre-registration, the serving base station and the neighbour base station(s) exchange handover information of the MSS and negotiates handover capability. One target base station is selected, and a handover response message is sent to the MSS trying to hand over. Then the real handover takes place. The MSS releases the connection with its serving base station and makes a new connection with the target base station, involving a network re-entry process.

Handovers in WiMAX are hard, meaning it is a break-before-make handover. This may cause disruption at a level not tolerable for real-time traffic. The disruption delay should however be less than what is the case for Wi-Fi networks because of the pre-registration phase. Regarding authentication, the target base station could get the necessary security information of the MSS from the serving base station by the backbone network, resulting in the possibility of skipping re-authorisation and re-registration during network re-entry. This will reduce handover delay.

Hard handovers are the basic handover solution in IEEE 802.16e, but IEEE P802.16e/D4 [21] also adopts soft handover solutions where the MSS is registered to several base stations at the same time.

2.4 Hybrid Network Handover Considerations

The above discussions of the different access technologies have shown that the WLAN technology is likely to be the main challenge when it comes to realising fast handovers. Up till now we have however only discussed handovers within one technology, not handovers between technologies, e.g. handovers between a Wi-Fi access point and a UMTS base station.

We will not discuss details of hybrid network handovers – this topic would require a whole article by itself – but rather discuss one of the important characteristics of such handovers.

For Wi-Fi handovers as described above, there are restrictions regarding the number of simultaneous connections to access points. For handovers between heterogeneous networks such restrictions do not apply. VUs can negotiate with new access points or base stations before leaving the previous one and hence speed up handover by performing authentication in advance. This means that although interoperability between technologies certainly is a challenge, fast handovers seem to be obtainable in such situations.

3 Possible Speed-up Solutions

As described above, speeding up handover between WLAN access points is the main challenge that needs to be solved to be able to reach the goal of seamless handovers in OBAN. Reducing the time needed for authentication will be a major contribution for reaching this goal, and authentication is the main focus when we consider speed-up solutions in this article. Different approaches can be taken to reduce authentication delays. In this section the main approaches are outlined before the following sections describe two alternative solutions in more detail.

3.1 Improve Current Standards

The common way of performing authentication with today's solutions is to use RADIUS or DIAMETER together with an EAP protocol. With such an approach multiple round trips between several servers, potentially situated physically far from each other are needed. This results in unacceptably long communication delays.

The protocols mentioned above are not created with fast handovers in mind, and there may be a lot to gain from improving these protocols when it comes to delay. The number of messages or the amount of involved servers may be reduced, resulting in better performance. Changing a standard, though, is a time-consuming process. The amount of delay that needs to be removed is also so big that it is unlikely that fine-tuning the standard solution wills reduce delay sufficiently.

Some work has already been done on fast handovers in the IEEE 802.11 standards, specifically in IEEE 802.11i. Since the focus for 802.11 has been private or enterprise networks, existing work on pre-authentication in 802.11i has assumed that the terminal is a "returning customer"; i.e. exploiting that the terminal has either visited this access point before, or visited an access point with which the current access point has a trust relationship. In a public network like OBAN such assumptions will not hold in general, and thus we must look for other approaches.

3.2 Meddle with Sequencing and Time

Generally, you would first connect to a network at the physical level and establish a link to the access point, then perform authentication, and third be granted access to use the network services. This is also reflected in the Finite State Machine of the 802.11 association and authentication process (see Figure 6) where user data traffic (class 3 frames) is only allowed when associated and authenticated. If not, only messages that convey control information like authentication data and negotiation parameters are allowed (class 1 & 2 frames). To speed up handover it is however possible to change the order of things:

- One could perform authentication before connecting to the new access point (pre-authentication).

- One could perform authentication in parallel to being granted access to the network services – of course only within a limited amount of time and until a full authentication is completed (delayed authentication). This means that a change of the state diagram to include a pending-authentication state is necessary (not shown in the figure) that allows for class 3 frames.

With delayed authentication, the user is allowed access to the communication services before authentication has taken place. This means that no extra time is needed for authentication at the time of handover, but it results in reduced control on who are utilizing the communication service, at least for short messages and similar. This may not be satisfactory, neither for service providers nor for regulatory authorities. Measures like blacklisting of MAC addresses can however be taken to reduce the chances that this is utilized maliciously.

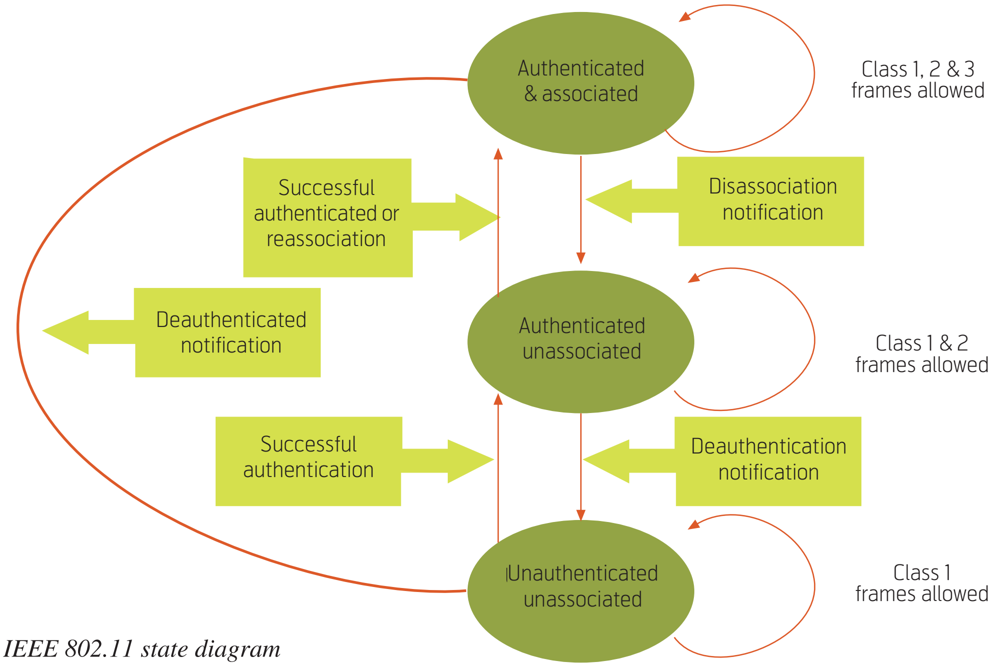

Authenticated & associated
Class 1, 2 & 3 frames allowed
Successful authenticated or reassociation
Disassociation notification
Deauthenticated notification
Authenticated unassociated
Class 1 & 2 frames allowed
Successful authentication
Deauthentication notification
Unauthenticated unassociated
Class 1 frames allowed

Figure 6 The IEEE 802.11 state diagram

ISSN 0085-7130 © Telenor ASA 2006

With pre-authentication, the user will be authenticated before performing the actual handover towards the new network. This results in no extra time needed for authentication at the time of handover, but requires means to predict what access point to connect to next, and ways to communicate with this access point to perform authentication. As stated before, current standards for wireless networks do not allow for simultaneous connections to several access points. Therefore, other means have to be used to allow communication for pre-authentication. One option is to use an alternative wireless technology, another option is to communicate to the new access point via the access point one is currently using, and still a third option is to utilize the Mobility Broker introduced in subsection 2.2. Utilizing the Mobility Broker seems like the best alternative, since the MB already needs to have knowledge of all the access points within its cell, and because this alternative requires less complexity in the access points.

One way of performing pre-authentication is to create tickets beforehand that can be used by access points to determine if the roaming VU is to be allowed access to OBAN. Then the time needed for authentication at the time of handover will be reduced to the validation of a ticket. Access points can make access control decisions by themselves, without involving a whole lot of different parties. Different types of tickets can be made. One solution is to create tickets that are distributed to both access points and terminals. Terminals and access points would then need to be in possession of tickets that belong to each other for authentication to be possible. Another possibility is to create tickets that are only understandable by the access point and distribute these tickets to the terminal together with some corresponding secret. The terminal will then need to present a valid ticket and a corresponding secret to the access point to be allowed access to OBAN. The last option seems most advantageous since this results in a less complex ticket distribution mechanism.

In the following sections, delayed authentication and a ticket based solution are described in more detail. The ticket solution is inspired by Kerberos [4].

4 Delayed Authentication

Delayed authentication is a principle that can be applied to several technologies. In this section delayed authentication in handovers between different OBAN access points is discussed. First the basic idea is described in a WLAN setting before the risks and technical challenges of the solution are discussed.

4.1 Basic Idea

Subsection 2.2 outlined the multi-domain aspects of handover in OBAN. Figure 7 shows the same type of handover situation as described before with the elements necessary in a WLAN solution. The VU has established a session with RGW_1, and is now moving to RGW_2 after detecting that RGW_2's AP is in better radio coverage range and has a spare capacity. Before accepting the VU, RGW_2 must communicate with the VU's Home ISP ($H\text{-}ISP_{RU}$) that grants authorization

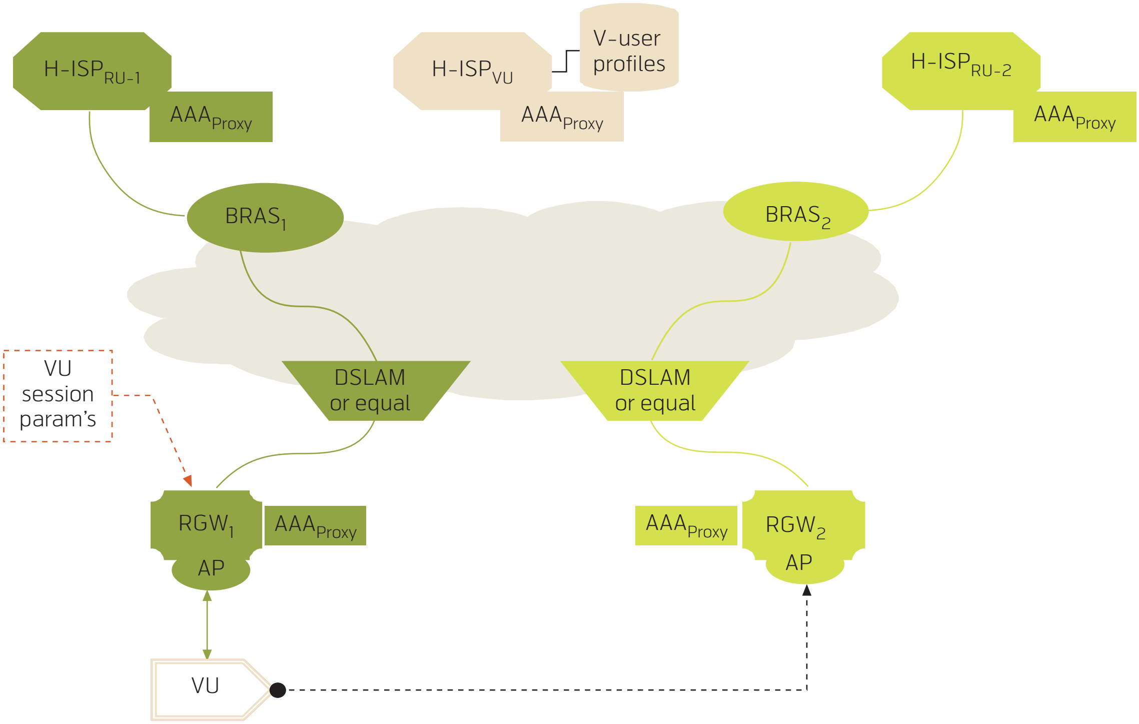


Figure 7 OBAN architecture

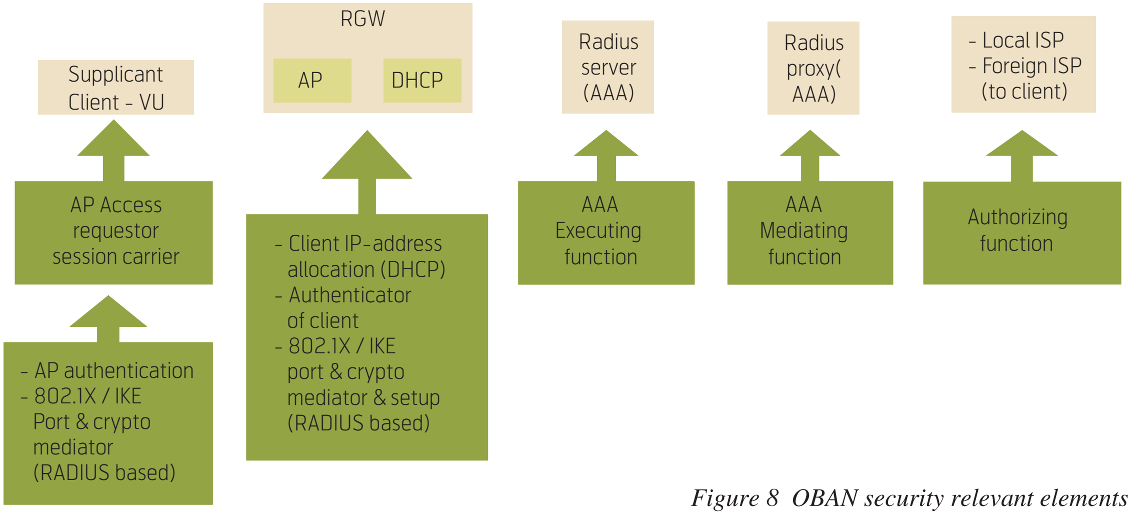


Figure 8 OBAN security relevant elements

and accounting. These AAA procedures are handled through the set of RADIUS-based AAA-proxies and AAA-server. If granted, the RGW_2 signals its 802.1X port control, executes key exchange for encryption of the radio link, and finally conveys the session through its routing system.

In order to convey the needed AAA and IEEE 802.1X port control functionality, various elements cooperate to complete the tasks as indicated in Figure 8.

The various tasks involved in handover are sequenced as shown in Figure 9. The time values $T_1 – T_5$ are based on rough estimates, indicating that T_4 represents the longest delay:

- T_1: Physical connection setup between the VU and the next AP/RGW

- T_2: Messaging session parameters, including VU's ID / authentication info between the VU and the next AP/RGW

- T_3: Processing of rerouting of the traffic to and from the VU via the new AP

- T_4: AAA/RADIUS roundtrip for re-authentication of the VU between AP/RGW and H-ISP for VU

- T_5: 802.1X port handling and encryption of radio link between VU and AP

The standard mandates that these parts have to be carried out in sequence implying the session will be discontinued for total time = $T_1 + T_2 + T_3 + T_4 + T_5$ < 120 msec. As already stated, a scrutiny of the different times shows that T_4 is the major delaying factor, i.e. the RADIUS AAA roundtrip as depicted in Figure 9. T_4-variations can arise depending on whether the RGW and VU belong to different domains or not, and also on the RADIUS traffic flow since it depends on network capacities.

The idea of delayed (or better: parallel processed) authentication is based on a possibility to open the port for traffic before the authentication is completed and the link is encrypted (the 802.1X / Key exchange and encryption protocol depends on the completing authentication). The earliest possible time to this is after the session parameters are handed over and new routing is completed, i.e. after T_3. Thus, we have the more convenient situation depicted in Figure 10.

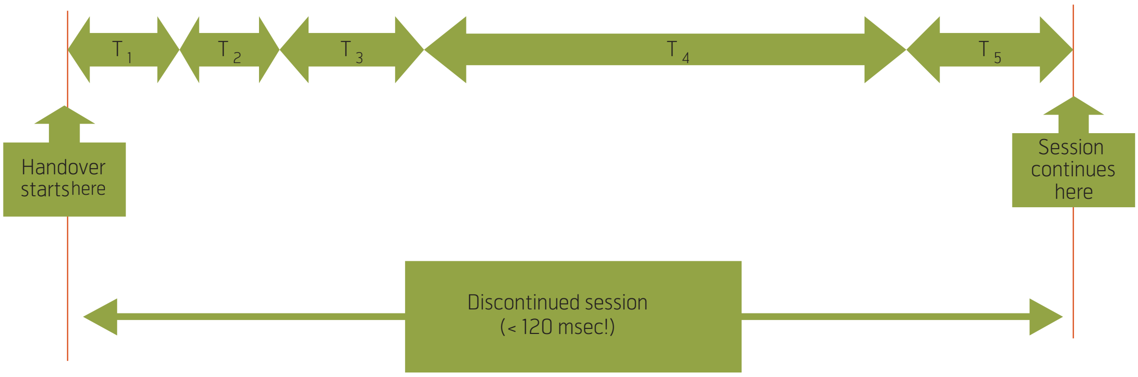
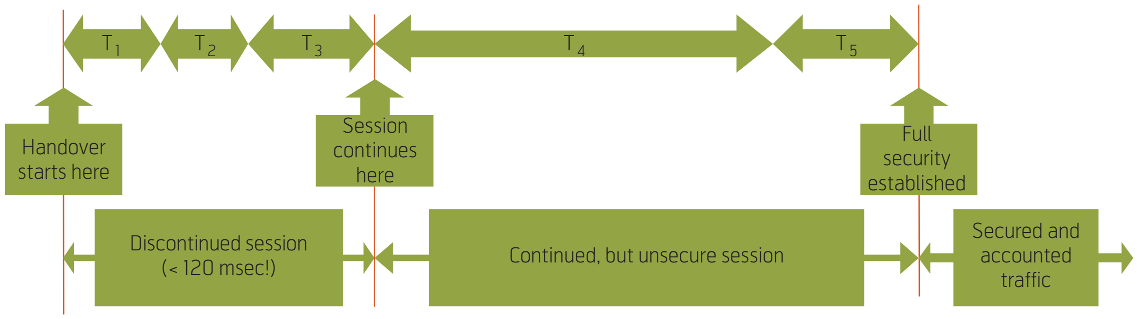


Figure 9 Roundtrip delays (T_1: Physical connection setup, T_2: Session parameters, T_3: Rerouting. T_4: AAA/RADIUS roundtrip, T_5: 802.1X port handling and encryption)



T_1
T_2
T_3
T_4
T_5
Handover starts here
Session continues here
Full security established
Discontinued session (< 120 msec!)
Continued, but unsecure session
Secured and accounted traffic

Figure 10 Delayed Authentication (T_1: Physical connection setup, T_2: Session parameters, T_3: Rerouting. T_4: AAA/RADIUS roundtrip, T_5: 802.1X port handling and encryption)

4.2 Risks

From a security standpoint, the delayed authentication has three main risks:

1 The radio link is unprotected during T_4 and T_5 (a few seconds), something that may harm the VU's interests. The means for this is that the VU may establish a VPN session on a higher level to achieve continued end-to-end protection. Note that handover must also be able to handle VPN sessions.

2 The user traffic cannot be accounted for if the re-authentication fails. Thus the RGW may have business losses caused by unaccountable resource consumption. This may be a reasonable price for a popular service if it is a question of seconds. This risk may be exacerbated if a user/client changes its MAC address repeatedly in order to achieve "free surfing". However, this chance is minimal, since if the client is not capable of presenting correct session parameters then his communication fails.

3 Denial of service attacks on the RGW/AP caused by overloaded management handling of handover attempts, e.g. caused by a client that changes its MAC addresses and presents false session parameters.

Risk 2 and 3 above can be countered to some extent, partly by caching blacklist of rejected client IDs, partly by having the option to change policy by toggling between undelayed (normal) handover and delayed handover. If unaccounted traffic is measured above a defined threshold, all security steps are mandated, e.g. for a certain time and until the attack is over.

In order to avoid pending states where the time gets too long while waiting for T_4 and T_5 to complete, a configurable timer controls the unsecured session maximum time and terminates the connection for that Visiting User.

4.3 Technical Challenges

The IEEE 802.1X mechanisms in use today are not implemented to cater for the delayed authentication policy. Hence, changes in both the AP and the VU client software must be done. Also, delayed authentication is in conflict with the 802.11 standards and its inherent state machines. This means that also an attempt for changing the standard(s) must be carried out.

4.4 Conclusion

At the cost of security (for the user traffic) and unaccounted traffic for some seconds, delayed authentication may be a solution to convey sessions at handover between APs in a fashion that the session discontinuity gets below 120 msec, which is a target especially for real-time voice and streaming.

5 Pre-Authentication using Kerberos-style Tickets

In the following we provide a brief refresher of the Kerberos concept and then go on to explain how Kerberos can be used in OBAN.

5.1 Explanation of the Kerberos Concept

Kerberos is an authentication protocol developed at Massachusetts Institute of Technology (MIT) to protect campus network services. Variants of Kerberos have since then been used as authentication protocol in several products. Kerberos uses tickets for authentication, and similar tickets can be used in OBAN to achieve fast authentication at the time of handover. This section describes the Kerberos protocol in more detail, based on [1] and [2].

5.1.1 An Allegorical Description

Let us cast our imagination back to medieval times and imagine sending an envoy from the King of Norway to the Emperor of China. A Kerberos ticket can be viewed as a sort of sealed letter of reference containing a secret password. It is assumed that the recipient (the Emperor) can recognize the King's seal, and that it is not possible to open the envelope without breaking the seal (and the seal cannot be forged). When the King hands the "ticket" over to his envoy, he simultaneously informs him of the secret password within (e.g. "42").

Upon reaching his destination, the bearer of the ticket (i.e. letter of reference) presents the sealed envelope to the Emperor, who breaks the seal and extracts the contents. The Emperor then asks the bearer about the secret inside the letter ("What is the answer to life, the universe, and everything?"). When the envoy responds correctly ("42"), the Emperor can be satisfied that this is indeed the King's trusted servant, etc. etc.

Note that there is one important difference between this allegorical example and a real Kerberos ticket: The letter cannot be opened without breaking the seal, while the Kerberos ticket cannot be "opened" by a third party (or the envoy) *at all* (we assume that the cryptography is strong enough to make opening "impossible" if one does not possess the correct key).

5.1.2 A Step Closer to the Real World

In a Kerberos ticket, the secret password is a session key (which we in the following will refer to as *access key*, in order to avoid confusing it with the session key for encrypting the wireless connection), and the seal is realized by encryption with a key shared between the King (or, Authentication Server – AS) and the Emperor (or, Ticket Granting Server – TGS). To complicate matters, there is a third party involved as well, i.e. the server ("V") that provides the specific application service (mail, file transfer, etc.), but for the time being we will ignore this.

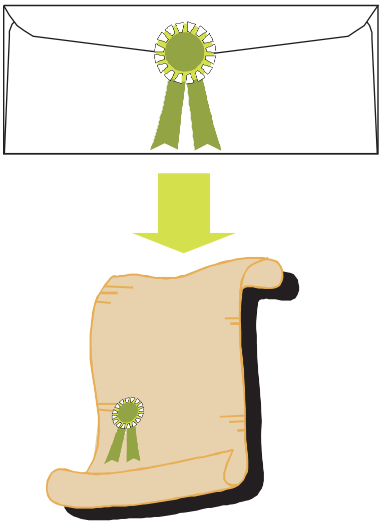
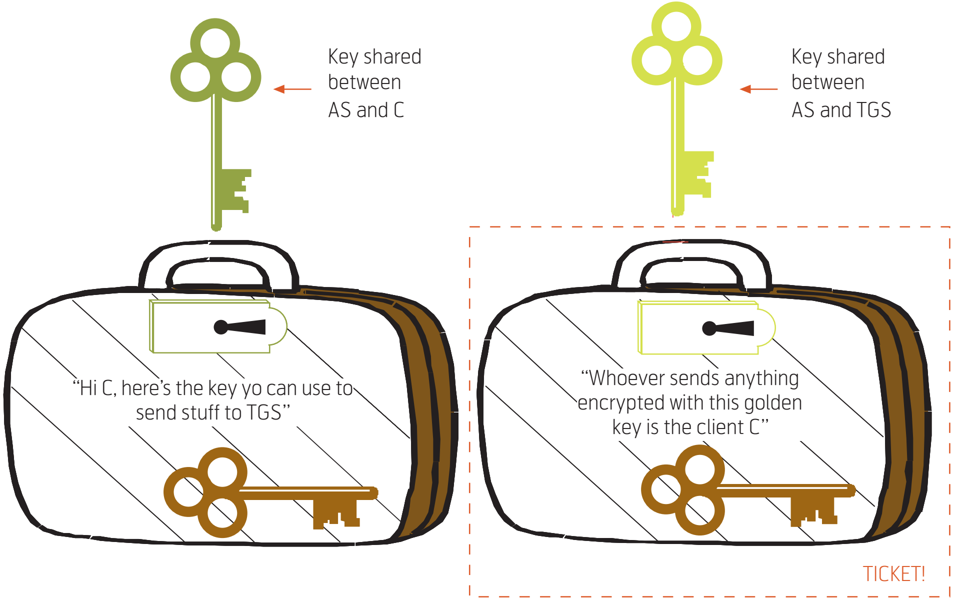


Figure 11 A ticket as a sealed letter of reference

The task of the AS is to authenticate the client (done implicitly[1] by issuing data encrypted with the client's password), and issue a Ticket-Granting-Ticket (TGT) that the client will use when authenticating to the TGS. The task of the TGS is to issue a ticket for the specific service that the client wants, as can be seen in Figure 14.

When the envoy (or Client – C) initially requests a ticket, it needs a pre-shared secret with the AS, normally in the form of a password. This secret (the



Key shared between AS and C
Key shared between AS and TGS
"Hi C, here's the key yo can use to send stuff to TGS"
"Whoever sends anything encrypted with this golden key is the client C"
TICKET!

Figure 12 Simplified illustration of ticket and accompanying information

[1] *In practice modern Kerberos systems also use some form of pre-authentication in order to avoid issuing tickets to unauthorized parties, but this is primarily a countermeasure against denial of service attacks, and need not concern us here.*

ISSN 0085-7130 © Telenor ASA 2006

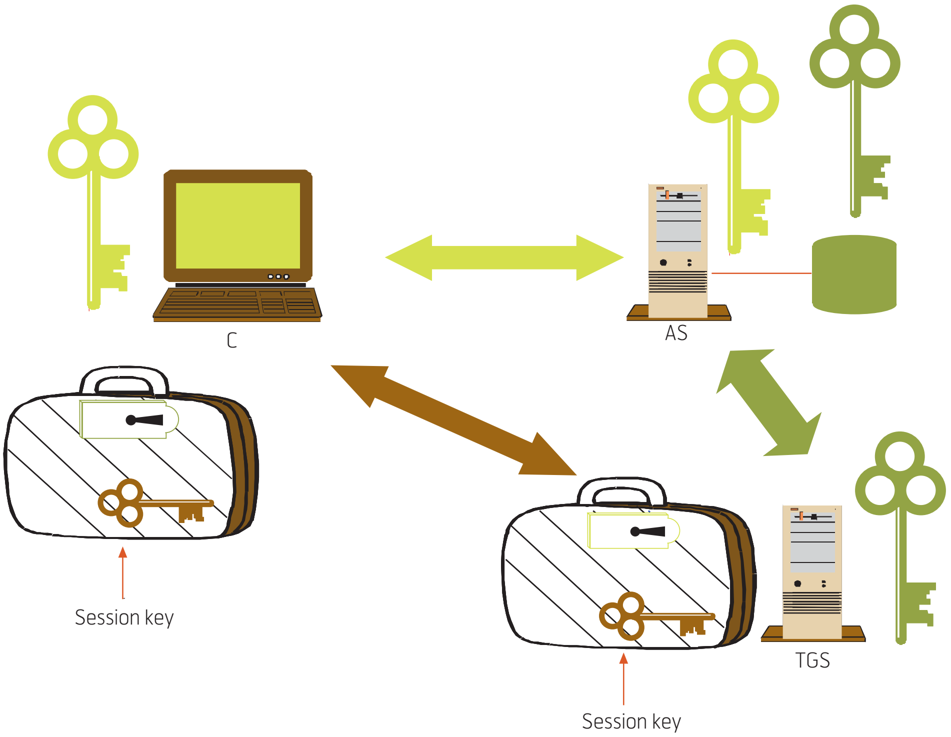


Figure 13 Trust relations and shared keys

upper left key in Figure 12) is used to protect the dynamic access key (chosen by AS) that is also embedded in the ticket. Thus, the ticket in itself is worthless if the bearer cannot prove that it also knows the access key. As illustrated in Figure 12, the client C receives two elements from the AS:

- The ticket (which the client cannot decrypt)

- The accompanying information, including (most importantly) the access key (this is encrypted with the shared secret that C and AS possess).

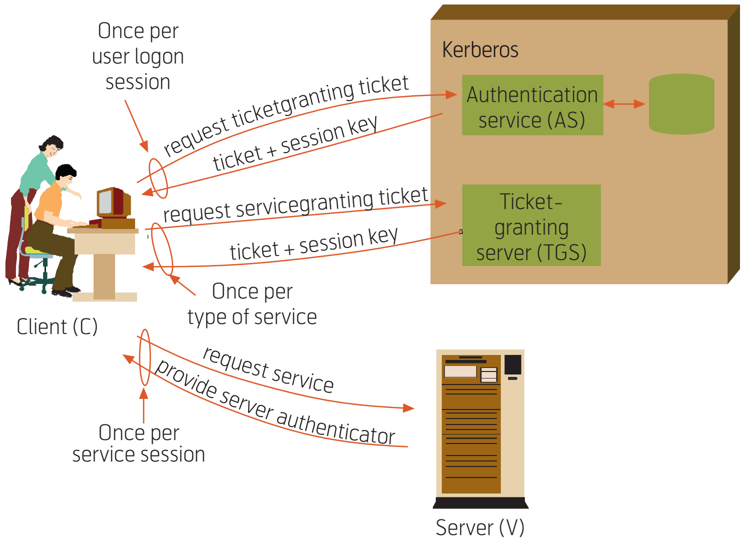


Figure 14 Kerberos overview (adapted from Stallings [2])

The ticket is used to create a dynamic (indirect) trust relation between C and TGS, based on the fact that there are static (direct) trust relationships in the form of shared secrets between AS and C (upper left key) and between AS and TGS (upper right key). This is illustrated in Figure 13.

When finally the service granting server (V) enters the picture, the interactions previously performed toward AS are basically repeated toward TGS, with similar trust relations (except that the direct trust relation between C and AS is replaced with the indirect (dynamic) trust relation between C and TGS). Thus, if we disregard whether trust relations are direct or indirect, we can replace AS by TGS and TGS by V (i.e. serVice granting server) in Figure 13.

The “full picture” can be seen in Figure 14 (adapted from [2]).

In OBAN, the terminal will need access to OBAN services via different RGWs. In handover situations, the terminal will already have authenticated via one RGW (RGW_{old}), and now needs to authenticate via the new RGW (RGW_{new}).

5.2 Kerberos Players vs. OBAN parties

As Table 1 shows, the trust relations in standard Kerberos and OBAN are completely analogous; the ISP_{VU} and Visiting User have a shared secret (in the SIM), the ISP_{VU} and each ISP_{RU} need to have a shared RADIUS secret (for the trust relationship between the AAA server and the AAA proxy), and the RGW and ISP$_{RU}$ also need a shared RADIUS secret (between the authenticator in the RGW and the [proxy] AAA server at ISP$_{RU}$). Note that there is *no direct trust relationship* between the terminal and ISP$_{RU}$.

The fact that the roles of both AS and TGS are assumed by ISP$_{RU}$ is no anomaly in Kerberos terms; this occurs so often that the combined AS-TGS pair is frequently simply referred to as the Key Distribution Centre (KDC).

Kerberos player	OBAN party
AS - (Authentication Server)	MB (but acting as proxy toward ISP$_{RU}$ and ISP$_{VU}$)
TGS - (Ticket Granting Server)	MB
C - (Client)	Visiting User (terminal)
V - (serVice granting server)	RGW

Table 1 Mapping from Kerberos to OBAN

5.3 Assumptions

Our proposed solution is based on a number of assumptions, as detailed in the following.

5.3.1 Pre-shared Secrets

Since a Kerberos ticket is protected by a symmetric key, this implies that shared secrets must exist between various pairs of players in any given scenario. Looking at Figure 3 we can see that this holds true for all the static participants; i.e. the RGW (or AP$_{A1}$) shares a RADIUS secret with the MB, the MB shares a RADIUS secret with ISP$_{RU}$ (or ISP$_{AP1}$) and ISP$_{RU}$ shares a RADIUS secret with ISP$_{VU}$. The Visiting User shares a secret with the ISP$_{VU}$, but it cannot directly traverse this transitive trust path. However, by using an EAP method that conforms to [8], the MB can (by proxying the authentication protocol via ISP$_{RU}$ to ISP$_{VU}$) exploit the trust relationship between Visiting User and ISP$_{VU}$ to create a new shared secret that is propagated back to the MB.

Once the MB is in possession of this (short-term) shared secret with the Visiting User, it is in a position to issue a Kerberos ticket that is protected by the MB-RGW secret, accompanied by a copy of the enclosed access key protected with the short-term secret.

5.3.2 Minimum Stay

Authentication by use of tickets enables fast handover, but only if the connected period prior to handover is long enough to ensure that the terminal has sufficient time to request the necessary ticket(s). This period of minimum stay may be shorter or longer depending on how successful the MB is at predicting the next destination RGW, and also depending on which applicable tickets the terminal already possesses. For instance, a naïve prediction algorithm may simply be to ensure that the terminal receives tickets for *all* candidate RGWs that are in range; for areas with a relatively sparse RGW distribution (e.g. if there are only four candidate RGWs in range), this could actually work pretty well. In areas with higher RGW density, downloading a large amount of tickets would increase the minimum stay and might mandate a more intelligent prediction approach. At any rate, it is unlikely that the minimum stay can be less than the time to request and process at least a couple of tickets.

5.3.3 Loosely Synchronised Clocks

Kerberos tickets have a limited validity, both to enable dynamic access control (just because you were allowed access yesterday, does not mean that you are necessarily entitled to access today), and to offset brute-force attacks against the access key. In order to achieve this, the three entities involved in the ticket scheme (MB, terminal and RGW) all need to have roughly the same idea of what the current time is. Kerberos allows for a certain (configurable) clock skew between the various players, which means that e.g. the authenticator message that the terminal transmits along with the ticket must have a time stamp that does not differ more than a specific number of seconds from the RGW's current time. The reason for this is to prevent an intruder from replaying an authenticator message to gain illicit access.

Currently, there is no automatic mechanism to ensure this loose synchronisation in OBAN, although the MB and the RGW may exploit their trust relationship to allow e.g. the MB to act as "time authority" for its cell. Future research will explore whether the full authentication toward ISP$_{VU}$ can be extended to allow the terminal to synchronize its clock to "cell time".

5.4 Informal Description of the Resulting Protocol

A detailed description of the proposed protocol is given in [3]; in the following we will attempt to outline the main results.

5.4.1 Mobility Broker as a New Essential Element

Although it would have been possible to create a scheme for fast handover in a multi-ISP scenario where each ISP$_{RU}$ could issue tickets for RGWs under its control, inter-ISP handovers would have been a greater challenge. Furthermore, determining which RGW to request tickets for would have required a much more complex protocol and possibly more processing capability etc. in the RGWs.

The MB elegantly solves these problems by maintaining a database of RGWs where physical location and other attributes are recorded. When a request is received via a given RGW, the MB will instantly know which other RGWs are in the immediate surroundings, and may also have other, more dynamic information that contributes to singling out a subset of the surrounding RGWs as handover destination candidates.

The MB has a fixed trust relationship with all RGWs and associated ISP_{RU}s in its cell and can thus issue tickets to all these RGWs, no matter which ISP_{RU} they belong to.

5.4.2 Initial Authentication

An OBAN RGW will always assume that a new terminal has a ticket and issue a ticket request immediately following a new association. If this is a new session for the terminal, it will not possess an appropriate ticket[2], and must reply with a non-acknowledgment message (EAP-NAK) to this request. The RGW must then be configured to initiate a conventional EAP-SIM authentication as fall-back method. The RGW will proxy this authentication towards MB, which proxies toward ISP_{RU}, which finally proxies the authentication toward ISP_{VU}. This is illustrated in Figure 15.

All these proxies may seem confusing, but from the terminal's point of view it is rather simple – it is allowed to authenticate towards an RGW that (somehow) has a trust relationship with the terminal's ISP_{VU}.

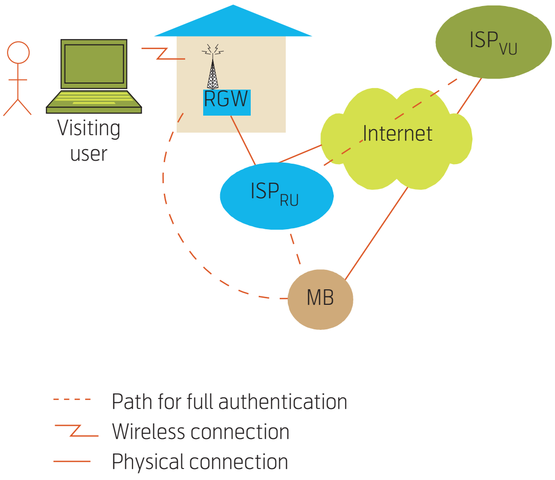


Figure 15 Trust path for initial full authentication

Once the full EAP-SIM exchange is complete, the terminal is authenticated and admitted to the access network. However, at this point the terminal is not yet in a position to perform a fast handover; in order for the MB to issue tickets to the terminal, the two actors must first possess a shared key. For this purpose the key just arrived at during the EAP-SIM negotiation cannot be used, as that would enable an RGW operator to impersonate the Visiting User (since the RGW needs to have access to this key in order to encrypt the air interface). Thus, a *second* EAP-SIM conversation is initiated directly towards the MB (proxied back to ISP_{VU} as before).

At the completion of the second (tunnelled) EAP-SIM exchange, the terminal and the MB share a secret that can take the place of the user password ("key shared between C and AS" in Figure 12) in a traditional Kerberos setting. Armed with this shared key, the MB can now issue a Ticket-Granting Ticket (TGT) to the terminal. Upon the receipt of this TGT, the terminal may request access tickets to specific RGWs.

5.4.3 Access Ticket Request

Once the terminal is authenticated, the MB will inform it about candidate handover RGWs via a dedicated protocol. For each candidate RGW, the terminal will request a ticket via an HTTP[3] GET request. The request must include the TGT and Kerberos authenticator, and multiple requests may be performed in parallel. Once the terminal is in possession of the access tickets, it is ready to perform a fast handover to any of the corresponding RGWs.

5.4.4 Ticket Usage

When the terminal associates with a new RGW, it can now reply to the ticket request with a valid ticket (and associated Kerberos authenticator). The ticket and authenticator are evaluated locally by the RGW, and the terminal is immediately granted access to the network. The terminal may then proceed to send other messages aimed at restoring a Mobile IP session etc.

A simplified depiction of the communication involved in a full authentication with a subsequent fast handover is given in Figure 16.

5.4.5 Interaction between Kerberos and 802.1X Key Distribution

In a traditional 802.1X scenario, the wireless access point will base the key for encrypting the wireless connection on the shared secret arrived at during the chosen EAP method. In the Kerberos case, no new secret is arrived at, but on the other hand the RGW

[2] *Or possibly only an expired ticket.*

[3] *HTTP is merely used for convenience – any suitable encapsulation would work just as well.*

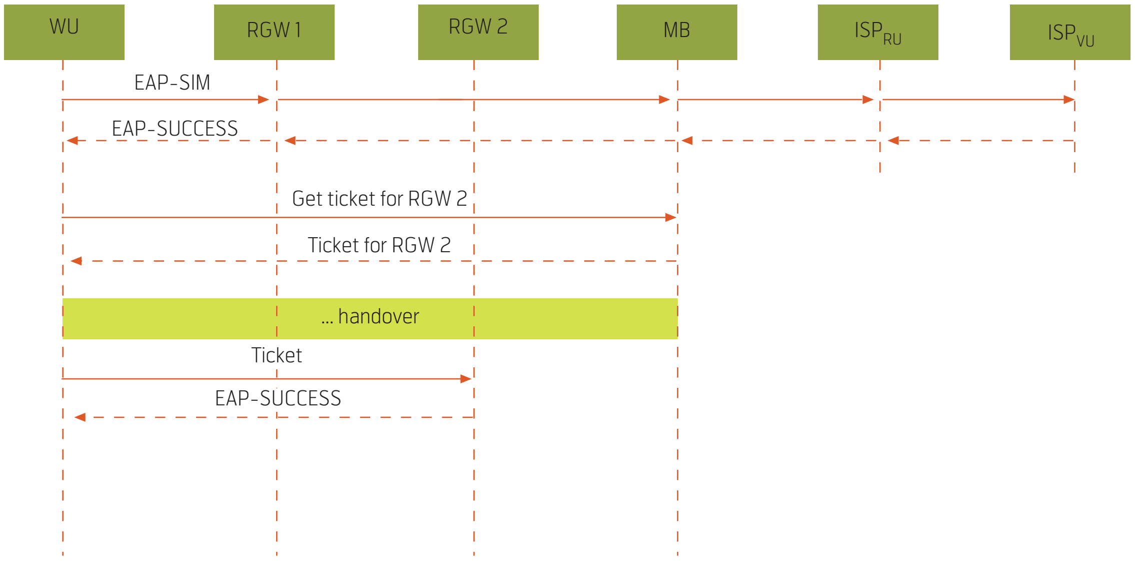


Figure 16 Simplified message sequence chart for full authentication with subsequent handover

and terminal already share the access key embedded in the ticket. One option here would be to employ the TKIP mechanism specified in IEEE 802.11i [11], with the access key in the ticket as the pre-shared secret.

6 Conclusion/Summary

Several mechanisms for fast handover were considered in the OBAN project, two of which were delayed authentication and Kerberos tickets. The latter solution was ultimately selected for implementation, primarily for pragmatic reasons.

Delayed authentication has its own merits, but fell through primarily on two counts: It would have required changes in the 802.1X authenticator in all OBAN wireless access points (which effectively would have meant that no existing equipment could have been used for OBAN), and it would have introduced a small window of vulnerability in every RGW, which the "wireless enthusiast" community undoubtedly would find a way to exploit.

The Kerberos solution in combination with the Mobility Broker allows pre-authentication to be performed in connection with the process of choosing candidate RGWs for handover. Once a terminal has a valid ticket for an RGW, verification of the ticket can be done locally on the RGW, without involving the MB or other actors; this makes authentication with a ticket very fast. The Kerberos solution relies on established, well-known standards, and should allow any wireless access point in use today to be employed as the wireless component of an RGW.

The Kerberos authentication solution will co-exist with EAP-SIM or similar methods for full authentication. For handovers between heterogeneous networks (e.g. from Wi-Fi to UMTS) it may not be applicable, not least because of the opportunities for make-before-break handovers.

Acknowledgement

This article is based on joint research in the EU 6th Framework Programme, and the authors would like to thank all the participating OBAN partners for their contribution to the fast handover effort. In particular, Frédéric Paint (Telenor R&D) introduced the Mobility Broker, and Frans Panken (Lucent Technologies Netherlands) first suggested the use of tickets for fast handover, as well as proposing to separate the ticket acquisition phase from the authentication phase. Special thanks to Thomas J. Wilke (TUB), first OBAN WP2 security activity leader, for fruitful discussions on secure handover, and to Einar Edvardsen (Telenor R&D) for initiating the OBAN project, as well as this special issue of *Telektronikk*.

References

1 Jaatun, M G. *Kerberos – en trehodet sikkerhetsvinkling for framtiden*. Presentation at Studiemøtet 2001, Lillehammer, Norway, 14–15 June 2001.

2 Stallings, W. *Cryptography and Network Security* (3rd ed). Prentice-Hall, 2003.

3 Jaatun, M G et al. Secure Fast Handover in an Open Broadband Access Network using Kerberos-style Tickets. In: *Proceedings of IFIP SEC2006, Security and Privacy in Dynamic Environments*, Karlstad, Sweden, 22–24 May 2006, 389–400.

4 Neuman, B C, Ts'o, T. Kerberos : An Authentication Service for Computer Networks. *IEEE Communications*, 32 (9), 33–38, 1994.

5 Neuman, C, Yu, T, Hartman, S, Raeburn, K. *The Kerberos Network Authentication Service (V5).* The Internet Engineering Task Force (IETF), RFC 4120, July 2005.

6 Edvardsen, E, Eskedal, T G, Årnes, A. Open Access Networks. In: McDonald, C (ed). *INTERWORKING, ser. IFIP Conference Proceedings*, 247, 91–107. Kluwer, 2002. (Presented at Interworking'2002, Perth, Australia, 13–16 October 2002.)

7 Jaatun, M G, Tøndel, I A, Dahl, M B, Wilke, T J. A Security Architecture for an Open Broadband Access Network. In: *Proceedings of the 10th Nordic Workshop on Secure IT Systems (Nordsec)*, Tartu, Estonia, 20–21 October 2005.

8 Stanley, D, Walker, J R, Aboba, B. *Extensible authentication protocol (EAP) method requirements for wireless LANs*. The Intenet Engineering Task Force (IETF), RFC 4017, March 2005.

9 Choi, S, Hwang, G-H, Kwon, T, Lim, A-R, Cho, D-H. Fast Handover Scheme for Real-Time Downlink Services in IEEE 802.16e BWA System. In: *2005 IEEE 61st Vehicular Technology Conference (VTC 2005-Spring)*, 2005, 3, 2028–2032.

10 Kim, K, Kim, C-K, Kim, T. *A Seamless Handover Mechanism for IEEE 802.16e Broadband Wireless Access*. Lecture Notes in Computer Science, Berlin, Springer, 3515, 527–534, 2005.

11 *IEEE Standard for Information technology – Telecommunications and information exchange between system – Local and metropolitan area networks. Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements*. 2004. (IEEE 802.11i-2004)

12 *Wireless Service at Boingo: Wireless Internet, Wi-Fi, Wireless Access, Hotspot*. 22 June 2006 [online] – URL: http://www.boingo.com

13 *LinSpot – Sell your Air!* 22 June 2006 [online] – URL: http://www.linspot.com

14 *FON: Wi-Fi everywhere!* 22 June 2006 [online] – URL: http://en.fon.com

15 ITU. *General Characteristics of International Telephone Connections and International Telephone Circuits*. International Telecommunication Union, 1988. (ITU-TG.114)

16 *IEEE Standards for Local and metropolitan area networks – Port-Based Network Access Control*. 2001. (IEEE 802.1X-2001)

17 Rigney, C et al. *Remote Authentication Dial In User Service (RADIUS)*. The Internet Engineering Task Force (IETF), RFC 2865, June 2000.

18 *IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems*. 2004. (IEEE Std. 802.16-2004)

19 *OBAN*. 22 June 2006 [online] – URL: http;//www.ist-oban.org

20 Panken, F et al. Architecture for sharing residential access with roaming WLAN users. *Telektronikk*, 102 (3/4), 48–59, 2006 (This issue).

21 Draft IEEE Standard for local and metropolitan area networks, IEEEP802.16e/D4. *Air Interface for Fixed and Mobile Broadband Wireless Access Systems; Amendment for Physical and Medium Access Control*. 2004.

For a presentation of Martin Gilje Jaatun, please turn to page 59.

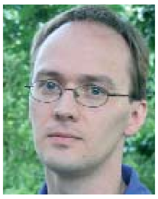
Inger Anne Tøndel holds an MSc from the Norwegian University of Science and Technology (NTNU), department of Telematics. She is now a research scientist at SINTEF ICT, where she works with different aspects of information security.
email: Inger.A.Tondel@sintef.no

For a presentation of Tor Hjalmar Johannessen, please turn to page 59.

Resource Allocation and Guarantees for Real-Time Applications in WLANs

FRANS PANKEN, GERARD HOEKSTRA, SIETSE VAN DER GAAST

Frans Panken is a senior member of the technical staff at Lucent Technologies



Gerard Hoekstra is a member of the technical staff at Lucent Technologies

Sietse van der Gaast is a senior member of the technical staff at Lucent Technologies

WLAN has become a cost-effective wireless technology for the residential market. The residential PC infrastructure did not require QoS from the beginning, but as WLAN is gradually moving in the enterprise and public areas with the growing demand for real time applications, the need for QoS is increasing. In addition, to offer the network services transparently to end-users in a converged network environment, WLAN access networks require a resource allocation mechanism and QoS guarantees similar to 3G networks. Current QoS support in WLANs enables prioritization to e.g. differentiate between real time and elastic traffic flows. This paper complements this by showing how QoS assurance can be achieved by associating subscriptions with transmit and receive rates. The main focus is on the complete end-to-end QoS solution, including admission control and resource allocation, taking into account the varying channel conditions and the need to adapt to these conditions dynamically to guarantee a predefined QoS level.

1 Introduction

WLANs have been applied successfully as an important home and last mile technology in the increasingly pervasive computing environments where mobile users access Internet services. If the subscription and usage of real-time multimedia applications increase, the demand increases for the support of end-to-end QoS guarantees in both wired and wireless networks. As WLANs are deployed on a world wide scale, its users may potentially access real-time and Internet services virtually anytime, anywhere, enjoying the flexibility of connectivity while being mobile. Although the forecasts of the explosive WLAN usage in public areas observed today have not yet become a reality ([1]), faith remains that this will happen over time. A base for this faith is the various announcements of WLANs coverage throughout cities (see e.g. [2]) and that network convergence is an important precondition for the next generation telecom network, with the key promise to develop and deploy innovative and profitable services rapidly and efficiently. The integration of WLAN in 3G devices and the convergence of various access network technologies indicate that WLAN is no competition for 3G access networks but should rather be seen as another alternative of offering connectivity. In order to offer services transparently to end-users in a converged access network environment, WLAN access networks must provide resource allocation and QoS guarantees in a similar manner as offered by e.g. 3G networks. As 3G networks offer QoS guarantees for end-users, a true convergence of access networks poses the same requirements on WLAN. The ease of use and equal end-user's experience is an important side condition to realize this convergence. The end-user should not be bothered with which network interface or technology is used to realise its communication.

Current QoS solutions for WLAN can be classified in three categories (see [3]):

- Link adaptation in the physical layer
- Channel access coordination in the MAC layer
- Admission control strategies in MAC and higher layers.

These approaches focus on different network layers and are tightly interrelated. Park et al. [4] propose mappings between traffic class identifiers to realize a collaborative end-to-end QoS architecture across wired WAN, wired LAN, and WLAN, based on the QoS solutions in these networks: DiffServ, IEEE 802.1D/Q, and IEEE 802.11e. Proper mappings are essential to achieve bounded and predictable network characteristics. However, without admission control and resource allocation, providing QoS guarantees only by differentiating flows and coordinating the order of channel access cannot be sufficient when dealing with high traffic load conditions. In addition, the WLAN channel conditions vary fast and need to be taken into account to deliver guaranteed QoS, comparable with 3G networks.

Admission control and resource allocation require a subscription that reflects the expectations to the communication for both parties: the provider and the user. Important for providers is the ability to differentiate between various end users. The solution found is to define a subscription as a set of *QoS profiles* that are stored in the network and communicated to the edges of the network when new users authenticate. These QoS Profiles then form the individual base for the decision to grant a new user access or to deny service. If access is granted, the various QoS profiles (that are associated with data rates and are used to define the user's subscription) allow various levels of network commitment. This is explained in Chapter 2.

ISSN 0085-7130 © Telenor ASA 2006

Although the QoS solution described in this paper is generic of nature, it is applied to a specific use case, namely to guarantee QoS to users who casually pass a WLAN equipped home and can utilize the otherwise idle part of the fixed broadband access line capacity. This concept – referred to in the remainder of this paper as the *home spot solution* – may be looked upon as a method to provide wireless (mobile) broadband services over the existing fixed broadband network, as an alternative for a new or an upgrade of today's mobile network. When the WLAN antenna is placed optimally in a home, signal attenuation to reach public domain is equivalent to 40 m distance (real distance + walls / windows, see [5]). At this distance it is still possible to offer WLAN connectivity of a sufficient capacity via the residential equipment. The challenge is to realize the home spot solution without replacing existing residential equipment. In urban areas, it is envisaged that the residential WLANs can offer near-contiguous radio coverage, potentially allowing casually passing users to roam seamlessly through a landscape of home spots while maintaining the desired level of QoS. Roaming should be realized with a minimum of personal involvement such as typing in passwords and answering questions.

Two kinds of users are distinguished, namely residential users and visiting users. Residential users are the users that own a broadband modem or residential gateway and a wireless access point (AP) and offer this equipment to casually passing users, referred to as visiting users. Note that the term visiting user refers to the visiting of the AP located in a house and not to a visit to a person living in the house where the AP is located. In general, the visiting user will be a complete stranger to the person who opens the residential equipment to those who casually pass (or are close) to the home. The visiting user is expected to use a single device and the terms visiting stations and visiting users are used interchangeably in the remainder of this paper. The residential user may have several home WLAN stations and/or other terminals. This paper assumes knowledge about the IEEE 802.11 protocols and refers to [6] for a good and complete description of these protocols.

Various alternatives to the home spot solution have been announced recently. Companies such as FON, BOINGO and Linspot offer third party Wi-Fi network access without involving the access provider and offering neither QoS for real-time applications nor roaming. Francis et al. mention in [7] other challenges of the home spot situation, whereas [8] computes that to realize full coverage via WLAN in the Swiss town Olten (17,500 inhabitants), the cooperation from 4 % – 7 % of the households is sufficient.

This paper shows how QoS enabled WLAN services can be realized by incorporating a QoS solution near the access point, which receives QoS parameters from the network as part of the visiting user's authentication process. The solution presented can be applied to hotspots or e.g. wireless mesh networks. Since the home spot situation distinguishes multiple user types (home and visited), it is chosen as a base for explaining and applying the QoS solution. The focus of this paper is on predictable network behaviour under varying channel conditions for stations supporting real-time applications in a situation where various WLAN stations compete for sending and receiving traffic. It concentrates on the algorithms and results and does not include measurements that show the feasibility of the solution. More in detail, this paper solves how:

1 Available resources can be shared among all stations in an efficient manner and in such a way that it leads to predictable resource consumption in the (wireless) access network;

2 The assigning of resources to each station can lead to a predictable level of quality for a pre-defined set of applications used by the stations;

3 The admittance of the number of visiting users is limited such that an acceptable and configurable level for the home user is maintained. This also means that access to stations may be denied if this is expected to jeopardize point 2.

Chapter 2 describes the home spot architecture and discusses and justifies the underlying QoS model and principles. It also discusses solutions for regulating traffic from and to visiting users in the home spot solution. Chapter 3 focuses on the QoS solution within the residential gateway (RGW), explaining how the committed profile can be selected and how the desired QoS level can be maintained for all users under varying channel conditions.

2 QoS approach and architecture

Contemporary QoS models require mechanisms to reserve capacity on a per-flow basis. When an application requests network connectivity, the terminal negotiates with a QoS entity in the network about a set of network parameters needed to assure the end-to-end QoS of the application. This way of reserving network connectivity on a per-flow basis has its roots in ATM (Asynchronous Transfer Mode). It was also the base for IETF's Resource Reservation Protocol (RSVP) [9] and was the main technical driving force of the Integrated Services (IntServ) working group. The QoS home spot solution deviates from these principles, explained in Section 2.1. Section 2.2 subsequently explains the home spot architecture and shows which QoS functionality is needed where to realize QoS in the home spot solution. Special conditions for traffic regulations apply, as explained in Section 2.3.

Direction	BPP (average Bytes Per Packet in bytes)	PPS (average Packets Per Second)
Upstream	200	50
Downstream	400	75

Table 1 QoS Profile Specification Example

2.1 QoS model

For the visiting user to experience seamless roaming, fast handovers between one home spot to another are essential. Therefore, the QoS mechanism must act fast. In addition, the maximum data rate of a station depends on the distance from the access point and hence a per-flow guarantee is difficult (if not impossible) to realize. If a station needs to negotiate complex structures of QoS parameters for all active connections, the communication needed to negotiate and to handover the flows as the station moves from one access point to another is considered to be too complex and is therefore expected to fail. In addition, the per-flow QoS reservation techniques as e.g. RSVP were never widely deployed and besides are not supported anymore by new versions of the Windows operating system. This observation was a motivation to find a simple way of dealing with network resources. The solution found and selected is to communicate a *QoS Profile* which was defined such that it easily maps to real-time applications (see Table 1).

The usage of the scarce transmission resource at WLAN level is dominated by both the mean segment size (BPP, or Bytes Per Packet) used by the applications (in practice often not larger than 1500 bytes but up to 2304 bytes) and the rate (PPS, or Packets Per Second) in which WLAN data segments are sent. The visiting user's subscription is defined by various QoS profiles, each existing of the mean packet size and the frequency in which packets can be sent and/or received. By defining the subscription as a set of QoS profiles, various potential levels of committed network rates can be distinguished. The level assigned to the station and committed by the network may depend on the network usage, the user subscription level (gold/silver/bronze), and/or a QoS policy (e.g. maximize WLAN usage, maximize the total number of allowed users).

Note that multiplication of the parameters *BPP* and *PPS* will provide the rate in the associated direction. The next section explains where the QoS profiles of visiting users are stored and how they can be obtained.

A subscription exists of various QoS Profiles and Chapter 3 explains how the committed and peak profiles can be selected from this subscription and how the committed profile characteristics can be maintained under varying channel conditions. The selected peak and committed QoS profiles are communicated to a station which is expected to use this associated network resource wisely and is assumed to accommodate its applications to prevent sending too much data. Distinguishing various classes and storing traffic of each class in a separate queue that is served with different priorities (as proposed in e.g. the window's traffic control API [10] or by IEEE 802.11e) can ensure that the station locally gives priority to time sensitive applications. The competition for WLAN transmission rights within a station depends for each packet on its time sensitivity and is consequently solved in the terminal of (residential and visiting) users by applying Wireless Multi Media (WMM) or IEEE802.11e. Reference [14] discusses how the WMM parameters can be applied to the home and visiting user groups to realize that home users still receive their preferred and desired priority level.

2.2 Home spot and QoS architecture

Figure 1 depicts a simplified topology of the various network elements in the access network that are relevant for QoS considerations to realize the home spot situation.

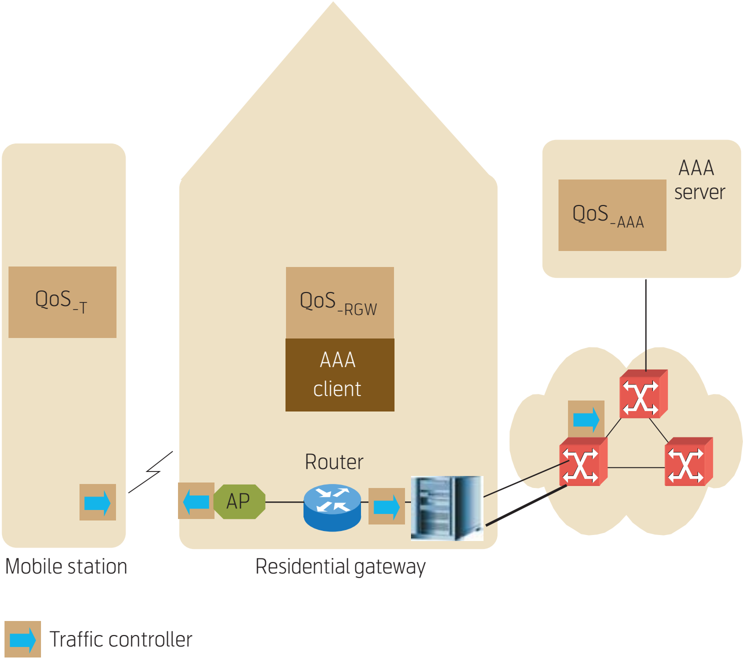


Figure 1 Home spot access network and QoS elements

ISSN 0085-7130 © Telenor ASA 2006

The access network basically consists of IEEE 802.11 stations and access points (APs) equipped with several queues to distinguish and give priority to various traffic classes. To assign a packet to the desired traffic class either the Type of Service (ToS) field of the IP packets or the bits reserved in the IEEE 802.1q standard ([15]) for differentiation can be used. The AP is part of the residential gateway, connected to a fixed broadband access network that gives home users access to their service providers and subsequently to the Internet. The capacity used for visiting users can be defined as the surplus capacity, determined by the maximum access line capacity minus the broadband subscription of the home user. As the fixed broadband technology can differ per home and also the broadband subscriptions may vary per home, the capacity available for visiting users per home spot varies per residential gateway. These parameters are input for the Capacity Distribution Algorithm (CDA), see [11]. The fixed access technology used could be xDSL, cable or fibre; the proposed solution does not depend on the access technology chosen.

To prevent interference between traffic originating from and destined to the wireless stations, the transportation paths of home and visiting traffic should be logically separated. At the backhaul of the RGW this can be realized by e.g. separate ATM VPCs or separate VLANs in the case of Ethernet, or in a technology independent way by using separate PPP sessions for each visiting user. In Figure 1, the two lines that connect the modem in the RGW with the access network depict this aspect. The assigned rates could either be configured fixed or they could vary.

A total of three QoS entities are defined, located in the terminal (QoS_T), the residential gateway (QoS_{RGW}) and in the Authentication, Authorization, and Accounting (AAA) server (QoS_{AAA}). These QoS entities communicate with one another to guarantee the desired QoS level of visiting users. Before visiting users gain network access through a home spot, their credentials need to be checked during the authentication phase. In addition, the QoS subscription parameters for each user need to be retrieved from a capacity allocation database to determine the maximum capacity that can be granted. These parameters can be obtained as part of the authentication and authorization process. Therefore, it makes sense to piggyback initial settings that are communicated between the QoS entities on the authentication protocols being used (e.g. IEEE 802.1X / RADIUS, see [16]). This also explains why the residential gateway entity (QoS_{RGW}) in Figure 3 is located on top of the AAA client. In the case RADIUS is used, vendor specific attributes could be used to exchange QoS profile information. This requires a connection between the AAA server and the capacity allocation database, which together represent the entity (QoS_{AAA}). After a successful authentication, the QoS element QoS-RGW checks whether the newly arrived station can be added from a QoS point of view and determines the gross capacity this station is allowed to consume during its presence. This check takes into account the QoS profile information received for the QoS_{AAA} and also takes place when a station wants to roam to a neighbouring RGW. To prevent that a lack of capacity results in a denial of connectivity, capacity can be reserved for roaming users. Note that this solution does not assume an explicit security solution. A web server running on the RGW can receive and consequently pass user credentials to the AAA server, or this can be realised by a security client in the RGW that terminates IEEE 802.1X.

The QoS element QoS_{RGW} determines the capacity (gross data rate at IP level) each station can use and subsequently splits the value into two (not necessarily equal) parts: upstream and downstream. How the gross data rate can be determined will be explained in Section 3.1.

The upstream capacity that can be consumed by a station is subsequently communicated to the QoS element QoS_T. This could be realized as part of the authentication process, or directly. The latter requires a separate protocol but it also allows communicating QoS boosts and updates. Various candidate protocols exist to realize this (e.g. RSVP; IntServ). From the WLAN QoS point of view, an AP can also be treated as a station and is therefore informed about the maximum downstream capacity that can be used for each station. The maximum WLAN capacity that can be consumed by the AP therefore equals the sum of all downstream capacity values of all stations belonging to the basic service set. All downstream WLAN traffic (destined to either visiting or residential stations) compete with one other based on their IEEE 802.11e/WMM priority level. Section 3.1 explains details on how the QoS_{RGW} determines the values.

2.3 Traffic regulation

Traffic regulation consists of two components, namely traffic policing and traffic shaping. Traffic policing occurs when the received traffic rate reaches the predefined maximum rate and drops excess traffic. In contrast to policing, traffic shaping retains excess packets in a queue and then schedules the excess for later transmission over increments of time to prevent the traffic being discarded by a traffic policer. Traffic shaping takes place at external network boundaries (terminal to RGW, RGW to network) whereas traffic policing takes place at the internal network interface boundaries: in the RGW to police traffic from visiting users and in the access network to police traffic from a RGW. Traditionally, traffic policing takes place at the entrance of the network to be capable of dimensioning the network properly and to protect the network against high bursts of packets. The wireless part of the home spot solution consists of sharing both the up- and the downstream transmit capacity among all users. Guaranteeing a part of the shared WLAN capacity to a station means managing the total WLAN transmit capacity and hence it requires traffic policing in both the upstream and in the downstream directions. Apart from determining the data rate that can be granted to visiting users, the actual capacity consumption needs to be compared with the capacity granted. Traffic controllers (TCs), located in the terminal, the residential gateway and in the access network realize this and can be instructed by the QoS elements.

Upon reception of the maximum capacity that can be used, the QoS elements communicate this parameter with the appropriate TC, which regulates the traffic. For the internal instructions from QoS elements to TCs, various protocols could be used. Note that the TC and the QoS elements may coincide in a single box, which is the case in the RGW. Appropriate settings for each TC are calculated based on given capacity reservations for the residential users, the sum of the subscription capacity of the granted visiting users and the available capacity in the access network. Section 3.2 provides more insight into how this can be realised.

2.3.1 Regulating upstream traffic

The TC located in the terminal is instructed to shape all upstream traffic to prevent that the upstream rate exceeds the capacity granted to QoS_T. The shaping of traffic in the terminal can be realized by applying well known shaping algorithms, performed by e.g. the windows traffic controller API (see [10]) and it can be combined with applying the 802.11e traffic admission controller functionality. The TC in the RGW, instructed by the QoS element QoS_{RGW}, polices upstream traffic to discourage stations to exceed the designated data rate. In the domain of the access network provider, a TC located in the access router polices the upstream traffic received from each residential gateway according to the sum of the parameters exchanged between QoS_{RGW}, and QoS_{AAA}. Standard mechanisms (e.g. the traffic control part of the Linux operating system) can be used to realize these policing actions.

2.3.2 Regulating downstream traffic

The downstream TC is challenged to regulate the traffic according to the total downstream capacity provided by the QoS element QoS_{RGW} in such a manner that only stations that are about to receive more downstream traffic than was assigned to them, are penalized. This rules out the possibility of shaping, as the shaping of downstream traffic enforces a minimum time between two consecutive WLAN packets and therefore increases the queuing delay of all packets stored, possibly destined for various stations. This could be avoided by assuming separate queues for each station. However, this is not realistic from a practical/implementation point of view. Just as

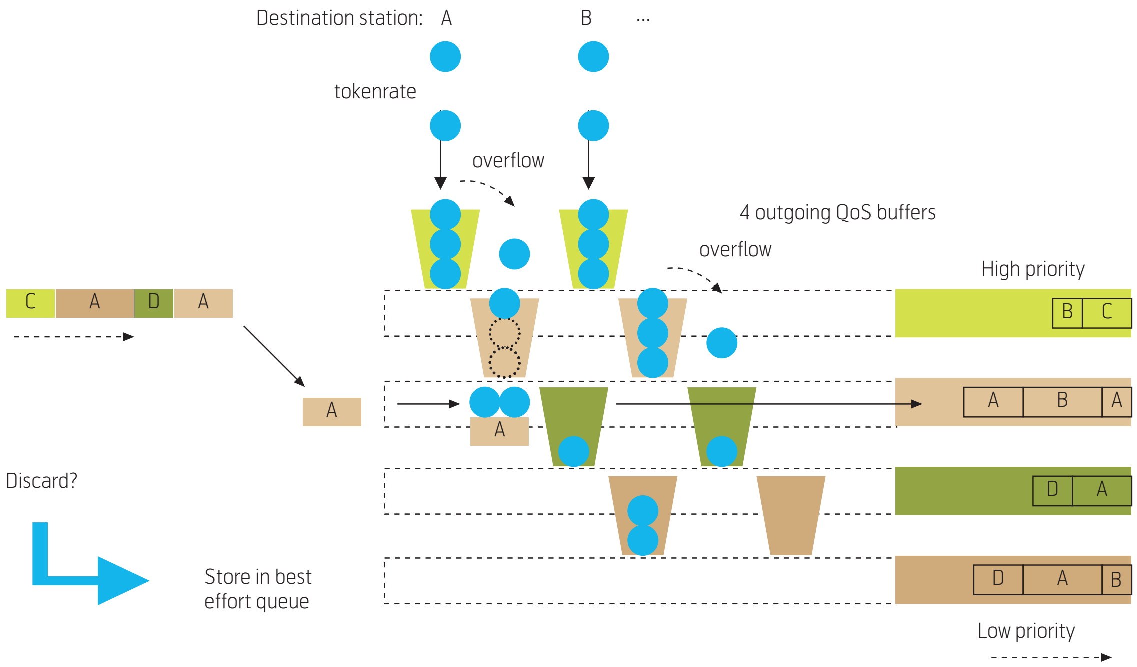


Figure 2 Downstream policing in the access point using cascade leaky buckets

ISSN 0085-7130 © Telenor ASA 2006

regular WLAN stations, the AP (but also the router in the RGW) can be equipped with queues to buffer various traffic classes, independently of the destined station. WLAN is the shared medium and the undesired situation that best effort packets consume transmit opportunities in favour of high and real-time priority traffic need to be avoided. The solution for downstream regulation is found in a cascade of token buffers per destination. Each high priority traffic class has its own token buffer that determines autonomously whether packets are conformant and can proceed to one of the outgoing buffers, or should be treated as non-compliant and should be degraded to the lowest priority class, i.e. best effort. Figure 2 depicts this situation in the case of four traffic classes, and consequently four output queues.

Each destination has four token bucket levels, each policing traffic for a corresponding priority class. The token bucket of the highest QoS class is fed with a token rate that corresponds with the allocated downstream capacity for the destination. Each token bucket has a limit and if the bucket overflows, tokens flow into the second bucket, which corresponds with the second highest QoS class, etc. Bucket sizes may be different for different QoS classes, corresponding to different allowed burst sizes for different QoS classes. The token rate is determined by the Capacity Distribution Algorithm (CDA), explained in Section 3.1.

Upon arrival of a packet travelling in the downstream direction, the token buffer of the destined station for the corresponding QoS class is checked. If the number of tokens in the bucket equals or is larger than the packet size, the packet is considered compliant and is stored in the corresponding QoS output queue. The token level is subsequently reduced by the size of the packet. If the number of tokens in the bucket is less than the packet size, the packet is considered to be non-compliant. As dropping of the packet would be too drastic (after all, the packet has traversed its way through the network and almost reached its destination) and if the token level allows, the packet is stored in the best effort queue. The best effort queue is emptied only if the three other QoS queues are empty (enabling truly best effort), or alternatively a round robin or weighted fair queueing discipline could be used to serve the queues. To maximize the usefulness of high priority packets that were found incompliant, one may consider serving the best effort queue according to a last-in-first-out discipline. Counters that do not require much memory or processing can implement the token rates and token buckets and hence their number can easily be increased.

Both capacity granting and policing must be based on the gross capacity (considering both payload and overhead) as will be explained in the next chapter. The traffic classes used in the WLAN need to be mapped to the classes used in the fixed broadband access network, and vice versa [4].

3 QoS solution in the residential gateway

The fundamental problem with offering an acceptable level of QoS on for example WLAN is that wireless network resources are scarce and thus need to be distributed over the stations effectively. The resources not only need to be (re)distributed; the entity that determines it also needs to (instruct to) check whether the stations consume according to the resources allocated. Finally, the channel conditions need to be monitored and action need to be taken if the committed profile granted to a station cannot be met because of changing channel conditions. These three fundamentals work together in close conjunction and are realised in the QoS$_{RGW}$ whose complete set of components is depicted in Figure 3.

Figure 3 depicts the QoS$_{RGW}$ architecture, consisting of a total of four components. The core component glues together the internal components and is the only one with access rights to write information in the user database. The QoS user database stores the user name, MAC and IP addresses as well as the QoS subscription and the assigned data rate of a station. The core component also offers interfaces to other RGW components such as the traffic controller, the DHCP server, the GUI and the QoS plug-in build on top of the security client.

As the name suggests, the component named “terminal communication” communicates the assigned data rate with the WLAN stations. The main functionality of the QoS$_{RGW}$ is realized by the components named *capacity distribution* and *capacity maintaining*, discussed separately in the remaining subsections.

3.1 Capacity distribution

The elements in the QoS profile are defined such that it matches requirements for real-time services. The subscription of a visiting user can consist of various QoS Profiles that can reflect different QoS levels (e.g. different levels of VoIP qualities, video transmission codec, low/medium/heavy web browsing, or a combination). If there is not enough WLAN capacity to guarantee the QoS Profile that corresponds to the highest rate, a QoS Profile that corresponds to a lower gross data rate can be selected. Knowing the two parameters of each profile, the corresponding WLAN capacity usage is based on the corresponding IEEE 802.11 transmission cycle. For both the upstream and the downstream direction the transmission

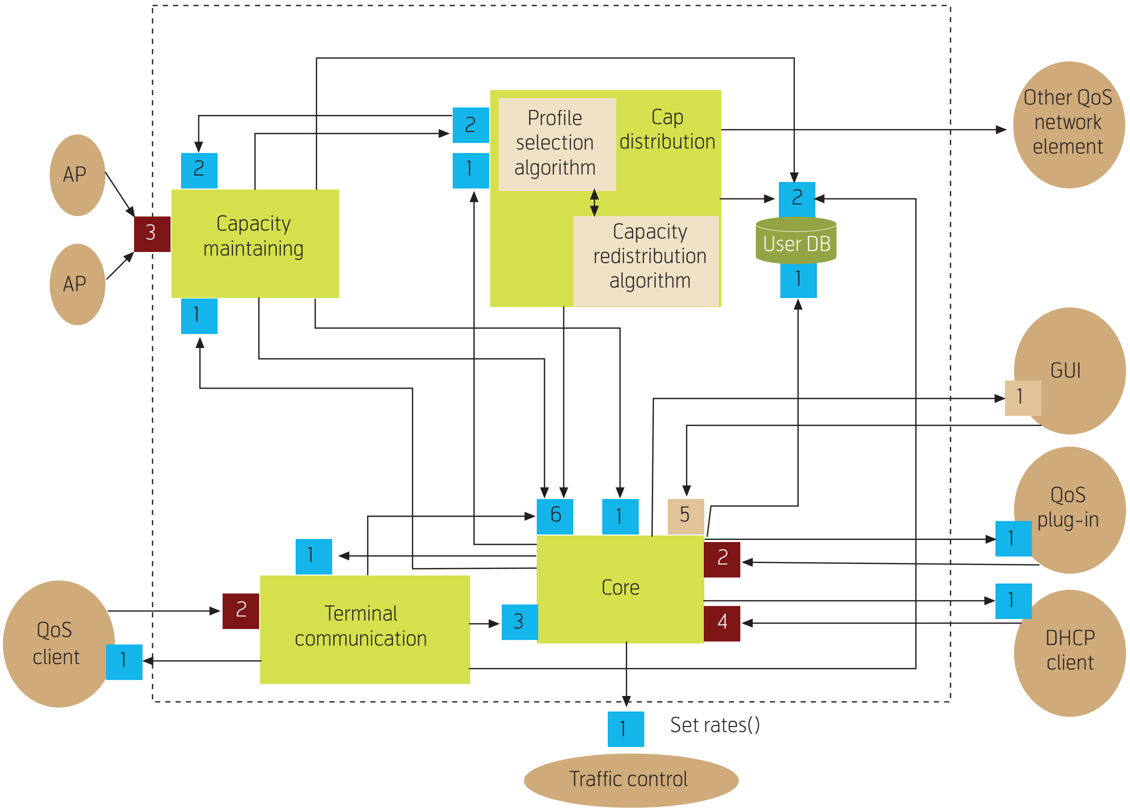


Figure 3 Component view of the QoS solution in the residential gateway

cycle is computed and subsequently used to estimate the WLAN capacity usage if that particular QoS Profile is committed. Figure 4 illustrates the WLAN transmission cycle in the case of sending 640 bits voice data. The packet frequency of the profile dictates how often the transmission cycle is repeated.

Each family of WLAN protocols (i.e. IEEE 802.11a/b/g) has their own overhead, which depends on the station's transmission speed. Stations using the IEEE 802.11a standard use the 5 GHz band and do not experience presence of IEEE 802.11b/g stations, which operate in the 2.4 GHz band. The performance of the IEEE 802.11g users is influenced if IEEE 802.11b users share the same WLAN access point. Based on each element out of the QoS profile (mean packet size, BPP, mean packet frequency, PPS) and the station's transmission speed TS, the CDA computes the WLAN transmission cycle based on the nature of the WLAN stations as shown in Table 2 (assuming an IEEE802.11g access point). The Transmission Speed (TS) can be obtained from the Capacity Maintaining component just as the type (a/b/g) of station and the configured BSS basic Rate Set. Note that the WLAN reservation RTS/CTS may be applicable here, as the home spot solution may have to serve stations over a wide area and likely has to cope with the well-known WLAN hidden node problem. The CDA can cope with this by incorporating the overhead associated with RTS and CTS in the transmission cycle. The formulas in Table 2 do not include this.

The CDA computes the associated WLAN capacity with each element of the QoS profile. The highest element of the QoS profile that does not contribute to a predefined capacity level is subsequently assigned to the committed profile. The peak profile can be the name-value of the QoS profile that associates the highest rate, which may be the same as the committed profile. The peak profile will be used by the traffic controller to police the station whereas the committed profile is forwarded to the *capacity maintaining* component.

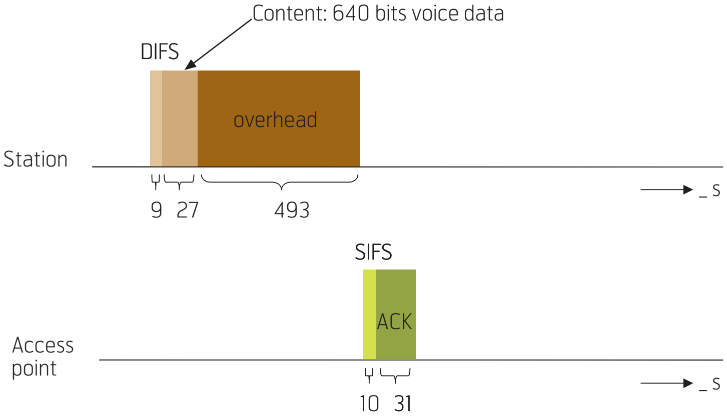


Figure 4 IEEE 802.11g transmission cycle (on scale) to send 80 bytes payload at a transmission speed of 24 Mbit/s

Station type	Formula used to compute WLAN consumption in one direction of a QoS Profile specified by mean BBP and mean PPS
802.11a	(DIFS + DATA + ACK + SIFS + CW) * PPS Where: $DATA = \left\lceil \frac{BPP * 8 + 352 \text{ (overhead IP + RTP/UDP, TCP)} + 256 \text{ (MAC)}}{216} \right\rceil * \frac{216}{TS} + 24 * 10^{-6} \ (PLCP)$ $ACK = \left\lceil \frac{112}{216} \right\rceil * \frac{216}{\min(TS, \ \max(IEEE802.11aBSSBasicRateSet))} + 24 * 10^{-6} (PLCP)$ DIFS = $34 \cdot 10^{-6}$ SIFS = $16 \cdot 10^{-6}$

802.11b	(DATA + ACK + DIFS + SIFS + CW) * PPS
	Where:
	DATA = {BPS * 8 + 352 (overhead IP + RTP / UDP; TCP) + 256 (MAC)} / TS + 192 · 10^{-6} (PLCP)
	ACK = 112 / min(TS,max(IEEE802.11b BSSBasicRateSet)) + 192 · 10^{-6} (PLCP)
	DIFS = $50 \cdot 10^{-6}$
	SIFS = $10 \cdot 10^{-6}$

802.11g	(DATA + ACK + DIFS + SIFS + CW) * PPS Where: $DATA = \left\lceil \frac{BPP \ * \ 8 + 352 \text{ (overhead IP + RTP/UDP, TCP)} + 256 \text{ (MAC)}}{216} \right\rceil * \frac{216}{TS} + 26 * 10^{-16} (PLCP)$ $ACK = \left\lceil \frac{112}{216} \right\rceil * \frac{216}{\min(TS, \ \max(IEEE802.11aBSSBasicRateSet))} + 26 * 10^{-6} (PLCP)$ DIFS = $9 \cdot 10^{-6}$ SIFS = $10 \cdot 10^{-6}$
+802.11b +802.11g	(DIFS + [CTS (to self) + PLCP] + SIFS + DATA +SIFS + ACK + CW) * PPS Where: $DATA = \left\lceil \frac{BPP \ * \ 8 + 352 \text{ (overhead IP + RTP/UDP, TCP)} + 256 \text{ (MAC)}}{216} \right\rceil * \frac{216}{TS} + 26 * 10^{-6} (PLCP)$ $ACK = \left\lceil \frac{112}{216} \right\rceil * \frac{216}{\min(TS, \ \max(IEEE802.11aBSSBasicRateSet))} + 26 * 10^{-6} (PLCP)$ CTS = 112 / min(TS,max(IEEE802.11b BSSBasicRateSet)) (CTS to self @ max. 11 Mbit/s) + 192 · 10^{-6} (long PLCP header) DIFS = $50 \cdot 10^{-6}$ SIFS = $10 \cdot 10^{-6}$

Table 2 Formulas used to compute a station's WLAN resource consumption

Based on the QoS policy, the Capacity Distribution Algorithm (CDA) estimates the WLAN consumption by computing the transmission cycle in both upstream and downstream directions. The WLAN consumption associated with each QoS Profile can be sorted and ranked. The peak profile selected should always have a ranking larger than or equal to the ranking of the committed profile. A QoS policy dictates which rule should be followed to assign a QoS Profile to a certain visiting user. Only one QoS policy can be active at the same time and examples of QoS policies include maximizing the number of admitted highly ranked visiting users (gold/silver/bronze status, simply reflected in rate associated with their QoS profiles), maximizing the total number of visiting users and the optimization of the WLAN resources.

As an example, consider a QoS Profile for high quality voice, using the G711 codec with 10 ms voice samples, corresponding with a WLAN payload of 80 bytes and a packet frequency of 100 packets/s. If an IEEE802.11g station authenticates and the AAA server informs the RGW that the QoS Profile is part of the subscription, the CDA computes the corresponding formula in Table 2, resulting in 0.017, equivalent to a 1.7 % consumption usage in one direction. If adding this number to the sum of the consumption of all committed profiles assigned to that direction in the past does not pass a pre-defined threshold (that can dictate the multiplexing gain), the CDA decides that this high quality QoS Profile can be committed. If not, a less demanding QoS Profile may be selected. The peak profile is subsequently communicated with the traffic regulation mechanisms to adjust the token rates and the committed profiles with the capacity maintaining component to guarantee the rate. The order of the stations to compute the WLAN consumption is dictated by the QoS policy. Various QoS policies can be distinguished that should reflect the user expectations. Examples include: maximize network resources, maximize the total number of users, prioritize the home users, and prioritize the most valued users (those who have the most expensive subscription).

3.2 Capacity maintaining

Once the CDA has computed the committed profile and calculated the associated committed rate for a newly arrived station, this profile should (under acceptable conditions) be guaranteed to the station. If, however, the station moves away too far from the access point, the signal is simply too weak to guarantee the committed rate. In this case the station's committed rate can be changed and consequent actions must be taken if the action results in insufficient network capacity (handover to neighbouring home spot, moving close to the AP).

Local WLAN variables of the access point are measured to gain insight into channel conditions. Based on these measurements, the Capacity Maintaining component monitors if the committed profiles can be met for each associated and authenticated station. Besides comparing the monitored channel conditions, one can use the information to predict whether the channel conditions can support the committed profiles in the near future. Several options for channel prediction have been considered and two mechanisms that provide a reasonable trade-off in terms of complexity and performance are further explored. The selected prediction mechanisms include a linear prediction based technique, taking as input the measured goodput of the time series, and a two state Gilbert-Elliot channel modelling, [12] and [13]. For linear prediction, an order recursive and very efficient algorithm, namely the Levinson-Durbin algorithm can be used to predict the coefficients and identification of statistical ill conditions that may exist in the estimate of the autocorrelation matrix due to time averaging. Finally, Hidden Markov Models (HMMs) could be used for channel prediction, although complexity of the algorithms inhibits their use with the exception of the Gilbert-Elliot model that may be viewed as a simplified HMM. If the prediction is such that the committed rates cannot be maintained in the near future, an alarm is generated towards the CDA that in turn redistributes the capacity over the various visiting stations.

If the capacity maintenance component decides that either a station's committed rate cannot be met or predicts that this rate cannot be met in the near future, it informs the distribution algorithm which in turn recalculates how the WLAN resources should be distributed over all stations. To guarantee convergence towards an acceptable QoS level, the advice given by the CDA as a result of a request for redistribution should differ from the previous advise.

The network commitment should be defined at the IP level such that users can continue their applications that require network connectivity with minor degradation. At the WLAN level, the airtime consumption depends on various factors, and the solution presented shows how the use of QoS profiles and the combination of network monitoring and capacity redistribution can minimize the impact of these factors on the user's quality of service experience. However, without 100 % WLAN coverage, it is unavoidable that users will experience network degradation if they move too far from a WLAN access point.

4 Conclusions

This paper argues that since WLAN is gradually moving in the enterprise and public areas, and in order to be part of the overall network convergence that takes place, the need for QoS increases. The paper shows how in WLAN available resources can be shared among all stations in an efficient manner and in such a way that it leads to predictable resource consumption in the wireless access network. Although the QoS solution described in this paper is generic of nature, it is applied to a specific use case, namely to guarantee QoS to users who casually pass a WLAN equipped home and can utilize the remaining part of the fixed line broadband access line capacity. The admittance of the number of visiting users is limited such that an acceptable and configurable level for the residential user is maintained. The assigning of resources to each visiting WLAN user is based on subscription information obtained from the network. A QoS policy at the residential gateway can be used to dictate how the capacity distribution algorithm should optimize WLAN resources, e.g. maximize the number of home stations, or maximize the total number of allowed stations, or maximize WLAN resource usage. An important and integral aspect of the QoS solution is that it maintains the quality level assigned to a station. To reach this goal, the channel conditions are monitored and a mechanism that predicts whether the committed rate assigned to a certain station can be obtained. If not, the capacity distribution algorithm is informed and re-calculates how the WLAN resources should be distributed over all users, obeying the local QoS policy.

Acknowledgments

This work was carried out as part of the OBAN project funded in part by the European Commission. The authors thank Jeroen van Bemmel (Lucent Technologies) for, among other things, his ideas to integrate QoS with security; Fred Danishgaran (Euro concepts) for his prediction ideas in the capacity maintaining component; and Willem Romijn (Lucent Technologies) for reviewing early versions of this manuscript.

5 References

1 Anderson, C. The Wi-Fi Revolution – The wireless Internet has arrived – and now the sky's the limit. *Wired Magazine*, Issue 11.03 Unwired, May 2003.

2 Chu, O. Taiwan soon to be WLAN-connected land. *Taiwan Journal*, 15 October, 2004.

3 Zhu, H, Li, M, Chlamtac, I, Prabhakaran, B. A survey of quality of service in IEEE 802.11 networks. *IEEE Wireless Communications*, August 2004, 6–14.

4 Park, S-Y et al. Collaborative QoS Architecture between DiffServ and 802.11e Wireless LAN. *Proc. IEEE VTC '03-Spring*, Jeju, Korea, April 2003.

5 CISCO white paper. *Capacity Coverage & Deployment Considerations for IEEE 802.11g*. 2006, October 24 [online] – URL: http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_white_paper09186a00801d61a3.shtml

6 Roshan, P, Leary, J. *802.11 Wireless LAN Fundamentals, a practical guide to understanding, designing and operating 802.11 WLANs*. Cisco Press, 2004.

7 Francis, J C. Open Broadband Access Networks. *Comtec Jour.*, Bern, 5/2004.

8 Francis, J C, Schneider, J. Towards Mobile Broadband. *Lecture Notes in Computer Science*, 3420, 2005.

9 Zhang, L, Berson, S, Herzog, S, Jamin, S. *Resource ReSerVation Protocol (RSVP)*. IETF RFC 2205, Sep 1997.

10 *QoS Traffic Control in Windows 2000, Window TC API*. 9 August 2006 [online] – URL: http://support.microsoft.com/

11 Medepalli, K, Gopalakrishnan, P, Famolari, D, Kodama, T. Voice capacity of IEEE 802.11b, 802.11a and 802.11g Wireless LANs. *Proceedings of IEEE GLOBECOM*, Dallas, TX, 29 Nov – 3 Dec 2004.

12 Gilbert, E N. Capacity of a burst-noise Channel. *Bell Syst. Technical Journal*, 39, 1253–1265, Sept. 1960.

13 Elliot, E O. Estimates of error-rate for codes on burst-noise channels. *Bell Syst. Technical Journal*, 42, 1977–1997, Sept. 1963.

14 Hoekstra, G J, Østerbø, O, Schwendener, R, Schneider, J, Panken, F J M, van Bemmel, J. QoS solutions for open wireless access networks. *IST summit*, Dresden, June 2005.

15 *IEEE 802.1Q Standards for Local and metropolitan area networks Virtual Bridged Local Area Networks*. IEEE Computer Society, 7 May 2003.

16 Rigney, C, Willens, S, Rubens, A, Simpson, W. *Remote Authentication Dial In User Service (RADIUS)*. RFC 2865, June 2000.

For a presentation of Frans Panken, please turn to page 58.

For a presentation of Gerard Hoekstra, please turn to page 60.

Sietse van der Gaast received his MSc degree in computer science from the University of Twente, Enschede, the Netherlands in 1994. He works for Bell Labs Europe, Lucent Technologies in Hilversum, the Netherlands. His recent activities include research on efficient content distribution techniques, end-to-end quality of service in next-generation networks, modelling the perceived quality of web browsing and quality of service in Wi-Fi home-spots. Sietse van der Gaast is rapporteur in ETSI-TISPAN in the area of SIP and IMS, and previously worked on user interface design and implementation, firewall control protocols, voice over IP architecture and prototyping, and open API prototyping for service platforms.

An EAP-SIM Based Authentication Mechanism to Open Access Networks

CORRADO DERENALE, SIMONE MARTINI

Corrado Derenale is Software Engineer in Motorola

Simone Martini is a Technology Specialist in Motorola

Given the diffusion of cellular phones and WLANs, using mobile phones as authentication devices to allow a mobile terminal (laptop, PDA or PC) to log into a WLAN network would be an easy and secure means for final users. Wireless Service Providers are proposing solutions that exploit GSM Subscriber Identity Modules (SIMs) for network authentication, but the proposed solutions require buying ad-hoc SIM cards and separate smart card readers, without being able to exploit mobile phones.

In this paper we provide a way to override the requirement of additonal SIM and hardware by defining a mechanism and a corresponding interface so that a mobile terminal can use a mobile phone and its stored SIM credentials to get authenticated into an Open Access Network layered on top of a WLAN.

The solution proposed in this paper exploits the EAP-SIM [5] authentication protocol that provides the authentication steps and defines the information needed to authenticate a client by the credentials retrieved from a SIM card.

1 Introduction

Nowadays, Service Providers (SPs) offer three main categories of services to their subscribers: (i) network access, (ii) data transport and (iii) added value services, but get revenues from the latter two only. Wireless Internet SPs (WISPs) are emblematic examples. They get revenues from data transfer and added value services, compete on price and quality of those two categories of services, but nevertheless they must operate and maintain also their own access network to provide access to their customers.

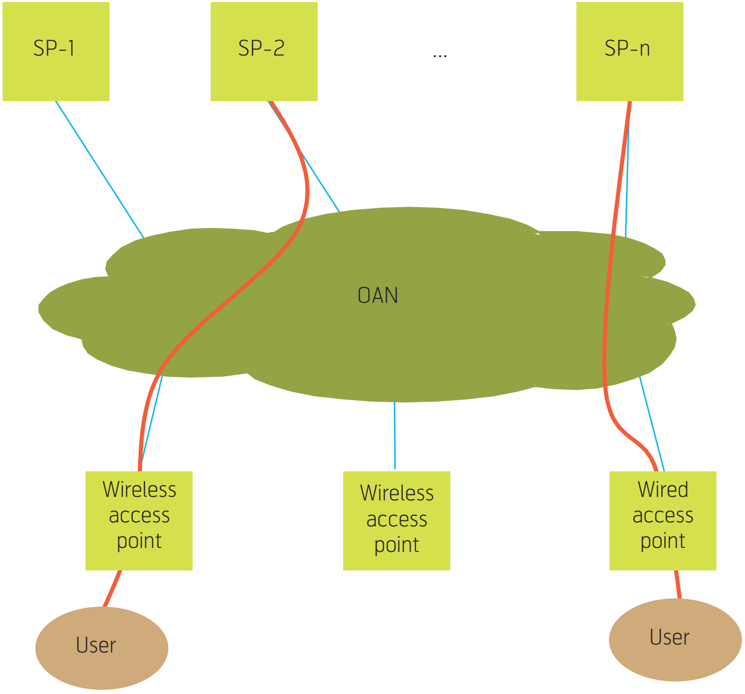


Figure 1 OAN architecture

Open Access Networks (OANs) are a means to separate SPs from access networks. They are shared by multiple SPs and provide network access to end users, as depicted in Figure 1. OANs are not related to a specific SP and consequently are not bound to a geographic area covered by an SP. This characteristic makes OANs of particular interest for nomadic or mobile users, who can obtain access to their service providers from an extended area of coverage, no more related to the specific geographical boundaries physically covered by their SPs.

Currently there are mainly two different business models behind OANs. One foresees private or public companies managing and operating OANs, getting revenues from SPs or public grants. The other foresees the spontaneous expansion of OANs by exploiting the unused bandwidth at the border of the network. In this latter case, the OAN is built by access points (e.g. Wi-Fi access point) that residential Internet users install at home and do not fully exploit. In fact, most of the time, domestic or SOHO users do not use all the bandwidth they pay for, so that they can re-sell it to the SPs (see Figure 2).

The IST OBAN [1] project and the FON Movement [2] are two examples of OANs built exploiting the users' unused bandwidth. In the OBAN vision home users provide the OBAN SP with their unused bandwidth, and mobile users having a contract with the OBAN SP can access their services through the nearest OBAN enabled access point.

Access to OANs will be authorized by an SP only if the requiring entity has a contract or specific permission. SPs are in charge of authenticating their users before granting them access authorization. The

ISSN 0085-7130 © Telenor ASA 2006

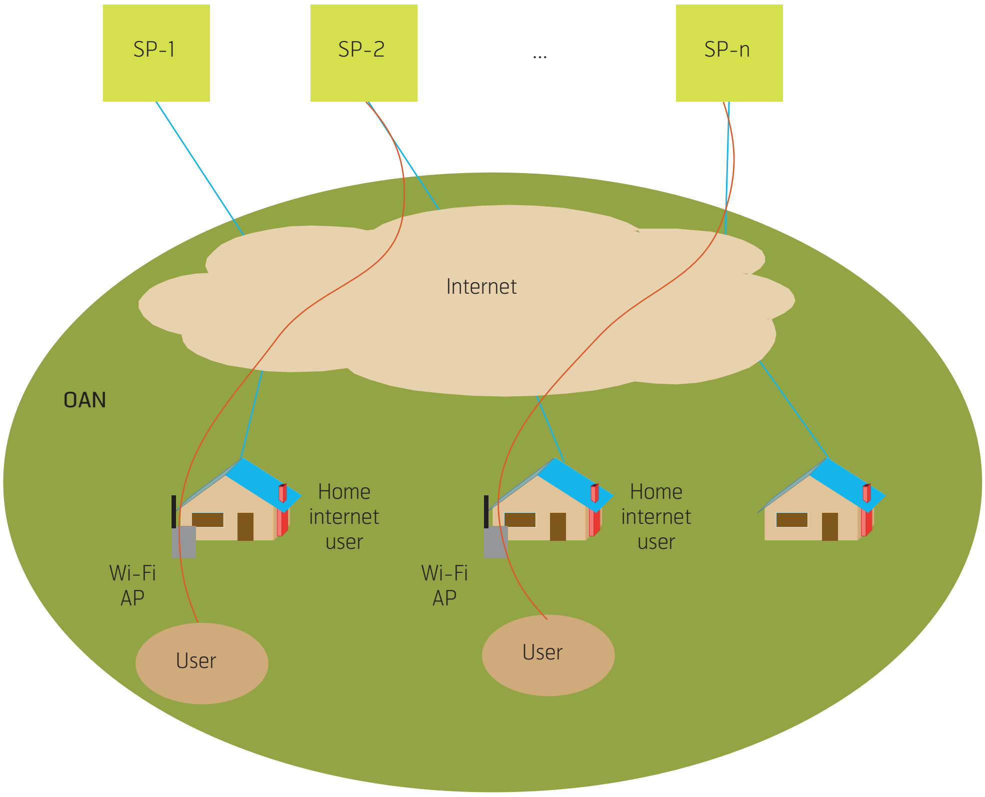


Figure 2 Building OAN by exploiting the unused bandwidth

authentication process adopted must be strong enough to protect SPs and users from fraud, but must also be easy to perform by any user. A user-friendly mechanism can be achieved by exploiting a technology that users are already accustomed with. The user-friendly authentication method proposed in this paper exploits the credentials stored in the SIM cards to provide a strong mutual authentication between the SP and the mobile users wishing to access the OAN, and exploit the mobile phone as a way to access the SIM credentials.

This approach provides an authentication mechanism familiar to the users, but stronger than a simple username and password. In the username/password method the authentication is related only to something that the user knows: the username/password pair. In the proposed mechanism the authentication is related to something that the user knows (the Personal Identification Number (PIN) required to unlock the SIM), but also to something that the user owns: the SIM card storing the authentication credentials.

The paper is organized as follows: section 2 presents the operational scenario and the enabling technologies on which the proposed solution is based, section 3 provides a description on how the EAP-SIM Standard mechanism can be used to get authentication from SP, and section 4 presents a possible future evolution of the proposed solution in the OBAN vision.

2 Operational Scenarios

The authentication mechanism presented in this paper exploits a method of the Extensible Authentication Protocol (EAP) [3]. This paragraph describes the IETF EAP protocol, the EAP-SIM method and other enabling technologies.

2.1 The EAP framework

EAP is a framework developed by the IETF to transport authentication mechanisms and to export key materials. It is a request/response messages protocol where the number of the messages exchanged depends on the chosen authentication method. EAP was originally designed in 1998 to support the authentication over a PPP link but was swiftly adopted by many emerging and some consolidated technologies. Examples of emerging technologies adopting EAP are: Wireless Protected Access (WPA) for Wi-Fi and WiMax networks. Examples of consolidated technologies are IPsec via Internet Key Exchange protocol version 2 and Ethernet via the Port-Based Network Access Control protocol [6] (see Figure 3).

The growing consensus toward the adoption of EAP in so many emerging and consolidated technologies is due to its main benefits:

- Independence from the lower layers;

- Independence from the authentication method, it supports multiple authentication mechanisms;

- It can be used in situations where IP is not available (e.g. over the IEEE802.11 before IP connectivity is granted);

- The Network Access Server (NAS) does not need to implement the authentication algorithms; it can work as a pass-through node;

- NAS and the Authentication Server (AS) are decoupled, the AS can be installed in the back-end.

Figure 4 depicts a common EAP scenario involving the entity requiring authentication, the Authenticator (e.g. the Network Access Server), and the Authentication Server (AS), that verifies the supplicant identity and decides if the Authenticator can grant network access. As an example, Figure 4 – (a) shows the EAP-MSCHAP method (Microsoft Challenge Protocol) while Figure 4 – (b) shows the EAP-TLS (Transport Layer Security). The only difference between them is the authentication method, all the other layers below are the same in both configurations.

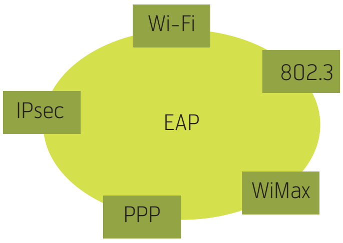


Figure 3 EAP exploitation

The Wi-Fi Alliance [4] adopted the IEEE802.1x along with the EAP framework as a means to authenticate users to establish a Wi-Fi Protected Access (WPA). EAP-SIM is included in the various EAP methods adopted by the Wi-Fi Alliance.

2.2 EAP-SIM Standard Mechanism

In January 2006 IETF ratified a 3GPP proposed EAP method, called EAP-SIM [5]. This method exploits the credentials stored in the GSM (Global System for Mobile Communications) Subscriber Identity Module (SIM), and the GSM security algorithms to provide authentication and session key distribution.

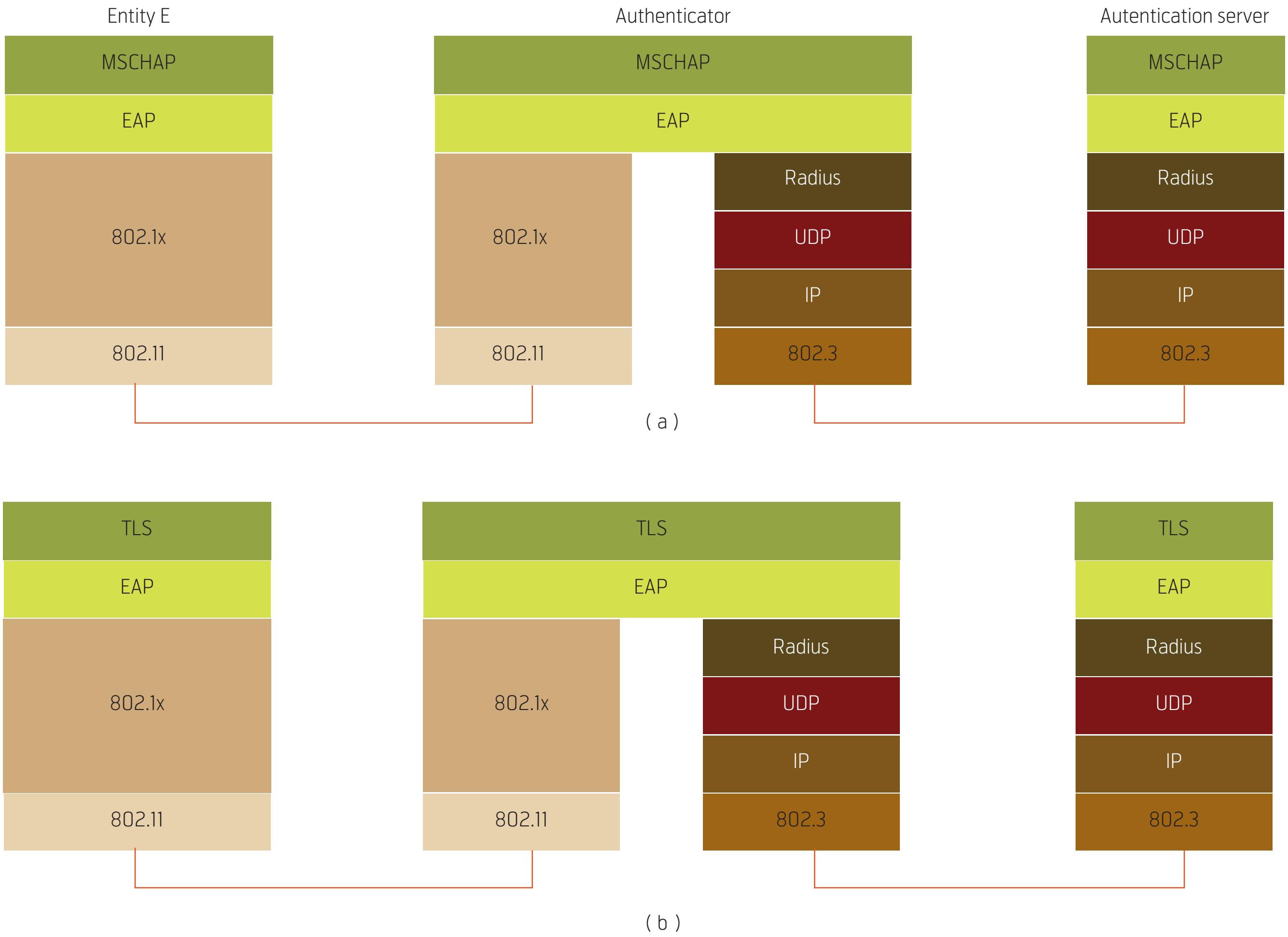


Figure 4 Common

ISSN 0085-7130 © Telenor ASA 2006

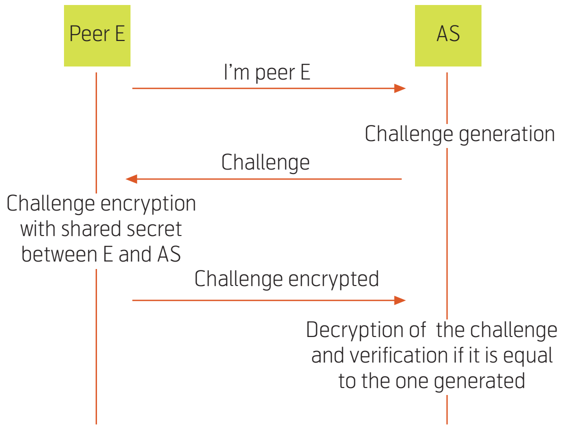

Peer E
AS
I'm peer E
Challenge generation
Challenge
Challenge encryption with shared secret between E and AS
Challenge encrypted
Decryption of the challenge and verification if it is equal to the one generated

Figure 5 Challenge/response mechanism

The GSM authentication mechanism is based on a challenge/response mechanism with shared key. In the challenge/response mechanism the Authentication Server (AS) and the entity (peer) that requires authentication share a common key, usually called shared secret. When an entity needs to be authenticated, it sends its identity, e.g. the username, to the Authentication Server. The AS, to ascertain that the entity is really who it claims to be, generates a random number and sends it back to the entity. If the entity is really who it claims to be, then it knows the shared secret and can encrypt the challenge sent by the AS. It encrypts the challenge and sends it back to the AS.

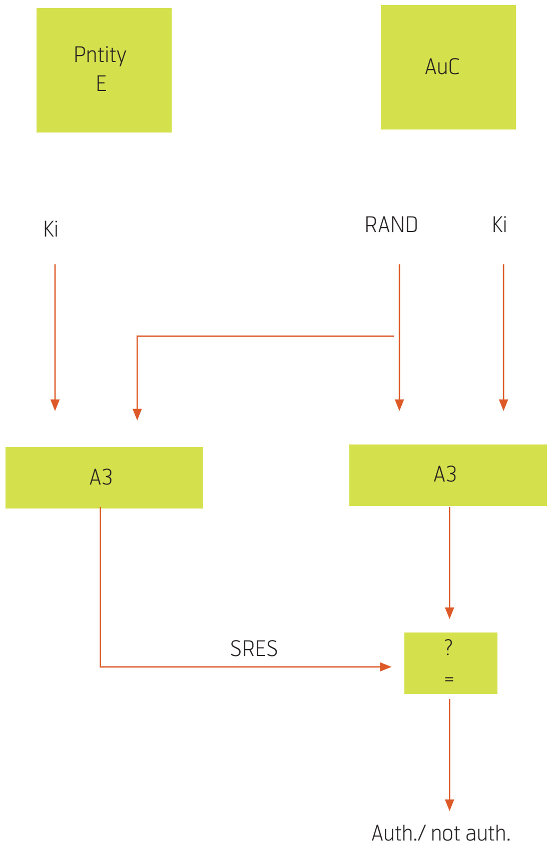


Figure 6 Authentication mechanism in GSM networks

The AS (that has the same key as the peer), decrypts the challenge and verifies whether the decrypted challenge is equal to the random number it has generated. If this is the case, the peer is authenticated. Figure 5 shows this challenge/response mechanism.

In GSM networks, the Authentication Center (AuC) shares a key (K_i) with the SIM: this is the shared secret between the user and the network used in the authentication challenge. When authentication is required, for example when the mobile phone performs a location update in a new Visitor Location Register (VLR), the AuC generates a random number (RAND) and sends it to the mobile. The SIM in the mobile applies the A3 algorithm on RAND and K_i. The result (Signed Response, SRES) is then sent back to the AuC that may authenticate the mobile by comparing the received response with the output of its own computation. Figure 6 shows this authentication procedure.

The key used to encrypt the data on the radio link, K_c, is generated from the K_i and the RAND number by running the A8 algorithm, see Figure 7. This key is sent by the AuC along with SRES and RAND to the VLR. These three numbers are known as Authentication Vector Response, or "the triplet".

EAP-SIM exploits the K_i as user credential and the A3/A8 algorithms running on the SIM to perform authentication and session key generation. The main players in an EAP-SIM exchange are the Peer requiring authentication, the Authenticator, the Authentication Server and the AuC. The first message is sent by the Authenticator asking for the peer identity with an EAP-Request/Identity message (Figure 8, step 1). The peer replies declaring its identity in the EAP-Response/Identity message (Figure 8, step 2). The authenticator then sends the list of EAP-SIM versions supported in the message EAP-Request/start (Figure 8, step 3).

At this stage the peer chooses the EAP-SIM version to be used and communicates it to the authenticator along with a random number in the EAP-Request/Challenge message (Figure 8, step 4). This random number is used to perform the mutual authentication, i.e. to authenticate the network to the peer. At this point, the Authenticator (upon receipt of the triplet from the AuC) sends the RAND to the peer along with the challenge response (Figure 8, step 5). The peer verifies the correctness of the response to the challenge and sends its response to the RAND challenge (Figure 8, step 6). Now the Authenticator verifies the response to the challenge received from the peer and, in case of successful verification, sends the EAP-Success message to the peer. This last message contains also the session key computed as a function of RAND, SRES and K_c. This key can be used to encrypt the communication between the peer and the authenticator.

2.3 Port Based Network Access Control IEEE 802.1X

The Port Based Network Access Control is a standard ratified by the IEEE in 2001 to permit access to IEEE 802 based LANs only after a successful authentication process [6].

According to this standard, access to LANs occurs through physical (e.g. the port of a switch) or logical points of attachment, as in Wi-Fi networks, called access ports. These access ports are controlled by a function able to open or close them, depending on the result of an authentication procedure. This procedure is carried by EAP layered over the IEEE 802.3 or IEEE 802.11, and can be of whatever type supported by EAP, like for example EAP-TLS, EAP-MSCHAP or EAP-SIM.

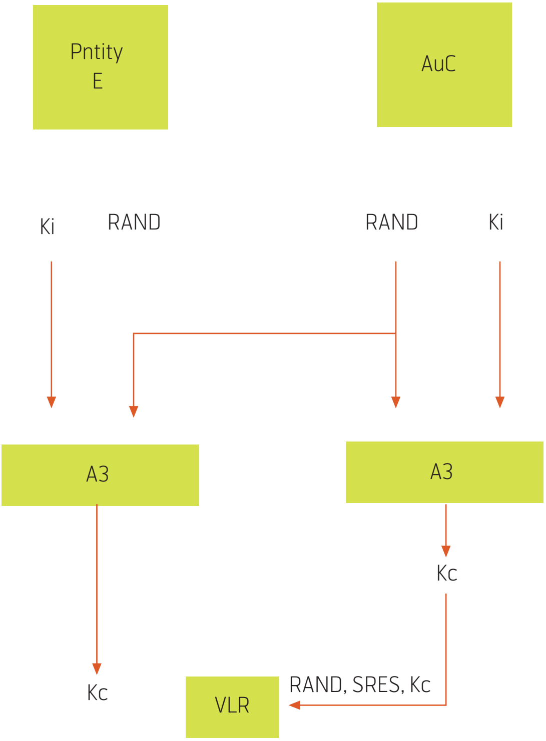
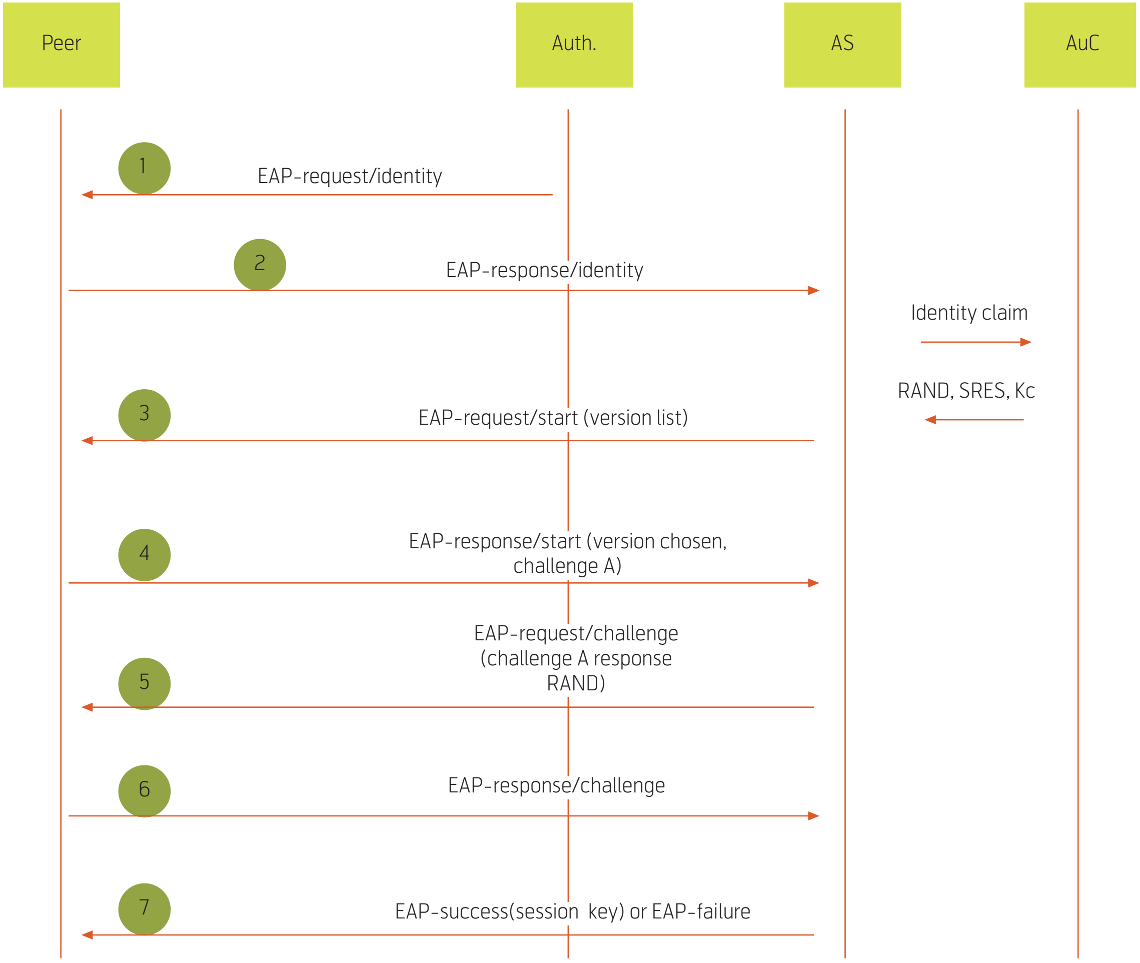


Figure 7 K_c and the "triplet"



Peer
Auth.
AS
AuC
1
EAP-request/identity
2
EAP-response/identity
Identity claim
RAND, SRES, Kc
3
EAP-request/start (version list)
4
EAP-response/start (version chosen, challenge A)
5
EAP-request/challenge (challenge A response RAND)
6
EAP-response/challenge
7
EAP-success(session key) or EAP-failure

Figure 8 EAP-SIM exchange

ISSN 0085-7130 © Telenor ASA 2006

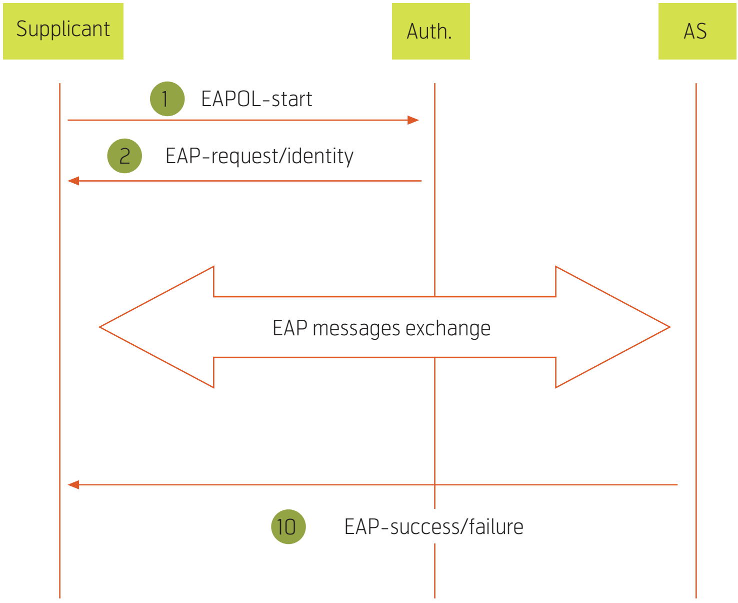


Figure 9 IEEE 802.1X messages exchange

The main players of this standard are the Supplicant, the Authenticator and the Authentication Server, as shown in Figure 9. The Supplicant is the entity requiring authentication. The Authenticator is the element that can block or open the access port to the Supplicant, based on the decision taken by a back-end Authentication Server. It is able to authenticate the Supplicant by running the chosen authentication procedure.

The IEEE 802.1X message exchange starts with the Supplicant sending to the Authenticator an EAPOL-Start message. The Authenticator responds by sending an EAP-Request Identity. This is the beginning of the EAP exchange, which lasts until the EAP-Success or EAP-Failure message is generated (see Figure 9). Note that the total number of messages exchanged depends on the chosen EAP method. If the EAP-method is the EAP-SIM, (see section 2.2) the total number of messages exchanged, including the EAPOL-Start, is 8.

3 EAP-SIM in a cellular environment

3.1 SIM Authentication Procedure in GSM systems

As described in section 2.2, in GSM systems the network authenticates the subscriber through the use of a challenge-response method. When a subscriber wants to start a conversation, the mobile station sets up a link to the base station and relays the IMSI (International Mobile Subscriber Identity) or TMSI (Temporary Mobile Subscriber Identity) from the SIM to the base station.

If the subscriber's IMSI registers at the base station, the mobile station receives the 128-bit random number (RAND) transmitted through the air interface and passes it to the SIM. It is then processed with the A3 algorithm together with the key K_i. The output of the A3 algorithm is the signed response (SRES). The result is a cipher text block, SRES, which is transferred from the mobile station to the base station via the air interface.

The network subsystem, which is linked to the base station, derives the card-specific key from IMSI and performs computation similar to the SIM and generates SRESes.

The SRES sent to the network subsystem is then compared with the SRESes to authenticate the subscriber and thus authorize him/her to set up a call. Background system and SIM use the A8 algorithm with the RAND number and the card-specific key (K_i) to compute the temporary ciphering key (K_c), which is used to encrypt data for transmission on the air interface. The computed key K_c is then passed from the SIM to the mobile station, which performs data encryption and decryption using the A5 algorithm. Eavesdropping the radio channel reveals no useful information, as the next time a new random challenge will be used. Authentication can thus be provided using this process. A random number is generated by the network and sent to the mobile. The mobile uses the Random number R as input (Plaintext) to the encryption, and, using a secret key unique to the mobile (K_i), transforms this into a Signed RESponse (SRES) (Ciphertext), which is sent back to the network. The network can check that the mobile really has the secret key by performing the same SRES process and comparing the responses with the ones received from the mobile.

3.2 SIM Standard Authentication Procedure in a GSM mobile phone

The communication and message exchange between the mobile phone and the SIM card is performed according to 3GPP TS 11.11 specifications [11]. As explained before, the key points of the authentication are the IMSI parameter and the result of the GSM authentication algorithm. The IMSI is a sensitive parameter but, in the authentication process, it acts logically as the username and, even if intercepted, does not allow hitchhikers to clone the SIM card. The intrinsic security of the whole authentication process comes from the impossibility to read, from something which is not the SIM card itself, the private key K_i (this operation is performed only by the GSM authentication algorithm). Furthermore, K_i is never sent over the air interface, only the result of the authentication algorithm is. As an additional security measure, the SIM card does not allow running the GSM algorithm an infinite number of times, but only a number of times large enough to cover the entire life of a few phones. This security measure avoids guessing the K_i by extensively trying all the possible combinations of the input parameters.

While the IMSI parameter can be easily retrieved from the SIM, by using the AT command set (the AT command for retrieving the IMSI is AT+CIMI, which is supported by most of the phones), the execution of the GSM authentication algorithm requires the use of lower level interfaces for smart cards (such as those defined by the PC/SC workgroup [9]) and their exposure to the external world: this is, generically, offered by the smart card readers.

In the framework of the OBAN project, the EAP-SIM authentication scheme has been implemented using a mobile phone. The use case developed foresees a user wishing to authenticate his laptop to a wireless LAN by reusing the credentials stored on the SIM card, without connecting the phone to the laptop with wires (using the Bluetooth interface, if available). The advantages arising from the implementation of such solution are several, both for users and telecom operators:

- *No need to buy a second and dedicated SIM card*. Since the phone becomes useless when the SIM card is not available in it, it is at present necessary to buy and use a dedicated SIM card for data traffic.

- *No need to connect an external smart card reader to the laptop*. Current solutions are based on smart card readers which have to be wire-connected to the laptop. Even if acceptable, this solution does not provide the same comfort as using a mobile phone.

- *User does not need to remember any login/ password*.

- *Authentication is performed by using the credentials stored on the SIM card and in the HLR of the operator*. This is of particular interest for telecom operators who are willing to provide Wi-Fi connectivity to their customers. Basically, with no or little effort on the network components, they can provide a reliable and secure authentication method.

- *Bluetooth frees the user from wires and provides a high degree of freedom*.

In the following paragraphs, when using the term PC or laptop, we will always consider Microsoft Windows XP as operating system. Later on, the rationale behind this choice will be discussed.

Being the target the usage of the mobile phone as an interface towards the SIM card the phone has to provide an interface similar to a smart card reader. There are different ways to achieve this goal:

- Writing a PC/SC compliant smart card driver (refer to [9]) for Windows XP which will transform the mobile phone into a real smart card reader;

- Make use of another protocol, such as the Bluetooth SIM Access profile, to have direct access to the SIM card in the phone.

The solution of a dedicated driver is mainly preferred if the phone is connected to the laptop through a wired USB or serial connection. In this case the driver is responsible for translating smart card commands and events coming from the operating system into the phone's internal operational codes. Implementing the second solution instead is more complex but provides a higher degree of user friendliness. For this reason, in OBAN we opted for the second alternative.

The particular implementation of EAP-SIM on which this document focuses is in the Wireless LAN environment. IEEE 802.1X provides a means for performing EAP-based authentication in an IEEE 802 environment (e.g. Ethernet, WLAN) using the port-based authentication. The software module developed as part of the OBAN Project provides the functionality to perform EAP-SIM authentication using the standard 802.1X authentication structure, by reusing the SIM card over a Bluetooth connection between the phone and the EAP-SIM supplicant running on a Windows XP computer.

3.3 The Bluetooth SIM Access Profile in the EAP-SIM authentication

The Bluetooth SIM Access Profile is a new profile and is not yet fully supported by Windows drivers. However, since it has the advantage of running over the Serial Port Profile (i.e., an emulated serial port over the Bluetooth wireless link), it can still be used with some small adaptations to the existing profiles. While waiting for a wider support on the laptop side, a still valid compromise is sending the messages of the SIM Access profile over the serial port emulated by the Bluetooth stack. This implementation allows not only to prepare the environment and the devices for a fully compliant support of the SIM Access Profile, but it also allows the implementation of the EAP-SIM authentication for devices which do not yet support this new profile.

The SIM Access profile defines two different entities, one acting as server (in the implementation described here the device containing the SIM Card and performing the role of smart card reader), the other acting as client (the EAP-SIM supplicant on the laptop) accessing the SIM card hosted in the server. The SIM Access Profile, by its own nature, is defined to enable all the scenarios currently supported by smart card readers, including:

- access to information stored in the SIM card such as the phonebook, short messages, appointments;
- registration of a client into the cellular network;
- e-payment.

The SIM Access Profile takes also into account the security of the communication link between the client and the server. This problem is specifically addressed in the profile requiring not only Bluetooth link ciphering, but also the support and use (by both client and server) of a key having the maximum length allowed by Bluetooth (64 bits). Furthermore, all security measures identified by the profile are mandatory.

Summarizing, the Bluetooth SIM Access Profile acts as a transport layer for the smart card commands and operational codes (which are usually referred to as T = 0 and T = 1 protocols) for the communication between the reader and the smart card. It is possible that in the near future, the SIM Access Profile will increase its importance as long as smart cards are gaining diffusion in e-wallet and digital signature applications. Although a detailed discussion about the security of an EAP-SIM authentication based on a wireless communication link between the supplicant and the mobile phone is beyond the scope of this paper, the authors would like to provide their feeling, primarily based on an objective and practical analysis of the system rather than on theoretical simulations. First of all, Bluetooth can provide the ciphering of the communication link. Someone could object that this is not secure enough, but this basic form of security can be increased to the extent to make it extremely difficult to decrypt the sensible parameters used in the EAP-SIM authentication. For instance (and this is just an example) a dedicated software module on the phone could be developed so that, when a paired device is requesting the retrieval of the IMSI or the execution of the GSM Authentication algorithm on the SIM, the data is ciphered with an additional algorithm, thus enforcing the strength and security of the whole solution.

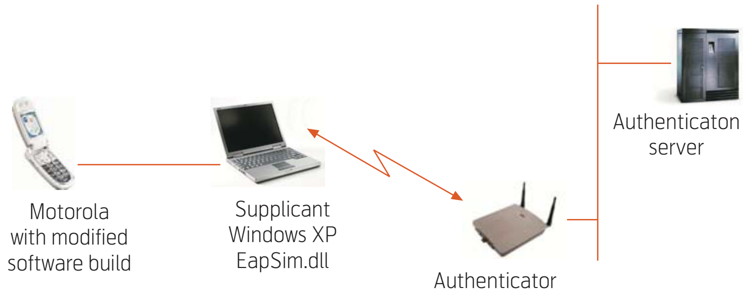

Authenticaton server
Motorola with modified software build
Supplicant Windows XP EapSim.dll
Authenticator

Figure 10 Test-bed architecture used for testing the EAP-SIM authentication

3.5 Solution developed in the OBAN framework

The solution developed in the OBAN project is based upon the Bluetooth Serial Port Profile. A software module has been developed, running on the Serial Port (and thus accessible also if the serial connection is performed via USB or IrDA interfaces) and translating the messages coming from the supplicant into the corresponding internal commands for the software module in charge of handling the SIM card.

On the laptop side, the EAP-SIM supplicant is in charge of handling the communication with Windows XP Operating System and accessing the information from the mobile phone. The reason why Windows XP has been chosen is because it natively supports the EAP protocols and the interfaces for the creation and installation of new EAP methods are extensively described and reasonably clear. The EAP-SIM supplicant must be developed as a system dynamic link library which, for security reasons, runs in a protected memory space of Windows XP.

The EAP supplicant has been installed onto a laptop running Windows XP (see Figure 10). The authenticator needs to be an access point supporting EAP-SIM, while the authentication server is a RADIUS server which is connected to the operator HLR (for a more comprehensive description of the protocols supported by the authenticator and authentication server, refer to section 2.1 and Figure 4). This basic architecture shows the minimal requirements needed to experiment with the EAP-SIM authentication solution.

4 Future evolutions

4.1 Towards Fast Handover

One of the major goals in today's networks is supporting multimedia applications for nomadic and mobile users into an always-on and seamless environment. Fulfilling this goal in the OBAN scenario requires OAN to support QoS and seamless hand-off among access points, but without losing security. The authentication procedure in such a context must be designed to be fast enough to support multimedia, real-time applications, but also to avoid any kind of abuse or misuse of the OANs and SP networks. To this purpose the OBAN project is proposing a modified EAP-SIM method to reduce the number of round trip messages exchanged between the Supplicant and the Authentication Server during the hand-off procedure.

This method, called EAP-OBAN, is a mediated authentication mechanism that exploits the Needham-Schroeder Protocol [8] to distribute keys among the OAN user and the Access Points of the OAN itself. It adds to EAP-SIM tickets similar to the Kerberos ones [7] to speed-up the authentication process. During a standard EAP-SIM procedure, users that hand-off from one AP to another must re-execute the whole EAP authentication process. With EAP-OBAN this is no more required and users that need to hand-off can use tickets previously received by a Key Distribution Center (KDC) to authenticate them to the new AP.

The differences with the EAP-SIM authentication method is represented by the introduction of Kerberos-like tickets and the AS proxy, acting as KDC. This KDC shares keys with each enabled AP but not with the supplicant. The shared key between the supplicant and the KDC required by the Needham-Schroeder protocol is the session key found in the EAP-Success message, sent by the AS to the Authenticator. The KDC is an AS proxy and thus can intercept the EAP-Success message and replace it with an EAP-Response message that contains a Ticket Granting Ticket (TGT) encrypted by the session key. The TGT is the ticket used by the supplicant to request further tickets to enable access to the OAN. When hand-off is required, the Supplicant (by presenting the TGT) asks the KDC one ticket for the AP that he is willing to connect to. If the TGT is valid, then the KDC issues the required ticket for the supplicant. Using this ticket the Supplicant can authenticate itself to the AP and connect to the OAN.

This mechanism speeds up the authentication process since, after the first authentication the messages exchanged between the KDC and the AS and between the AS and the AuC are no more required. Moreover, since the KDC is usually closer to the access network than the AS and the AuC, the required authentication messages have fewer networks and hops to traverse, consequently being faster. Security and fast handover techniques are more comprehensively treated in [10]

5 Conclusions

In this paper we presented a user-friendly authentication procedure for OANs that can help the OAN diffusion for two reasons, the security confidence of the user and the very low cost of hardware requirements.

The authentication proposed from the user perspective is identical to the procedure used for the authentication to GSM/GPRS networks and consequently it is as secure as the GSM/GPRS is. From the user perspective that actually means high security confidence. This makes users feel OAN secure enough to carry confidential data like for example credit card or e-commerce orders.

Acknowledgements

This work was carried out as part of the EC-funded project OBAN. The authors would like to thank the participants in the IST OBAN project for valuable technical collaboration.

6 References

1 *Open Broadband Access Network (OBAN) project website*. 18 October 2006 [online] – URL: http://www.ist-oban.org

2 *The FON Movement*. 18 October 2006 [online] – URL: http://en.fon.com/

3 Aboba, B, Blunk, L, Vollbrecht, J, Carlson, J, Levkowetz, H. *Extensible Authentication Protocol (EAP)*. The Internet Engineering Task Force (IETF), June 2004. (RFC 3748)

4 *Wi-Fi Alliance*. 18 October 2006 [online] – URL: http://www.wi-fi.org/

5 Haverinen, H, Salowey, J. *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*. The Internet Engineering Task Force (IETF), January 2006. (RFC 4186)

6 IEEE. *Port-Based Network Access Control*. Institute of Electrical and Electronics Engineers, June 2001. (IEEE standard 802.1X)

7 Neuman, C, Hartman, S, Raeburn, K. *The Kerberos Network Authentication Service (V5)*. The Internet Engineering Task Force (IETF), July 2005. (RFC 4120)

8 Needham, R, Schroeder, M. Using encryption for authentication in large networks of computers. *Communications of the ACM*, Dec. 1978.

9 *PC/SC Workgroup*. 18 October 2006 [online] – URL: http://www.pcscworkgroup.com/

10 Jaatun, M G, Tøndel, I A, Johannessen, T H. Security in fast handovers. *Telektronikk*, 102 (3/4), 111–124, 2006. (This issue)

11 3rd Generation Partnership Project (3GPP). Technical Specification Group Terminals – *Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface* (Release 1999). 3GPP TS 11.11, V8.13.0 (2005-06).

Corrado Derenale graduated from Turin Polytechnic in Computer Engineering in 2000, obtained the Professional Engineer Licensure in 2003 and received a PhD in Computer and System Engineering from the Turin Polytechnic in 2004. His main field of research is the computer network security with focus on wireless technologies. He joined Motorola in April 2005 and is now a Software Engineer in the GSG Italy network group.

email: corrado.derenale@motorola.com

Simone Martini graduated from Turin Polytechnic in Telecommunication Engineering in 1997. He obtained the Professional Engineer Licensure in 1999 and is a member of the IT Committee for the National Society of Professional Engineers. He joined Motorola in July 1999 and is now a Technology Specialist in the Wireless Engine Area.

email: simone.martini@motorola.com

Section 5 – Expected Capacity and Coverage

EINAR EDVARDSEN

Einar Edvardsen is Senior Adviser in Telenor R&I

The main topic of section 5 is to estimate the potential coverage and capacity of a typical OAN. A stand-alone WLAN (IEEE802.11g) performs about 25 Mb/s net capacity when users are located relatively near the access point. However, due to the fact that WLAN operates in an unlicensed frequency band and that there are only three independent radio channels available, a network consisting of many adjacent access points will suffer from severe interference. This section contains three papers: One of them gives a brief overview of relevant radio technologies while the two others aim at estimating the performance of typical open access networks as regards potential capacity and coverage. The two papers complement each other in the way that the one focuses most on physical level analysis while the second focuses on service and traffic level simulation and analysis.

Wireless LANs based upon the IEEE802.11 standard has become the enabler for open access networks. The main reason is the popularity of WLAN among the public due to simplicity and low cost. However, from a technical point of view WLAN is not an optimal choice and other standards performing better could have been chosen. The paper *A Brief Overview of Radio Technologies* by Per Hjalmar Lehne gives a brief overview and evaluation of alternative standards that could have been used and a summary and analysis of these alternatives.

The second paper, *Multi-cell WLAN Coverage and Capacity* by Jan Erik Håkegård, approaches the problem by analysing coverage and reach from an analytic point of view. Analytic methods to calculate radio wave propagation are used to estimate the theoretical coverage and capacity of stand-alone WLAN access points. These methods are further enhanced in order to estimate the influence of physical layer and MAC-layer interference on capacity and reach.

The third paper, *Traffic Capacity and Coverage in a WLAN-Based OBAN* by Terje Ormhaug, Per Hjalmar Lehne and Olav Østerbø targets also estimation of capacity and coverage in networks of WLAN access points, but this time with a focus on how traffic load, traffic types, QoS mechanisms and access point density interfere with each other and influence on service availability for visiting users; i.e. what is the probability of a casually passing user to get the services he wants at different locations in the network.

ISSN 0085-7130 © Telenor ASA 2006

A Brief Overview of Radio Technologies

PER H. LEHNE

Per Hjalmar Lehne is Researcher at Telenor R&I and Editor-in-Chief of Telektronikk

Several short to mid range radio technologies exist and are being developed and standardized. Some of these may be suitable for an open access network (OAN) provision. The most widespread is the WLAN standards of the IEEE 802.11 family, but others could be considered. This paper contains a survey of existing and future radio technologies and a brief evaluation of their suitability to fill the needs of an OAN. A classification in range vs. data rate clearly shows that WLAN technologies currently represent the best choice, however mobile WiMAX may become interesting in the future. As more and more players are entering this market and the users' demands increase, one possible differentiator may be to choose a radio technology that offers better services and coverage. Short-range technologies, like Bluetooth and WPANs have, literally speaking, shortcomings in providing sufficient coverage, even though some of the latest provide impressive data rates.

1 Introduction

The whole idea of open access is based on utilizing and sharing capacity of private access lines for providing public access. This implies the use of wireless technology to deliver the services both to the home user and to the visiting user. The intention of this article is to present some of the possible technologies and standards which are available today, or will become available in the near future. The list is not exhaustive, and a rigorous evaluation has not been done, thus readers interested in this should make their own inquires on the subject.

The article starts with a discussion on some criteria for technologies to be feasible for an open access provision. Then descriptions and a list of current and future standards are given. Finally, a short discussion is added.

2 Criteria for choice of wireless technology

A lot of technological advances during the last decades have resulted in a steadily growing number of standards and concepts for wireless communications. The main characteristics vary based on different design criteria and targeted use, from short to wide range, from low to high data rate, and from simple to advanced functionality.

This chapter presents a discussion around some of the criteria that should be considered in order to say whether one technology or standard is feasible to use in an open access concept or not. The discussion is not meant to be exhaustive because this would demand much more space.

2.1 Data rates, throughput and capacity

A wireless hop must provide a sufficient data rate to the end user to support the expected use. This again depends on the services and applications offered. We should expect a user's demand to be a mix of real-time and streaming services on the one hand to file transfer and browsing type services on the other. The first puts stronger demands on the available data rate in that they are not elastic, thus a minimum rate must be maintained during the whole session. Burst services are more robust and tolerant, variations in data rate do not usually destroy the service; however, the user may suffer varying delays and elapsed times for the service to complete.

A 64 kb/s voice over IP connection (VoIP) often results in a bit rate of 100 – 150 kb/s when different protocol overhead has been added. The short packet size worsens this. Wireless links usually have large overhead due to error correcting techniques. If we then go down to the physical layer, the data rate must be doubled or tripled resulting in a necessary physical layer bit rate of 300 – 500 kb/s. Video services demand more. Even if it is possible to code e.g. video telephony (including sound) into a 64 kb/s channel, we should expect a demand for higher quality video. We could estimate at least 1 Mb/s for a video service resulting in 3 – 4 Mb/s on the physical layer.

Elastic traffic is much more tolerant for different data rates. An up- or download of a digital photo of medium to high quality (2 – 5 Megapixels) makes a file size of 2 – 5 Mb (JPEG compression 1:3). It takes 5 – 15 seconds to transfer this on a 3 Mb/s connection (application rate). This is probably acceptable for the moment.

Capacity of access technologies is often specified by giving the instantaneous peak data rate either on the physical layer or on the medium access layer. This is the total rate which must be shared among all simultaneous users. When the effect of scheduling between

ISSN 0085-7130 © Telenor ASA 2006

several users is taken into account, the net available capacity may be halved.

A system's total capacity in e.g. data rate per area depends not only on the peak rates available per access point, but the number of available, non-overlapping channels in the operating frequency band is of high importance. Co-channel interference effectively reduces capacity, both by physically raising the noise floor and by influencing medium access protocol performance. A small number of operating channels limit the frequency reuse distance, giving rise to a higher interference level.

2.2 Coverage and range

An open access system is not meant to compete with e.g. mobile technologies on a large scale, but complement them and compete on a local scale. In order for the concept to offer a reasonable coverage the range must at least be some tens, preferably a few hundred metres.

A long range may seem attractive at first sight. But it is usually a trade-off between the coverage from a single access point or base station and the offered capacity or throughput per area. A single access point has the capability of supporting the same amount of traffic within its coverage area, whether it is large or small. Consequently, the "optimal" range is obtained when the offered traffic capacity per area is just high enough to serve the demand.

Interference from neighbouring stations (access points and terminals) is another factor influencing both range and capacity. A system operating in a narrow frequency band has few non-overlapping channels. In order to provide a continuous coverage using several access points the same channel must be reused and few channels means close distance between cells with same channels. The co-channel interference may be significant, resulting in both reduced range and lower traffic capacity.

This property directly influences the suitability of the different technologies in order to provide continuous coverage in a larger geographical area.

2.3 Prices and costs

In order to have a good uptake, the price must be right. The right price is not fixed but a function of several other factors. The end-user's willingness to pay is given by the experienced value for money. The best reference today is probably the price of a Wi-Fi access point, which may vary from 50 to 250 EUR.

2.4 Physical size and form factor

Even though the tolerance for visible technical equipment (PCs etc.) in the home sphere has increased, no-one wants a big equipment rack in the house. The physical size must be residential friendly and the design discrete. Additionally, the installation must be noiseless.

2.5 Radio frequencies and bandwidths

Any communication system needs a physical medium, and the use of radio assumes available radio resources in terms of frequencies and bandwidths. There are two prerequisites which the operating frequencies must meet:

- Physical suitability
- Regulatory availability.

2.5.1 Physical suitability

The physical properties of radio communications vary with the frequency; the most important being the following:

- A low frequency signal has a longer range than a high frequency signal.
- A high frequency signal provides more bandwidth than a low frequency signal.
- The antenna's physical size is large for low frequencies and small for high frequencies.
- A low frequency signal is more suitable for obtaining coverage behind obstructions due to reflections and diffractions, so-called non-line of sight operation (NLOS) than a high frequency signal.

We can see that some of these demands are contradictory and a suitable combination must be found as shown in Figure 1.

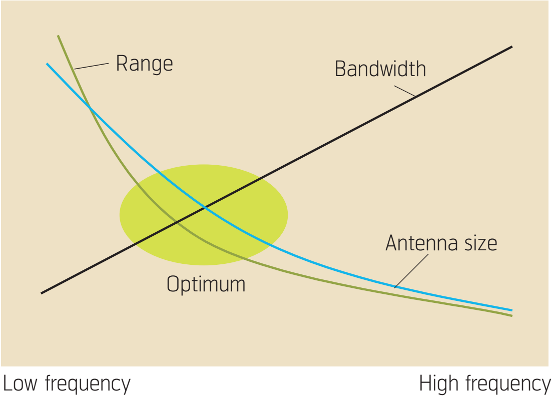


Figure 1 Range, bandwidth and antenna size dependence on radio frequency

ISSN 0085-7130 © Telenor ASA 2006

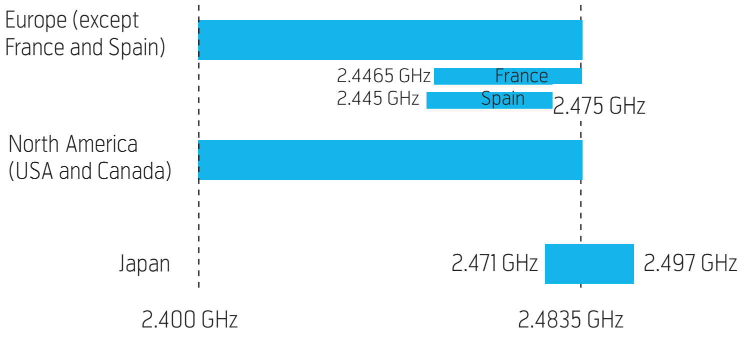


Figure 2 Regulations for unlicensed operation in the ISM 2.4 GHz frequency band

2.5.2 Regulatory availability

The other factor is whether the most suited frequency band is available for the purpose from a regulatory point of view. Regulatory authorities allow unlicensed operation in some bands with the simplicity this gives. But it also gives problems with unpredictable interference situations etc., which can effectively destroy both capacity and coverage. It may be better to use licensed bands in order to provide a predictable quality.

There are several more or less standardized ways of dividing the whole radio frequency range of the electromagnetic spectrum, however for the purpose of this article we divide it into three:

- Below 1 GHz
- From 1 to 10 GHz
- Above 10 GHz.

The frequencies below 1 GHz are generally very heavily utilized and available bandwidth is scarce. This band is used for long range, narrowband communications for maritime and aeronautical purposes, sound and TV broadcast and wide-area cellular systems like GSM and D-AMPS, to mention just a few. In addition there are different ground based radio navigation aids. Consequently, there are few, if any options for broadband wireless below 1 GHz.

The band between 1 and 10 GHz becomes much more interesting, both from a physical point of view as discussed in the previous section and because parts of this spectrum are already regulated to short to medium range wireless systems. Current systems operating in this range are GSM1800/1900 and 3G. The specific bands which are currently regulated for wireless access are:

- The unlicensed band between 2.4 and 2.485 GHz, also called ISM – Industrial, Scientific and Medical. It is available globally with local adjustments as shown in Figure 2. This band can be used for any wireless access system which conforms to the power constraint demands given in Table 1. Current use is e.g. Bluetooth, Zigbee and Wi-Fi (see sections 3.1 and 3.2).

- The band from 2.5 to 2.690 GHz is globally recommended as the "UMTS extension band". It is possible that this may be available for other systems.

- The licensed band between 3.4 and 3.5 GHz is regulated in most European countries for Broadband Fixed Wireless Access (BFWA) systems like e.g. WiMAX (see section 3.3.1).

- Above 5 GHz there are several bands which are regulated for unlicensed use, similar to the ISM band. Regional details and conformance demands are given in Figure 3 and Table 2. Current systems are Wi-Fi, 802.11a/HiperLAN (see section 3.2), but actual use is not yet heavy.

- The whole frequency band from 3.1 to 10.6 GHz is in the USA allowed for so-called Ultra Wideband

Region/country	Available frequencies	Transmit power constraints
North America (USA and Canada)	2.4 – 2.4835 GHz	1 W (30 dBm) transmitter power
Europe (except France and Spain)	2.4 – 2.4835 GHz	100 mW (20 dBm) EIRP[1)] maximum
France Spain	2.4465 – 2.4835 GHz 2.445 – 2.475 GHz	The power can be adjusted in the equipment in order to intentionally reduce the range
Japan	2.471 – 2.497 GHz	500 mW (27 dBm) transmitter power

Table 1 Emission limit regulations for the ISM 2.4 GHz frequency band

[1)] *EIRP – Effective Isotropic Radiated Power, the amount of power one has to feed into an omni-directional (isotropic) antenna in order to obtain the same electromagnetic power density or field strength in a given direction, compared to a practical, directive antenna. EIRP is usually given for the direction of maximum power.*

ISSN 0085-7130 © Telenor ASA 2006

(UWB) technologies, providing very low power spectral densities. It is supposed that such operation shall not influence on other conventional systems operating within the same band. Such operation is not yet allowed in Europe

Above 10 GHz the available bandwidth is huge. Current use includes satellite broadcast, point-to-point radio links and point-to-multipoint distribution systems. The bandwidth availability makes it very attractive for future wireless broadband use, however the limitations in range and NLOS coverage are the most difficult obstacles for open access provision using low power, private access points. It is most suited for overlay and distribution systems.

2.6 Mobility, security and quality of service

The whole idea behind an open access provision is to use several private coverage "islands" to provide a larger, public coverage. Consequently the wireless access should support a degree of mobility, i.e. that services are maintained when moving from one coverage area to another. The sophistication can be discussed. Minimum security must also be maintained, thus the system must support security against unauthorized intrusion, denial of service, as well as protection against eavesdropping. If a mix of real-time and best-effort services is to be offered, a simple kind of quality of service (QoS) functionality must be included.

2.7 IP-based

The Internet Protocol (IP) has evolved to be the dominant technical standard for link layer communication. It is therefore necessary that a wireless access technology can be easily plugged into an IP-based network and support end-to-end IP-based services.

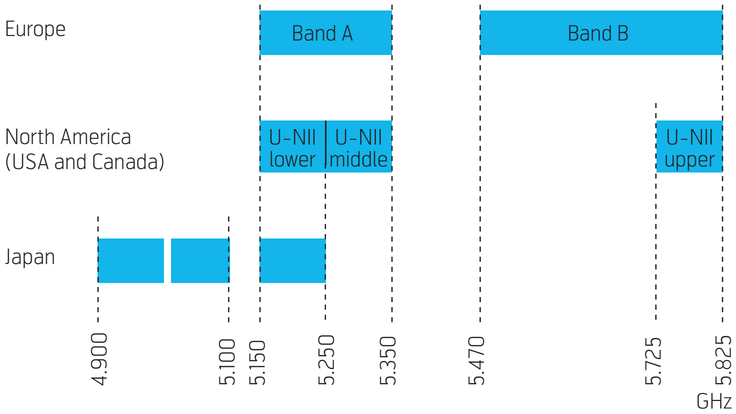


Figure 3 Regulations for unlicensed operation in the 5 GHz frequency band

3 Candidate technologies

The discussion above narrows the search to technologies supporting IP as a wireless replacement for Ethernet. Therefore mobile systems like 2G and 3G (e.g. GSM and UMTS) have been ruled out of the discussion. The candidates can be sorted according to different criteria. We have chosen to sort them along the range axis, using the following classification:

- Very short range (personal area network (PAN) technologies), less than 10 m;
- Short range (local area network (LAN) technologies), between 10 and 300 m;
- Medium range (metropolitan area network (MAN) technologies), more than 300 m.

This is not a rigorous and scientific classification since several access technologies have properties making them belong to more than one category above. The large variations in radio communication conditions also make this an approximate sorting.

Region/country	Available frequencies	Transmit power constraints
North America (USA and Canada)	5.15 – 5.25 GHz (U-NII[2] lower band) 5.25 – 5.35 GHz (U-NII middle band) 5.725 – 5.825 GHz (U-NII upper band)	40 mW (16 dBm), 6 dBi antenna 200 mW (23 dBm), 6 dBi antenna 800 mW (29 dBm), 6 dBi antenna
Europe	5.15 – 5.35 GHz (band A) 5.47 – 5.725 GHz (band B)	200 mW (23 dBm) EIRP, indoor 1 W (30 dBm) EIRP, outdoor
Japan	4.9 – 5.1 GHz 5.15 – 5.25 GHz	250 mW (24 dBm) transmitter power 125 mW (22 dBm) transmitter power

Table 2 Emission limit regulations for the 5 GHz frequency bands

[2] *U-NII – Unlicensed National Information Infrastructure*

ISSN 0085-7130 © Telenor ASA 2006

A short description of each technology and the status of the standards, as well as a list of some essential parameters are given in Table 3.

3.1 Very short range technologies

Bluetooth, ZigBee and IEEE 802.15 are the most widespread standards for *Wireless Personal Area*

Technology/ Standard	Gross bit rates offered on the physical layer	Frequency band(s)	Available channels@BW	Transmitter power levels	Typical range	Main applications
IEEE 15.1 / Bluetooth v 1.1	1 Mb/s (v 1.1, 1.2) 1 – 3 Mb/s (v 2.0 + EDR)	ISM 2.4 GHz	79 @ 1 MHz	100 mW (Class 1 radios) 2.5 mW (Class 2 radios) 1 mW (Class 3 radios)	100 m 10 m 1 m	Connecting devices Cable replacements WPAN
IEEE 15.3: High Rate Wireless Personal Area Networks (WPAN)	11 – 55 Mb/s	ISM 2.4 GHz	5 @ 11 MHz	< 100 mW EIRP	~10 m	Portable consumer digital imaging and multimedia applications
ECMA-368: High Rate Ultra Wideband	53 – 480 Mb/s	3.6 – 10.6 GHz (UWB band, USA)	14 @ 528 MHz	- 41.3 dBm/MHz (0.074 μW/MHz)	~ 10 m	Imaging and multimedia
IEEE 15.3c: Millimetre Wave Alternative PHY	2 – 3 Gb/s	57 – 64 GHz			A few metres	High speed internet access, streaming content download, real time streaming and wireless data bus for cable replacement
IEEE 15.4 Low rate WPANs (ZigBee)	20, 40, 250 kb/s	868.3 MHz (USA) 915 MHz (USA) ISM 2.4 GHz	1 @ 2 MHz 10 @ 2 MHz 16 @ 5 MHz	< 100 mW EIRP (2.4 GHz)	10 – 100 m	Home automation, Remote monitoring and control
IEEE 15.4a: Low Rate Alternative PHY Task Group		3.1 – 10.6 GHz (UWB band, USA) ISM 2.4 GHz		- 41.3 dBm/MHz (0.074 μW/MHz) < 100 mW EIRP	1 – 10 m 10 – 500 m	Communications and high precision ranging / location capability (1 m accuracy and better), high aggregate throughput, and ultra low power
HomeRF SWAP	1, 10 Mb/s	ISM 2.4 GHz		< 100 mW EIRP (Europe)	~ 50 m	An industry standard targeting the consumer market. Technically a mix between DECT and IEEE 802.11
IEEE 802.11 WLAN	1, 2 Mb/s	ISM 2.4 GHz	13 @ 22 MHz 3 non-overlapping	< 100 mW EIRP (Europe)	10 – 500 m	WLAN and hotspot
IEEE 802.11b WLAN, Higher-Speed Physical Layer Extension	5.5, 11 Mb/s	ISM 2.4 GHz	13 @ 22 MHz 3 non-overlapping	< 100 mW EIRP (Europe)	10 – 300 m	WLAN and hotspot
IEEE 802.11g WLAN, Further Higher Data Rate Extension	6 – 54 Mb/s	ISM 2.4 GHz	13 @ 22 MHz 3 non-overlapping	< 100 mW EIRP (Europe)	10 – 250 m	WLAN and hotspot
IEEE 802.11a High Speed Physical Layer in the 5 GHz Band	6 – 54 Mb/s	5 GHz bands	126 @ 20 MHz 12 non-overlapping	< 200 mW / 1 W (Europe)	10 – 200 m	WLAN and hotspot
IEEE 802.11n, High throughput WLAN	Up to 200 Mb/s	ISM 2.4 GHz 5 GHz bands		< 100 mW EIRP (Europe)	10 – 500 m	WLAN and hotspot
ETSI HiperLAN/2	6 – 54 Mb/s	5 GHz bands	126 @ 20 MHz 12 non-overlapping	< 200 mW / 1 W (Europe)	10 – 200 m	WLAN and hotspot
IEEE 802.16e – "Mobile WiMAX"	240 Mb/s	< 6 GHz, licensed and unlicensed bands	In the 3.5 GHz band: 10 @ 20 MHz 160 @ 1.25 MHz Or any combination	Depends on frequency band	300 m – a few kilometres	WMAN, Mobile Broadband

Table 3 Wireless technology standards

Networks (WPANs). Both Bluetooth and ZigBee are standards developed and partly maintained by industry, but parts of them have been adopted by the IEEE 802.15 Working Group for WPANs. While IEEE only specifies the physical (PHY) and medium access (MAC) layers, the Bluetooth and ZigBee standards describe the higher layers as well, in order to specify access, networking and application profiles.

3.1.1 Bluetooth

Bluetooth is an established technology, mostly used for connecting different computer and communication accessories. The currently most used application is connecting wireless hands-free earplugs with mobile phones. The Bluetooth technology is however capable of providing most communication services, demanding both elastic and non-elastic traffic. The first version of Bluetooth was developed and specified by Ericsson starting in 1994. In 1998, the Bluetooth Special Interest Group (SIG) [1] [2] was established and has taken responsibility for further evolution of the standard. The Bluetooth SIG has currently more than 4000 member companies.

Bluetooth enabled electronic devices connect and communicate wirelessly through short-range, ad hoc networks called *piconets*, which can contain up to eight devices. Each device can also belong to several piconets simultaneously. Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave radio proximity. A fundamental Bluetooth wireless technology strength is the ability to simultaneously handle both data and voice transmissions.

The current core specification versions are Version 1.2, adopted November 2003 [3] and Version 2.0 + Enhanced Data Rate (EDR), adopted November 2004 [4].

The Bluetooth wireless specification gives both link layer and application layer definitions, which support data and voice applications. It operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz. Bluetooth uses a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec. Adaptive frequency hopping (AFH) capability was designed to reduce interference between wireless technologies sharing the 2.4 GHz spectrum.

Three device classes have been defined, giving different ranges and possible applications (see Table 3 for more details). The most commonly used radio is Class 2 with 2.5 mW of transmitter power. The data rate is 1 Mb/s for Version 1.2; up to 3 Mb/s is supported for Version 2.0 + EDR. The previous version of Bluetooth (1.1) has been adopted by the IEEE 802.15 Working Group for WPAN [5] (see below).

3.1.2 ZigBee

ZigBee is a standard for low data rate communication [6]. The targeted markets span from industrial sensor networks to consumer electronics, including toys and games. It has some of the same applications as Bluetooth on connecting computer devices (keyboards, mouse), but the considerably lower data rate makes it unfit for broadband communication. It basically supports communication needs for control and monitoring. It is promoted by an industry association called the ZigBee Alliance [7]. The lower layers (physical and medium access) are basically identical to IEEE 802.15.4 (see below), however ZigBee also includes the higher layers, including applications, similar to Bluetooth vs. IEEE 802.15.1.

ZigBee can operate at 868 MHz (1 channel), 902–928 MHz (10 channels, 2 MHz spacing) and in the ISM band from 2.4 to 2.485 GHz (16 channels, 5 MHz spacing).

3.1.3 IEEE 802.15

The IEEE 802.15 Working Group for WPAN [5] has further developed and released several standards for WPANs utilizing different frequency bands and providing different data rates. The initial specification, offering medium speed data rates is *IEEE 802.15.1-2002*, “Wireless Personal Area Networks (WPANs)”. It is an adaptation of the physical and medium access layers of the Bluetooth version 1.1 and was approved in June 2002. It offers up to 1 Mb/s data rate and a range up to approximately 100 m, depending on the power class (see Table 3) [8].

Later several initiatives for high data rate WPANs have come up. The only one completed so far is the *IEEE 802.15.3* High Rate (HR) WPANs. It specifies a high data rate WPAN in the 2.4 – 2.485 GHz ISM band, providing data rates from 11 to 55 Mb/s. The standard was approved in September 2003 [9].

Two other standards have been initiated but are not yet finished. The *IEEE 802.15.3a*, High Rate Alternative PHY, is based on a so-called ultra wide band (UWB) technique operating from 3.1 – 10.6 GHz. It was targeted for finalization in late 2006, however it has been difficult to reach a consensus on this matter, thus the project was stopped (PAR[3]) withdrawn), but work has continued among the participants outside the IEEE.

[3]) *PAR – Project Authorization Request, a formal document describing the scope and need for a project study in the IEEE 802.*

Two concepts with nearly identical performance were standing against each other: Direct Sequence UWB (DS-UWB) and multi-band OFDM (MB-OFDM). Later, through the WiMedia Alliance [10] and the Multi-Band OFDM Alliance (MBOA), the European Computer Manufacturer's Association (ECMA) [11] finalized and issued the *ECMA-368* standard for the MB-OFDM physical and medium access layers in 2005 [12]. The standard supports physical layer data rates from 53 to 480 Mb/s.

Late in 2004 the proponents of the DS-UWB proposal created the UWB forum [13] to bring forward their solution to UWB communication. The DS-UWB physical layer specification is completed and the original IEEE 802.15.3 MAC is used with some small modifications. But it has slim chances of achieving 75 % of the votes in IEEE. Thus it seems like the MB-OFDM solution is most likely to succeed as the future standard for high rate WPANs.

The third high rate WPAN standard is the *IEEE 802.15.3c*, Millimeter Wave Alternative PHY, which shall operate in the 57 – 64 GHz bands offering data rates of up to 2 – 3 Gb/s. It is currently under work and the target is to be finished in second half of 2008 [14].

In addition to the standards for physical and medium access layers, some recommended practices for coexistence [15] and interoperability have been issued.

At the other end, low data rate communications are also addressed. The *IEEE 802.15.4-2003*, Low-Rate Wireless Personal Area Networks (LR-WPANs) is the same as the physical and medium access layers of ZigBee, operating in the 2.4 – 2.485 GHz ISM band. It was approved in October 2003 [16]. Two optional physical layers are standardized as *IEEE 802.15.4a*, Low Rate Alternative PHY; one based on UWB in the 3.1 – 10.6 GHz band and one direct sequence chirp based in the ISM 2.4 GHz band. It was targeted for publication in Q2/2006, but seems to be delayed.

A draft revision for specific enhancements and clarifications to the IEEE 802.15.4-2003 standard was issued as *IEEE 802.15.4b* in June 2006 with an expected publication in September 2006. Another task group, *802.15.5*, is working to specify mesh network architecture for WPANs and is targeted to be finished by the end of 2006 [17].

3.2 Short range

In the so-called short range class we find the most successful wireless technology (possibly apart from GSM) today, the IEEE 802.11 family of *Wireless Local Area Network* (WLAN) standards. Others exist, at least on paper, like the ETSI standard HiperLAN, however never made it to the market. Now it should be mentioned that concepts from HiperLAN have been adopted to a great extent by the IEEE 802.11, among others to allow 5 GHz systems to be used on the European market. In Japan, other standards have been developed and are in use. A curiosity which is mentioned is the HomeRF standard, a technical blend of a circuit-switched mode based on the DECT[4] protocol, and a packet switched mode based on the IEEE 802.11.

3.2.1 IEEE 802.11 family WLAN and Wi-Fi

The IEEE 802.11 [18] family of standards has been a formidable success for home and enterprise wireless local access. Since the first standard for physical and medium access came in 1999, offering physical layer bitrates of 2 Mb/s, the technology has been developed further, now capable of 54 Mb/s physical layer rates, providing approximately 20 Mb/s for the application. The latest addition is a MIMO[5]-based physical layer standard promising more than 100 Mb/s available to the applications.

The IEEE 802.11 specifications are wireless standards that specify an over-the-air interface between a wireless client and a base station or access point, as well as among wireless clients. The 802.11 standards can be compared to the IEEE 802.3 standard for Ethernet on wired LANs. The IEEE 802.11 specifications address both the physical (PHY) and medium access control (MAC) layers and are tailored to resolve compatibility issues between manufacturers of Wireless LAN equipment. The 802.11 standards are modules which in total describes a multitude of different WLAN implementations with bit rates ranging from 1 Mb/s to 54 Mb/s in both the ISM 2.4 GHz and the 5 GHz bands.

The original *IEEE 802.11* [19] standard covered the physical and MAC-layers at 2.4 GHz with supported data rates of 1 and 2 Mb/s. The *802.11b* [20] specifies a higher rate physical layer in the same band supporting data rates on the physical layer at 5.5 and 11 Mb/s. *IEEE 802.11g* [21] is a later PHY extension to enhance the performance and the possible applications

[4] *DECT – Digital Enhanced Cordless Telecommunication, an ETSI standard for digital portable phones, commonly used for domestic or corporate purposes.*

[5] *MIMO – Multiple input – multiple output, a combined transmitter-receiver diversity concept utilizing multiple antennas at both ends of the link, in order to increase the link capacity.*

of the 802.11b compatible networks by increasing the data rate. These are the most common WLAN standards in use today.

The *IEEE 802.11a* [22] standard operates in the 5 GHz band and supports data rates on the physical layer up to 54 Mb/s. This standard was not allowed to operate in Europe due to regulatory constraints; however the introduction of the *IEEE 802.11h* [23] solved this. It enhances the current 802.11 MAC and 802.11a physical layers with network management and control extensions for spectrum and transmit power management in 5 GHz license exempt bands. It enables regulatory acceptance of 802.11 5 GHz products in Europe.

The *IEEE 802.11e* [24] enhances the current 802.11 MAC to expand support for LAN applications with Quality of Service requirements and provide improvements in the capabilities and efficiency of the protocol. The *IEEE 802.11i* [25] further enhances the MAC to improve security and authentication mechanisms. Further improvements on security is worked on in *802.11w* where one is seeking to create enhancements to the IEEE 802.11 MAC layer to provide mechanisms that enable data integrity, data origin authenticity, replay protection, and data confidentiality for selected IEEE 802.11 management frames. This includes frames for de-authentication and disassociation.

Implementation of access points and distribution systems was purposely not defined by IEEE project 802.11 because there are many ways to create a Wireless LAN system. As 802.11 based systems have grown in popularity, this has become an impediment to WLAN market growth. *802.11f* [26] contains guidelines defining basic functionality needed to ensure interoperability between access points from different vendors across the same distribution system.

The latest addition to the physical and medium access layer standards in this family is the *IEEE 802.11n*. This started as the "High Throughput Study Group" (HT SG) in 2002 and was from September 2003 Task Group *n* with the aim of standardizing a new physical and MAC layer with the ability of providing at least 100 Mb/s data rate on the MAC data service access point (SAP). The aim was to reach approval in 2005, however due to disagreements in merging different proposals, the process has been delayed. It should be ready in 2007. 802.11n uses MIMO techniques to support more than 200 Mb/s on the physical layer.

Future enhancements of the 802.11 standards are on network management. Radio Resource Measurements is specified in *IEEE 802.11k*, which is currently undergoing the last revisions and is expected to be published in July 2007. It specifies mechanisms to higher layers for radio and network measurements. Management mechanisms on the upper layers are addressed by the *IEEE 802.11v* in order to make a complete and coherent upper layer interface for managing 802.11 devices in wireless networks. The latter is expected to be finished in April 2009.

Vehicular communications is addressed by the *IEEE 802.11p*. This will be a new MAC and physical layer in the 5 GHz band intended for vehicle-to-roadside and vehicle-to-vehicle communications for speeds up to 200 km/h and ranges up to 1 km. It targets the new markets and applications on Intelligent Transportation Systems (ITS) providing applications for e.g. collision avoidance, traveller information, toll collections and traffic management. In addition the intention is to support applications that would be of broader interest to motorists and those interested in providing services to these motorists. Finalization is expected in April 2008.

Mesh technology is the ability to interconnect several devices in a mesh in order to provide e.g. larger coverage and self-organization. The *IEEE 802.11s* is working to specify such mechanisms. The scope is to develop a Wireless Distribution System (WDS) using the IEEE 802.11 MAC and physical layers that support both broadcast/multicast and unicast delivery over self-configuring multi-hop topologies. Today's 802.11 technology uses fixed Ethernet wiring to connect to the backbone network, thus the introduction of mesh technologies adds to the flexibility and mobility ability. It is expected to be finished in December 2008.

Inter-working with other networks becomes more and more important and the *IEEE 802.11u* is working to provide amendments to the IEEE 802.11 physical and MAC layers which enable inter-working with other networks. This includes both enhanced protocol exchanges across the air interface and provision of primitives to support required interactions with higher layers for inter-working.

The term *Wi-Fi* (Wireless Fidelity) is often used when talking about the IEEE 802.11 technologies, and the terms Wi-Fi, WLAN and 802.11 are often mixed and interchanged. Strictly speaking, the technical standard is called "IEEE 802.11 WLAN", while the term Wi-Fi is introduced by an industrial cooperation called the Wi-Fi Alliance [27]. The Wi-Fi Alliance has issued conformance specifications for a subset of all options in the WLAN standard together with test methods, in order to ensure interoperability between products from different vendors.

3.2.2 ETSI HiperLAN

In the area of WLANs other access technologies have been developed but have lost their market (or never had one). One of them is *HiperLAN (High Performance Radio LAN)*.

HiperLAN is standardized by the ETSI Project BRAN (Broadband Radio Access Networks). In addition to WLAN type of standards it is also working on broadband fixed wireless systems (HiperACCESS, HiperLINK). Two WLAN standards exist; HiperLAN/1 and HiperLAN/2 [28].

HiperLAN/1 was the first standard, designed to provide high-speed communications (20 Mbit/s) between portable devices in the 5 GHz band. *HiperLAN/2* is a radio LAN standard designed to provide high-speed access (up to 54 Mbit/s at physical layer) to a variety of networks including 3G mobile core networks, ATM networks and IP based networks, and also for private use as a wireless LAN system. The HiperLAN/2 operates in the 5 GHz band. No commercial equipment has been made available, and it is generally accepted that it is "replaced" by the IEEE 802.11a in combination with 11h.

3.2.3 HomeRF

The Home Radio Frequency is a single specification (Shared Wireless Access Protocol – SWAP) [29] for a broad range of interoperable consumer devices. SWAP is an open industry specification that allows PCs, peripherals, cordless telephones and other consumer devices to share and communicate voice and data in and around the home. Technically it is a mix between a DECT-like mode for real-time (isochronous) services and an asynchronous mode based on the IEEE 802.11 MAC. It does not seem to have gained any real interest in Europe, and just a few product announcements are found for the US. It was specified by the Home Radio Frequency Working Group, which was disbanded in 2002. The HomeRF specification does not seem to have any significant penetration and could be regarded as a curiosity.

3.2.4 MMAC HiSWAN

The Japanese promotion council MMAC (Multimedia Mobile Access Communication System) [30] has developed two WLAN standards available on the market, the HiSWANa for the 5 GHz band, and the HiSWANb for the millimetre wave band. MMAC is now a part of ARIB (Association of Radio Industries and Businesses), which is given public authority to develop radio standards for the Japanese market. The MMAC Forum, ETSI BRAN and IEEE 802.11 has been working together to harmonise the use of WLAN in the 5 GHz band.

3.3 Medium range

Increasing the range of the wireless hop leads us into the class of wireless metropolitan area networks (WMANs) suited to cover smaller or larger areas with more than one household. Current offering is mostly the WMAN standards from *IEEE 802.16*, however ETSI has similar concepts called *HiperMAN*. It has been developed in very close cooperation with IEEE 802.16, such that the HiperMAN standard and a subset of the IEEE 802.16a-2003 standard will interoperate seamlessly. It will not be discussed further here.

WMANs are generally more complex than WPANs and WLANs and demand more planning and operation. Still, it is interesting to consider them, especially because it is possible to use them in unlicensed frequency bands.

3.3.1 IEEE 802.16 WMAN and WiMAX

The *IEEE 802.16* Working Group on Broadband Wireless Access Standards [31] has standardised a "Wireless Metropolitan Area Network" (WMAN) technology.

Initially designed as a standard for fixed wireless access, a wireless alternative to cable based broadband technologies like e.g. DSL, the first version was finished in 2001 standardising a Broadband Fixed Wireless Access (BFWA) system for line-of-sight (LOS) operation in the 10 – 66 GHz band. In 2003 an amendment was released, *IEEE 802.16a*, adding support for non line-of-sight (NLOS) operation in the frequency band from 2 to 11 GHz. A revision of the standard, the *IEEE 802.16-2004* [32] replaced the 2001 version as well as the 802.16a and 802.16c (system profiles for the band 10 – 66 GHz).

The latest amendment is the mobile version, *IEEE 802.16e*, which was approved in 2005 and published in January 2006 [33].

In 2001 the *WiMAX*[6] Forum [34] was formed, a non-profit association with the task of promoting the adoption of IEEE 802.16 compliant equipment by operators of broadband wireless access systems. It works on the compatibility and interoperability of broadband wireless equipment. Therefore, equipment and standards are often referred to as WiMAX and mobile WiMAX. This overview will not consider the fixed WiMAX standards but concentrate on the mobile version.

[6] *Worldwide Interoperability for Microwave Access*

The *mobile WiMAX* based on 802.16e offers a large amount of flexibility with respect to channel bandwidth, utilizing a scalable OFDMA (Orthogonal Frequency Division Multiple Access) technique. Channel bandwidths can vary from 1.25 to 20 MHz.

Mobile WiMAX is currently relevant for three different frequency bands in Europe [35]. The band from 2.5 to 2.690 GHz is currently regulated as the "UMTS extension band"; however, we will probably see the possibility of opening up also for 16e usage. The band from 3.4 to 3.6 GHz is the preferred band for fixed wireless access applications within the CEPT countries, precluding the mobile version at the moment. It will come as no surprise, however, if nomadic and full mobile use will be the natural step. Both these bands are licensed and make it less interesting for an open access provision. The third relevant band is the unlicensed band above 5 GHz, especially from 5.725 to 5.825 GHz. The downside is that some WiMAX manufacturers seem to plan only equipment profiles for the 2.5 and 3.5 GHz bands. In the 5 GHz band mobile WiMAX may compete directly with the 802.11a WLAN standard.

Mobile WiMAX offers high throughput and data rates, up to 30 Mb/s in a 10 MHz channel. Range is generally higher than for WLAN, around 400 – 800 metres in the 2.5 GHz band, a bit lower for 3.5 GHz and even lower for 5 GHz. It also supports the use of MIMO antenna systems which increase the spectral efficiency typically with a factor 2, making it possible to increase the link data rate. Being a complete system, WiMAX supports and specifies mechanisms for both QoS and security.

Since there is a lot of flexibility along several axes, the WiMAX Forum is working to define so-called "profiles"; a subset of elements from the standard with associated frequency band, duplex method and channel bandwidth. Release 1 of the mobile WiMAX profiles will cover 5, 7, 8.75 and 10 MHz channel bandwidths in the 2.3, 2.5, 3.3 and 3.5 GHz frequency bands. Current data rates supported are (e.g.) up to almost 16 Mb/s in a 5 MHz channel using 64-QAM modulation [36].

All IEEE 801.16 standards are designed as systems run by operators and connected to dedicated distribution and core networks. It is then probably most interesting as an overlay for an OAN to maintain the coverage. The modular thinking recognized in all the standards from the IEEE 802 project (both wired and wireless) makes it also possible to imagine the mobile WiMAX used for open access provision alone.

3.4 Summary of standards

Table 3 lists the standards and technologies with some relevant properties regarding bit rates, power, range and frequency bands. Several of the standards

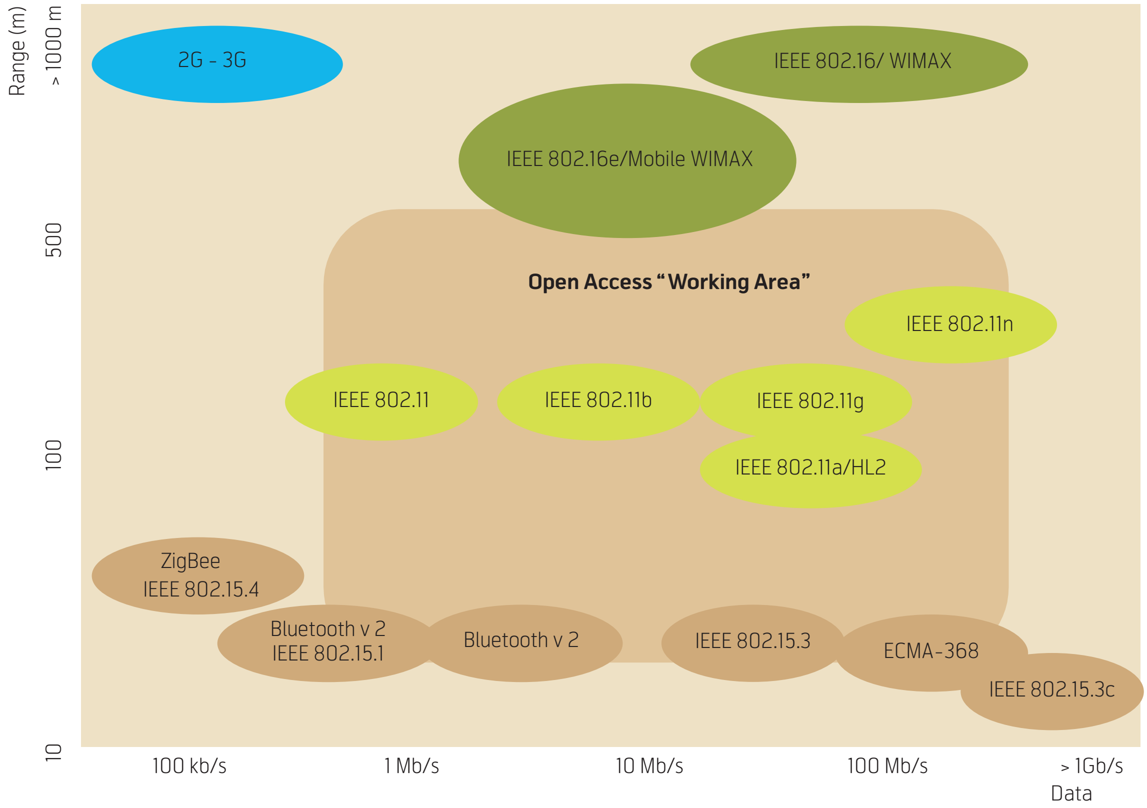


Figure 4 The wireless landscape and the "working area" for an open access provision

ISSN 0085-7130 © Telenor ASA 2006

operate in the unlicensed band from 2.4 to 2.485 GHz, shortened to "ISM 2.4 GHz", and some differences in the regulatory requirements exist between regions and countries as shown in Figure 2 and Table 1. Similar is the situation for the two bands 5.15 – 5.35 GHz and 5.470 – 5.825 GHz, shortened to "5 GHz", as shown in Figure 3 and Table 2. Figure 4 shows the wireless landscape, range vs. data rate, and the interesting "working area" for an open access provision.

4 Discussion

The overview of different wireless technologies available or under work shows a huge amount, and the number is steadily increasing. New standards are providing better and better performance and more and more advanced functionality. A lot of factors are important to assess when evaluating whether a technology is suitable for an OAN provision. The most essential being the ability to provide suitable coverage and traffic capacity. From Figure 4 we see that the WLAN type of technologies is currently in the mainstream of this. However, it is worth noting the mobile WiMAX (802.16e), which by reduced transmitter power will seem very attractive. The question is whether use in unlicensed bands will be available, and whether the other criteria listed (price, form factor, ease of installation) are met. Other articles in this issue of *Telektronikk* give analyses of different OAN provisions [37] [38]. All of these use the cheap and easily available IEEE 802.11 WLAN technology. Comprehensive studies have shown that 802.11 is experiencing severe problems with capacity and range when there is a high density of stations [39] [40]. Maybe the future enhancements must come by using a more advanced technology than WLAN? The short range technologies, like Bluetooth and 802.15 WPANs have shortcomings in providing sufficient coverage. Most technologies (with one exception) operate on frequencies between 2 and 5 GHz, a band most suited to provide the combination of bandwidth / data rate and range / coverage needed.

5 References

1 *The official Bluetooth Web site*.16 July 2006 [online] – URL: http://www.bluetooth.com

2 *The official Bluetooth Membership site*. 16 June 2006 [online] – URL: https://www.bluetooth.org

3 *The Bluetooth SIG. Specification of the Bluetooth System, Version 1.2*. 5 November 2003 [online] – URL: http://www.bluetooth.com/NR/rdonlyres/1F6469BA-6AE7-42B6-B5A1-65148B9DB238/840/Bluetooth_Core_Specification_v112.zip.

4 *The Bluetooth SIG. Specification of the Bluetooth System, Version 2.0 + EDR*. 4 November 2004 [online] – URL: http://www.bluetooth.com/NR/rdonlyres/1F6469BA-6AE7-42B6-B5A1-65148B9DB238/840/Core_v210_EDR.zip.

5 *IEEE 802.15 Working Group for WPAN*. 16 July 2006 [online] – URL: http://www.ieee802.org/15

6 The ZigBee Alliance. *ZigBee Specification. ZigBee Document 053474r06, Version 1.0*. 14 December 2004, Document date: 27 June 2005.

7 *ZigBee Alliance*. 17 July 2006 [online] – URL: http://www.zigbee.org

8 IEEE. *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPANs)*. IEEE, NY, USA, 14 June 2002. (IEEE Std 802.15.1 – 2002)

9 IEEE. *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs)*. IEEE, NY, USA, 29 September 2003. (IEEE Std 802.15.3 – 2003)

10 *WiMedia Alliance Home Page*. 19 July 2006 [online] – URL: http://www.wimedia.org

11 *The European Computer Manufacturer's Association (ECMA) Home Page*. 19 July 2006 [online] – URL: http://www.ecma-international.org

12 The European Computer Manufacturer's Association. *High Rate Ultra Wideband PHY and MAC Standard*. ECMA-368, 1st Edition, December 2005.

13 *UWB Forum Home Page*. 19 July 2006 [online] – URL: http://www.uwbforum.org

14 *IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs). TG3c Project Plan*. Doc. No: IEEE 802.15-05-0311-07. 18 March 2006. 18 July 2006 [online] – URL: ftp://ieee:wireless@ftp.802wirelessworld.com/15/05/15-05-0311-07-003c-tg3c-project-plan.ppt

15 IEEE. *IEEE Recommended Practice for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands*. IEEE, NY, USA, 28 August 2003. (IEEE Std 802.15.2 – 2003)

16 IEEE. *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*. IEEE, NY, USA, 1 October 2003. (IEEE Std 802.15.4 – 2003)

17 *IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs). IEEE P802.15 SG5 PAR and 5C*. 13 January 2004. 18 July 2006 [online] – URL: ftp://ieee:wireless@ftp.802wirelessworld.com/15/04/15-04-0042-01-0005-sg5-par-and-5c.doc

18 *IEEE 802.11 Wireless Local Area Networks – The Working Group for WLAN Standards*. 19 July 2006 [online] – URL: http://www.ieee802.org/11/

19 IEEE. *IEEE Standard for 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*. IEEE, NY, USA, 12 June 2003. (ANSI/IEEE Std 802.11, 1999 Edition (R2003))

20 IEEE. *Supplement to IEEE Standard for 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, NY, USA, 12 June 2003. (IEEE Std 802.11b – 1999 (R2003))

21 IEEE. *IEEE Standard for 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, NY, USA, 27 June 2003. (IEEE Std 802.11g – 003)

22 IEEE. *Supplement to IEEE Standard for 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, NY, USA, 12 June 2003. (IEEE Std 802.11a – 1999 (R2003))

23 IEEE. *IEEE Standard for 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: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe*. IEEE, NY, USA, 14 October 2003. (IEEE Std 802.11h – 2003)

24 IEEE. *IEEE Standard for 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 8: Medium Access Control (MAC) Quality of Service Enhancements*. IEEE, NY, USA, 11 November 2005. (IEEE Std 802.11e – 2005)

25 IEEE. *IEEE Standard for 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 6: Medium Access Control (MAC) Security Enhancements*. IEEE, NY, USA, 24 June 2004. (IEEE Std 802.11i – 2004)

26 IEEE. *IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation*. IEEE, NY, USA, 12 June 2003. (IEEE Std 802.11f – 2003)

27 *Wi-Fi Alliance – Home Page*. 20 July 2006 [online] – URL: http://www.wifialliance.org

ISSN 0085-7130 © Telenor ASA 2006

28 *HiperLAN2 Information Page*. 20 July 2006 [online] – URL: http://portal.etsi.org/radio/HiperLAN/HiperLAN.asp

29 The HomeRF Technical Committee. *HomeRF Specification. Revision 2.01*. 1 July 2002. Available at http://www.palowireless.com/homerf/docs/HomeRF-2.01-us.zip

30 *MMAC Forum – Multimedia Mobile Access Communication Systems*. 20 July 2006 [online] – URL: http://www.arib.or.jp/mmac/e/

31 *The IEEE 802.16 Working Group on Broadband Wireless Access Standards*. 19 July 2006 [online] – URL: http://www.ieee802.org/16/

32 IEEE. *IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems*. IEEE, NY, USA, 24 June 2004. (IEEE Std 802.16 – 2004)

33 *IEEE 802.16e Task Group (Mobile WirelessMAN)*. 19 July 2006 [online] – URL: http://www.ieee802.org/16/tge/index.html

34 *WiMAX Forum – WiMAX Home*. 19 July 2006 [online] – URL: http://www.wimaxforum.org

35 Rheinsson, G B. *Mobile WiMAX – Technical overview and techno-economic analysis*. EURESCOM Project Report, Deliverable D3 from P1554 WiMAP – WiMAX for Mobile Applications. Heidelberg, Germany, EURESCOM, March 2006. Available at http://www.eurescom.de/~pub/deliverables/documents/P1500-series/P1554/D3/P1554-D3.pdf

36 WiMAX Forum. *Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation. WiMAX Forum White Paper*, June 2006. Available at http://www.wimaxforum.org/news/downloads/Mobile_WiMAX_Part1_Overview_and_Performance.pdf

37 Elkotob, M et al. The Open Access Network architectural paradigm viewed versus peer approaches. *Telektronikk*, 102 (3/4), 33–47, 2006 (this issue).

38 Eskedal, T G, Johannessen, T H. Actors, activities and business opportunities in open broadband access markets today. *Telektronikk*, 102 (3/4), 72–84, 2006 (this issue).

39 Håkegård, J E. Multi-cell WLAN coverage and capacity. *Telektronikk*, 102 (3/4), 159–170, 2006 (this issue).

40 Ormhaug, T, Lehne, P H, Østerbø, O N. Traffic capacity and coverage in a WLAN-based OBAN. *Telektronikk*, 102 (3/4), 171–194, 2006 (this issue).

Per Hjalmar Lehne is Researcher at Telenor R&I and Editor-in-Chief of Telektronikk. He obtained his MSc from the Norwegian Institute of Science and Technology (NTH) in 1988. He has since been with Telenor R&I working with different aspects of terrestrial mobile communications. His work since 1993 has been in the area of radio propagation and access technology, especially on smart antennas for GSM and UMTS. He has participated in several RACE, ACTS and IST projects as well as COST actions in the field. His current interests are antennas and the use of MIMO technology in terrestrial mobile and wireless networks and on access network convergence.

email: per-hjalmar.lehne@telenor.com

Multi-Cell WLAN Coverage and Capacity

JAN ERIK HÅKEGÅRD

Jan Erik Håkegård is Research Scientist at SINTEF

As WLAN coverage accelerates, in particular in urban and sub-urban areas, the mutual effect closely located WLAN cells have on each other becomes increasingly important. Interfering WLAN signals that are received with sufficient strength will lead to reduced capacity within a cell, as the interfering signals will trigger "busy channel" detections in the receivers which then defer transmission. Weaker interfering signals entail an increased total noise level in the receivers and reduced coverage. When WLAN coverage is required over a large area, multiple WLANs are needed, and co-channel interference between cells becomes an issue. The capacity per cell is reduced compared to the mono-cell case, and the coverage is reduced and experiences rapid variations. Frequency planning is the most effective strategy for reducing the effect of interference, as the frequency bands allocated to WLAN equipment are large enough to contain several non-overlapping frequency channels.

1 Introduction

WLAN equipment operates in licence free frequency bands, which implies that anyone can buy and set up a WLAN Access Point (AP) and start communication to and from one or several stations (STAs). The 2.4 GHz ISM band used by IEE802.11b and g equipment is in addition open for other communication technologies such as Bluetooth and Zigbee, and equipment such as microwave ovens emit energy in the same band. The 5-6 GHz band used by IEEE802.11a equipment is allocated to WLAN equipment. A major question mark related to the future of the WLAN technology is how the technology will support the increased level of interference, as the number of WLAN networks and other networks transmitting in the same frequency bands accelerates. In this paper we consider the effect of WLAN interference on coverage and capacity.

The first WLAN installations consisted of a single AP, and this is still the case in most WLAN installations; e.g. in homes. In many environments, however, a single AP does not suffice to cover the service area, and several cooperating APs are necessary to provide the required service. Typical examples are large facilities such as office complexes, apartment buildings, hospitals, university campuses and warehouses. The OBAN project is investigating how APs can be joined in an open broadband access network (OBAN) providing security and mobility as well as QoS. A key question in the project is whether the OBAN concept has the potential to provide sufficient coverage and capacity to enable open broadband wireless services to users distributed over a given area. The OBAN concept is described more in detail on the OBAN web site (http://www.ist-oban.org).

The first papers addressing multi-cell WLAN coverage appeared some years ago. The purpose of these papers was to show how multi-cell WLANs could be planned, i.e. where to place APs, based on signal measurements. Rodriquez [1] reported results on optimal AP placement for an indoor environment based on real measurements with no co-channel interference. Hills [2] proposed a two step approach where first optimal AP locations are found and coverage maps created, and then AP frequencies are assigned to maximise the distance between two cells operating on the same frequency. Park [3] reported results for an indoor office environment, and Kamentsky [4] for outdoor campus environments. Common for all these papers are that they base the network planning solely on RF measurements. At about the same time there were other publications addressing WLANs for multi-hop ad-hoc networks. These papers (see e.g. [5] [6]) focused on the characteristics of the IEEE802.11 MAC layer and its poor compatibility with the multi-hop routing protocols developed for ad hoc networks. The problems occurring for multi-hop communications are also relevant for multi-cell WLAN systems. Several recent papers address the MAC-layer interference between APs and STAs belonging to difference cells. Li [7] studied the case where two cells are slightly overlapping, while Panda [8] considered the case where two cells overlap completely. Ling [9] proposed an optimal AP placement method taking into account MAC-layer interference.

In this article we jointly consider the effect of "far" interfering WLAN cells reducing the signal-to-interference ratio (SIR) in the receivers and consequently the size of the cell, and the effect of "close" interfering WLAN cells reducing the throughput within the cell. By jointly considering both types of interference, an assessment of performance of small cells providing continuous 54 Mb/s coverage is compared to larger cells only supporting lower data rates close to the cell borders.

ISSN 0085-7130 © Telenor ASA 2006

In Section 2, we provide a short description of the elements of the OFDM[1)] WLAN standards IEEE802.11a and g that are of importance for interference. Communication coverage and interference ranges are defined in Section 3. The effects of co-channel interference on capacity and coverage are described in Section 4, and quantified for multi-cell networks in Section 5. The main conclusions are drawn in Section 6.

2 Elements of the WLAN OFDM standards

2.1 The packet reception procedure

In order to understand how signals from STAs and APs belonging to closely located WLAN cells interact with traffic within a WLAN, insight is needed into how a WLAN receiver captures a packet. Figure 1 shows the PPDU[2)] frame format. When a PPDU frame is received, synchronisation is obtained through the PLCP preamble. The preamble consists of ten short symbols and two long symbols. The short training symbols contain 12 sub-carriers and are used for signal detection, AGC, diversity selection, coarse frequency offset estimation and timing synchronisation. The long training symbols consist of 53 sub-carriers, and are used for channel and fine frequency offset estimation.

Once synchronisation is obtained, the PLCP header is decoded to give information about the rest of the frame. The PLCP header consists of several fields. The RATE, LENGTH, reserved bit and parity bit constitute a separate single OFDM symbol, denoted SIGNAL. It is transmitted with BPSK modulation and a coding rate of R = 1/2, which corresponds to the lowest and most robust data rate mode of 6 Mb/s. The RATE field contains information about the modulation and coding rate used in the rest of the packet. The following data rates are allowed: 6 Mb/s, 9 Mb/s, 12 Mb/s, 18 Mb/s, 24 Mb/s, 36 Mb/s, 48 Mb/s, and 54 Mb/s. The LENGTH field indicates the number of bytes in the PSDU that the MAC requests the PHY to transmit, and takes on values from 1 to 4095. Hence, after decoding the PLCP header, the receiver knows which modulation and coding rate is used, and the length of the frame. The PSDU (Physical layer Service Unit) is then handed to the MAC layer, which decodes the MAC header to capture the frame type, the transmitting and receiving addresses, etc.

2.2 The CCA mechanism

In the previous sub-section we explained how a receiver obtain information about the data rate mode and the length of a packet it receives with sufficiently good signal quality by decoding the low data rate PLCP header. The PLCP sub-layer also defines how the receiver should react on this information. This is handled by the Clear Channel Assessment (CCA) mechanism, which sends a report to the MAC layer when a "busy medium" condition is detected. The CCA mechanism is defined differently in the two OFDM standards. For IEEE802.11a, the standard states the following:

> *"The start of a valid OFDM transmission at a receive level equal to or greater than the minimum 6 Mbit/s sensitivity (-82 dBm) shall cause CCA to indicate busy with a probability >90 % within 4 μs. If the preamble portion was missed, the receiver shall hold the carrier sense (CS) signal busy for any signal 20 dB above the minimum 6 Mbit/s sensitivity (-62 dBm)."*

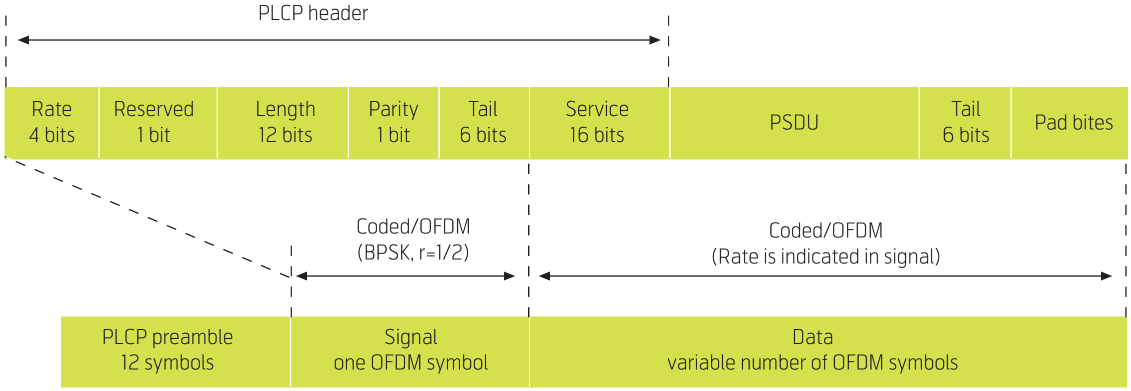


Figure 1 PPDU frame format [10]

[1)] *OFDM (Orthogonal Frequency Division Multiplexing) is a modulation technique where the transmitted information is distributed over a number of orthogonal sub-carriers. It possesses a number of benfits such as high spectrum efficiency and multipath resistance.*

[2)] *PPDU: PLCP (Physical layer convergence protocol) protocol data unit. The PLCP sub-layer is defined to simplify the interface between the MAC layer and the PHY layer.*

In the IEEE802.11g standard the CCA mechanism is defined as follows:

> *"The CCA shall indicate TRUE if there is no CCA "medium busy" indication. The CCA parameters are subject to the following criteria:*
>
> *a) When a valid signal with a signal power of -76 dBm or greater at the receiver antenna connector is present at the start of the PHY slot, the receiver's CCA indicator shall report the channel busy with probability CCA_Detect_Probability within a CCA_Time. CCA_Time is SlotTime – RxTxTurnaroundTime. CCA_Detect_Probabilty is the probability that the CCA does respond correctly to a valid signal. The values for these parameters are found in Table 123E. Note that the CCA Detect Probability and the power level are performance requirements.*
>
> *b) In the event that a correct PLCP header is received, the ERP PHY shall hold the CCA signal inactive (channel busy) for the full duration, as indicated by the PLCP LENGTH field. Should a loss of carrier sense occur in the middle of reception, the CCA shall indicate a busy medium for the intended duration of the transmitted PPDU."*

For both IEEE802.11a and IEEE802.11g equipment, when the PLCP header is received a "busy channel" signal is sent to the MAC layer for the full duration of the frame. In this paper we do not consider the cases where preambles or headers are not correctly received. The CCA sensitivity is then equal to the 6 Mb/s sensitivity in the receivers.

3 Communication coverage and interference areas

3.1 Definitions of communication coverage, CCA area and CCI area

In real implementations, the coverage areas are highly dependent on the surroundings, and on any objects and structures in the propagation environment. Moreover, movements in the propagation environment will make the ranges vary in time, even when the STAs are fixed. In order to obtain analytical results, however, we model the coverage areas as circular.

Two different ranges are of importance for the coverage and capacity of a WLAN:

- The *communication range* R_c is the range from which a receiver can receive and decode data packets with error rates smaller than a given threshold. Each of the data rate modes has its unique coding and modulation scheme, and different modes therefore have different communication ranges. The area which is within communication range of a unit is denoted the *coverage area*.

- The *CCA range* R_{CCA} (also called *sensing range*) is the range from which the CCA mechanism in a receiver can detect a busy channel. Transmissions from any STA or AP within CCA range of an STA or AP will trigger busy channel detection. It does not matter if the transmitting STA/AP is associated to the same BSS or not. When a STA/AP detects a busy channel, it halts the countdown of the back-off mechanism and waits until the channel is idle before it continues. The CCA range is equal to the 6 Mb/s communication range. The area which is within CCA range of a unit is called its *CCA area*.

A unit transmitting from outside the CCA area may cause increased noise plus interference level in the receiver. The required signal level for correct decoding is then increased, as the minimum signal-to-noise-plus-interference ratio (SNIR) must be maintained. This is the traditional effect of co-channel interference (CCI). Units that transmit signals leading to CCI are located within the *CCI area* of the receiver.

Each STA and AP has its communication range and CCA range. Figure 2 illustrates the coverage areas for an AP. The CCA and CCI areas of STA1 are included

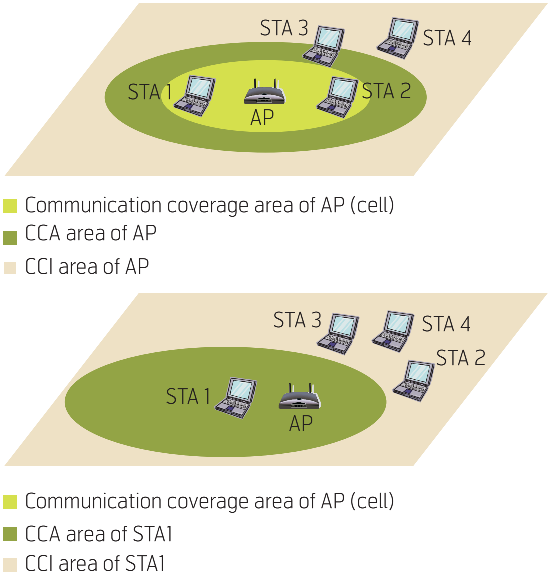


Figure 2 Illustration of communication coverage area, CCA area and CCI area. A communication coverage area smaller than the CCA area corresponds to the case where the minimum data rate mode is higher than 6 Mb/s

in the bottom half of the figure. In the figure R_c is smaller than R_{CCA}. This corresponds to the case where the AP only admits STAs that experience good enough channel conditions to operate on a data rate mode higher than the minimum 6 Mb/s mode. If the AP admits STAs that can only operate on 6 Mb/s, R_c would be equal to R_{CCA}. Symmetrical links is also assumed, i.e. that the STAs and the AP transmit at the same power, and that the sensitivity of all receivers is equal. Hence, if an STA is within the coverage area of the AP, the AP is within the coverage area of the STA.

In the example in Figure 2 the following apply:

- STA1 and STA2 are located within the communication area of the AP, and can be associated with the BSS.

- STA3 and STA4 are located outside the communication range of the AP and consequently cannot be associated with the BSS. They may however be associated with another BSS (which AP is not included in the figure).

- STA3 is located within the CCA area of the AP, which implies that the AP will not transmit when STA3 is transmitting.

- STA4 is located outside the CCA area of the AP and its transmission may lead to reduced communication coverage for the AP, and STA1 and STA2 risk falling outside the communication range of the AP.

- The AP is inside the communication range of STA1. If this was not the case, STA1 could not be part of the BSS.

- STA2 is outside the CCA area of STA1, which means the RTS/CTS access scheme should be applied. If the RTC/CTS scheme is not applied, one would risk STA1 starting to transmit a packet to the AP when STA2 is already transmitting, as STA1 is not able to sense STA2's transmissions. Loss of packets due to collisions and reduced throughput would be the result.

- STA3 is outside the CCA area of STA1, which means that transmissions from STA3 will not prevent STA1 from transmitting, even if the AP is unable to transmit while STA3 is transmitting. The AP may therefore be prevented from transmitting ACK packets when STA3 is transmitting. The communication range of STA1 will also be reduced due to transmissions from STA3, and one risks the AP falling outside the communication range of STA1.

- STA4 is outside the CCA area of both STA1 and the AP. Its transmissions will however reduce the communication range of both STA1 and the AP, and STA1 risks falling outside the communication range of the AP.

3.2 Channel model

The size of the coverage and CCA areas depend on the propagation channel, which can best be modelled in a probabilistic manner. Often, a dual slope model is used, where the path loss is given by the equation shown at the bottom of this page.

The carrier frequency in GHz is denoted f_c, and d is the distance in metres. The breakpoint distance is denoted d_{BP} and the γ-parameter is called the exponential loss factor as it becomes exponential in linear scale. The slope γ_1 before the break point is set to 2 and the slope γ_2 after the break point to 3.5. The s parameter is a zero mean Gaussian random variable modelling the log-normal shadowing function. This channel model is among others used in ETSI and IEEE802.11 documents [15][16].

In the following we use a so-called indoor channel model with break point distance 5 metres and a standard deviation of the shadowing variable equal to 4. The resulting path loss as a function of distance without shadowing is shown in Figure 3.

3.3 Communication and interference ranges

The maximum allowed path loss is a function of transmit power and receiver sensitivity. Table 1 shows the maximum tolerable path loss allowed to operate in three selected data rate modes. The numbers in the table are based on the following parameters (a more detailed description of the parameters can be found in [10][12]):

- Omnidirectional transmit and receive antennas.

- For 802.11 a: EIRP = 30 dBm. This is the maximum mean EIRP allowed in Europe for indoor and outdoor use of IEEE802.11a equipment in the 5.470 – 5.725 GHz band [13]. Use of dynamic frequency selection (DFS) and transmit power control

$$L = \begin{cases} \left[20\log_{10}\left(\frac{40\pi}{3}\right) + 20\log_{10}(f_c) + 10\gamma_1\log_{10}(d)\right] + s, & d \le d_{BP} \\ \left[20\log_{10}\left(\frac{40\pi}{3}\right) + 20\log_{10}(f_c) + 10\gamma_1\log_{10}(d_{BP})\right] + 10\gamma_2\log_{10}\left(\frac{d}{d_{BP}}\right) + s, & d > d_{BP} \end{cases}$$

(TPC) is required to transmit at maximum EIRP. For 802.11g: EIRP = 20 dBm. This is the maximum mean EIRP allowed by the European Radio Communications Committee (ERC) in the 2.4 GHz ISM band [14].

- Thermal noise N_T in the receiver is set to -174 dBm/Hz and the bandwidth B to 20 MHz.

- Noise factor N_F is set to 10 dB.

- Interference margin M_I is set to 5 dB.

- The minimum E_s / N_0 is that required to obtain a bit error rate (BER) less than or equal to 10^{-5}.

The sensitivity S_{RX} (i.e. the minimum required power for the received signal) and the maximum tolerable attenuation $L_{\max}$ are then given by (all in dB):

$$S_{RX} = (E_s / N_0)_{\min} + (N_T + B + N_F) + M_I$$

$$L_{\max} = \text{EIRP} - S_{RX}$$

Table 1 contains the arithmetic mean μ and the standard deviation σ of the communication range for the data rates 54 Mb/s, 24 Mb/s and 6 Mb/s.

In Figure 4 the CCA range of an AP is plotted in a continuous cell pattern with hexagonal cells. The CCA area corresponds to the cell size for 6 Mb/s cells. For the 24 Mb/s cells, it encompasses about half of the six neighbouring cells while for 54 Mb/s it encompasses the six neighbouring cells and almost half of the 12 cells in “ring 2”. These figures call for several comments:

- The shadowing process leads to a dynamic cell size. To obtain, say, 95 % availability of a service the cells would need to be smaller than those in the figures.

- CCI will reduce the size of the cell (and the CCA area).

- The ranges in the figures apply for the AP at the centre of the cell. The closer to the border of the cell a STA is located, the more it will be affected by STAs (and APs) in neighbouring cells.

These three comments all indicate that Figure 4 in many cases will be rather optimistic, and that the effective CCA range may be larger than those indicated in the figure.

4 Effect of co-channel interference on coverage and capacity

4.1 Reduced throughput due to CCA interference

The effect of CCA interference is illustrated by an example where two WLAN cells operating on the

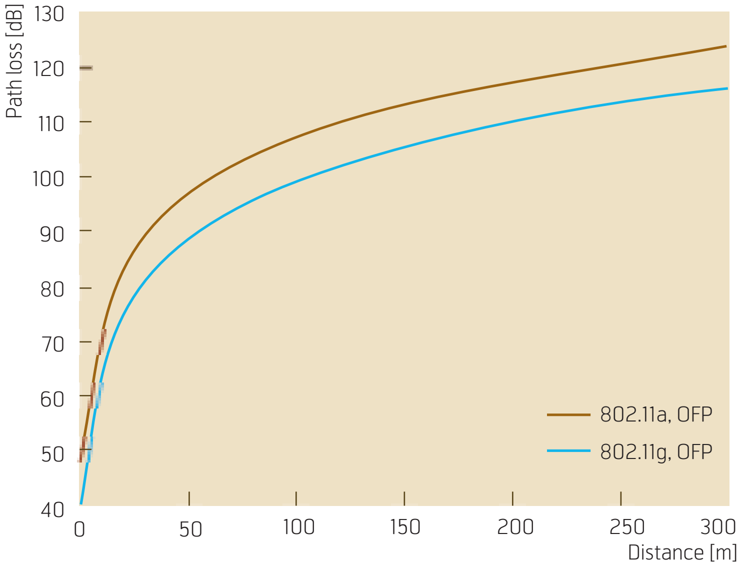


Figure 3 Path loss as a function of distance for the channel model (without shadowing) used

Data rate mode [Mb/s]	54	24	6 (CCA)
Minimum received Es/N0 [dB]	21	12	4
Sensitivity [dBm]	-65	-74	-82
802.11 a (EIRP = 30 dBm)			
Max tolerable attenuation [dB]	95	104	112
Range arithmetic mean μ [m]	48	86	145
Range standard deviation σ [m]	13	23	39
802.11g (EIRP = 20 dBm)			
Max tolerable attenuation [dB]	85	94	102
Range arithmetic mean μ [m]	30	70	118
Range standard deviation σ [m]	8	19	32

Table 1 Communication ranges for IEEE802.11a and IEEE802.11g equipment

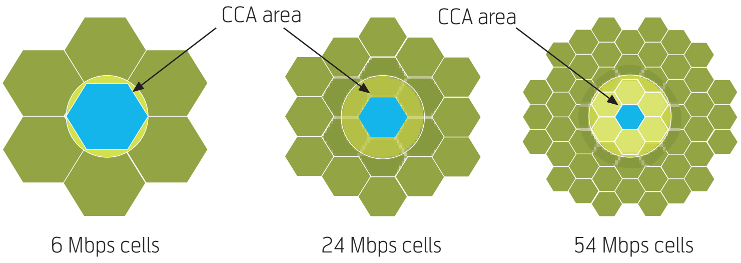


Figure 4 Communication range and CCA ranges for 6 Mb/s, 24 Mb/s and 54 Mb/s cells

ISSN 0085-7130 © Telenor ASA 2006

same frequency channel have overlapping CCA areas (see Figure 5). Each cell contains a number of STAs. The CCA areas of the two APs are denoted A_1 and A_2 and the overlapping area A_{12}. The size of the overlapping area is given by:

$$A_{12} = 2R_{CCA}^2 \arccos\left(\frac{d}{2R_{CCA}}\right) - d\sqrt{R_{CCA}^2 - \left(\frac{d}{2}\right)^2}$$

If $d = 0$ the cells are completely overlapping and all STAs and APs contend for the same channel. Assuming that the two cells are similar in terms of spatial distribution and number of STAs, offered traffic etc., the capacity is then shared equally between the two cells so that each cell obtains half of its original capacity. The other extreme case occurs when $d > 2R_{CCA}$. In that case CCA interference will not occur, and the capacity is equal to the mono-cell capacity.

It is cumbersome to obtain accurate analytical results of the capacity reduction in the partly overlapping case for several reasons:

- Each STA and AP have different interfering STAs within their CCA area. As an approximation we assume that the number of STAs within the CCA area of the APs, which are located in the centre of the cells, is equal to the average number of STAs within the CCA area of all units.

- The data rate modes the STAs operate in depend on their distance to the AP. STAs located close to the AP may operate at 54 Mb/s, and then the data rate is reduced with distance until it reaches 6 Mb/s for STAs located close to the border of the cell. The busy time for a packet transmission highly depends on the data rate mode, and for cells with little overlap only STAs transmitting at low data rates will be in the intersecting area.

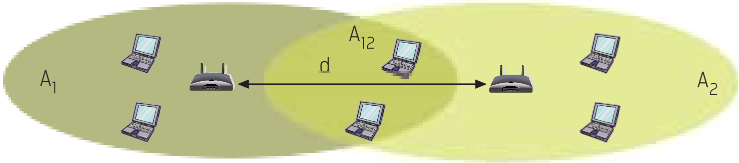


Figure 5 Overlapping cells

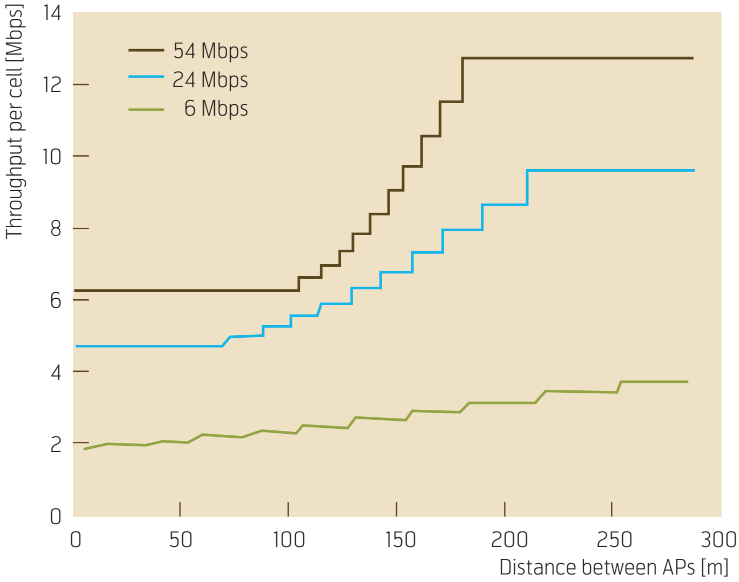


Figure 6 Throughput per cell as a function of distance between APs for IEEE802.11g. The number of STAs per cell is 10. RTS/CTS is used. Frame length is 512 bytes. All STAs operate in same data rate mode

In order to get insight into the effect of CCA interference we have assumed that all STAs in both cells operate in the same data rate mode. The mean communication ranges in Table 1 are then used to calculate the total throughput per cell as a function of the distance between the APs. Denoting the number of STAs within cell 1 and 2 N_1 and N_2, respectively, the number of STAs contending for the same channel resources as AP_1 can be approximated as:

$$N_{Tot}^{CCA} = N_1 + \text{round}\left(\frac{A_{12}}{A_2}N_2\right)$$

The resulting throughput as a function of data rate mode and distance between APs is illustrated in Figure 6 for UDP traffic. The stepwise variation of the throughput is due to the fact that an integer number of STAs contend for the channel. When one more STA is added, the throughput is reduced by a certain interval.

4.2 Edge effects

Figure 4 shows how some cells may be completely within the CCA area of another cell, while others are partly within and partly outside the CCA area of each other. Two problems encountered in partially overlapping cells are the hidden terminal problem and the exposed terminal problem.

The hidden terminal problem is easiest illustrated using a sketch as in Figure 7. The brown and green cells contain one AP and in addition one STA. STA1 communicates with AP1 within the brown cell 1 and STA2 communicates with AP2 within the green cell 2. The two APs do not hear the other AP or the STA belonging to the other cell. The two STAs do however hear each other.

The hidden terminal problem may occur when AP1 transmits data to STA1. STA2 is not aware of this transmission as AP1 is outside its CCA coverage area, and it may start a transmission to AP2 while AP1 is transmitting. The packet from STA2 then interferes with the packet from AP1 at STA1, and as a result the packet transmitted by AP1 to STA1 is lost. Hence, transmission in one cell may cause packets being lost in the other cell.

The effect of the hidden terminal problem can be reduced by using the RTS/CTS access scheme. In this case STA1 will transmit a CTS packet as a response to an RTS packet from AP1. STA2 will hear this CTS packet and not transmit before the AP1-STA1 exchange of packets is terminated. The RTS/CTS will however not always help. STA2 may transmit a packet after AP1 transmits the RTS packets. The RTS packets are however much shorter than most data packets so that the capacity loss due to an RTS packet collision is smaller than the loss due to a data packet collision. RTS/CTS would not help either in the case where AP2 transmits a packet to STA2 and STA2 should return a MAC ACK packet to AP2 during an AP1 transmission to STA1. The MAC ACK packet may then interfere with the packet transmitted by AP1 to STA1. What an STA will do in this case is not clear. The unselfish thing to do would be not to transmit the ACK packet, although AP2 then would retransmit the packet that was successfully received.

The exposed terminal problem may occur in the same scenario as the hidden terminal problem. Figure 7 also illustrates the exposed terminal problem. Again, STA2 transmits data to AP2. In this case however, STA1 does not receive a packet from AP1. Instead, it wants to transmit a packet to AP1. Unfortunately, it hears STA2's transmission and defers transmission because its CCA mechanism reports that the channel is busy. It could however have transmitted its packet, because AP1 cannot hear the transmission from STA2. Hence, a transmission in one cell may lead to increased back-off time in another cell.

In this case it does not help to use the RTS/CTS access scheme as in any case STA1 will refrain from transmitting while STA2 is transmitting. STA1 and STA2 contend for the same channel in the same way as STAs belonging to completely overlapping cells.

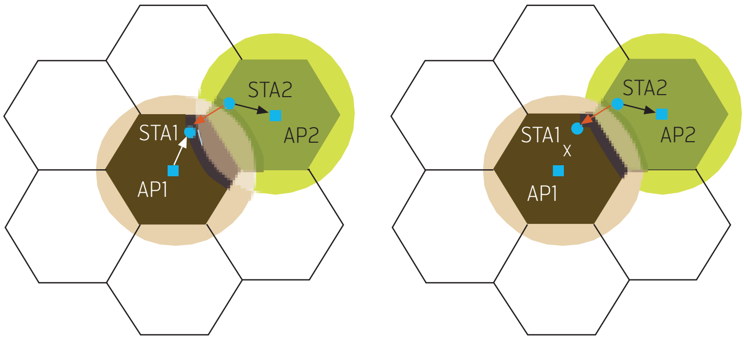


Figure 7 Illustration of hidden terminal problem (left) and exposed terminal problem (right)

From the above descriptions of the hidden and exposed terminal problems, we can conclude that the hidden terminal problem can be significantly reduced also in multi-cell systems by using RTS/CTS schemes, while it would not reduce the exposed terminal problem. Regarding the exposed terminal problem, it can be considered by increasing the number of STAs within the CCA area in a similar way as when analysing completely overlapping cells.

When RTS/CTS is applied the CCA area of cells in a multi-cell network can be approximated to include only complete cells. This is illustrated in Figure 8.

4.3 Reduced communication range due to CCI

Without any interference, the receivers will experience a certain background noise level. Given a thermal noise level of -174 dBm/Hz, a noise factor of 10 dB, and 20 MHz bandwidth, the background noise level is equal to -91 dBm.

Transmissions from interferers that are located outside the CCA area will increase the total noise level (i.e. noise plus interference level) N_{Tot} in a receiver. A signal transmitted from just outside the edge of the CCA area will be received with a power -82 dBm and thus increase N_{Tot} from -91 dBm to -81.5 dBm. If as

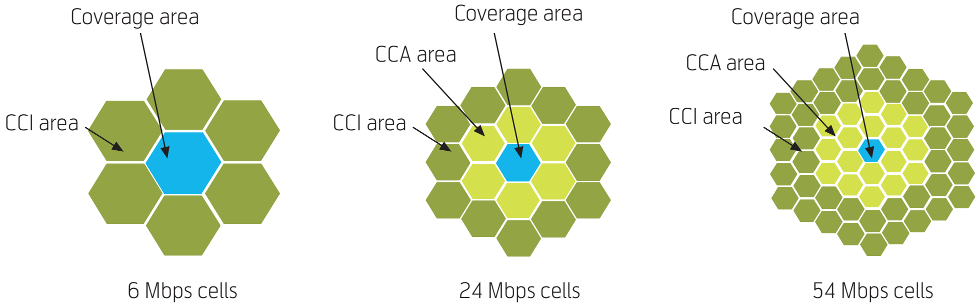


Figure 8 Approximated coverage area, CCA area and CCI area not taking into account edge effects due to partly overlapping cells

ISSN 0085-7130 © Telenor ASA 2006

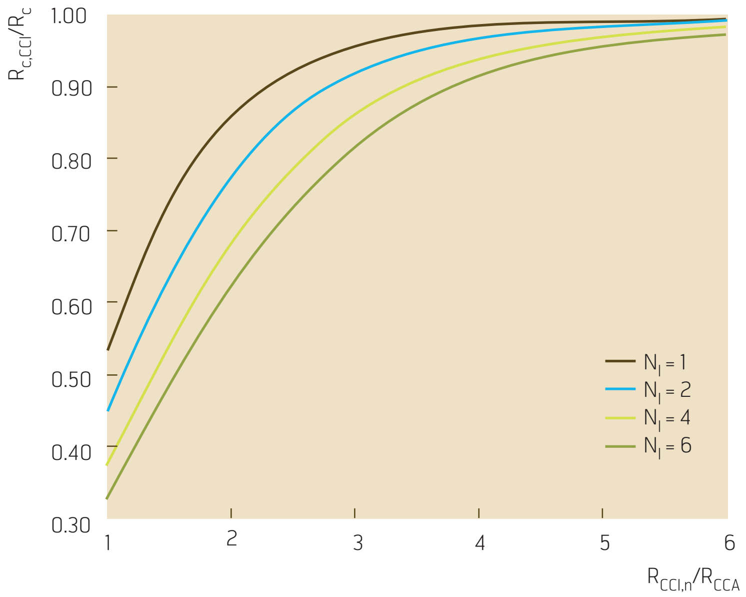


Figure 9 Reduction in cell radius as a function of distance to interfering STAs and number of interfering STAs

many as six interferers are transmitting simultaneously from just at the edge of the CCA area, N_{Tot} will be increased further to -74.1 dBm. As the receivers require a minimum SNR to be able to decode a packet, the interference will lead to reduced communication range. The reduction in communication range can be calculated as (see Appendix A):

$$\frac{R_{c,CCI}}{R_c} = \left(1 + 10^{\frac{M_I + (E_s/N_0)_{\min}}{10}} \sum_{n=1}^{N_I} \left(\frac{R_{CCI,n}}{R_c}\right)^{-\gamma}\right)^{-\frac{1}{\gamma}}$$

where $R_{c,CCI}$ is the communication range with CCI, N_I is the number of simultaneously transmitting interferers, and $R_{CCI,n}$ is the distance to interferer n.

In Figure 9, the reduction in communication range is depicted as a function of the distance to the interfering STAs with respect to the CCA range. The curves show that R_c is reduced to about 55 % of its original size when one STA is transmitting just outside the CCA area. If a total of six interferers, all at the same distance from the receiver are transmitting just outside the CCA area, the communication range is reduced to about 33 % of its original size. The impact of the interference is then reduced as the distance to the source is increased up to a distance 4–6 times R_{CCA}. Beyond this distance, signals will not have any direct impact on neither capacity nor coverage.

In realistic scenarios the interference level will vary in an unpredictable manner. Different STAs and APs will increase the interference level in different degree depending on their location and distance from the receiver. How fast the CCI varies depends on the time it takes to transmit packets, which is a function of data rate mode and packet length. To transmit a 512 byte packet takes about 0.1 ms and 0.75 ms in 54 Mb/s and 6 Mb/s mode, respectively. Moreover, much of the busy channel time caused by a packet transmission is spent transmitting short control packets (RTS, CTS and ACK packets) and in inter-frame spaces with no transmission. Hence, in situations with heavy traffic the level of the CCI will change rapidly.

Another important factor is that each of the interfering STAs also has their CCA areas. There is therefore a limit for how many interfering STAs that can transmit at a given time. As will be apparent later, no more than six interferers in a "ring" around the receiver can transmit simultaneously. Then more interferers can transmit from distances much further away, only having limited impact on the communication range.

The CCA mechanism relies on information in the 6 Mb/s PLCP header. In the presence of interference, the received signal must be stronger also for the CCA mechanism to detect a busy channel. Hence, also the CCA range is reduced as a consequence of CCI, and there is a risk that interfering STAs originally within the CCA coverage area will fall outside and contribute to the CCI with even stronger interference levels.

5 Multi-cell capacity and coverage

In this section we consider the capacity and coverage of multi-cell WLANs, taking into consideration both CCA interference and CCI. AP locations and antenna types should be carefully selected to provide complete coverage of the target space and in most cases it will be necessary with large overlaps between some cells to avoid gaps in the coverage.

There are principally two mechanisms that can be applied to increase the coverage and capacity. They are dynamic transmit power control and frequency planning. The main problem related to AP transmit power control is that it only affects the downlink direction. If the transmit power of the STA is unchanged, the effective coverage area of the AP in the uplink direction is also unchanged. We do not therefore consider transmit power control in this publication, but concentrate on the effect of frequency planning. We assume that the traffic is uniformly distributed over the entire coverage area, and that all cells are identical.

In multi-cell WLANs, continuous high data rate coverage can be obtained with a high density of APs. If APs are located further apart, continuous coverage can still be obtained, but only guaranteeing lower data rates. The latter solution has a few drawbacks. First, the total potential throughput within a cell will be reduced when some users are operating at low

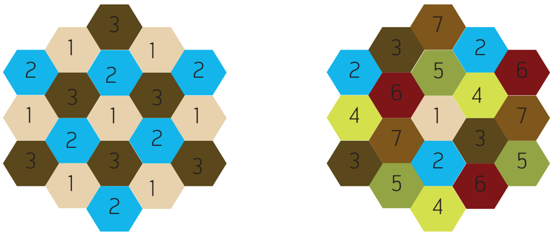


Figure 10 Multi-cell coverage with optimal frequency planning

data rates. Due to the CSMA/CA mechanism of the IEEE802.11 MAC, also users operating at high data rates will experience reduced throughput due to low data rate users. This is commonly known as the anomaly of the IEEE802.11 MAC. Second, it will be necessary to apply the RTS/CTS access to avoid the hidden terminal problem which reduces the throughput. And finally, there will be unfairness within the cell, as users located close to the AP will experience higher throughput than users located close to the border of the cell.

5.1 Frequency planning

The frequency bands allocated to 802.11a and 802.11g equipment permit WLANs to operate on different non-overlapping frequency bands. The 5.6 GHz 802.11a band permits 11 non-overlapping channels (the 5.15-5.35 GHz band is not considered as it is restricted to indoor use), while the 2.4 GHz band used by 802.11g only permits three non-overlapping channels. It is impossible to create repetitive cell groups of size 11 with hexagonal cell pattern. For 802.11a equipment, frequency groups of size 7 are therefore used.

Figure 10 illustrates how frequency groups of sizes 3 and 7 can be created for 802.11a and 802.11g WLANs, respectively, and how the distance between cells operating on the same frequency can be maximised. The number of co-channel cells within the CCA area N_{CCA} when all cells operate on the same frequency channel and with optimal frequency planning (OFP) is shown in Table 2.

The CCI level will also be reduced with OFP. The "close" CCI area is defined as the green cells in Figure 8. The number of co-channel cells within this area containing simultaneously transmitting STAs or AP is denoted N_{CCI}. When all cells operate on the same frequency, N_{CCI} equals 6 as each STA and AP have their own CCA area preventing them from transmitting while other units in their CCA area transmit. Table 2 also contains N_{CCI} with one frequency channel and with OFP.

5.2 Effect of CCA interference

The main effect of CCA interference is that STAs and APs from several co-channel WLANs contend for the same channel resources, and that the throughput per cell consequently drops. In multi-cell networks, the important measure is however throughput per area, rather than throughput per cell, as high density of APs leads to smaller cells.

In order to illustrate the impact of CCA interference we consider the saturation throughput obtained for downlink UDP streaming. Similar results can be obtained considering uplink and mixed uplink/downlink traffic. Bianchi [17] introduced a model for the MAC saturation throughput of WLANs, and the model is referred to and extended in numerous publications. Saturation throughput is defined as the throughput when all STAs and the AP have packets ready for transmission at all times. We use for simplicity the original model and only subtract the traffic generated by the 28 byte UDP-IP header. The model has been verified by means of OPNET simulations, and the difference between analytical and simulation results is within 5 %.

For illustration and simplicity, the hidden and exposed terminal problems are not considered. The CCA area can then be considered to contain a number of complete cells as illustrated in Figure 8. The saturation throughput per CCA area can then be expressed as:

$$S_A = \eta S \frac{N_{CCA}^{1f}}{N_{CCA}}$$

where η is the UDP payload length divided by the total MAC payload length and S is the saturation throughput calculated by means of the expression in [17]. N_{CCA}^{1f} and N_{CCA} are the total number of cells and the number of co-channel cells within the CCA area, respectively.

Figure 11 shows the throughput per CCA area for the three cell size alternatives. For the minimum 6 Mb/s cell case, it does not matter whether frequency plan-

Cell size (min. data rate [Mb/s])	6	24	54
N_{CCA}: One freq.	1	7	19
N_{CCA}: OFP 802.11g	1	1	7
N_{CCA}: OFP 802.11a	1	1	1
N_{CCI}: One freq.	6	6	6
N_{CCI}: OFP 802.11g	0	6	6
N_{CCI}: OFP 802.11a	0	0	6

Table 2 Number of co-channel cells within CCA area N_{CCA} and within "close" CCI area N_{CCI} with one frequency and with OFP

ISSN 0085-7130 © Telenor ASA 2006

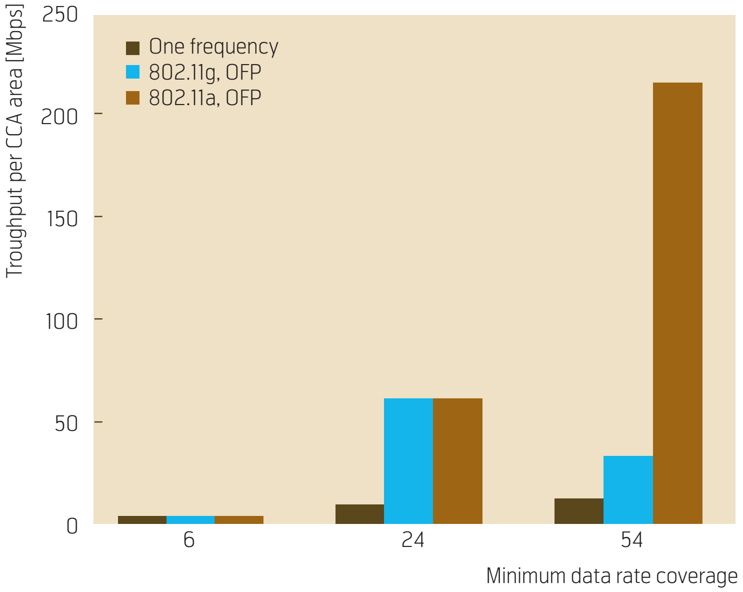


Figure 11 Throughput per CCA area for downlink UDP streaming with OFP and when only one frequency channel is used. Payload length 512 bytes, RTS/CTS enabled

ning is used or not, as CCA interference will not occur in any case according to our model. For the minimum 24 Mb/s cell case, OFP will eliminate CCA interference for both 802.11a and 802.11g equipment. For the 54 Mb/s cell case, OFP reduces the CCA interference significantly with 802.11g equipment and eliminates CCA interference with 802.11a equipment. For 802.11a equipment, the throughput is increased by a factor 58 with continuous 54 Mb/s coverage compared to continuous 6 Mb/s coverage (with OFP and all traffic using minimum permitted data rate mode). The figure also shows that for 802.11g networks, it is better from a capacity perspective to design cells that provide minimum 24 Mb/s coverage than cells that provide 54 Mb/s coverage. The gain obtained by reducing the number of CCA interfering cells from seven to one is then larger than the loss caused by reducing the data rate from 54 Mb/s to 24 Mb/s. When all the cells operate on the same frequency, it is best to have continuous 54 Mb/s coverage. This is as expected, as only one of the STAs and APs within the CCA area can transmit at any time instant, and it is then best that the data is transmitted in 54 Mb/s mode.

5.3 Effect of CCI

The effect of CCI is that the communication range of each data rate mode varies according to the intensity of the interference. Figure 12 illustrates how much the communication range changes as a function of the number of interferers when all interferers are located just at the edge of the CCA area. The mean μ of R_c is used in the calculations. The figure shows that the 6 Mb/s range is reduced significantly. Hence, multi-cell networks planned to provide continuous coverage without taking into account CCI will experience large gaps in coverage. Moreover, an STA located within the 54 Mb/s coverage area of an AP with no CCI is only able to decode packets with maximum data rate 24 Mb/s in the presence of one strong interferer, and packets with maximum data rate 6 Mb/s with six strong interferers. This worst case situation will not occur very often, but also interferers located further away than R_{CCA} will cause the channel conditions to vary significantly. As seen in Sec. 4.3 the CCI varies faster than the busy channel duration of a transmission. It will consequently be difficult to use link adaptation algorithms based on SNR measurements to find the optimal data rate, and traditional statistical algorithms based on counting ACK packets may prove to perform best in systems that experience fast multi-cell CCI.

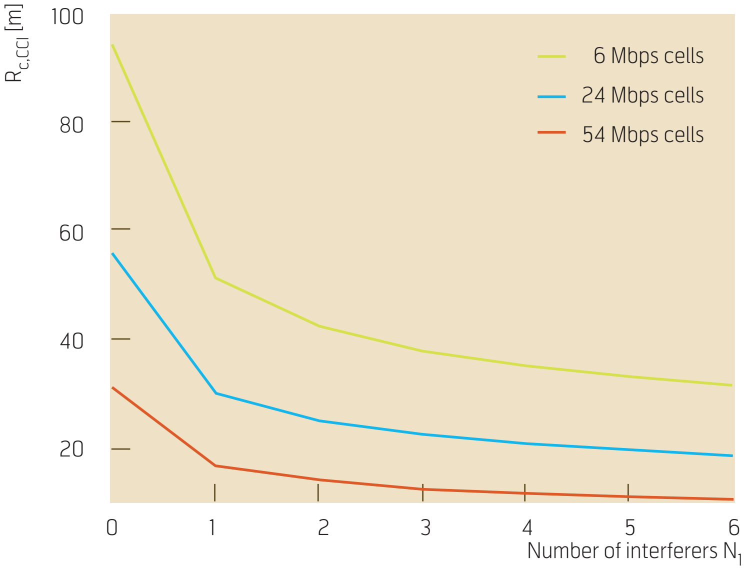


Figure 12 Communication range as function of data rate mode and number of interferers N_I. $R_{CCI,n} = R_{CCA}$ for all n

6 Conclusions

Co-channel interference is an important issue in multi-cell WLAN systems. The worst case occurs when all cells operate on the same frequency channel. When APs are located so densely that the CCA area of one cell contains several other cells, as is the case for e.g. continuous 54 Mb/s coverage, the throughput per cell will be significantly reduced compared to the mono-cell case. Still, such dense AP deployments provide the highest throughput per area as packets transmitted at high data rate need shorter time to be transmitted than packets of similar length transmitted at low data rate.

Interference originating from outside the CCA area will lead to fluctuating coverage. The variations in communication range can be 50 % and even more in worst case scenarios. The fluctuations are very rapid, with time periods less than a millisecond, and unpredictable. These fluctuations will dominate the relatively slow fading and shadowing variations of the propagation channel, favouring ACK based link adaptation algorithms rather than algorithms based on SNR measurements.

When the cells operate on different frequency channels, both throughput and coverage can be enhanced through proper frequency planning. In some cases it may be advantageous to reduce the density of APs as the throughput gain obtained by reduced CCA interference will be larger than the throughput loss due to low data rate coverage. This will however entail unfairness, as STAs located close to the AP will experience higher throughput than STAs located far from the AP.

Multiple frequencies and frequency planning will also reduce the CCI. In contrast to CCA interference, however, frequency planning is combating CCI most effectively when the cells are large. With small cells, there will be no significant reduction in transmitted packets per frequency channel within an area if the increased number of frequency channels is exploited to increase the total traffic. Hence, there will be a trade-off how to exploit the extra bandwidth available in multi-channel networks. Either the capacity can be increased by dense deployment of APs, or more stable coverage can be obtained by increasing the cell size.

Acknowledgement

This work was done as part of the OBAN project supported by the EU 6th framework program, the project partners and the Swiss Bundesamt für Bildung und Wissenschaft (EC contract no 001889). The author would like to thank Per Hjalmar Lehne (Telenor R&D) and Marina Mondin (Euroconcepts) for their contributions related to radio propagation conditions and link budget calculations.

References

1 Rodrigues, R C et al. On the Design and Capacity Planning of a Wireless Local Area Network. *Network Operations and Management Symposium (NOMS)*, Honolulu, Hawaii, 10–14 April 2000, 335–348.

2 Hills, A. Large-Scale Wireless LAN Design. *IEEE Commun. Mag.*, 39 (11), 98–107, 2001.

3 Park, J A et al. Analysis of spectrum channel assignment for IEEE802.11b wireless LAN. *5th International Symposium on Wireless Personal Multimedia Communications*, 3, Honolulu, Hawaii, 27–30 Oct. 2002, 1073–1077.

4 Kamentsky, M, Unbehaun, M. Coverage planning for outdoor wireless LAN systems. *International Zurich Seminar on Broadband Communications, Access – Transmission – Networking*, ETH Zurich, Switzerland, 19–21 Feb 2002, 49.1–49.6.

5 Xu, S, Saadawi, T. Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks? *IEEE Commun. Mag.*, 39 (6), 130–137, 2001.

6 Xu, K et al. How effective is the IEEE 802.11 MAC Handshake in Ad Hoc Networks? *Globecom 2002*, Taipei, Taiwan, 17–21 Nov. 2002, 1, 72–76.

7 Li, Y et al. Co-channel Interference Avoidance Algorithm in 802.11 Wireless LANs. *VTC2003-Fall*, Orlando, FL, USA, 6–9 Oct 2003, 4, 2610–2614.

8 Panda, M J et al. Saturation Throughput Analysis of a System of Interfering IEEE802.11 WLANs. *6th International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM)*, Taormina-Giardini Maxos, Italy, 13–16 June 2005, 98–108.

9 Ling, X, Yeung, K L. Joint Access Point Placement and Channel Assignment for 802.11 Wireless LANs. *Wireless Communications and Network Conference (WCNC)*, New Orleans, LA, USA, 13–17 March 2005, 1583–1588.

10 IEEE. *Supplement to IEEE Standard for 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 for the 5 GHz band*. 2003. (IEEE Std. 802.11a-1999 (R2003))

11 Håkegård, J E et al. *Scenarios and wireless performance and coverage.* IST project OBAN, IST 6FP Contract No 001889, Deliverable D8.

12 Håkegård, J E et al. *D26: Intermediate Report on Coverage and Capacity*. IST project OBAN, IST 6FP Contract No 001889, Deliverable D26.

13 Electronic Communications Committee. *ECC Decision of 12 November 2004 on the harmonised use of the 5 GHz frequency bands for the implementation of Wireless Access Systems including*

Radio Local Area Networks (WAS/ RLANs). November 2004. ECC/DEC/(04)08.

14 *ERC Decision of 12 March 2001 on harmonised frequencies, technical characteristics and exemption from individual licensing of Short Range Devices used for Radio Local Area Networks (RLANs) operating in the frequency band 2400 – 2483.5 MHz.* March 2001. ERC/DEC/(01)07.

15 Medbo, J, Berg, J-E. *Measured radiowave propagation characteristics at 5 GHz for typical HIPERLAN/2 scenarios*. March 1998. ETSI/BRAN document no. 3ERI084A.

16 Erceg, V et al. *IEEE P802.11 Wireless LANs. TGn Channel models*. May 2004. Doc. IEEE 802.16.3c-01/940r4.

17 Bianchi, P. Performance Analysis of the IEEE 802.11 Distributed Coordination Function. In: *IEEE JSAC*, 18 (3), 535–547, 2000.

Appendix A Expression for reduced cell size due to CCI

In this appendix we develop the equation for the reduction in cell size due to CCI. With CCI the communication range of an AP is denoted $R_{c,CCI}$. R_c and $R_{c,CCI}$ are related to the path losses and the channel's exponential loss factor γ:

$$\frac{R_{c,CCI}}{R_c} = 10^{\frac{L_{c,CCI}-L_c}{10\gamma}}$$

where $L_{c,CCI}$ is the path loss in dB for the signal from a STA at the edge of the cell with CCI, and L_c is the path loss in dB for the signal from an STA at the edge of the cell without CCI. The path losses are given by:

$$L_c = EIRP - S = EIRP - ((E_s / N_0)_{\min} + N + M_I)$$
$$L_{c,CCI} = EIRP - ((E_s / N_0)_{\min} + N_{Tot} + M_I)$$

where S is the receiver sensitivity and N_{Tot} is the noise plus interference level. Then we have:

$$\frac{R_{c,CCI}}{R_c} = 10^{\frac{L_{c,CCI}-L_c}{10\gamma}} = 10^{-\frac{N_{Tot}-N}{10\gamma}} = 10^{-\frac{I}{10\gamma}}$$

where I is the interference power. We know that the received signal power from a STA at distance R_c is equal to S. The power of a signal from an interfering STA at distance $R_{CCI,n}$ is then:

$$I = S - 10\gamma \log_{10} (R_{CCI,n} / R_c)$$

For a total of N_I interferers the noise plus interference level N_{Tot} is then given by:

$$N_{Tot} = 10\log_{10}\left(10^{\frac{N}{10}} + \sum_{n=1}^{N_I} 10^{\frac{S-10\gamma\log_{10}(R_{CCI,n}/R_c)}{10}}\right)$$
$$= 10\log_{10}\left(10^{\frac{N}{10}} + 10^{\frac{S}{10}} \sum_{n=1}^{N_I} (R_{CCI,n}/R_c)^{-\gamma}\right)$$

Then we have:

$$I = 10\log_{10}\left(10^{\frac{N}{10}} + 10^{\frac{S}{10}} \sum_{n=1}^{N_I} (R_{CCI,n}/R_c)^{-\gamma}\right) - N$$
$$= 10\log_{10}\left(10^{\frac{N}{10}}\left(1 + 10^{\frac{S-N}{10}} \sum_{n=1}^{N_I} (R_{CCI,n}/R_c)^{-\gamma}\right)\right) - N$$
$$= 10\log_{10}\left(1 + 10^{\frac{M_I+(E_s/N_0)_{\min}}{10}} \sum_{n=1}^{N_I} (R_{CCI,n}/R_c)^{-\gamma}\right)$$

where we have used that $\log_{10}(A \cdot B) = \log_{10}(A) + \log_{10}(B)$. Then:

$$\frac{R_{c,CCI}}{R_c} = 10^{-\frac{I}{10\gamma}}$$
$$= 10^{-\frac{1}{\gamma}\log_{10}\left(1+10^{\frac{M_I+(E_s/N_0)min}{10}} \sum_{n=1}^{N_I} (R_{CCI,n}/R_c)^{-\gamma}\right)}$$
$$= \left(1 + 10^{\frac{M_I+(E_s/N_0)min}{10}} \sum_{n=1}^{N_I} \left(\frac{R_{CCI,n}}{R_c}\right)^{-\gamma}\right)^{-\frac{1}{\gamma}}$$

Dr. Jan Erik Håkegård obtained the degree Siv.Ing. (MSc) in 1990 at the Department of Electronical Engineering and Informatics, Norwegian Institute of Technology (NTH), Trondheim, Norway. In 1997 he got a Docteur (PhD) degree in Electronics and Communications at Ecole Nationale Supérieure des Télécommunications (ENST), site de Toulouse, France. The subject was "Digital receivers for communications over frequency non-selective fading channels". During his PhD studies he had research fellowships at RF System Department, ESTEC (ESA) and at Dipartimento di Electronica, Politecnico di Torino, Italy.
Since 1997 Dr. Håkegård has been working at SINTEF ICT, only interrupted by a one year post doc as a guest researcher at National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA in 1998/1999. At NIST he worked with LMDS systems. At SINTEF he has been working on research and development projects related to various types of wireless communication systems, including satellite communication, 3G mobile communication and short range communication systems.

email: Jan.E.Hakegard@sintef.no

Traffic Capacity and Coverage in a WLAN-Based OBAN

TERJE ORMHAUG, PER HJALMAR LEHNE, OLAV ØSTERBØ

Terje Ormhaug is Senior Research Scientist at Telenor R&I

Per Hjalmar Lehne is Researcher at Telenor R&I and Editor-in-Chief of Telektronikk

Olav N Østerbø is Senior Research Scientist in Telenor R&I

The main idea of the OBAN concept is that the future deployment of broadband access lines and wireless LANs will have so much excess capacity, beyond what will be utilized by the host households, that it can also accommodate public wireless access services. The purpose of this paper is to analyse the viability of this idea with respect to traffic capacity. In the study we have presented three types of results. *Radio coverage* has been analysed for three cases of OBAN environments. This part shows that WLANs are very susceptible to interference from other WLANs. Planning and deploying dense WLAN networks must take this into account, and providing very dense coverage combined with high capacity may seem more difficult than first thought of. Generic *traffic capacity* results show that dense WLAN networks also may bring about MAC interference among a large number of adjacent cells. The consequence is that radios in such clusters of cells have to share the radio medium among them, which severely degrades the traffic capacity. Another decisive parameter is the chosen priority regime between Home Users and Visiting Users. With large MAC clusters, a strict priority regime breaks down. On the other hand, it can be argued that some kind of shared regimes may be beneficial for both the Home Users and Visitors.

In the last part of this article, the results on radio coverage and generic traffic capacities have been combined to derive traffic capacity results for three cases of OBAN environments. The results show that approximately 200 – 300 Visitors making voice calls can be accommodated in environments having the size of 25 – 40,000 m^2. This requires, however, that the radio coverage is based on indoor antennas. When antennas are placed outside the host buildings coverage increases, but so does the MAC interference, with net result that the traffic capacity is reduced to about one third of the indoor cases.

1 Introduction

The main idea of the OBAN [1] concept is that the future deployment of broadband access lines and wireless LANs will have so much excess capacity, beyond what will be utilized by the host households, that it can also accommodate public wireless access services. The purpose of this paper is to analyze the viability of this idea with respect to traffic capacity. Analyzing traffic capacity is about finding quantitative values that characterize the performance of the OBAN concept in terms of business opportunities. *Radio coverage* will be the basis for offering services to OBAN users, but the real test of the concept is whether there is enough *traffic capacity* to carry user applications with a certain probability of success.

1.1 Measure for capacity

An OBAN environment is illustrated in Figure 1. Users entering such an area will not be aware of or care about locations of OBAN access points or shading of radio signals when trying to access services. An ideal quantitative measure for available capacity in a situation could be: Probability of access for specific applications in an OBAN environment. Since we do not have any data about general traffic levels for OBAN type services, we shall in this paper instead apply as measure:

> **Ability to accommodate *N* OBAN Visiting Users running a defined application with a blocking probability less than ε**

The threshold ε may be chosen to be e.g. 1 %. The number of OBAN users depends on what applications they are running, and one may choose one specific application as a yardstick to represent this load. A prerequisite is furthermore that a defined quality of service shall be fulfilled.

To make coverage and capacity figures useful they must be related to situations and conditions that give insight into the usability of the OBAN concept.

- Capacity figures must be given for relevant combinations of terminals and applications. Each application will on the one hand give a traffic load on the network, and on the other hand have quality requirements that must be fulfilled to be successful.

- Different *environments* may offer different conditions for success of an OBAN call. The environments may be characterized by a set of parameters, being either fixed or conditional. Fixed parameters are physical data like density of buildings that are typical for an environment, while conditional

ISSN 0085-7130 © Telenor ASA 2006

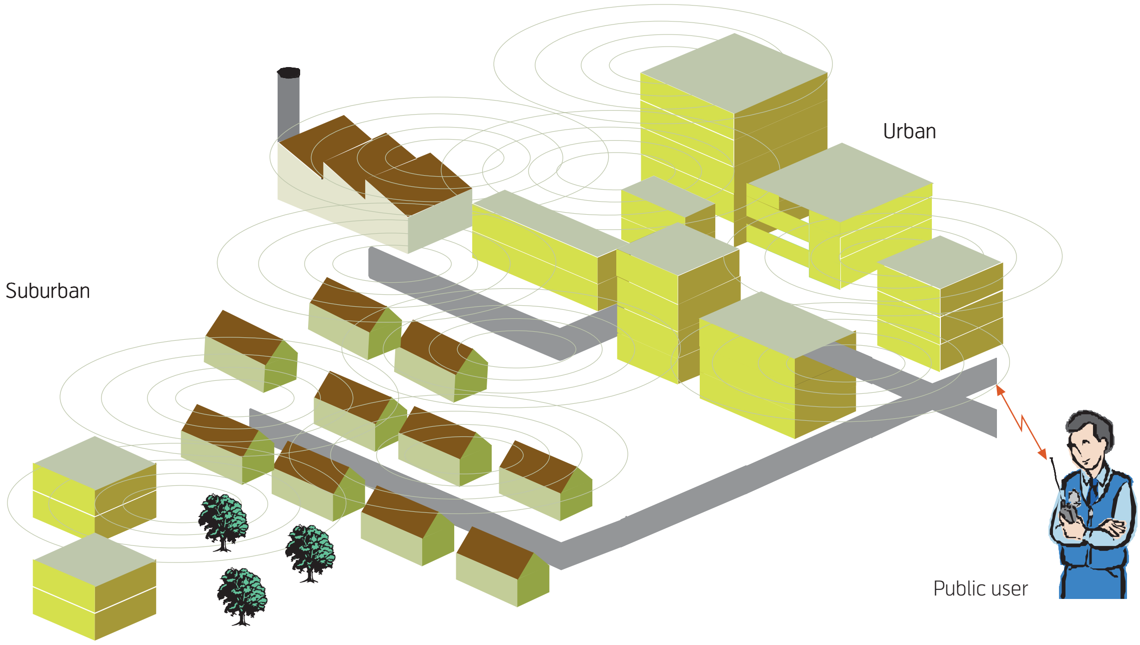


Figure 1 OBAN environment where excess private wireless and broadband capacity is used to offer a public wireless access service

parameters will describe different assumptions about "best case – worst case" situations. Examples are density of OBAN access points within the environment, types of access points, traffic handling schemes, etc.

- Within an environment the success for a user will depend on *stochastic events* like whether he happens to be close to or far from an access point, if he is in a location where the radio signal is obstructed by a wall or trees, if there happens to be few or many users active at the same time, etc.

1.2 Outline

The scope of this paper is to present simulation and analytical studies on OBAN radio coverage and traffic capacity, both for generic situations and for three selected OBAN environments. In order to segment the problem in possible autonomous parts, we have taken the following approach for the study:

1 Three scenarios are defined with respect to physical layout of OBAN environments, deployment of access points and OBAN cells, user behaviour, and priority regimes and QoS handling (section 2).

2 For each of the environments, scenarios for radio coverage are set up and analyzed (section 3).

3 Traffic capacities measured in generic terms are analyzed, conditioned on possible distributions of traffic profiles and location of users within different coverage zones, and different assumptions about density of OBAN cells (section 4).

4 Traffic capacities defined as a probability measure are analyzed for the three environment cases, by combining spatial coverage data, generic capacity results and assumed stochastic user behaviour (section 5).

The paper is organized according to these four steps, with a summary given in section 6.

2 OBAN scenario assumptions

2.1 Three OBAN environments

Three types of areas in the city of Lillestrøm, Norway, have been selected to represent OBAN environments, see Figure 2. These encompass an area with undetached houses and villas, an area with multi apartment buildings, and a central city area.

Characteristics of the areas are shown in Table 1. The number of access points are scenarios for what may be likely or possible deployment of OBAN sites within a time span of 2 – 5 years, based on assumptions about roll-out of number and size of fixed access lines, and take rate for OBAN hosts [2]. The low and high numbers assume a "passive" vs. "active" policy by operators on promoting OBAN among site-owners. The pedestrian activity is only indicative as background for how one could imagine possible public traffic. The figures are measurements from similar environments in Norway [3].

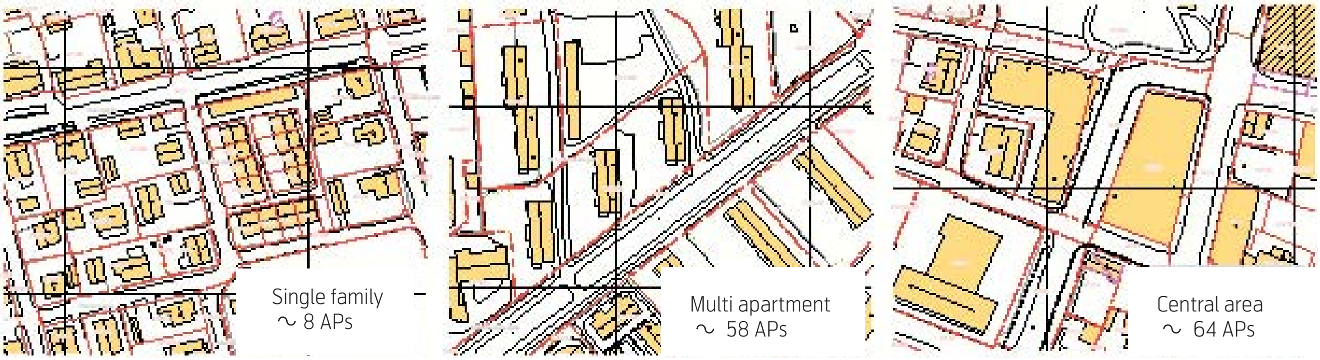


Figure 2 Three environments in the City of Lillestrøm, Norway, used as cases for OBAN capacity and coverage studies, sparse suburban *with single family and undetached houses,* dense suburban *with multi apartment houses, and a* dense urban *area in the city centre. Grid size is 100x100 m*

	Area size [m²]	Number of dwellings/ households	Other facilities	Pedestrian activity ~ persons passing per hour	Assumed number of access points
Sparse suburban (Undetached and detached houses)	25,000	35	2 shops	50	5 – 8
Dense suburban (Multi apartment buildings)	40,000	230	Home for the aged	60	32 – 58
Dense urban (Central city area)	25,000	60	Shops, offices, restaurants, hotel, cinema, etc	900	21 – 64

Table 1 Characteristics of the three OBAN environments in Lillestrøm

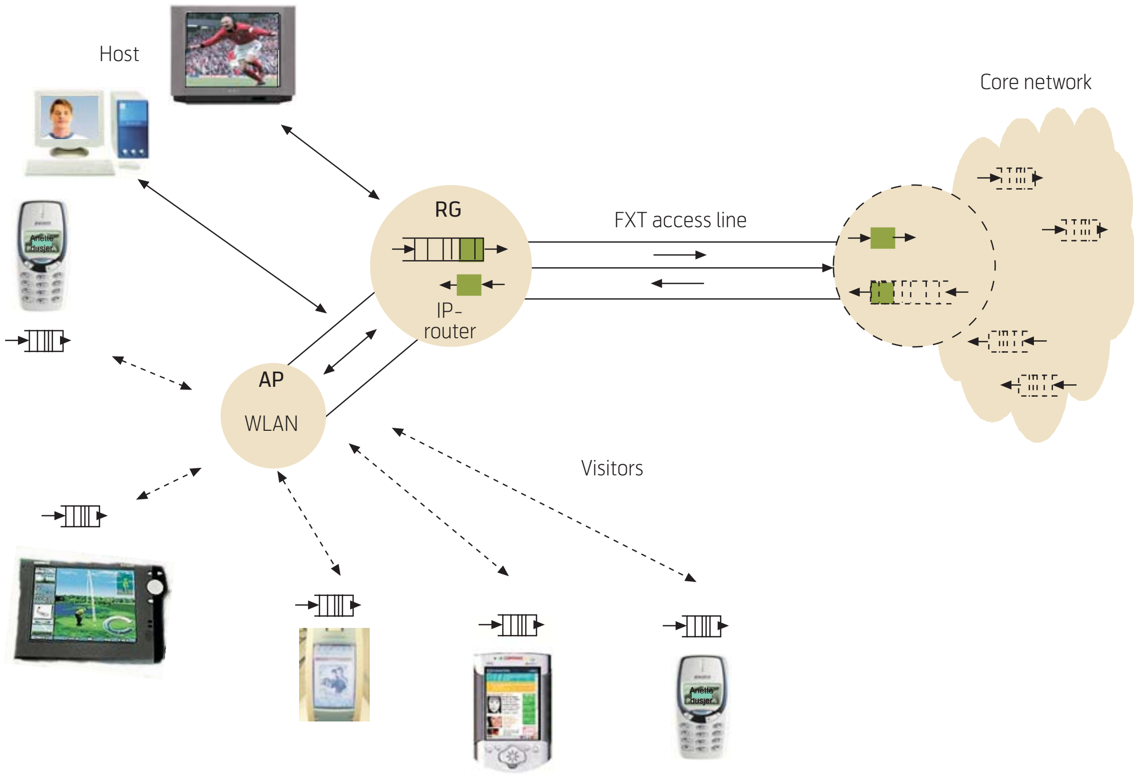


Figure 3 The OBAN traffic machine

ISSN 0085-7130 © Telenor ASA 2006

2.2 The OBAN traffic machine

OBAN traffic in an environment will be handled by traffic machines as illustrated in Figure 3. The main elements of the traffic machine are located at a *Host site*, which is also the domain for the *Home Users (HU)*. The OBAN customers, or the *Visiting Users (VU)* are people who may ask for OBAN services while being in the vicinity of the host site. The OBAN services are operated by some *operator*, who sets the rules and is responsible for securing the quality of the services. The traffic machine consists of the following main elements with functional characteristics:

- *The wireless access point:* The access point is assumed to apply one of the IEEE 802.11a, b or g [4][5][6] access mechanisms. Flow level priority may be applied by use of IEEE 802.11e [7]. The AP may have one or two antennas, located indoor or outdoor at the host site.

- *Residential gateway:* The access point is connected to a residential gateway, consisting of a modem and a router, including SW for handling control and management functions. The router will normally also have interfaces for wired connections to HU's terminals.

- *Fixed access line:* The fixed access line is the broadband connection from the host site to the core network. The connection may be realised on different technologies, like DSL, cable modems, optical fibre, etc. The main generic characteristics are the down and uplink net bitrates. These may be considered either to be subscribed capacities or capacities allocated by the OBAN operator. The operator can extend the capacity on the fixed line beyond what the HU has subscribed for, up to the physical limits of the medium, to better accommodate for VUs' needs.

- *Home User terminals:* The HU's terminals may be both wireless stations and wired units. It is a general assumption that the HU shall have good radio coverage and attain high data rates for their connections. The applications will determine the load and performance of the system. Along with the application bit rate, the segmentation in smaller or larger packets is very decisive for the performance, especially on the wireless drop.

- *Visitors' terminals:* The visitors' terminals are WLAN enabled terminals that also may have multi mode capabilities for access to other wireless technologies when needed. The attainable data rate for a Visitor will depend on the radio coverage, which in general may vary and be of less quality than the Home User experiences.

- *Radio coverage and operational conditions:* Radio coverage depends on technological and environmental conditions and will vary within an OBAN cell. The general situation is also that traffic in adjacent cells will interfere with each other. Depending on distance and general conditions, the interference may be as electromagnetic noise, reducing the radio coverage levels. If however the OBAN cells are so close to each other that stations in one cell can decode the control messages from stations in other cells, stations will back off for each other to avoid radio interference, but instead compete for access to the same radio medium, across the cells. This latter effect is called MAC interference.

- *Operational rules:* Call control will be applied to keep the traffic load within acceptable limits in order to maintain acceptable QoS. There will be priority regimes that discriminate between the HU and the VUs, and possibly between types of services.

2.3 Specific assumptions made for this study

We have restricted this study to only consider IEEE 802.11g as WLAN technology, operating with the DFC (Distributed Coordination Function) [8] access mechanism, and applying the RTS/CTS (Request to send, Clear to send) mechanism. We have furthermore based our analysis on some best-case assumptions that will be described in the course of the presentation.

2.3.1 The single cell and multi cell view

When we analyze coverage and capacity for OBAN environments, we may apply two different views: either consider single OBAN cells with one access point each, or consider an area consisting of several cells. If we apply the single cell view, the traffic in neighbouring cells should be considered as external traffic, generating either kind of interference. The main view taken in this paper, however, is to analyze capacity jointly for several OBAN cells, but still it is also useful to have the single cell view in mind.

2.3.2 Applications and user traffic

The vision is that an OBAN network should be able to handle "any" broadband nomadic or mobile application for Visiting Users, along with serving the Home Users' fixed or wireless services. For the studies it is important to ensure that the applications span realistic alternatives with respect to how the network may be loaded. In addition to bit rate requirements, the segmentation of data in large or small packets is decisive for *useful* network utilization, as described in section 4.

Another important characteristic is the applied transport protocol, i.e. use of UDP or TCP. Applications carried on TCP are able to adapt the data rate to the available capacity at any time.

For the study as presented in this paper we have selected a limited set of applications that we consider to be representative for OBAN traffic, as shown in Table 9 and Table 10.

2.3.3 Priority regimes and traffic control

The Home Users and the Visiting Users are sharing the capacity of the local fixed access and wireless network, but the general idea for the OBAN concept is that the Home Users shall not suffer for allowing Visitors to use their network. The two will therefore normally have different priorities to network resources, but several priority schemes may be envisaged. Alternatives may vary between very strong priorities for the Home Users vs. capacities being shared on equal terms. The latter may be motivated by economic incentives for the Home Users.

In this paper we shall investigate two different priority regimes for allocation of capacity to Home Users and Visitors. One is based on a strict reservation of capacity for the Home User, which cannot be utilised in any way by Visitors, even if it is unused. The other regime still gives priority to Home Users' traffic, but allows a more flexible utilisation of temporarily unused capacity.

Several traffic control mechanisms may be applied to enforce traffic control and priority rules in an OBAN network, ranging from access priorities, to transmission media at flow level, to traffic acceptance at call level.

- The QoS broker proposed for OBAN [9] will control set up of new, and possibly discard established calls, based on priority criteria among traffic types and users. Decisions may be based on traffic monitoring and/or status of established calls

- Mechanisms at the transport layer make TCP traffic give way to un-elastic UDP traffic, and otherwise try to utilize all available capacity.

- On the wireless drop IEEE 802.11e can be applied to give priorities for media access between four defined types of traffic classes. This may be useful in order to avoid short time disruptions of real-time traffic.

- At the fixed access queuing priorities between traffic flows may be applied to avoid flow disruptions.

3 OBAN scenarios and radio coverage

With radio coverage we mean the area in which certain signal quality parameters are above a given threshold. Different parameters may be used to quantify this. Radio engineers will usually measure coverage based on physical parameters like signal strength, signal-to-noise ratio (SNR) or the signal's bit/packet error rate. A service provider, on the other hand will be quite indifferent to these kinds of measures and prefer service availability as the measure. Service availability is of course a function of the radio signal's physical quality, but other factors also come into it. In this section, we will elaborate on the coverage from a radio physical point of view, while later sections take this up to higher levels.

3.1 Path loss models

Path loss, *L*, is defined as the ratio between the transmitted power and the received power over a radio link in the case of isotropic[1)], lossless antennas. This means that the path loss describes the effect of the physical medium between the transmitter and the receiver without the influence of directive antennas and equipment impairments. Note that $L > 1$ (or $L > 0$ dB). This is shown in Figure 4.

If we want to calculate the received power in a specific case when transmitter power, antenna gains and losses are known we can then use the following equation:

$$P_R = \frac{G_T \cdot G_R}{L} \cdot P_T \qquad (1)$$

where

G_T is the transmitter antenna gain
G_R is the receiver antenna gain
P_R is the received power
P_T is the transmitter power
L is the propagation path loss.

3.1.1 Free space propagation

There are numerous models for path loss prediction in the outdoor case. The simplest method to use is to

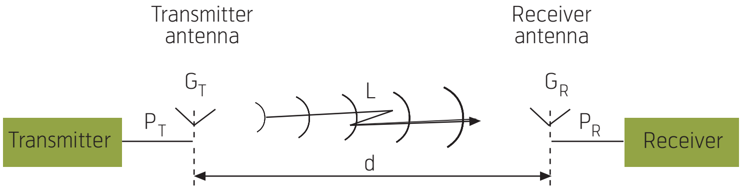


Figure 4 Wireless transmission chain showing essential parameters

[1)] *An isotropic antenna has unity directivity and gain in all directions. It is a theoretical construction.*

ISSN 0085-7130 © Telenor ASA 2006

assume free space, in which the Friis equation gives the ratio between received and transmitted power:

$$\frac{P_R}{P_T} = G_T G_R \left[\frac{c}{4\pi f d}\right]^2, \tag{2}$$

where we can recognize the path loss in the last factor:

$$L_{FS} = \left[\frac{4\pi f d}{c}\right]^2 \tag{3}$$

The distance d is given in metres and the frequency f in Hz. Expressed in dB and inserted values for π and the light speed c we get:

$$L_{FS(dB)} = 32.4 + 20 \log f_{(MHz)} + 20 \log d_{(km)} \tag{4}$$

The free space model can often be used in cases where there is good line-of-sight (LOS) between transmitter and receiver; however possible reflections from the surroundings (terrain and buildings) distort this. Therefore better models have been developed based on a combination of measurements and analytical methods.

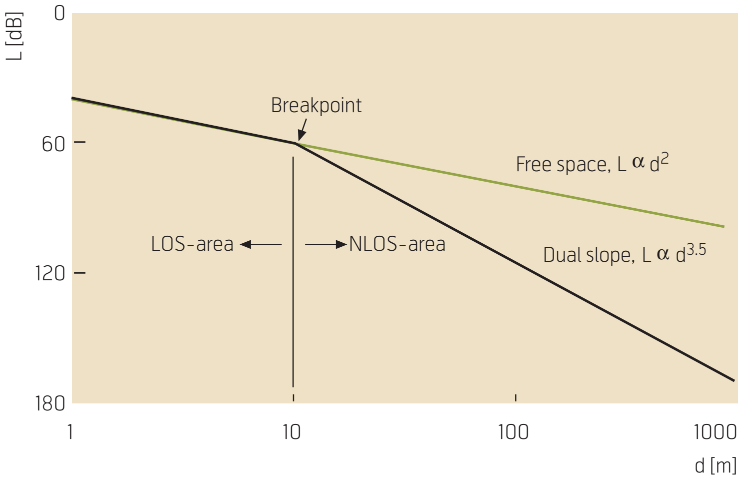


Figure 5 Distance properties of the free space and dual slope path loss models

3.1.2 Empirical dual slope models

There are several empirical models for different frequency bands and geographical environments. In this article we will concentrate on a suite of models developed by the IEEE 802.11, Task Group n for the purpose of system evaluation in real scenarios [10]. The path loss property of the models belongs to a class called "dual slope", opposed to the free space model which is described by a single slope.

In case of indoor propagation, up to the so-called breakpoint distance, d_{BP}, the free space signal attenuation model applies (where the attenuation is proportional with d^2), while for longer distances the additional attenuation increases with $d^{3.5}$ as shown in Figure 5. The random property of shadowing can also be accounted for through a random variable s with proper statistical characteristics. The signal attenuation can therefore be expressed as:

$$L_{(dB)} = L_{FS(dB)} + s \quad \text{with } d \leq d_{BP} \tag{5}$$

$$L_{(dB)} = L_{FS(dB)}(f_c,\ d_{BP}) + 35 \cdot \log_{10}\left(\frac{d}{d_{BP}}\right) + s$$
$$\text{with } d > d_{BP} \tag{6}$$

The breakpoint distance, d_{BP}, models that the path loss is basically line-of-sight nearer than this, and, at least partly, non-line-of-sight (NLOS) further away. The parameter s is a zero mean Gaussian random variable modelling statistical shadowing of the channel.

In summary, the characteristics of the models suggested for different environments are shown in Table 2.

3.1.3 Propagation through buildings and walls

Path loss estimations can be further tuned by introducing additional attenuation due to walls etc. Table 3 shows the attenuation one can expect when the signal is propagating through different materials [11].

			Slope exponent		Standard deviation of shadowing variable, *s*	
Model	Environment	Breakpoint distance, d_{BP}	Near, $d \leq d_{BP}$	Far $d > d_{BP}$	Near $d \leq d_{BP}$	Far $d > d_{BP}$
A	Indoor (no multipath)	5 m	2	3.5	3 dB	4 dB
B	Residential	5 m	2	3.5	3 dB	4 dB
C	Residential / Small Office	5 m	2	3.5	3 dB	5 dB
D	Typical Office	10 m	2	3.5	3 dB	5 dB
E	Large Office	20 m	2	3.5	3 dB	6 dB
F	Large Space (indoors/outdoors)	30 m	2	3.5	3 dB	6 dB

Table 2 Channel models definitions from IEEE 802.11 [10]

Material	Attenuation
No wall	0 dB
Window in brick wall	2 dB
Metal door in brick wall	12 dB
Thick concrete wall	40 dB

Table 3 Attenuation through walls [11]

3.2 Channel multipath

A real wireless channel can be described by several more properties than just path loss. Multipath transmission occurs when reflected and diffracted copies of the transmitted signal mix with different time of arrival in the receiver and distorts the signal pulse shape. Such delayed and attenuated echoes may arrive much later than the signal's symbol duration, thus creating interference in later symbols. Such behaviour is usually modelled with a finite impulse response (FIR) filter containing a number of taps given in the last columns. The value of each tap is however a stochastic number, usually Rayleigh distributed. This property of the radio transmission is very important, especially for high mobility cellular systems like GSM and UMTS. These systems have mechanisms to deal with this and improve reception. WLANs however, have no techniques; thus a general degradation of the signal-to-noise ratio is the result. Multipath propagation is not considered further in this article.

3.3 Range calculations

The shadowing variable introduces a stochastic element which gives us a measure of the uncertainty. Statistical shadowing of the channel means that the range also will have a statistical distribution. The path loss values calculated by the equations above are Gaussian distributed with the same standard deviation as the shadowing variable *s*. Since the path loss *L* in dB is linear in $\log_{10}d$, it follows directly that $\log_{10}d$ is Gaussian distributed for a given value of *L*. The deterministic parts of the equations give the mean value of $\log_{10}d$, while the standard deviation is scaled by the inverse of the slope and given in Table 4.

It follows that the distance itself, *d*, is log-normally distributed with mean and variance (square of standard deviation) given by:

$$\mu_d = e^{\ln 10\cdot\mu_{\log 10_d} + \frac{1}{2}\cdot(\ln 10)^2\cdot\sigma^2_{\log 10d}} \tag{7}$$

$$\sigma_d^2 = e^{2\cdot\ln 10\cdot\mu_{\log 10d}}\cdot \left(e^{2\cdot(\ln 10)^2\cdot\sigma^2_{\log 10d}} - e^{(\ln 10)^2\cdot\sigma^2_{\log 10d}}\right) \tag{8}$$

Where 'ln' is the natural logarithm, ln10 ≈ 2.3. From the expressions we see that both the mean and standard deviation vary with the distance.

The parameters of the model B are often recommended for indoor use in residential areas and could also give reasonable results for the outdoor coverage with an indoor antenna. The F model could be suitable for residential areas, where the antenna is placed outdoors.

In the remaining part of this article, we have mostly chosen to use model B for both indoor-to-outdoor coverage and for outdoor coverage with outdoor antennas. This is also a reasonable choice for outdoor conditions with a fairly high building density.

3.3.1 Single-cell OBAN coverage

The formulas and method above make it possible to estimate the coverage of a wireless system. Additionally, we need system specific data about transmitter power, antenna gain and receiver sensitivity. In this article, we will concentrate on the IEEE 802.11g standard. The standard defines eight possible data rates ranging from 6 to 54 Mb/s, but we have concentrated on doing estimations only for three of them: 6, 24 and 54 Mb/s. The essential parameters necessary for coverage calculations are given in Table 5.

If we insert the values for the mean and the standard deviation of $\log_{10}d$, we get the range values given in Table 6 for the three chosen data rate modes.

The average (arithmetic mean) value for the cell size is larger than the value we get if the shadowing part *s* is omitted. This is because the log-normal distribution is asymmetrical. The median and quantiles are unaffected by this and are better measures because they give directly the probability of having the outcome above/below the given value. The median (50 %) and quantiles are also given in Table 6. These are not biased due to the change in distribution.

The cumulative probability functions (cdf) of the range limits give us the probability that the limit is less than a given value. This is the complementary probability of actually being within the boundary:

	Standard deviation for $\log_{10}d$	
Model	Near (LOS) $d \leq d_{BP}$	Far (NLOS) $d > d_{BP}$
B	0.150	0.114
F	0.150	0.171

Table 4 Standard deviation of log-distance for the channel models B and F

Bit rate (data rate)	6 Mb/s	24 Mb/s	54 Mb/s
Maximum EIRP[2] according to European regulations	100 mW / 20 dBm		
Receiver antenna gain	0 dBi		
Thermal noise	–174 dBm/Hz		
Channel bandwidth	22 MHz		
Receiver noise factor	10 dB		
Receiver noise power	–90.6 dBm		
Implementation/fading margin	5 dB		
Minimum signal to noise ratio at receiver	4 dB	12 dB	21 dB
Minimum power at receiver (sensitivity)	–81.6 dBm	–73.6 dBm	–60.6 dBm
Maximum allowed path loss between transmitter and receiver	101.6 dB	93.6 dB	80.6 dB

Table 5 Parameters of relevance for coverage estimations for the 802.11g standard. The minimum signal to noise ratio (SNR) and sensitivity are those defined by the 802.11g [6] standard in order to obtain a bit error rate, BER, of less than 10^{-5}

	Indoor and outdoor, channel model B			Outdoor open space, channel model F		
Available data rate	6 Mb/s	24 Mb/s	54 Mb/s	6 Mb/s	24 Mb/s	54 Mb/s
Arithmetic mean, μ	118 m	70 m	30 m	266 m	158 m	67 m
Standard deviation, σ	32 m	19 m	8 m	109 m	65 m	27 m
10 %-Quantile	81 m	49 m	21 m	148 m	88 m	37 m
Median (50 %)	114 m	68 m	29 m	246 m	146 m	62 m
90 %-Quantile	160 m	95 m	41 m	408 m	242 m	103 m

Table 6 Resulting values for mean (μ), standard deviation (σ), 10 %, 50 %, and 90 % quantiles for the cell sizes when stochastic shadowing is taken into account. IEEE 802.11g at 2.45 GHz

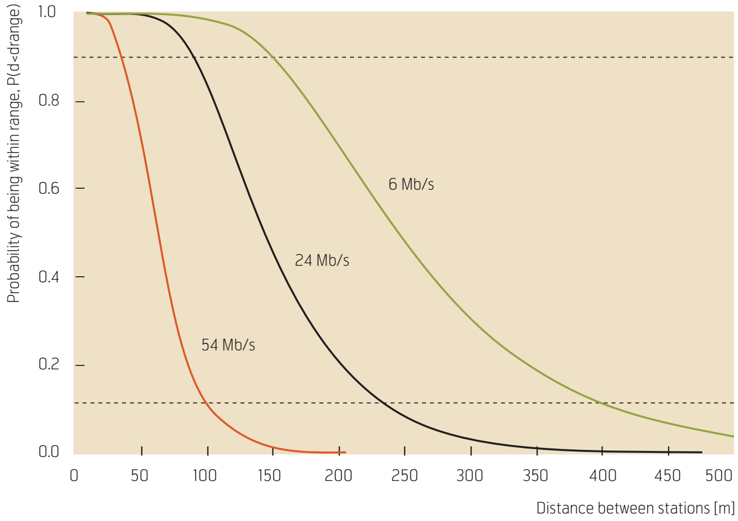


Figure 6 Probability of being within range of 6, 24 and 54 Mb/s service areas for IEEE 802.11g at 2.45 GHz with antennas placed outdoors (Channel model F)

$$P(d < d_{range}) = 1 - P(d \geq d_{range}) \\ = P('\text{I am within range}') \qquad (9)$$

Figure 6 shows an example of this probability distribution. As we can see, a significant variation in coverage can be expected.

3.3.2 Multi-cell interference

So far we have considered the range and coverage aspects of a WLAN system under the assumption that there is no disturbance of the radio signal. In real life sources of disturbance always exist, and in communication terms this is called interference. WLANs operate in unlicensed bands with a limited number of channels as shown in Figure 7 for the 2.45 GHz band. Since there is no coordinated channel use, the likelihood of ending up at the same channel is quite high, which means that the main source of interference

[2] *EIRP – Effective Isotropic Radiated Power is the amount of power that would have to be emitted by an isotropic antenna (that evenly distributes power in all directions) to produce the peak power density observed in the direction of maximum antenna gain.*

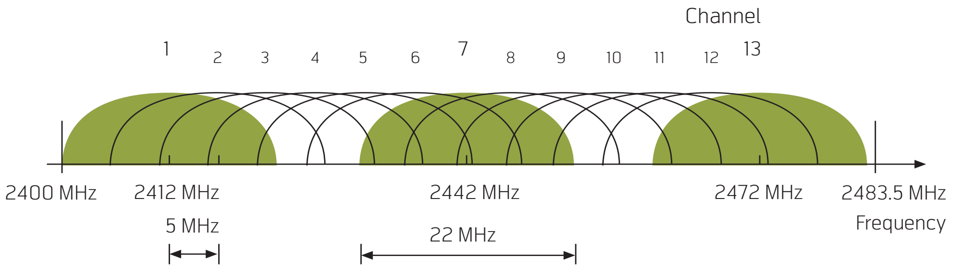


Figure 7 European channel plan for 802.11b and g in the 2.45 GHz band

is other WLAN stations. Choosing 802.11a in the 5 GHz band improves the situation significantly; however most use of WLANs today is in the 2.45 GHz band.

The performance of WLANs is degraded in two ways when subjected to foreign WLAN signals, dependent on the distance from the disturbing station ("interferer").

If stations are within detection range of each other, mechanisms are built into the medium access layer (MAC) protocol in order to avoid simultaneous access of the channel. WLANs of the 802.11 standard use a channel access technique called Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). Before a WLAN station attempts to send a packet, it checks for ongoing traffic. If such traffic is detected, a signal called Clear Channel Assessment (CCA) is sent from the physical layer upwards to notify the MAC layer of the channel status. If the channel is detected busy, the transmission is deferred to a later point in time. The effect of this mechanism is that average throughput for a station is reduced when several stations contend for the same channel. We can call this a near-neighbourhood effect, or MAC interference, which turns out to be very decisive for the traffic capacity of OBAN networks, as described in section 4.

However, even if stations are not within detection range of each other, they are still susceptible to disturbance. In this far-neighbourhood setting, other stations will be perceived as noise. A station will not detect a busy channel, and if it tries to establish a link to another station, the signal quality will be degraded due to co-channel interference (CCI).

The interference ranges are illustrated in Figure 8. The so-called CCA coverage range defines the area in which the busy detection technique makes the station defer transmissions if other stations in the area are active. The CCA range is defined by the detection threshold with is for 802.11g in the 2.45 GHz band defined to be at maximum -76 dBm [6], while for the 802.11a in the 5 GHz band it is -82 dBm [4]. The threshold for the physical layer interference (CCI) can typically be defined to be the same as the receiver input noise level. This is defined by the thermal background noise, the channel bandwidth, and the receiver's own noise figure (typically 10 dB). The resulting threshold can then be assumed to be -91 dBm (ref Table 5). A single remote source providing this level at the receiver's input, will then de-sensitize the receiver by 3 dB.

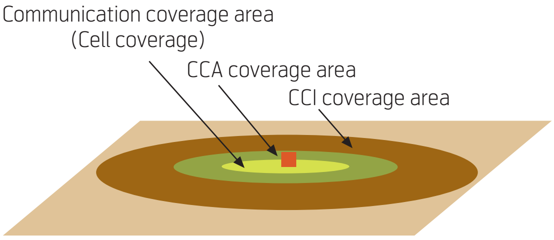


Figure 8 Illustration of interference ranges

The range corresponding to the thresholds are dependent on the propagation conditions as explained earlier. Again, concentrating on the most deployed WLAN standard, the 802.11g, the ranges for MAC and physical layer interference are given in Table 7, given that all stations transmit at maximum allowed power of 100 mW.

The interference ranges can reach quite far, especially in outdoor settings. This means that the interference

	Indoor and outdoor, Channel model B		Outdoor open space, Channel model F	
	CCA range	CCI range	CCA range	CCI range
Arithmetic mean, μ	82 m	213 m	185 m	481 m
Standard deviation, σ	22 m	57 m	76 m	197 m
10 %-Quantile	56 m	147 m	103 m	268 m
Median (50 %)	79 m	206 m	171 m	445 m
90 %-Quantile	111 m	289 m	284 m	738 m

Table 7 Resulting values for mean (μ), standard deviation (σ), 10 %, 50 %, and 90 % quantiles for the detection range (CCA) and the physical layer interference range (CCI)

ISSN 0085-7130 © Telenor ASA 2006

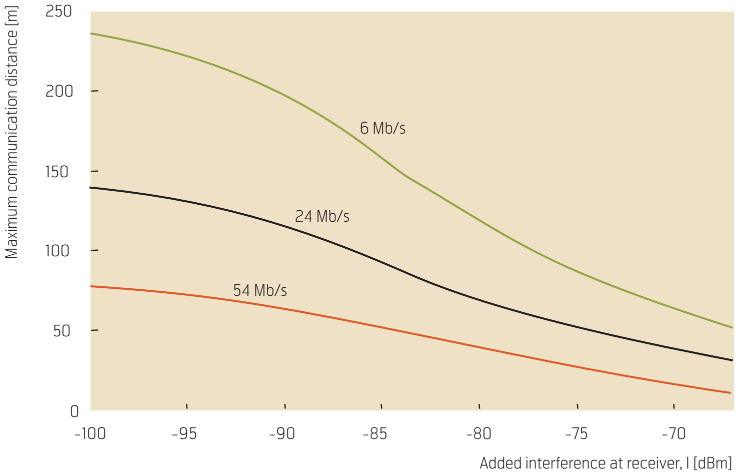


Figure 9 Range reductions (median values) due to physical layer interference for an outdoor scenario of 802.11g operating in the 2.45 GHz band

level can be significant when the density of active stations, e.g. in a hotspot area or a dense residential area is high. It is also quite typical that many stations use the same channel, since these are often factory presets. In the OBAN project comprehensive studies of this effect have been done [2][12]. Typical values for the interference level have been estimated based on traffic levels and station densities. For example, 12 foreign stations in the "far" neighbourhood using the same channel as "our" station on average 300 m away in an outdoor scenario results in a noise contribution of approximately -84 dBm if all stations are simultaneously active. The OBAN studies also revealed that there is a maximum level due to the CCA mechanism of approximately -67 dBm for the 802.11g[3]. Figure 9 shows possible range reductions as a function of the physical layer interference level.

3.4 Coverage scenarios

So far we have not distinguished between access points (AP) and mobile stations. From a radio technical point of view, these two types of stations are equivalent, but only access points are "deployed". However in an infrastructure based WLAN network all traffic is between pairs of stations, of which one is an access point; and any number of active communication links is equal to the number of active access points (transmitting or receiving). When we consider a large network with a high degree of randomness in the actual positions of the stations it makes multi-cell coverage estimations easier. We only have to consider the number of access points to see whether the traffic actually is originated or terminated there.

In order to make reasonable estimations of the coverage we have to make intelligent guesses of the plausible deployment of WLAN stations. Two deployment scenarios have been studied in the OBAN project [2]:

- An "active" operator policy leading to a WLAN penetration of 25 % of all households;
- A "passive" operator policy leading to a WLAN penetration of 14 % of all households.

These deployment scenarios have been applied on three environments presented in the previous section.

Thirdly, access point antennas placed both indoors and outdoors are considered, and in order to predict outdoor coverage plausible values for the building penetration attenuation must be chosen. All in all, this adds up to 2 · 3 · 2 = 12 different cases. Only some samples are given in this article.

Environment	Sparse suburban	Dense suburban	Dense urban
		Active deployment	
Station density	320 per km^2	1450 per km^2	2560 per km^2
Cell size	3125 m^2	690 m^2	391 m^2
Average distance between stations	60 m	28 m	21 m
		Passive deployment	
Station density	200 per km^2	800 per km^2	840 per km^2
Cell size	5000 m^2	1250 m^2	1190 m^2
Average distance between stations	76 m	38 m	37 m
		Both deployment scenarios	
Building penetration attenuation	6 dB	10 dB	12 dB

Table 8 Summary of environments and deployment cases for coverage estimations

[3] *The cause for this maximum limit is that when stations are brought tight enough, the CSMA/CA protocol will self-regulate the transmitter activity of the population. More reading about this can be found in [D26].*

These environments basically differ in two aspects: the people densities and the radio propagation conditions. Table 8 contains typical values for station densities and cell sizes and average distance between stations for the two deployment scenarios and three environments. The values are calculated from the numbers in Table 1.

3.5 Expected coverage in multi-cell scenarios

Finding expected coverage of a multi-cell WLAN deployment is a problem with many inputs and assumptions. In the sections above we have gone through some of the basic knowledge which is needed in order to do this and defined some plausible scenarios of deployment. In addition, we have to define some input variables and their ranges. Referring to Figure 10 we define coverage as the ratio between the real coverage as shown by the circles, and the cell size as given in Table 8.

3.5.1 Traffic and channel utilization

Since WLANs do not transmit continuously, but only when packets are to be sent, it follows that the interference level also varies with the offered traffic. Therefore coverage estimations must be done assuming certain traffic over the stations. We have defined an "activity factor", or channel utilization, ranging from 0 to 100 %, where 0 % means that all stations are idle and 100 % means that the channel is constantly busy. No traffic (0 %) gives the same answer as the single-cell case. Dependent on the actual density of WLAN stations, 100 % traffic may result in reaching the maximum permissible interference level as explained above.

3.5.2 Station frequencies

We have so far not mentioned frequency planning. The considerations above have implicitly assumed that all stations try to access the same channel. As shown in Figure 7 there are 13 channels available for WLAN operation in the 2.45 GHz band, however only three are so-called non-overlapping. In principle any combination of channels may exist; fully overlapping, partly overlapping or non-overlapping, however to simplify the analysis we can look at two extremes: All stations operate on the same channel, or we employ an optimum planning scheme. In this case, the latter means utilizing a perfect three-cell cluster. The main model is shown in Figure 10. For WLANs operating in the 5 GHz band, i.e. 802.11a, the number of channels is higher and there are effectively eight non-overlapping channels (Band A from 5.15 – 5.35 GHz). Deploying 7-cell clusters is then applicable planning strategy.

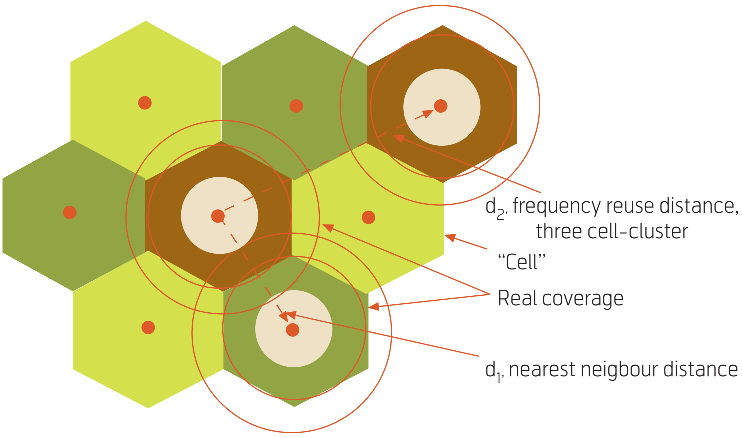

d_2, frequency reuse distance, three cell-cluster
"Cell"
Real coverage
d_1, nearest neigbour distance

Figure 10 Simplified coverage model

In the figure, two important distances are defined; the frequency reuse distance in the case of single-frequency, and in a triple-frequency operation d_1 and d_2. From the geometry it remains clear that $d_2 = d_1 \cdot \sqrt{3}$. Thus, a triple-frequency network can be analyzed as three co-existing single-frequency networks in which the interference pressure is effectively reduced to 1/3 (-4.8 dB).

Based on these assumptions the coverage can be estimated for several combinations of deployment scenarios, environments, frequency planning and channel utilization, of which just a few results are given in this article.

3.5.3 Coverage effects of channel utilization

The degree of channel utilization clearly has a severe effect on the coverage due to added physical layer interference as discussed earlier. Figure 11 shows an example of how the outdoor interference level increases with channel utilization while Figure 12 shows how this influences the expected coverage.

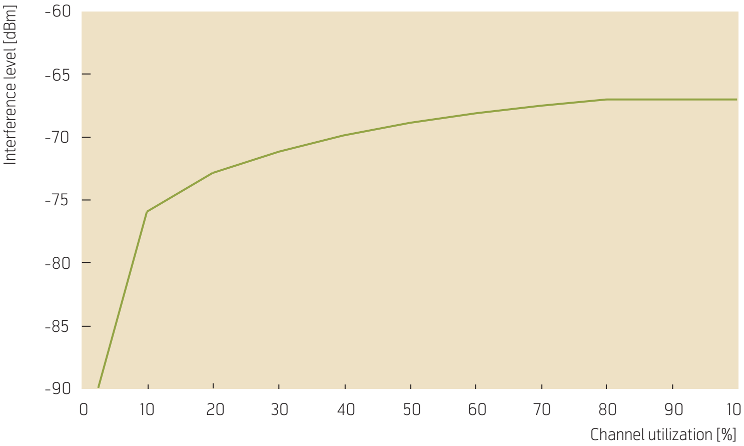


Figure 11 Added interference level as a function of channel utilization for indoor placed stations with an average distance of 21 m (Dense urban environment, scenario "C" and 12 dB building penetration)

ISSN 0085-7130 © Telenor ASA 2006

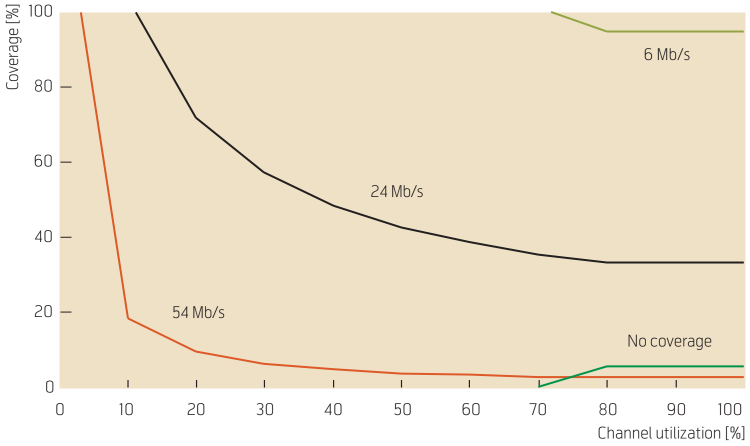


Figure 12 Expected coverage as a function of channel utilization for indoor placed stations with an average distance of 21 m (Dense urban environment, scenario "C" and 12 dB building penetration)

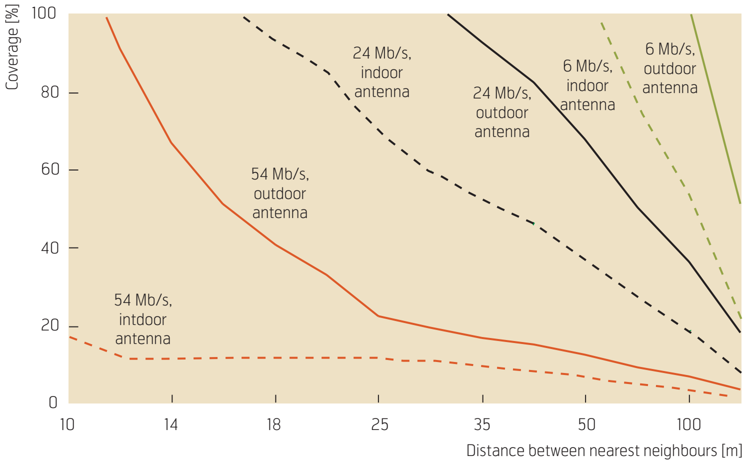


Figure 13 Coverage as a function of the distance between nearest neighbours for 20 % channel utilization in a single frequency network. Building penetration loss is 10 dB. Note that the distance scale is not linear

The example is for a dense urban environment with 21 m between stations and 12 dB building penetration attenuation.

3.5.4 Station density

Improved coverage and capacity should be a question of just packing the access points tight enough and the question is: how tight. This is not a linear function. When packing the stations tighter, the interference level rises and reduces the range effectively counteracting the effect of packing stations tighter. Figure 13 shows the expected coverage as a function of average distance between neighbour access points in the case of a single frequency network with 20 % channel utilization. Indoor-to-outdoor coverage is calculated with 10 dB building penetration loss (multi-apartment buildings). Channel B is used in all cases.

3.5.5 Coverage in specific environments

Figure 14 shows a summary of the relative coverage of multi-cell WLAN networks for some cases with saturated traffic for both the single-frequency case and the triple-frequency case at 2.45 GHz.

4 Generic traffic capacity

When we analyze the performance of the OBAN traffic machine, as presented in section 2.2, there are some general characteristics that determine the effective throughput of WLAN/IEEE 802.11 systems. In particular the packet and frame sizes are cardinal for the performance. In addition the capacity results will to a large degree depend on assumptions that are generic and may be valid for many different real life situations. The main decisive factors are:

- MAC interference conditions
- Attainable data rates per user on the wireless drop
- Application profiles and mixes
- Call control and priority regimes
- Assumptions on fixed line capacities and interplay with the wireless drop.

The data rate and the application profiles are stochastic variables that depend on random behaviour of the users. The MAC interference and the assumed priority regimes are scenario parameters, partly depending on the assumed environment and partly depending on the deployment and policy decisions made by the OBAN operator. In this section we will first introduce some general WLAN characteristics and then present results that are conditioned on possible ranges of values for conditional and stochastic variables and parameters. The results presented are obtained by combined use of analytical modelling and OPNET simulations [13].

The conditional results will in section 5 be applied on scenario assumptions and coverage data from sections 2 and 3 to give us "real life" results valid for the three Lillestrøm environments.

4.1 General characteristics of the IEEE 802.11g

The general traffic performance of WLAN systems is governed by the IEEE 802.11 MAC layer access mechanisms and interplay with the higher layers of the IP protocol stack. This has been described and analyzed in [2][12]. Figure 15 shows the maximum throughput over the air for a WLAN system. The curves give a very clear evidence of the influence of packet lengths for the performance. Only a fraction of the gross 54 Mb/s can be utilized for transfer of useful payload, and the shorter the packet lengths are, the less is the useful fraction.

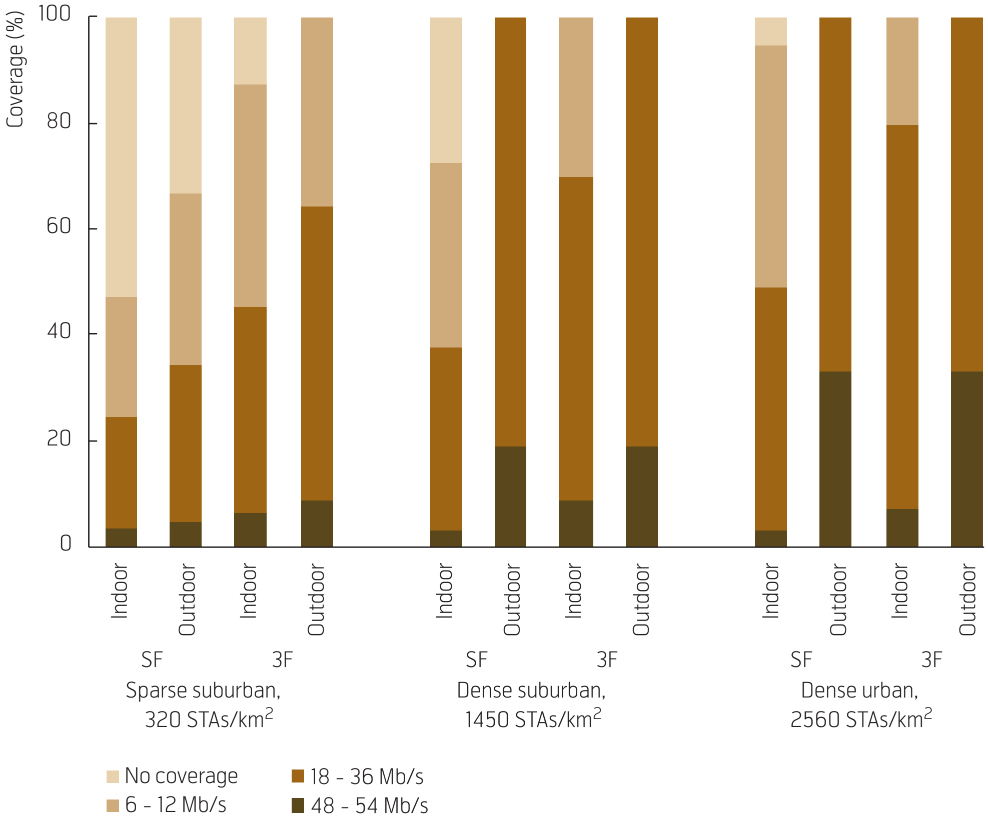


Figure 14 Expected coverage for multi-cell WLAN networks in different environments
SF: Single-frequency operation, all stations use the same channel
3F: Three-cell optimum clustering using three non-overlapping frequencies. Channel model B is used for all cases

To better understand the results of Figure 15 and results presented in the remaining part of this section, we shall outline some main (and simplified) characteristics of a WLAN system.

For WLANs the radio medium is a shared resource for the stations and access point, and the IEEE 802.11g MAC provides the mechanisms that give each of the radios a part of the airtime to transmit information. The application data (the payload) are segmented in packets that are added with several layers of protocol data to form frames (MAC Protocol Data Units, MPDUs) that are transmitted one by one over the air. Each 802.11 station only transmits packets when there is no other station transmitting. If another station happens to be sending a packet, the other stations defer access and wait until the medium is free. The actual protocol is somewhat more complex, but some main characteristics are as follows. For each access of a frame, time is needed to assure that the frame has reservation of the medium, and to allow confirmation of successful transmission. The airtime needed for transmission of one frame consists then of an access time F_a and the transmission time

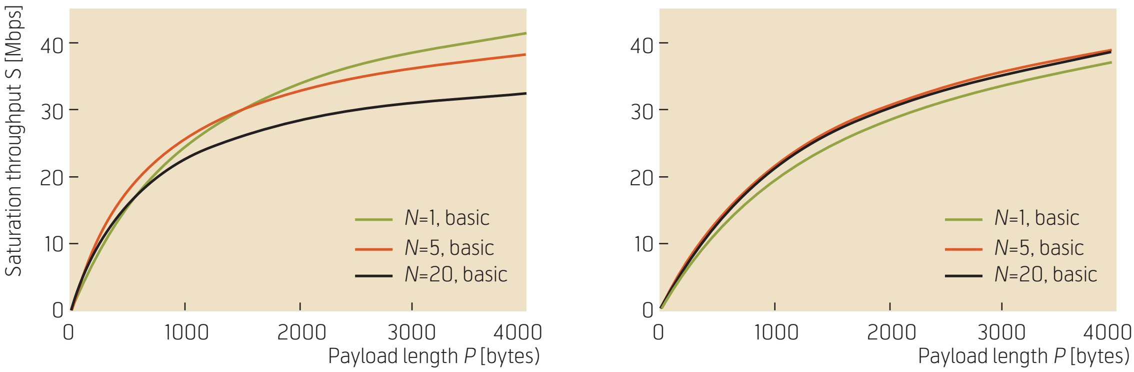


Figure 15 Saturation Throughput as a function of payload length for 802.11a/g
Left: Basic access scheme. Right: RTS/CTS access scheme [2]

ISSN 0085-7130 © Telenor ASA 2006

L_m / R_d, where L_m is the length of the MPDU and R_d is the obtained data rate given by the radio conditions. We introduce the notation cycle time C needed to transmit one frame:

$$C = F_a + \frac{L_m}{R_d} \tag{10}$$

The traffic load on the radio medium is given by the sum of airtimes needed by each application. We introduce f as notation for frames per second for a traffic stream (~ IP packets per second), and A as notation for relative airtime occupancy:

$$A = f \cdot C \tag{11}$$

The MAC mechanism for WLANs works as a distributed queuing system. The packets and frames will experience a stochastic waiting time W before getting access, which is due to the probabilities for more than one station wanting to access the medium at the same time and the mechanisms used for stations to wait and back off before a new trial, and possibly waiting for other frames being queued up at the same station. The total transfer time T from MAC layer to MAC layer is then:

$$T = W + C \tag{12}$$

As in all queuing systems W will "explode" if the utilization of the airtime becomes close to 100 %. To maintain an acceptable QoS, the traffic capacity is therefore determined by a utilization of the airtime that must be kept lower than a factor ρ:

$$\sum A_i < \rho, \tag{13}$$

where A_i is the relative airtime for the stream, i, of packets.

The waiting time W will to some extent influence the access time F_a, as there will be some "waste" of airtime when several stations contend for the medium at the same time. We introduce the notation D as the stochastic influence on the access time. Furthermore, we let t represent the sum of several fixed "waiting stages" during the access for transmitting the frame, c represent the total length of control packets that are exchanged between the radio station and the access point, at a control data rate R_c. This gives:

$$F_a = t + \frac{c}{R_c} + D \tag{14}$$

A special mechanism that may be activated is called "Request to send/Clear to send" – RTS/CTS. In addition to just listening for a free period on the medium, the radio that wants to send a frame also makes a handshake with its peer and asks it to broadcast information about the planned transmission of a frame. This mechanism takes some extra airtime capacity but reduces the chance of collisions, see Figure 15. For IEEE 802.11g with RTS/CTS activated, t = 138 μs, c = 350 bits and R_c may take on one of the rates 6 Mb/s, 12 Mb/s or 24 Mb/s, depending on the attained value of the data transmission rate R_d. D will depend on the number of active stations, with typical value 50 – 100 μs.

The outline given above is an abstracted and simplified description of the IEEE 802.11g MAC. The full details of these mechanisms are described in [2][6]. The parameter values are different for different flavours of WLANs. For IEEE 802.11g with RTS/CTS activated, a typical value for F_a can be about 240 μs. Compared to the time to transmit an MPDU of length L_m = 548 bytes at a data rate of R_d = 54 Mb/s, which is 81 μs, we understand the low throughput on the radio medium as shown in Figure 15.

If we instead consider *goodput* capacities over the WLAN; i.e. the net capacity for transmission useful data between application layers, we must also take into account the protocol overhead of 72 bytes of the MPDU and retransmissions when frames are lost because of collision. From Figure 15 we see that medium throughput is not much influenced by the number of radios, as we here only consider the ability to transmit frames. From a goodput point of view, however, an increasing fraction of the transmitted frames will be retransmissions when the number of stations increases.

In view of this outline we see that a useful characterisation of OBAN applications is the pair *packet length* and *packets per second*. In OBAN context this has been designated as the profile P and defined as the MSDU (MAC Service Data Unit = MPDU minus MAC header) L_s, and the packet rate f:

$$P : < L_s, f > \tag{15}$$

From the formulas above it follows that P determines the approximate airtime consumption of an application. Because of linearity properties we can also express the profile for an assembly of applications, which then determines the approximate, accumulated airtime:

$$P^* : < L_s^*, f^* >, \text{ where} \tag{16}$$

$$L^* = \frac{\sum_i f_i L_i}{\sum_i f_i} \text{ and } f^* = \sum_i f_i$$

The results presented in the following sections are based on OPNET simulations [13], which take into account the details and the stochastic behaviour of such WLAN systems.

4.2 Airtime spent by some OBAN applications

The Visiting Users will not in general have any idea of signal strength when they want to make an OBAN call. A casual user may appear in any of the coverage zones that were described in section 3, allowing connections of 0 Mb/s up to 48 Mb/s or even 54 Mb/s. For this article we have simplified the analysis and only consider four bit rate zones: 0 Mb/s, 6 Mb/s, 18 Mb/s and 48 Mb/s, ref. Figure 14.

The Home Users will experience a more predictable situation, even if the radio coverage may also vary at the host site. Our assumption is that the Home User typically will obtain a data rate of 48 Mb/s.

Table 9 shows airtime values for real time applications that may be relevant in an OBAN context, specified for the three data rate classes. The values are obtained by use of the OPNET simulation tool, but also fits quite well with calculated values by use of the formulas (10 – 16). The table also shows examples of how single airtime values can be aggregated.

The UDP protocol used by real time applications is inelastic in the way that, contrary to the TCP protocol it does not adapt its application bit rates to available data rate capacities. TCP do adapt to available capacities, for instance to the rest capacity after UDP traffic has taken its share. Several TCP applications running at the same time will share the capacity among themselves in a “fair” way, but sometimes in the way that each application is running in parallel with the same application rate, or at the other extreme, that each application (download, etc.) is finished in turn.

Table 10 shows calculated airtime values for three cases of file download, depending on the share of data rate.

In the following we shall apply the 64 kb/s phone service with 30 ms packet filling (G.711/30 ms) as a *yardstick* for the capacity studies. A possible yardstick for TCP capacity could be downloading of 5 Mb files. We assume that three minutes is an upper limit for acceptable download times, which may occur when a number of TCP users share the capacity simultaneously. With an average MSDU length of 1540/2 bytes, the TCP yardstick is equivalent to a download of 5 Mb at 220 kb/s, occupying 3 – 1 % of the airtime, depending on data rate.

4.3 Multi cell aspects and MAC interference

The radio medium cannot in general be considered as a shared resource for traffic in one OBAN cell only, but must rather be viewed as a common resource for traffic in an area with several cells. The general situation is that traffic in adjacent cells will interfere with each other. Depending on distance and environmental conditions, the interference may be as electromagnetic noise, reducing the radio coverage levels, which is treated in section 3. If however the OBAN cells are so close to each other that stations in one cell can decode the control messages from stations in other cells; i.e. are within the CCA range of each other, stations will defer for each other to avoid radio inter-

	Rate at IP application layer		Profile		Airtime on wireless drop with attained data rate		
Applications	Up (kb/s)	Down (kb/s)	L: MSDU (Byte)	f: Packets per sec – up + down	6 Mb/s	18 Mb/s	48 Mb/s
1 Phone G.711/10 ms	64	64	120	200	6.9 %	4.0 %	3.1 %
2 Phone G.711/30 ms	64	64	240	67	4.7 %	2.7 %	2.0 %
3 Phone G.723.1/30 ms	16	16			1.8 %	1.1 %	1.0 %
4 Video telephony	456	456	512	240	23.4 %	11.3 %	7.4 %
5 Web TV		960	512	254	25.8 %	12.7 %	8.5 %
6 Standard IP TV		4000	1356	380	87.7 %	33.3 %	18.0%
Sum single rows 2+4+5 – OPNET simulation	520	1480	484		53.9 %	26.7 %	17.8 %
Airtime compound traffic of 2+4+5 – Simulation				560	54.7 %	26.7 %	17.9 %
Airtime compound traffic of 2+4+5 – Formula (10–16)					54.6 %	26.6 %	17.4 %

Table 9 airtime consumption for a selection of applications that may be transferred over the wireless drop. The three lower rows show examples of approximations that are valid at moderate loads

TCP based applications	Share of data rate for application – adjusted by TCP		Profile		Airtime on wireless drop with attained data rate		
	Up	Down	L:	f:	6 Mb/s	18 Mb/s	48 Mb/s
Browsing at 2.0 Mb/s		2000	1540	330	40.1 %	16.1 %	8.5 %
	53		40	330	5.6 %	3.7 %	3.0 %
					45.7 %	**19.8 %**	**11.6 %**
Browsing at 0.5 Mb/s		500	1540	83	10.1 %	4.0 %	2.1 %
	13		40	83	1.4 %	0.9 %	0.8 %
					11.4 %	**4.9 %**	**2.9 %**
Browsing at 0.25 Mb/s		250	1540	41	5.0 %	2.0 %	1.1 %
	7		40	41	0.7 %	0.5 %	0.4 %
					5.7 %	**2.5 %**	**1.4 %**

Table 10 Calculated airtime values for TCP based download of file at mean adjusted data rate. Approximation calculated by the mean of the data and ACK frames imposes a small error as ACK frames are transferred without use of RTS/CTS

ference, but instead compete for access to the same radio medium across the cells. This latter effect is called MAC interference.

The main view taken in this paper is to analyze capacity jointly for several OBAN cells. This may turn out to be a very many-sided picture in real life situations. Some radios in a cell may hear some foreign radios, other radios may hear other foreign radios, and some radios in the cell may not be disturbed directly by foreign radios at all. This means also that it may not be straightforward to define one area with cells sharing a common radio medium, as there may also be border effects caused by cells next to this area, etc.

For the results presented here we have however made the following simplified assumptions. We consider clusters of *N* access points with associated stations, that are transmitting on the same frequency and all are within CCA range of each other. A justification of this assumption is the size of CCA ranges as compared to cell sizes as described in section 3. Table 11 presents two assumptions for radio channel conditions in the outdoor environment, either shading of the signal by buildings and vegetation, or an open space. The open space assumption gives very large clusters of cells with mutual MAC interference, and is a quite non-viable condition for OBAN services. In a case of such environmental conditions, the access point antennas must either be placed indoors or be operated with reduced power. For the results presented in this paper we have assumed an environment with signals shaded by buildings for the outdoor antenna cases.

4.4 Home User traffic and priority regimes

The OBAN traffic capacity for Visiting Users depends on how much is left after the Home User has taken his share. One way to argue is that the reserved capacity for Home Users on the wireless drop should match the sum of the Home Users' subscribed up- and downlink capacities on the fixed line, including the amount accounting for the access time to the wireless medium.

With reference to Table 9 we see that the applications Phone G.711/30 ms, Video telephony and Web TV add up to 17.4 % of the airtime and fit quite well with a subscribed fixed line capacity of 1 Mb/s up and 2 Mb/s down. This leaves 2.6 % airtime for file download at 0.5 Mb/s going on at the same time.

This example motivates as a fair assumption that a more or less exclusive reservation of 20 % of the airtime will satisfy his needs to match the subscribed capacity at the fixed line. In this reasoning we have not taken into account applications on wired terminals at the user's site. It can however be argued that the 1 + 2 Mb/s is a rather low access capacity and that wired applications like standard or high definition IPTV will account for spending additional subscribed capacity on the fixed line.

If a regime with *strict reservation* of capacity for the Home User is assumed, it means that visitors are restricted to using the remaining 80 % of the airtime, and conversely, the Home User is restricted within his 20 %. For the single cell case this seemingly leaves a fair amount of wireless capacity for Visiting Users. It may be argued that the fixed access line will

Environment	CCA-range	Average distance to nearest neighbour	Size of MAC-cluster, Single frequency	Size of MAC-cluster, 3 frequencies
Indoor antennas, channel model B and added building penetration loss				
Sparse suburban	53 m	60 m	3	1
Dense suburban	41 m	28 m	8	3
Dense urban	36 m	21 m	10	3
Outdoor antennas, building environment assumptions, channel model B				
Sparse suburban	79 m	60 m	6	2
Dense suburban	79 m	28 m	28	9
Dense urban	79 m	21 m	50	17
Outdoor antennas, open space assumptions, channel model F				
Sparse suburban	171 m	60 m	29	10
Dense suburban	171 m	28 m	133	44
Dense urban	171 m	21 m	236	79

Table 11 Estimations of likely number of stations within CCA-range of each other – MAC cluster size – for three OBAN environments. Two assumptions for outdoor environment

limit the utilization of the wireless capacity for visitors. The access line may however be of VDSL type or even fibre, allowing the operator to allocate enough capacity for visitors. Anyhow, the visitors will not in general be able to utilize the available airtime as efficiently as the Home User, whom we have assumed will obtain an average data rate of some 48 Mb/s for his transmissions.

In the multi cell cases, a strict priority rule will break down if some four or more cells share the same radio medium and impose full MAC interference on each other. The total Home User reserved capacity in such a cluster will then be the sum of the reserved Home User airtimes in each cell, because exclusive reservation also means exclusive reservation against visitors in neighbouring cells as well. In a situation with four cells and strict reservation of capacity, 80 % of the airtime will be excluded for the visitors, and in a case with eight cells, there will not even be 20 % available for each Home User as can be interpreted from Table 11.

We will therefore also investigate *shared priority* regimes, where it is assumed that both parties may benefit from letting Visitors be allowed to use unused capacity on a non priority basis. It is unlikely that the Home Users will utilize their allocated radio capacity all the time. The following reasoning is based on an example of what may be viewed as a possible usage pattern. During the afternoon it may be assumed that the Home User is passive 50 % of the time, and the rest of the time has a profile of low – 5 %, medium – 10 %, high – 15 %, and full activity – 20 %, airtime occupancy. Assuming as a possible probability profile 50 %, 25 %, 10 %, 10 %, and 5 % of these occupancy states, and assuming independence among the Home Users in adjacent cells we get probability distributions for airtime occupancy as shown in Figure 16.

The diagram reflects only assumed examples of Home User's activity profiles, but illustrates nevertheless a likely situation where a substantial part of the allocated Home Users' capacity is not utilized.

4.5 Visitor capacities in single and multi cell environments

In the following we shall consider situations with a single cell and clusters of several OBAN cells that share the same medium.

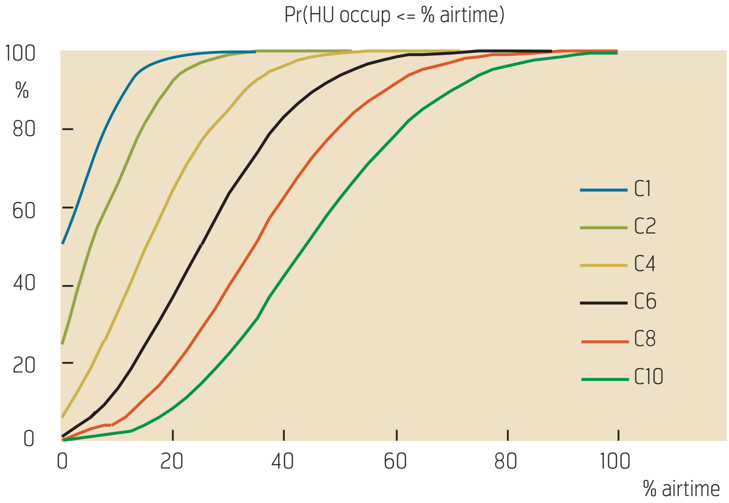


Figure 16 Probabilities for aggregate airtime occupancy by Home Users, for MAC clusters of 1, 2, 4, 6, 8, and 10 cells

APs in cluster	Prob. HU occupancy ≤ airtime		Number of Visiting Users allowed in bitrate zones – appl. phone 64 kb/s/30 ms (G.711) as yardstick		
	Prob.	HU airtime	6 Mb/s	18 Mb/s	48 Mb/s
1	0.85	10 %	18	32	43
	1.00	**20 %**	16	29	39
2	0.95	25 %	14	28	32
	1.00	**40 %**	10	18	26
3	0.94	45 %	9	16	21
	1.00	**60 %**	6	9	15
4	0.49	15 %	12	22	32
	0.96	40 %	8	16	24
	0.99	55 %	7	11	20
8	0.40	30 %	8	16	24
	0.87	55 %	3	6	10
	0.97	70 %	0	~0	3
9	0.62	45 %	4	8	19
	0.86	60 %	3	5	9

Table 12 Visitor capacity in terms of how many Visiting Users running the yardstick application are allowed in a single cell or a MAC cluster, as a function of Home User's airtime occupancy. Probability figures of 1.00 indicate situations with a strict priority regime

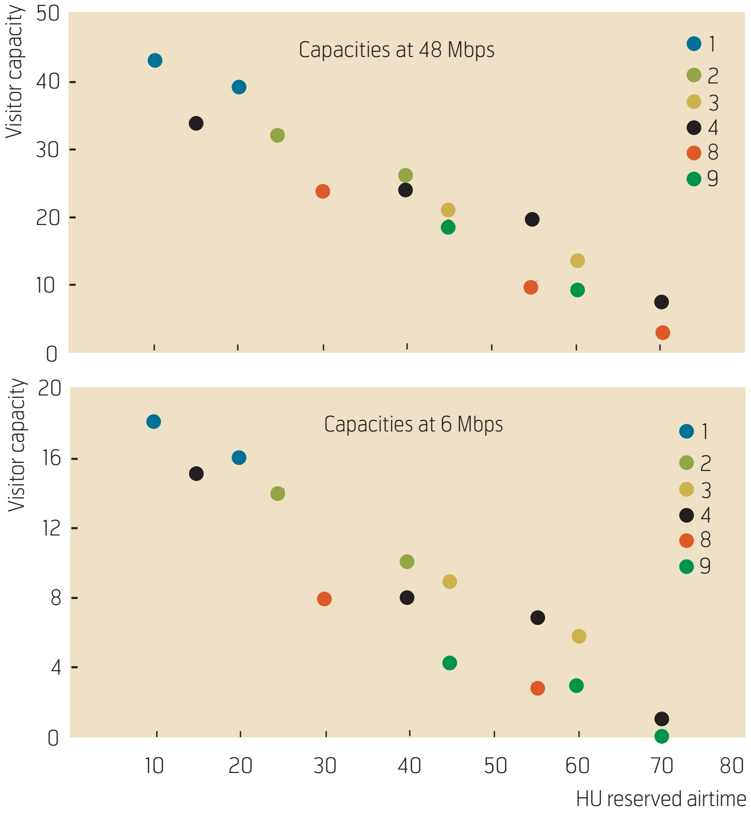


Figure 17 Visitor capacities as a function of Home Users' reserved airtime at 48 Mb/s (top) and 6 Mb/s (bottom) for MAC clusters of 1, 2, 3, 4, 8, and 9 cells

It is not obvious that if more OBAN access points are deployed in an area, the total traffic will increase linearly with the number of cells. One could argue that the Home User's traffic on new OBAN access points is only converted from existing traffic on non OBAN access points and that the Visitors' traffic is constant and only distributed on more access points. For the analysis in this paper, however, we have assumed that the number of OBAN access points reflects growth in total traffic.

4.5.1 All visitors located in the same data rate zones

With the use of the OPNET tool we have simulated how many Visiting Users running the UDP yardstick application can be served in single cells and MAC clusters of different sizes, *when all Visitors are in either of the three data rate zones*. These are very unlikely situations in real life, but the results set - conditions for the more realistic cases that will be addressed below.

The simulations have been done for different assumptions about how much airtime is occupied by the Home Users. For clusters of size 1, 2 and 3 we have simulated cases where Home Users have a strict reservation of 20 % of the airtime each. For larger clusters this assumption breaks down and leaves no practical capacity for Visitors. Figure 16 indicates, however, that during long periods of time a substantial part of the Home Users' capacity is not utilized and could be made available for Visiting Users. The results are shown in Table 12, where strict and shared schemes can be compared.

The terms for a shared priority regime should be that the Home Users still shall have first priority within his allocated airtime. This implies that Visitor's connections could be shut down. For that reason one should distinguish between Visitors' TCP and UDP traffic. Visitors' UDP traffic should have a low priority of being interrupted, which means that one should maybe only allow Visitors' UDP traffic to utilize airtime with a probability of being free of at least 90 %. For TCP traffic the situation is quite different. TCP traffic will adapt to higher priority traffic, both Home Users' and Visitors' UDP traffic. The table shows that there will be fairly good capacities suited for TCP traffic at some 60 to 70 % of the time. See also Table 13, which gives a clue for how to compare the yardstick applications applied in Table 12 with other applications and TCP connections at different data rates.

The Home User may also benefit from the shared priority regime, as for most of the time he may have access to extra airtime for running his TCP applica-

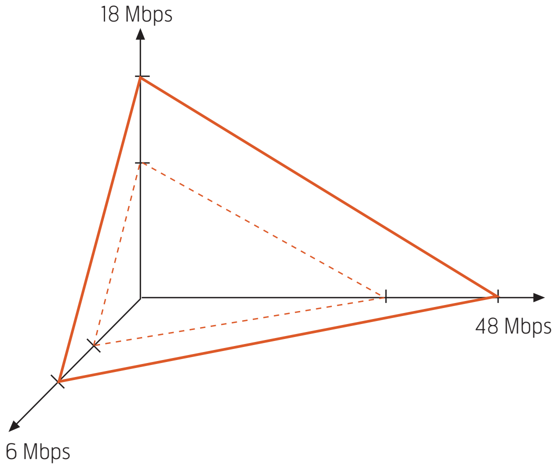


Figure 18 Values for number of yardstick users plotted on axes for the three data rate zones. The linear planes connecting triplets of plots give a good approximation of the capacity when users are distributed among the three zones

Applications		Airtime on wireless drop – relative to yardstick		
		6 Mb/s	18 Mb/s	48 Mb/s
Phone G.711/10 ms	UDP	1.47	1.48	1.55
Phone G.711/30 ms	**UDP**	**1**	**1**	**1**
Phone G.723.1/30 ms	UDP	0.38	0.41	0.50
Video telephony	UDP	4.98	4.19	3.70
Web TV	UDP	5.49	4.70	4.25
Standard IP TV	UDP	18.66	12.33	9.00
Browsing at 2.0 Mb/s	TCP	9.72	7.33	5.80
Browsing at 0.5 Mb/s	TCP	2.43	1.81	1.45
Browsing at 0.25 Mb/s	TCP	1.21	0.93	0.70

Table 13 Airtime consumption per application relative to consumption of G.711/30 ms phone application, used as yardstick for capacity analysis

tions. Part of the deal for the Home Users could also be economic compensation or that he is allowed to use extra capacity on the fixed line.

Figure 17 shows the capacity figures of the table ordered according to Home Users' airtime usage, when all Visitors are assumed to be located in 48 Mb/s or 6 Mb/s zones. The figure shows that the airtime left for Visitors is less efficiently utilized when the size of the cluster increases. In the mono cell case, approximately half of the traffic on the radio medium is ordered "in line" by passing over the access point. This "organisation" is deteriorated when the traffic is distributed on more access points, with increasing number of collisions and longer back-off intervals.

4.5.2 Capacities when users are distributed on different bit rate zones

When considering an ensemble of Visiting Users, they are most likely spread in some way among different data rate zones, depending on stochastic processes. The probabilities will depend on spatial layout of the actual environment, deployment of access points and choice of radio installations. The results shown above represent sets of values on the three axes shown in Figure 18. From formulas (1 – 7) it can be shown that the combined capacity for yardstick Visitors when distributed in more zones, is a good approximation determined by the linear planes connecting the plots on the axes.

The planes may represent different cases and conditions as shown in Table 12. The planes may also represent other examples of applications used as a yardstick. Table 13 shows a comparison of relative airtime consumption for different applications, and can be used as a guideline for estimating more general capacity figures.

5 Traffic capacity in the cases of OBAN environments

The analysis of radio coverage in section 3 gave tables for the probabilities that users at random would experience zero, 6 Mb/s, 12 Mb/s, etc. data rates when making or receiving a call. These results are specific for the three Lillestrøm environments. The generic results presented in section 4 show how many Visitors that can be accommodated if all appear in one of such bit rate zones, which also gives a good approximation of the number if the Visitors are distributed over all bit rate zones. In this section we shall combine the specific results on radio coverage from section 3 with the generic results on traffic capacity from section 4, in order to deduce traffic capacity figures from the three cases of OBAN environments.

5.1 Stochastic modelling of area capacities

We shall first define in more detail our measure for capacity and describe a method for how to calculate this measure.

Recall the data rate zones presented in Figure 14. We assume that Visiting Users may be in any of these zones when making or receiving a call, with probabilities as given by the zone size distributions. Further, we assume that there is already *N* other visitors with ongoing yardstick calls in the environment, who are distributed among the bit rate zones, also according to the probability figures of Figure 14. The condition

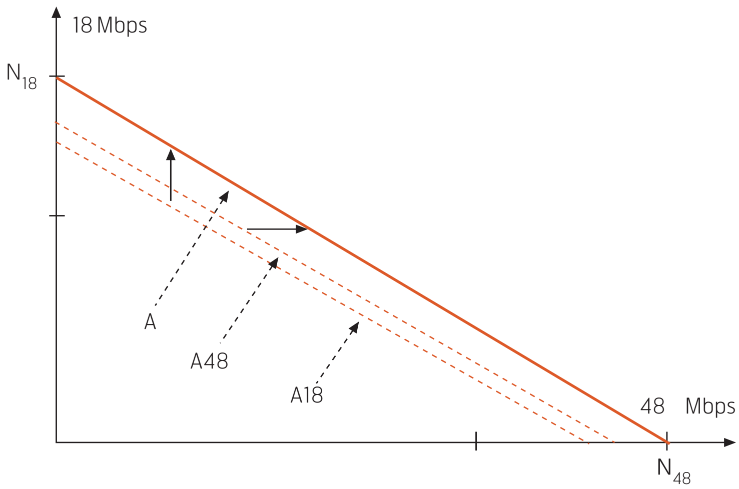


Figure 19 Limits for number of ongoing yardstick calls, as summed in two bit rate zones

- From simulations
  - If all users in *Ri* : *Ni* calls possible (*i* = 1, ..., *K*)
  - Where *N*1 > *N*2 > ... > *NK*
- Consider a case of *N* users
  - Assume multinomial distributed over the area
  - with the probability of being in *Ri*, *pi*. *Pi* proportional to the area of *Ri*
- Assumption the success region is linear: then

$$\frac{i_1}{N_1} + \frac{i_2}{N_2} + \ldots + \frac{i_K}{N_K} \le 1$$

- Probability of success is then

$$P_{success} = \sum_{\substack{\frac{i_1}{N_1}+\frac{i_2}{N_2}+\ldots+\frac{i_K}{N_K}\le 1 \\ i_1+i_2+\ldots+i_K=N}} \frac{N!}{i_1!i_2!\ldots i_K} p_1^{i_1}p_2^{i_2}\ldots p_K^{i_K}$$

Figure 20 Procedure for how to calculate the probability of success for a new call

then for accommodating a new call is depicted in Figure 19, which for simplicity only includes two bit rate zones. N is the sum of Visitors in each of the two zones, n_{18} and n_{48}, $N = n_{18} + n_{48}$, and $n_{18} \le N_{18}$ and $n_{48} \le N_{48}$. The max number of N existing Visitors will be less than N_{48}, and a fairly good approximate condition is that the pair $< n_{18}, n_{48} >$ must be within the solid line triangle on Figure 19. But if there shall still be capacity for one more yardstick call, the ongoing number of calls must be kept below either of the two dotted lines, depending on whether the new call starts in a zone with 18 Mb/s or with 48 Mb/s offered data rate.

We introduce the notation $P_{success}$ as the conditional probability of A ("access for a new call"), given N ongoing calls:

$$P_{success} = P_r\,(A \mid N) \qquad (17)$$

The measure for capacity is then defined as:

$$C = \max\,(N+1) \text{ so that } P_r\,(A \mid N) > 1 - \varepsilon \qquad (18)$$

Where ε is the blocking probability.

For the purpose of call control and securing QoS, the connection acceptance control should always reject new calls when $N = C$. But we still need to define the domain for C, N and ε.

Table 12 gives generic capacities for clusters sharing one common radio channel. IEEE 802.11g allows the use of three non-interfering channels, *a*, *b*, *c*, so the capacity in an OBAN area can be up to tripled by

Detached and undetached houses – sparse suburban						
Antenna	Indoor			Outdoor		
Cluster / pri scheme	Single cell	Strict 20 %	Shared 10 %	2 in cluster	Strict 40 %	Shared 25 %
	Coverage	Visitor capacity		Coverage	Visitor capacity	
No coverage	13 %			0 %		
6 Mb/s	42 %	16	18	36 %	10	14
18 Mb/s	39 %	29	32	55 %	18	28
48 Mb/s	6 %	39	43	9 %	26	32
Capacity in cluster		19	21		13	19
Capacity on 3 channels		57	63		39	57
Capacity per AP		19.0	21.0		6.5	9.5
Capacity in area with 8 Aps (25,000 m^2)		152	168		52	76
Capacity per km^2		6,080	6,720		2,080	3,040

Table 14 Capacity for Visiting Users in a sparse suburban environment in Lillestrøm, Norway. Figures are given for two alternatives for antenna placing, with two alternatives for priority regime. Results are for three-cell clusters

smart allocation of the channels among the access points. We assume that the OBAN terminals can select any of the three channels and will therefore define the blocking probability ε for environments where up to three channels are used.

Our choice for the results is to set $\varepsilon < 0.01$, which is fulfilled when $\varepsilon_a = \varepsilon_b = \varepsilon_c \leq 0.20$.

With reference to tele-traffic theory the described procedure gives us *call congestion* probabilities, i.e. the probability of call blocking when a new call arrives. It turns out, however, that the call congestion in our model is equal to the *time congestion* for at any instant finding the pair $< n_{18}, n_{48} >$ on the envelope surface. The mathematics for how to calculate the probability of $P_{success}$ for a new call is shown in Figure 20.

5.2 Results for the sparse suburban environment

The last row of Table 14 shows the capacity for accommodating Visiting Users making yardstick calls in the sparse suburban environment of Lillestrøm, for four combinations of conditional parameters. Two alternatives are to serve the outdoor Visitors from antennas placed either inside or outside the host building. Combined with these cases, we have assumed either a strict priority regime with exclusive reservation of 20 % of the airtime for Home Users at each cell, or a priority regime where the Home User allows Visitors to utilize some unused capacity, expressed by a reduced Home User percentage.

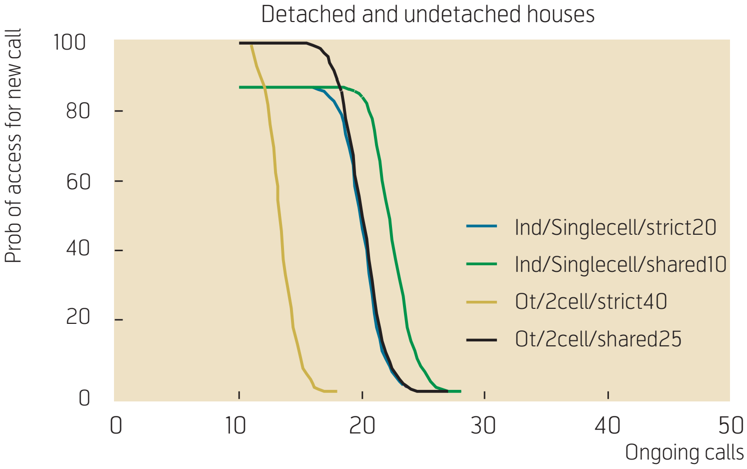


Figure 21 Probabilities for allowing a new yardstick call, conditioned on number of existing calls, for parameter values as shown in Table 14. The 80 % line defines the "capacity in cluster" figures in the table

As outlined in section 3 the choice of antenna placing determines the CCA ranges and how many cells will form a MAC interference cluster. For this environment the consequence is single cell conditions with indoor antenna and clusters of two cells for outdoor antennas, ref Table 11.

The resulting coverage figures are from Figure 14 and the generic Visitor capacity per cluster is determined from OPNET simulations as in Table 12.

Given the assumptions of Table 14, Figure 21 shows the probabilities for success of a new call as calculated with the procedure described above and shown in Figure 20. The 80 % line determines the "capacity

Multi apartment houses – dense suburban						
Antenna	Indoor			Outdoor		
Cluster / pri scheme	Mc 3	Strict 60 %	Shared 45 %	Mc 9	Strict 60 %	Shared 45 %
	Coverage	Visitor capacity		Coverage	Visitor capacity	
No coverage	0 %			0 %		
6 Mb/s	30 %	6	9	0 %	3	4
18 Mb/s	62 %	9	16	81 %	5	8
48 Mb/s	8 %	15	21	19 %	9	19
Capacity in cluster		7	12		5	9
Capacity on 3 channels		21	36		15	27
Capacity per AP		2.3	4.0		0.6	1.0
Capacity in area with 58 Aps (40,000 m^2)		135	232		32	58
Capacity per km^2		3,383	5,800		806	1,450

Table 15 Capacity for Visiting Users in a dense suburban environment at Lillestrøm, Norway. Figures are given for two alternatives for antenna placing, with two alternatives for priority regime. Results are for three-cell clusters

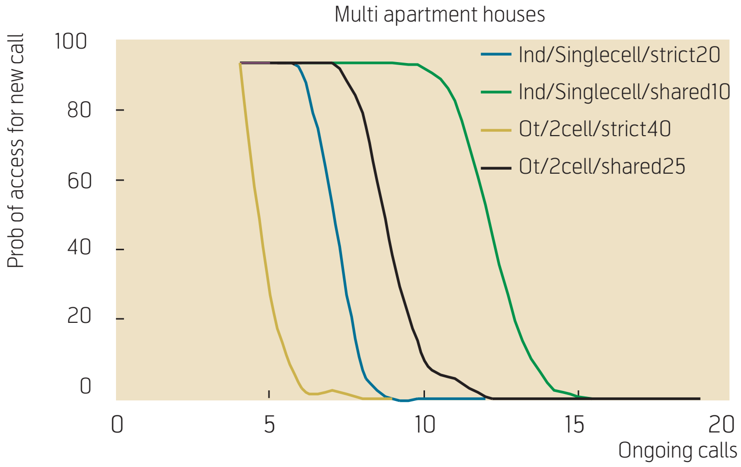


Figure 22 Probabilities for allowing a new yardstick call, conditioned on number of existing calls, for parameter values as shown in Table 16. The 80 % line defines the "capacity in cluster" figures in the table

in clusters" figures of Table 14. The figures are further adjusted for the possibilities to apply up to three channels, and extrapolated to the whole area with eight access points, to give the total Visitor capacity for yardstick services with a blocking probability of less than 1 %. A detail to be mentioned is that in some environments the density of access points will be too low to utilize three channels fully. Examples of this appear in the next tables.

On examining the results of Table 14 we see the perhaps astonishing result that the capacity drops drastically when improving the radio coverage by placing the antennas outside of the host buildings. This may however be understood for two reasons. First, with outdoor antennas the CCA ranges are increased and we get clusters of two cells sharing the same radio medium, and this effect is not compensated by better radio coverage. Second, when assuming a strict priority regime the implication is that the sum of Home Users' reserved capacities must be respected by all Visitors in the cluster, i.e. 40 % vs. 20 % is reserved by the Home Users.

5.3 Results for the dense suburban environment

For the case with multi apartment houses, Table 15 and Figure 22 shall be understood in the same way as described above. Here we see an even greater difference between the "Indoor" and "Outdoor" cases! Here there is no difference in Home User reservation of airtime. The radio coverage in the "Outdoor" case results in MAC interference clusters of nine cells, compared to clusters of three cells for the "Indoor" case. Even if the available airtime is the same for Visitors in the two types of clusters, we also see here the effect of having the traffic handled by a much higher number of radios in the "Outdoor" cases.

5.4 Results for the dense urban environment

In the central city environment we get clusters of three cells for the "Indoor case" and clusters of 17 cells for the "Outdoor case". The results for "Indoor" cases can be compared directly with the "Indoor" cases of the multi apartment environment. The only difference is that the radio coverage is slightly better in the central city cases, and we see that the capacity figures are practically the same.

Central city areas – dense urban						
Antenna	Indoor			Outdoor		
Cluster / pri scheme	Mc 3	Strict 60 %	Shared 45%	Mc 17	Shared 30 %	Shared all
	Coverage	Visitor capacity		Coverage	Visitor capacity	
No coverage	0 %			0 %		
6 Mb/s	21 %	6	9	0 %		
18 Mb/s	72 %	9	16	67 %	17	27
48 Mb/s	7 %	15	21	33 %	19	34
Capacity in cluster		7	13		17	28
Capacity on 3 channels		21	39		51	84
Capacity per AP		2.3	4.3		1.0	1.6
Capacity in area with 64 Aps (25,000 m^2)		149	277		64	105
Capacity per km^2		5,973	11,093		2,560	4,216

Table 16 Capacity for Visiting Users in a central city environment at Lillestrøm, Norway. Figures are given for two alternatives for antenna placing, with two alternatives for priority regime. Results are for three-cell clusters

For the "Outdoor" cases we see as above low capacity numbers, even with very low Home User reservation of capacity.

6 Summary and conclusions

In this study we have presented three types of results. The coverage analysis presented in section 3 clearly shows that WLANs are very susceptible to interference from other WLANs. The model and method shown are simple and the actual values predicted can of course be discussed. What should be clear, however, is the trend. This means that planning and deploying dense WLAN networks must take interference into account, and providing very dense coverage combined with high capacity may seem more difficult than first thought.

The generic traffic capacity analyses show results that take into account that dense WLAN networks also may bring about MAC interference among a large number of adjacent cells. The consequence is that radios in such clusters of cells have to share the radio medium among them, which severely degrades the traffic capacity. Another decisive parameter is the chosen priority regime between Home Users and Visiting Users. With large MAC clusters a strict priority regime breaks down. On the other hand, it can be argued that some kind of shared regimes may be beneficial for both Home Users and Visitors.

Finally, the results on radio coverage and generic traffic capacities have been combined to derive traffic capacity results for three cases of OBAN environments. The results show that about 200 – 300 Visitors making voice calls can be accommodated in environments the size of 25 – 40,000 m^2. This requires, however, that the radio coverage is based on indoor antennas. When antennas are placed outside the host buildings, coverage increases, but so does the MAC interference, with the net result that traffic capacity is reduced to about one third of the indoor cases.

7 Aknowledgements

This work was carried out as part of the OBAN project funded in part by the European Commission. The authors want to thank the project leader Einar Edvardsen from Telenor R&I for important discussions on the defintions and aim of the work, and Jan Erik Håkegård from SINTEF for contributions and comments on MAC and physical layer aspects of WLANs.

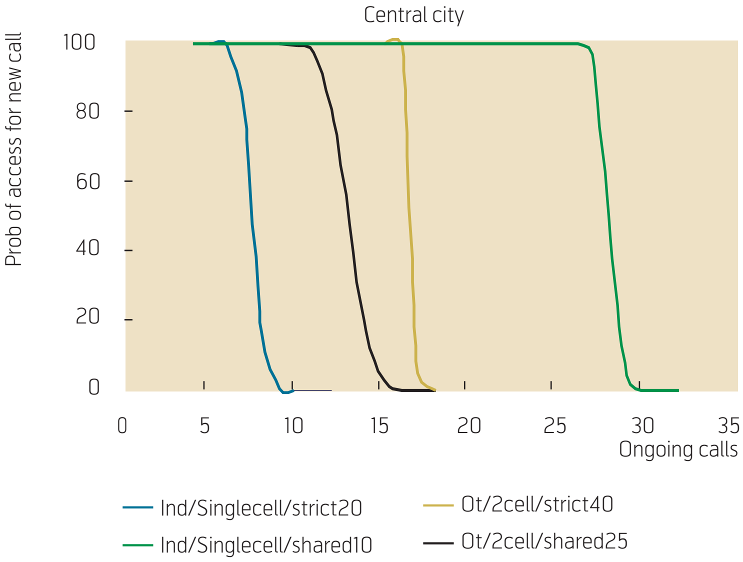


Figure 23 Probabilities for allowing a new yardstick call, conditioned on number of existing calls, for parameter values as shown in Table 17. The 80 % line defines the "capacity in cluster" figures in the table

8 References

1 *Open Broadband Access Network (OBAN).* 1 December 2006 [online] – URL: http://www.ist-oban.org/

2 Håkegård, J E et al. *Scenarios and wireless performance and coverage*. OBAN Deliverable D8. March 2005.

3 *PROMPT – New means to PROMote Pedestrian Traffic in cities. EC 5th FW: Energy, Environment and Sustainable Development, Key Action 4: The City of Tomorrow and Cultural Heritage*. 2000-2004. 1 December 2006, [online] – URL: http://prompt.vtt.fi/

4 IEEE. *Supplement to IEEE Standard for 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 Std 802.11a – 1999 (R2003). IEEE, NY, USA, 12 June 2003.

5 IEEE. *Supplement to IEEE Standard for 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 Std 802.11b – 1999 (R2003). IEEE, NY, USA, 12 June 2003.

6 IEEE. *IEEE Standard for 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 Std 802.11g – 003. IEEE, NY, USA, 27 June 2003.

7 IEEE. *IEEE Standard for 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 8: Medium Access Control (MAC) Quality of Service Enhancements*. IEEE Std 802.11e – 2005. IEEE, NY, USA, 11 November 2005.

8 IEEE. *IEEE Standard for 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*. ANSI/IEEE Std 802.11, 1999 Edition (R2003), IEEE, NY, USA, 12 June 2003.

9 Panken, F et al. *Crucial properties of a wireless LAN-based Open Access Network*. OBAN Deliverable D10, Dec 2005.

10 Erceg, V et al. *IEEE P802.11 Wireless LANs. TGn Channel Models*. Doc.: IEEE 802.11-03/940r4. May 2004.

11 ITU. Guidelines for evaluation of radio transmission technologies for IMT-2000. Geneva, ITU, February 1997. (Recommendation ITU-R M.1225)

12 Håkegård, J E, Lehne, P H, Østerbø, O N. *Intermediate report on coverage and capacity*. OBAN Deliverable D26. December 2005.

13 *OPNET Technologies, Inc*. 1 December 2006, [online] – URL: http://www.opnet.com

Terje Ormhaug holds an MSc in Cybernetics from the University of Oslo 1972. He worked for 12 years with projects in operations research and systems analysis within defence, transportation and energy research companies, before joining the research department of Telenor in 1984. At Telenor Ormhaug started to work on studies on switching and network dimensioning. In 1987 he became fully engaged in the development of broadband technologies, both in national and international projects. In the period 1992 – 2004 he filled various positions within management at Telenor Research. His present interests are on media distribution on broadband and wireless networks, and convergence of services across the traditional boundaries of broadcast-, telecom- and data networks.

email: terje.ormhaug@telenor.com

For a presentation of Per Hjalmar Lehne, please turn to page 158.

For a presentation of Olav N. Østerbø, please turn to page 110.

Terms and Acronyms in Open Access Networks

Acronym/ Term	Definition	Explanation	Web-resources
2G	Second Generation (mobile system)	Refers to the family of digital cellular telephone systems standardised in the 1980s and introduced in the 1990s. They introduced digital technology and carry both voice and data conversation. CDMA, TDMA and GSM are examples of 2G mobile networks.	
3G	Third Generation (mobile system)	The generic term for the next generation of wireless mobile communications networks supporting enhanced services like multimedia and video. Most commonly, 3G networks are discussed as graceful enhancements of 2G cellular standards, like e.g. GSM. The enhancements include larger bandwidth, more sophisticated compression techniques, and the inclusion of in-building systems. 3G networks will carry data at 144 kb/s, or up to 2 Mb/s from fixed locations. 3G comprises mutually incompatible standards: UMTS, FDD and TDD, CDMA2000, TD-CDMA.	
3GPP	Third Generation Partnership Project	Group of the standards bodies ARIB and TTC (Japan), CCSA (People's Republic of China), ETSI (Europe), T1 (USA) and TTA (Korea). Established in 1999 with the aim to produce and maintain the specifications for a third generation mobile communications system called UMTS. A permanent project support group called the Mobile Competence Centre (MCC) is in charge of the day-to-day running of 3GPP. The MCC is based at the ETSI headquarters in Sophia Antipolis, France.	http://www.3gpp.org
AAA	Authentication, Authorization and Accounting	Key functions to intelligently controlling access, enforcing policies, auditing usage, and providing the information necessary to do billing for services available on the Internet.	
ACK	Acknowledgement	A packet used in e.g. TCP to acknowledge receipt of a packet.	
ADSL	Asymmetric Digital Subscriber Line	A data communications technology that enables faster data transmission over copper telephone lines than a conventional modem can provide. The access utilises the 1.1 MHz band and has the possibility to offer, dependent on subscriber line length, downstream rates of up to 8 Mb/s. Upstream rates start at 64 kb/s and typically reach 256 kb/s but can go as high as 768 kb/s. Specified by ANSI T1.413 and by ITU-T recommendation G.992.1. A version called ADSL Lite providing up to 1.5 Mb/s downstream rates is specified as G.992.2.	http://www.itu.int
ADSL2+	Enhanced Asymmetric Digital Subscriber Line	The access utilises the 2.2 MHz band and has the possibility of offering considerably higher speed than ADSL, up to 25 Mb/s downstream. Specifed by by ITU-T in G.992.5.	http://www.itu.int
AIFS	Arbitration Interframe Space	Mechanism used in the Enhanced Distribution Channel Access (EDCA) of the IEEE 802.11e QoS amendment to the WLAN standard. It gives the time interval a WLAN station must wait until it can try to gain channel access after being deferred due to busy channel. Different stations can have different AIFS in order to differentiate the priority between them (access categories – AC). It differs from the standard DIFS in that different values can be assigned different stations. The value defines the wait time in milliseconds and can range from 1 to 255.	http://www.ieee802.org/11
AIFSN	Arbitration Interframe Space Number	An integer number used in the calculation of the AIFS.	http://www.ieee802.org/11
AP	Access Point	A point where users access the system/network, e.g. a base station in a wireless network.	
API	Application Programming Interface	The specific method prescribed by a computer operating system or by an application program by which a programmer writing an application program can make requests of the operating system or another application. A set of routines, protocols, and tools for building software applications. Most operating environments, such as MS-Windows, provide an API so that programmers can write applications consistent with the operating environment.	
AS	Authentication Server	A server that through the possession of a shared secret can authenticate a client, and issue a Ticket Granting Ticket. A Kerberos function, defined in IETF RFC 4120.	http://www.ietf.org http://tools.ietf.org /html/rfc4120
ATM	Asynchronous Transfer Mode	A high bandwidth, low-delay, connection-oriented, packet-like switching and multiplexing technique. ATM allocates bandwidth on demand, making it suitable for high-speed connections of voice, data and video services. Access speeds are up to 622 Mb/s and backbone networks currently operate at speeds as high as 2.5 Gb/s. Standardised by ITU-T.	http://www.itu.int

ISSN 0085-7130 © Telenor ASA 2006

Acronym/ Term	Definition	Explanation	Web-resources
B3G	Beyond 3rd Generation	A term used for the future wireless systems providing broadband mobile access, with high mobility and bit rates up to 100 Mb/s. It differs from the 4G term in that B3G is mainly used to describe a future integration of a multitude of wireless standards.	
BER	Bit Error Rate	The ratio of error bits to the total number of bits transmitted.	
BFWA	Broadband Fixed Wireless Access	BFWA consists of a radio link to the home or the office from a cell site or base station. It replaces the traditional wireless local loop, either if the wire based infrastructure is sparse, or to gain rapid expansion in denser urban and suburban areas.	
Bluetooth		A short-range wireless specification that allows radio connection between devices within a 10-metre range of each other. Bluetooth is designed as a Personal Area Network (PAN) technology with a wide variety of theoretical uses.	https://www.bluetooth.org
BPSK	Binary Phase Shift Keying	A digital modulation scheme that conveys data by changing, or modulating, the phase of a reference signal (the carrier wave) using two levels.	
BRAN	Broadband Radio Access Network	A standardization project in ETSI for Broadband Radio Access Networks. It was established in 1997 as the successor of the former Sub-Technical Committee RES10 which developed the HIPERLAN/1 specifications. The project prepares standards for equipment providing broadband (25 Mbit/s or more) wireless access to wire-based networks in both private and public environments, operating in either licensed or license exempt spectrum. These systems address both business and residential applications. Close relationships have been established with the ATM Forum, the HiperLAN2 Global Forum, the IEEE Wireless LAN Committees P 802.11a and IEEE 802.16, the Internet Engineering Task Force, the MMAC-PC High Speed Wireless Access Systems Group, the International Telecommunication Union Radio sector (ITU-R), and a number of internal ETSI Technical Bodies. ETSI BRAN currently produces specifications for three major Standard Areas: 1) HiperLAN2, a mobile broadband short-range access network; 2) HIPERACCESS, a fixed wireless broadband access network; and 3) HIPERMAN, a fixed wireless access network which operates below 11 GHz.	http://portal.etsi.org/bran
BSS	Basic Service Set	The basic building block of an IEEE 802.11 wireless LAN (according to the IEEE802.11-1999 standard). The most basic BSS is two STAs in IBSS mode. In infrastructure mode, a basic BSS consists of at least one STA and one Access Point (AP).	http://www.ieee802.org/11
CAM	Conditional Access Module	An electronic device, usually incorporating a slot for a smart card, which equips a DVB television or set-top box (STB) with the appropriate hardware facility to view conditional access content that has been encrypted using a conditional access system.	
CARD	Candidate Access Router Discovery	A protocol used by the mobile node to identify the IP address of nearby access routers and finding their capabilities. The CARD protocol is defined in IETF RFC 4066.	http://www.ietf.org http://tools.ietf.org/html/rfc4066
CCA	Clear Channel Assessment	A signal from the physical (PHY) layer to the medium access (MAC) layer of IEEE 802.11 WLAN. It notifies the MAC layer of the status of the channel. If the channel is detected busy, a signal will be sent to the MAC layer, which defers transmission while the interferer transmits and the channel is reported busy. It is a part of the CSMA/CA access technique.	http://www.ieee802.org/11
CCI	Co-Channel Interference	Interference between two or more different radio stations on the same radio frequency.	
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance	A network control protocol in which a carrier sensing scheme is used. A data station that intends to transmit sends a busy signal. After waiting a sufficient time for all stations to receive the busy signal, the data station transmits a frame. While transmitting, if the data station detects a busy signal from another station, it stops transmitting for a random time and then tries again. CSMA/CA is a modification of pure Carrier Sense Multiple Access (CSMA). Collision avoidance is used to improve the performance of CSMA by attempting to reserve the network for a single transmitter. This is the function of the "busy signal" in CSMA/CA. The performance improvement is achieved by reducing the probability of collision and retry. Extra overhead is added due to the busy signal wait time, so other techniques give better performance. Collision avoidance is particularly useful in media such as radio, where reliable collision detection is not possible. Apple's LocalTalk implemented CSMA/CA on an electrical bus using a three-byte busy signal. 802.11 RTS/CTS implements CSMA/CA using short Request to Send and Clear to Send messages.	
CTS	Clear To Send	RTS/CTS (Request to Send / Clear To Send) is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem and exposed node problem. A node wishing to send data initiates the process by sending a Request to Send frame (RTS). The destination node replies with a Clear To Send frame (CTS). Any other node receiving the CTS frame should refrain from sending data for a given time (solving the hidden node problem). The amount of time the node should wait before trying to get access to the medium is included in both the RTS and the CTS frame. Any other node receiving the RTS frame but not the CTS frame is permitted to transmit to other neighboring nodes (solving the exposed node problem). This protocol was designed under the assumption that all nodes have the same transmission range.	http://www.ieee802.org/11

Acronym/ Term	Definition	Explanation	Web-resources
D-AMPS	Digital Advanced Mobile Phone System	Second-generation (2G) mobile phone system, known as IS-54 and IS-136. It is used throughout the Americas, particularly in the United States and Canada. Often referred to as TDMA. D-AMPS has been competing against GSM and systems based on Code division multiple access (CDMA) for adoption by the network carriers, although it is now being phased out in favor of GSM technology. IS-54 was standardised by EIA and TIA, later adopted by ANSI as ANSI/EIA/TIA-627.	http://www.ansi.org http://www.tiaonline.org http://www.eia.org
DCF	Distributed Coordination Function	A type of Medium Access Control (MAC) technique used in Wi-Fi Wireless LANs. DCF manages the transmission over a medium by allowing each node to listen to surrounding nodes to see if they are transmitting, before transmitting themselves. DCF is de-facto default setting for Wi-Fi hardware.	http://www.ieee802.org/11
DHCP	Dynamic Host Configuration Protocol	DHCP is a client-server networking protocol. A DHCP server provides configuration parameters specific to the DHCP client host requesting, generally, information required by the client host to participate on an IP network. DHCP also provides a mechanism for allocation of IP addresses to client hosts. DHCP appeared as a standard protocol in October 1993. RFC 2131 provides the latest (March 1997) DHCP definition. The latest standard on a protocol describing DHCPv6, DHCP in a IPv6 environment, was published in July 2003 as RFC 3315.	http://www.ietf.org http://tools.ietf.org/html/rfc2131 http://tools.ietf.org/html/rfc3315
DIAMETER		DIAMETER is an AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility. The basic concept is to provide a base protocol that can be extended in order to provide AAA services to new access technologies. DIAMETER is intended to work in both local and roaming AAA situations. Defined in IETF RFC 3588.	http://www.ietf.org http://tools.ietf.org/html/rfc3588
DLP	Direct Link Protocol	The DLP in 802.11e provides a mechanism to allow direct station-to-station communication in the case where the stations are in range of each other. Direct link refers to the ability to exchange data directly between two stations in the network, without traversing the AP. The legacy 802.11 MAC specifies that stations may only communicate with APs.	http://www.ieee802.org/11
DRM	Digital Rights Management	Any of several technologies used by publishers (or copyright owners) to control access to and usage of digital data (such as software, music, movies) and hardware, handling usage restrictions associated with a specific instance of a digital work.	
DSLAM	Digital Subscriber Line Access Multiplexer	A DSLAM is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line (DSL) connections and puts the signals on a high-speed backbone line using multiplexing techniques. Depending on the product, DSLAM multiplexers connect DSL lines with some combination of asynchronous transfer mode (ATM), frame relay, or Internet Protocol networks.	
DVB	Digital Video Broadcasting	An international digital broadcast standard for TV, audio and data. DVB can be broadcast via satellite, cable or terrestrial systems. It has been initially used in Europe and the Far East.	http://www.dvb.org/
DVD	Digital Versatile Disc	Formerly Digital Video Disc, data storage format released in 1995. The discs have the same physical size as the CD, but the capacity is more than seven times higher, approx. 4.7 GB on one side. The discs can have dual layers per side, thus a double-sided, dual-layer disc can store approx. 17 GB of data. Used for storing video, sound, computer software and data, games, etc. A single-sided, single-layer disc can store a typical feature film of 130 minutes with eight different surround quality sound tracks. Available as read-only (DVD-Video, DVD-ROM), Once writable (DVD-R, DVD+R) and re-writable (DVD-RW, DVD+RW, DVD-RAM).	http://www.dvdforum.org
EAP	Extensible Authentication Protocol	An authentication framework that enables clients to authenticate with a central server. EAP can be used with several authentication mechanisms (EAP methods), such as: EAP-AKA, EAP-SIM, EAP-MD-5, etc.	
EAP-AKA	Extensible Authentication Protocol for UMTS Authentication and Key Agreement	Authentication and session key distribution using the Universal Mobile Telecommunications System (UMTS) UMTS Subscriber Identity Module (USIM). EAP AKA is defined in IETF RFC 4187.	http://www.ietf.org http://tools.ietf.org/html/rfc4187
EAP-OBAN	Extensible Authentication Protocol – Open Broadband Access Network	An EAP method unique for OBAN, where a Kerberos-style ticket that could be validated locally in the RGW is used to authenticate the user.	
EAP-SIM	Extensible Authentication Protocol – Subscriber Identity Module	An EAP method where the GSM Subscriber Identity Module (SIM) is used for authentication. EAP-SIM is defined in RFC 4186.	http://www.ietf.org http://tools.ietf.org/html/rfc4186

ISSN 0085-7130 © Telenor ASA 2006

Acronym/ Term	Definition	Explanation	Web-resources
ECMA	European Computer Manufacturers Association	Ecma International is an international membership-based standards organisation for information and communication systems. Until 1994 named the European Computer Manufacturers Association (ECMA) when it changed its name to express the organization's international reach. The name is no longer considered an acronym and no longer uses full capitalization. The organization was originally founded in 1961 to standardise computer systems in Europe. Membership is open to companies that produce, market or develop computer or communication systems in Europe.	http://www.ecma-international.org/
EDCA	Enhanced Distributed Channel Access	Part of the IEEE 802.11e standard. With EDCA, high priority traffic has a higher chance of being sent than low priority traffic: a station with high priority traffic waits a little less before it sends its packet, on average, than a station with low priority traffic. In addition, each priority level is assigned a Transmit Opportunity (TXOP). A TXOP is a bounded time interval during which a station can send as many frames as possible (as long as the duration of the transmissions does not extend beyond the maximum duration of the TXOP). If a frame is too large to be transmitted in a single TXOP, it should be fragmented into smaller frames. The use of TXOPs reduces the problem of low rate stations gaining an inordinate amount of channel time in the legacy 802.11 DCF MAC.	http://www.ieee802.org/11
EIRP	Effective Isotropic Radiated Power	The amount of power one has to feed into an omni-directional (isotropic) antenna in order to obtain the same electromagnetic power density or field strength in a given direction, compared to a practical, directive antenna. EIRP is usually given for the direction of maximum power.	
EPG	Electronic Program Guide	Also called an Interactive Program(me) Guide (IPG) or Electronic Service Guide (ESG). It is an on-screen guide to scheduled broadcast television programs, allowing a viewer to navigate, select, and discover content by time, title, channel, genre, etc, by use of their remote control, a keyboard or a phone keypad.	
ETSI	European Telecommunication Standards Institute	A non-profit membership organization founded in 1988. The aim is to produce telecommunications standards to be used throughout Europe. The efforts are coordinated with the ITU. Membership is open to any European organization proving an interest in promoting European standards. It was e.g. responsible for the making of the GSM standard. The headquarters are situated in Sophia Antipolis, France.	http://www.etsi.org
Eurescom	The European Institute for Research and Strategic Studies in Telecommunications	An organisation for collaborative R&D in telecommunications. Eurescom was founded in 1991 by major European network operators and service providers. Based in Heidelberg/Germany, the organisation provides services for initiating, managing and supporting distributed collaborative research programmes to network operators, service providers, suppliers and vendors who wish to collaborate on the issues facing the telecommunications industry.	http://www.eurescom.de
FA	Foreign Agent	A router on a mobile node's visited network which provides routing services to the mobile node while registered. The foreign agent detunnels and delivers datagrams to the mobile node that were tunneled by the mobile node's home agent. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes. It is defined in IETF RFC 3344.	http://www.ietf.org http://tools.ietf.org/html/rfc3344
FIR	Finite Impulse Response	A type of a digital filter. It is 'finite' because its response to an impulse ultimately settles to zero.	
FMC	Fixed Mobile Convergence	Convergence between the mobile and fixed line networks giving telecommunications operators the possibility to provide services to users irrespective of their location, access technology, and terminal.	
G.711		An ITU-T standard for audio companding. It is primarily used in telephony. The standard was released for usage in 1972. G.711 is a standard to represent 8 bit compressed pulse code modulation (PCM) samples for signals of voice frequencies, sampled at the rate of 8000 samples/second and 8 bits per sample. G.711 encoder will thus create a 64 kbit/s bitstream. There are two main algorithms defined in the standard, m-law algorithm (used in North America & Japan) and a-law algorithm (used in Europe and the rest of the world). Both are logarithmic, but the later a-law was specifically designed to be simpler for a computer to process. The standard also defines a sequence of repeating code values which defines the power level of 0 dB.	http://www.itu.int
G.723.1		An audio codec for voice that compresses voice audio in chunks of 30 milliseconds. A look-ahead of 7.5 ms duration is also used. Music or tones such as DTMF or fax tones cannot be transported reliably with this codec. G.723.1 is mostly used in Voice over IP (VoIP) applications for its low bandwidth requirement. It became an ITU-T standard in 1995. The complexity of the algorithm is below 16 MIPS. 2.2 kilobytes of RAM is needed for codebooks. G.723.1 can operate at two bit rates: 6.3 kbit/s (using 24 byte chunks) and 5.3 kbit/s (using 20 byte chunks).	http://www.itu.int
GERAN	GPRS/EDGE Radio Access Network	The Radio Access part of GSM/EDGE. More specifically: RF layer, Layer 1, 2 and 3, internal (Abis, Ater) and external (A, Gb) interfaces, conformance test specifications for all aspects of GERAN base stations and terminals and GERAN specific O&M specifications for the nodes in the GERAN. Specified by 3GPP.	http://www.3gpp.org

Acronym/ Term	Definition	Explanation	Web-resources
GFA	Gateway Foreign Agent	A Foreign Agent which has a publicly routable IP address. A GFA may, for instance, be placed in or near a firewall. Currently under work as an Internet draft by IETF.	http://www.ietf.org https://datatracker.ietf.org/public/idindex.cgi
GPRS	General Packet Radio Service	An enhancement to the GSM mobile communication system that supports data packets. GPRS enables continuous flows of IP data packets over the system for such applications as web browsing and file transfer. Supports up to 160 kb/s gross transfer rate. Practical rates are from 12 – 48 kb/s.	http://www.etsi.org http://www.3gpp.org
GSM	Global System for Mobile communications	A digital cellular phone technology system that is the predominant system in Europe, but is also used around the world. Development started in 1982 by CEPT and was transferred to the new organisation ETSI in 1988. Originally, the acronym was the group in charge, "Group Special Mobile" but later the group changed name to SMG. GSM was first deployed in 7 countries in Europe in 1992. It operates in the 900 MHz and 1.8 GHz band in Europe and 1.9 GHz band in North America. GSM defines the entire cellular system, from the air interface to the network nodes and protocols. As of October 2005, there were more than 2.1 billion GSM users in more than 200 countries worldwide. The ubiquity of the GSM standard makes international roaming very common between mobile phone operators which enable phone users to access their services in many other parts of the world as well as their own country. GSM differs significantly from its predecessors in that both signalling and speech channels are digital, which means that it is seen as a second generation (2G) mobile phone system. This fact has also meant that data communication was built into the system from very early on. GSM is an open standard which is currently developed by the 3GPP.	http://www.gsmworld.com/ http://www.etsi.org http://www.3gpp.org
GUI	Graphical User Interface	A GUI is a particular case of user interface for interacting with a computer which employs graphical images and widgets in addition to text to represent the information and actions available to the user. Usually the actions are performed through direct manipulation of the graphical elements.	
HA	Home Agent	A router on a mobile node's home network which tunnels datagrams for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node. Defined in IETF RFC 3344.	http://www.ietf.org http://tools.ietf.org/html/rfc3344
HCCA	Hybrid Coordinated Channel Access	Channel access function within the IEEE 802.11e Hybrid Coordination Function (HCF). The interval between two beacon frames is divided into two periods. The main difference with the Point Coordination Function (PCF) is that Traffic Classes (TC) are defined. Also, the Hybrid Coordinator (HC, usually the access point) can coordinate the traffic in any fashion it chooses (not just round-robin). Moreover, the stations give info about the lengths of their queues for each Traffic Class (TC). The HC can use this info to give priority to one station over another. Another difference is that stations are given a TXOP: they may send multiple packets in a row, for a given time period selected by the HC.	http://www.ieee802.org/11
HCF	Hybrid Coordination Function	Hybrid of Distributed Coordination Function (DCF) and Point Coordination Function (PCF) used in Wi-Fi Wireless LANs. Defined in the IEEE 802.11e.	http://www.ieee802.org/11
HDTV	High Definition Television	Broadcast of television signals with a higher resolution than traditional formats (NTSC, SECAM, PAL) allow. Except for an early analog format in Japan, HDTV is broadcast digitally, and therefore its introduction sometimes coincides with the introduction of digital television (DTV). An HDTV-compatible TV usually uses a 16:9 aspect ratio. The high resolution images (1920 pixels × 1080 lines or 1280 pixels × 720 lines) allow much more detail to be shown compared to analog television or regular DVDs. MPEG-2 is currently used as the compression codec. Like NTSC and PAL, 1920 × 1080 broadcasts generally use interlacing to reduce bandwidth demands. Alternating scan lines are broadcast 50 or 60 times a second, similar to PAL's 50 Hz and NTSC's 60 Hz interlacing. This format is entitled 1080i, or 1080i60. In areas traditionally using PAL 50 Hz 1080i50 is also used. Progressive scan formats are also used with frame rates up to 60 per second. The 1280 × 720 format is in practice always progressive scan (with the entire frame refreshed each time) and is thus termed 720p.	
Hiper ACCESS	High Performance Radio Access	A Point-to-MultiPoint (PMP) network architecture intended for high speed (up to 120 Mb/s) and high-QoS fixed wireless access. Applications include broadband access for residential and small business users to a wide variety of networks as a flexible and competitive alternative to wired access networks, however HiperACCESS is not an LMDS-type systems. HiperACCESS standardization focuses on solutions optimized for frequency bands above 11 GHz (e.g. 26, 28, 32, 42 GHz) with high spectral efficiency under LOS (Line Of Sight) conditions. For bandwidths of 28 MHz, both FDD and TDD channel arrangements as well as H-FDD terminals are supported. HiperACCESS is an interoperable standard, allowing for PMP systems with base station and terminal stations from different manufacturers. The HiperACCESS (HA) specifications are being developed by TC (Technical Commitee) BRAN.	http://www.etsi.org

ISSN 0085-7130 © Telenor ASA 2006

Acronym/ Term	Definition	Explanation	Web-resources
HiperLAN	High Performance Radio Local Area Network	A short-range variant of a broadband radio access network intended as a complementary access mechanism for UMTS systems as well as for private use as a wireless LAN type system. HiperLAN offers high speed (up to 54 Mb/s) access to a variety of networks including the UMTS core networks, ATM networks and IP based networks. Basic applications include data, voice and video, with specific Quality of Service parameters taken into account. HiperLAN/2 systems can be deployed in offices, classrooms, homes, factories, hot spot areas such as exhibition halls and, more generally, where radio transmission is an efficient alternative or complements wired technology. The HiperLAN/2 specifications are being developed by ETSI Project BRAN.	http://www.etsi.org
HiperMAN	High Performance Radio Metropolitan Network	A standard created by the European Telecommunications Standards Institute (ETSI) Broadband Radio Access Networks (BRAN) group to provide a wireless network communication in the 2 – 11 GHz bands across Europe and other countries which follow the ETSI standard. HIPERMAN is a European alternative to WiMAX (or the IEEE 802.16 standard) and the Korean technology WiBro.	http://www.etsi.org
HLR	Home Location Register	The Home Location Register or HLR is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network. More precisely, the HLR stores details of every SIM card issued by the mobile phone operator. Each SIM has a unique identifier called an IMSI which is one of the primary keys to each HLR record. The next important items of data associated with the SIM are the telephone numbers used to make and receive calls to the mobile phone, known as MSISDNs. The main MSISDN is the number used for making and receiving voice calls and SMS, but it is possible for a SIM to have other secondary MSISDNs associated with it for fax and data calls. Each MSISDN is also a primary key to the HLR record.	http://www.etsi.org
HMM	Hidden Markov Model	A statistical approach to extracting symbolic data from signal data, e.g. phonemes from speech. Basically, an HMM is a finite automaton with probability values for every arc and arc label.	
HomeRF	Home Radio Frequency	A working group which developed the SWAP (Shared Wireless Access Protocol) specification for a broad range of interoperable consumer devices. SWAP is an open industry specification that allows PCs, peripherals, cordless telephones and other consumer devices to share and communicate voice and data in and around the home without wires. The SWAP specification provides voice and data communications in the 2.4 GHz ISM band. The membership of the group exceeded 100 companies across the PC, consumer electronics, networking, peripherals, communications, software, retail channel, home control and semiconductor industries worldwide. The Home RF group was disbanded in January 2003.	http://www.palowireless.com/homerf/
HSDPA	High-Speed Downlink Packet Access	Enhancement of the 3G standard UMTS in order to provide higher bit rates on the downlink. The theoretical data rate can reach 14.4 Mb/s.	http://www.3gpp.org
HSPA	High Speed Packet Access	Common term for High Speed Downlink Packet Access (HSDPA) and Enhanced Dedicated Channel (EDCH, often referred to as HSUPA – High Speed Uplink Packet Access), which are enhancements of the 3G standard UMTS to provide higher data rates on both downlink and uplink. The theoretical data rate can reach 14.4 Mb/s on the downlink and 5.6 Mb/s on the uplink.	http://www.3gpp.org
HTTP	Hyper Text Transport Protocol	An application-level protocol for distributed, collaborative, hypermedia information systems. Used to request and transmit files, especially webpages and webpage components, over the Internet or other computer network.	http://www.w3c.org
IEEE	The Institute of Electrical and Electronics Engineers	USA based organisation open to engineers and researchers in the fields of electricity, electronics, computer science and telecommunications. Established in 1884. The aim is to promote research through journals and conferences and to produce standards in telecommunications and computer science. IEEE has produced more than 900 active standards and has more than 700 standards under development. Divided into different branches, or 'Societies'. Has daughter organisations, or 'chapters' in more than 175 countries worldwide. Headquarters are in Piscataway, New Jersey, USA.	http://www.ieee.org
IEEE 802.11	The IEEE 802 LAN/MAN Standards Committee Working Group for WLAN	Refers to a family of specifications developed by the IEEE for wireless local area networks. It also refers to the "Wireless LAN working group" of the IEEE 802 project. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997. There are several specifications in the 802.11 family, including i) 802.11 – provides 1 or 2 Mbit/s transmission in the 2.4 GHz band; ii) 802.11a – an extension that provides up to 54 Mbit/s in the 5 GHz band. It uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS; iii) 802.11b provides 11 Mbit/s transmission in the 2.4 GHz band and was ratified in 1999 allowing wireless functionality comparable to Ethernet; iv) 802.11g provides 20+ Mbit/s in the 2.4 GHz band, v) 802.11z is a method for transporting an authentication protocol between the client and access point, and the Transport Layer Security (TLS) protocol. More variants are also under preparation, including support of 100 Mbit/s traffic flows.	http://www.ieee802.org/11/

Acronym/ Term	Definition	Explanation	Web-resources
IEEE 802.11e	Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements	An amendment to the IEEE 802.11 WLAN standard that defines a set of Quality of Service enhancements for LAN applications. It was approved in 2005.	http://www.ieee802.org/11
IEEE 802.16	The IEEE 802 LAN/MAN Standards Committee Working Group on Broadband Wireless Access Standards	A specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture. Published on April 8, 2002, the standard defines the use of bandwidth between the licensed 10 GHz and 66 GHz and between the 2 GHz and 11 GHz (licensed and unlicensed) frequency ranges and defines a MAC layer that supports multiple physical layer specifications customized for the frequency band of use and their associated regulations. 802.16 supports very high bit rates in both uploading to and downloading from a base station up to a distance of 30 miles to handle such services as VoIP, IP connectivity and TDM voice and data.	http://www.ieee802.org/16/ http://www.wimaxforum.org/
IEEE 802.1X	IEEE Standards for Local and metropolitan area networks – Port-Based Network Access Control	An IEEE standard for port-based Network Access Control; it is part of the IEEE 802 (802.1) group of protocols. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. It is used for certain closed wireless access points, and is based on the EAP, Extensible Authentication Protocol.	http://www.ieee802.org /1/pages/802.1x.html
IETF	Internet Engineering Task Force	A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g. routing, transport, security, etc.). Much of the work is handled via mailing lists. The IETF holds meetings three times per year. The IETF working groups are grouped into areas, and managed by Area Directors (AD). The ADs are members of the Internet Engineering Steering Group (IESG). Providing architectural oversight is the Internet Architecture Board (IAB). The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB. The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. The IANA is chartered by the Internet Society (ISOC) to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters. IETF's mission statement is given in IETF RFC 3935.	http://www.ietf.org http://tools.ietf.org /html/rfc3935
IMS	IP Multimedia Subsystem	A standardised Next Generation Networking (NGN) architecture for telecom operators that want to provide mobile and fixed multimedia services. It uses a Voice-over-IP (VoIP) implementation based on a 3GPP standardised implementation of SIP, and runs over the standard Internet Protocol (IP). Existing phone systems (both packet-switched and circuit-switched) are supported. IMS was originally defined by an industry forum called 3G.IP (www.3gip.org) formed in 1999. 3G.IP developed the initial IMS architecture, which was brought to 3GPP for industry standardization as part of their standardization work for 3G mobile phone systems in UMTS networks. It first appeared in release 5 (evolution from 2G to 3G networks), when SIP-based multimedia was added. Support for the older GSM and GPRS networks was also provided. "Early IMS" was defined to allow for IMS implementations that do not yet support all "Full IMS" requirements. 3GPP2 (a different organisation) based their CDMA2000 Multimedia Domain (MMD) on 3GPP IMS, adding support for CDMA2000.	http://www.3gpp.org http://www.ietf.org
IMT-2000	International Mobile Tele-communi-cations 2000	The global standard for third generation (3G) wireless communications, defined by a set of interdependent ITU Recommendations. IMT-2000 provides a framework for worldwide wireless access by linking the diverse systems of terrestrial and/or satellite based networks. It will exploit the potential synergy between digital mobile telecommunications technologies and systems for fixed and mobile wireless access systems.	http://www.itu.int/home /imt.html
Internet		From the commissioning of ARPANET by the US DoD in 1969 the packet switched Internet has gained acceptance and users all over the world. The release of WWW at the end of the 90s and the browsing possibilities (see WWW) increased the demand for Internet. The inter-connection of heterogeneous sub networks of different bandwidths, the best-effort service model and the global end-to-end logical addressing of the internet protocol (IP) has arranged for Internet to be the common information network multiplexing text, pictures, and video as well as packet switched telephony.	

ISSN 0085-7130 © Telenor ASA 2006

Acronym/ Term	Definition	Explanation	Web-resources
IntServ	Integrated Services	A computer network architecture that specifies the elements to guarantee quality of service (QoS) on networks. IntServ can for example be used to allow video and sound to reach the receiver without interruption. IntServ specifies a fine-grained QoS system. The idea of IntServ is that every router in the system implements IntServ, and every application that requires some kind of guarantees has to make an individual reservation. "Flow Specs" describe what the reservation is for, while the Resource Reservation Protocol (RSVP) is the underlying mechanism to signal it across the network.	http://www.ietf.org http://tools.ietf.org/html/rfc1633
IP	Internet Protocol	A protocol for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.	http://www.ietf.org
ISM	Industrial Scientific and Medicine	The industrial, scientific and medical (ISM) radio bands were originally reserved internationally for non-commercial use of RF electromagnetic fields for industrial, scientific and medical purposes. The ISM bands are defined by the ITU-R in 5.138 and 5.150 of the Radio Regulations. Individual countries' use of the bands designated in these sections may differ due to variations in national radio regulations. In recent years they have also been shared with license-free error-tolerant communications applications such as wireless LANs and Bluetooth. ISM comprises frequencies in the 900 MHz band, the 1.8 GHz Band, the 2.4 GHz band and the 5.8 GHz band.	
ISP	Internet Service Provider	A vendor who provides access for customers to the Internet and the World Wide Web. The ISP also typically provides a core group of internet utilities and services like e-mail and news group readers.	
ISPRU	Internet Service Provider of the Residential User		
ISPVU	Internet Service Provider of the Visiting User		
IST	Information Society Technologies	Thematic Programmes of the 5th and 6th Framework Research Programmes funded by the European Union. The first IST programme ran from 2000 to 2004, the IST programme of the 6th Framework Research Programme started in 2003 and runs to 2006.	http://www.cordis.lu/ist/
ITS	Intelligent Transport Systems	Intelligent Transport Systems and Services (ITS) describes any system or service that makes the movement of people or goods more efficient and economical, thus more "intelligent".	http://www.ertico.com
JPEG	Joint Photographic Expert Group	A commonly used standard method of compression for photographic images. Also name of the joint ISO/CCITT committee which created the standard. The group was organized in 1986, issuing a standard in 1992 which was approved in 1994 as ISO 10918-1. JPEG provides for lossy compression of images. The file format which employs this compression is commonly also called JPEG; the most common file extension for this format is .jpg, though .jpeg, .jfif, .JPG, and .JPE are also used. JPEG itself specifies only how an image is transformed into a stream of bytes, not how those bytes are encapsulated in any particular storage medium. A further standard created by the Independent JPEG Group, called JFIF (JPEG File Interchange Format), specifies how to produce a file suitable for computer storage and transmission (such as over the Internet) from a JPEG stream. In common usage, when one speaks of a "JPEG file" the actual file is generally found to be JFIF, or sometimes an Exif JPEG file. There are, however, other JPEG-based file formats, such as JNG. Additionally, the TIFF format can carry JPEG data.	http://www.jpeg.org/
KDC	Key Distribution Center	The combination of Authentication Server and Ticket Granting Server of the Kerberos authentication protocol. It is defined in IETF RFC 4120.	http://www.ietf.org http://tools.ietf.org/html/rfc4120
Kerberos		Kerberos is a computer network authentication protocol which allows individuals communicating over an insecure network to prove their identity to one another in a secure manner. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos prevents eavesdropping or replay attacks, and ensures the integrity of the data. Its designers aimed primarily at a client-server model, and it provides mutual authentication – both the user and the server verify each other's identity. Kerberos builds on symmetric key cryptography and requires a trusted third party. It was developed by The Massuchussets Institute of Technology (MIT) in the 1980s and is now maintained by IETF. It is defined in IETF RFC 4120.	http://www.ietf.org http://tools.ietf.org/html/rfc4120
LAN	Local Area Network	A network shared by communicating devices, usually in a small geographical area. A system that links together electronic office equipment, such as computers and word processors, and forms a network within an office or building.	
LLUB	Local Loop Unbundling	Option to rent only the local loop (e.g. copper access line to a customer) by a non-incumbent operator.	
LOS	Line of Sight	This term is usually associated with radio transmission systems indicating there is a clear path between the transmitter and receiver.	

Acronym/ Term	Definition	Explanation	Web-resources
MAC	Medium Access Control	The lower of the two sub layers of the Data Link Layer. In general terms, MAC handles access to a shared medium, and can be found within many different technologies. For example, MAC methodologies are employed within Ethernet, GPRS, and UMTS.	
MAC Address	Medium Access Control Address	A hardwire address that uniquely identifies each node of a network.	
MAN	Metropolitan Area Network	Large computer networks usually spanning a campus or a city using wireless infrastructure or optical fiber connections to link their sites. Some technologies used for this purpose are Asynchronous Transfer Mode (ATM), Fibre Distributed Data Interface (FDDI) and Switched Multimegabit Data Service (SMDS). These older technologies are in the process of being displaced by Ethernet-based MANs in most areas. MAN links between LANs have been built without cables using either microwave, radio, or infra-red free-space optical communication links.	
MB	Mobility Broker		
MIMO	Multiple Input – Multiple Output	MIMO is an antenna technology for wireless communications in which multiple antennas are used at both the source (transmitter) and the destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed. MIMO is one of several forms of smart antenna technology, the others being MISO (multiple input, single output) and SIMO (single input, multiple output). MIMO technology has aroused interest because of its possible applications in digital television (DTV), wireless local area networks (WLANs), metropolitan area networks (MANs), and mobile communications.	
MIP	Mobile IP	A communication protocol that allows a device to move between different networks while maintaining a permanent IP address. The Mobile IP protocol is defined in RFC 3344.	http://www.ietf.org http://tools.ietf.org/html/rfc3344
MMAC	Multimedia Mobile Access Communication System	Portable Wireless Access Systems which can transmit ultra high speed, high quality Multimedia Information "anytime and anywhere" with seamless connections to optical fiber networks. These are systems which can transmit at up to 1 Gb/s using the SHF band (3–60 GHz), the millimeter wave radio band (30-300 GHz) and other bands. It can be used for mobile video telephone conversations and high quality TV conferences. Promoted by the Japanese MMAC Forum as 4th generation (4G) systems to be used after the IMT-2000 systems.	http://www.arib.or.jp/mmac/e/index.htm
Monte Carlo method		A widely used class of computational algorithms for simulating the behavior of various physical and mathematical systems. They are distinguished from other simulation methods by being stochastic, that is nondeterministic in some manner – usually by using random or pseudo-random numbers – as opposed to deterministic algorithms. Because of the repetition of algorithms and the large number of calculations involved, Monte Carlo is a method suited to calculation using a computer, utilizing many techniques of computer simulation. Monte Carlo methods are especially useful in studying systems with a large number of coupled degrees of freedom.	
MPDU	MAC Protocol Data Unit	Frame format on the medium access layer (MAC) of the IEEE 802.11 WLAN.	http://www.ieee802.org/11
MSISDN	Mobile Station Integrated Services Digital Network	MSISDN refers to the 15-digit number that is used to refer to a particular mobile station. It is the mobile equivalent of ISDN. The ITU-T recommendation E.164 defines the international numbering plan that MSISDN is based on.	http://www.itu.int
MSP	Mobile Service Provider		
MVNO	Mobile Virtual Network Operator	An MVNO is a mobile service operator that does not have its own licensed spectrum and does not have the infrastructure to provide mobile service to its customers (i.e. it does not own the network on which its voice and data traffic is carried). Instead, MVNOs lease wireless capacity from pre-existing mobile service providers and establish their own brand names different from the providers. (Cf. *Telektronikk*, 97 (4), 2001)	
NFC	Near Field Communication Technology	NFC, jointly developed by Sony and Philips, was approved as an ISO/IEC standard on December 8, 2003. It was approved as an ECMA standard earlier on. On March 18, 2004 Nokia, Sony and Philips formed NFC-forum to advance NFC development. NFC holds the promise of bringing true mobility to consumer electronics in an intuitive and psychologically comfortable way since the devices can handshake only when brought literally into touching distance.	http://www.nfc-forum.org http://www.iso.org http://www.iec.ch http://www.ecma-international.org
NLOS	Non-Line of Sight	A term used to describe radio transmission across a path that is partially obstructed, usually by a physical object in the Fresnel zone.	
OAN	Open Access Network	Network model which refers to a horizontally layered network architecture and business model that separates physical access to the network from service provisioning. The same OAN will be used by a number of different providers that share the investments and maintenance cost. The OAN concept is especially appropriate for deploying metropolitan WiFi Access Networks.	

ISSN 0085-7130 © Telenor ASA 2006

Acronym/ Term	Definition	Explanation	Web-resources
OBAN	Open Broadband Access Network	Research project in the European Union's 6th Framework Programme IST. The OBAN project introduces an approach to establishing a broadband mobile network based upon an Open Access Network (OAN) approach characterised by all private wireless LANs and broadband access lines being made available for public use, thus the stationary users (the hosts) can continue to use their wireless LAN as before, and casually passing users can access and maintain communication via these access point. The project is running from 2004 to 2006.	http://www.ist-oban.org http://oban.prz.tu-berlin.de/
OFDM	Orthogonal Frequency Division Multiplexing	A spread spectrum technique that distributes the data over a large number of carriers spaced apart at precise frequencies. This spacing provides the "orthogonality" in this technique, which prevents the demodulators from seeing frequencies other than their own. The benefits of OFDM are high spectral efficiency, resilience to RF interference, and lower multi-path distortion. This is useful because in a typical terrestrial wireless scenario there are multi-path-channels (i.e. the transmitted signal arrives at the receiver using various paths of different lengths). Since multiple versions of the signal interfere with each other (inter symbol interference (ISI)) it becomes very hard to extract the original information. OFDM is sometimes called multi-carrier or discrete multi-tone modulation. It is the modulation technique used for digital TV in Europe, Japan and Australia. It is used in DAB, ADSL and WLAN 802.11a and g and WMAN 802.16 standards.	
OFDMA	Orthogonal Frequency Division Multiple Access	A multi-user version of the OFDM digital modulation scheme. Multiple access is achieved in OFDMA by assigning subsets of subcarriers to individual users. This allows simultaneous low data rate transmission from several users. OFDMA is used in the uplink of the IEEE 802.16 Wireless MAN standard, commonly referred to as WiMAX.	
OFP	Optimal Frequency Planning		
OPNET		OPNET Technologies, Inc. is a provider of management software for networks and applications. It is also the name of the software itself. Its headquarters is in Bethesda, Maryland, USA.	http://www.opnet.com
OTP	One-Time Password		
PAN	Personal Area Network	A PAN is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one person. The devices may or may not belong to the person in question. The reach of a PAN is typically a few metres. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink). Personal area networks may be wired with computer buses such as USB and FireWire. A wireless personal area network (WPAN) can also be made possible with network technologies such as IrDA and Bluetooth.	
PC	Personal Computer	Usually a microcomputer whose price, size, and capabilities make it suitable for personal usage. Personal computers are normally operated by one user at a time to perform such general purpose tasks as word processing, internet browsing, e-mail and other digital messaging, multimedia playback, video game play, computer programming, etc. Unlike many special purpose and high performance computers, it is assumed that a typical personal computer will run software not written by its primary users.	
PCF	Point Coordination Function	PCF is a Medium Access Control (MAC) technique used in wireless networks which relies on a central node, often an Access Point (AP), to communicate with a node listening, to see if the radio resource is free.	http://www.ieee802.org/11
PDA	Personal Digital Assistant	Handheld device that combines computing, telephone/fax, Internet and networking features. A typical PDA can function as a cellular phone, fax sender, Web browser and personal organizer.	
PHY	Physical layer	Layer 1 of the OSI model which defines the electrical and optical signalling, line states, clocking guidelines, data encoding, and circuitry needed for data transmission and reception. Contained within the PHY are often several sub-layers that perform these functions including the physical coding physical media dependent sub-layer. The PHY layer connects the media to the MAC (Layer 2).	
PKI	Public Key Infrastructure	An arrangement which provides for third-party vetting of, and vouching for user identities. It also allows binding of public keys to users. This is usually carried by software at a central location together with other coordinated software at distributed locations. The public keys are typically in certificates. The term is used to mean both the certificate authority and related arrangements as well as, more broadly and somewhat confusingly, to mean use of public key algorithms in electronic communications. The latter sense is erroneous since PKI methods are not required to use public key algorithms.	
PLCP	Physical Layer Convergence Protocol	Procedures defined in IEEE 802.11 WLAN to map MAC Protocol Data Units (MPDU) into the appropriate physical layer format.	http;//www.ieee802.org/11
PPDU	PLCP Protocol Data Unit	Frame format on the physical layer (PHY) of the IEEE 802.11 WLAN.	http;//www.ieee802.org/11

Acronym/ Term	Definition	Explanation	Web-resources
PPS	Packets per Second		
PSDU	PLCP Service Data Unit		http://www.ieee802.org/11
PSK	Pre-Shared Key	In communication security, a secret which was previously shared between the two parties using an external channel. The characteristics of this secret or key are determined by the system which uses it. It can be a password, a passphrase or a hexadecimal string. This secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems.	
PSTN	Public Service Telephone Network	Common notation for the conventional analogue telephone network.	
QoS	Quality of Service	The "degree of conformance of the service delivered to a user by a provider, with an agreement between them". The agreement is related to the provision/delivery of this service. Defined by EURESCOM project P806 in 1999 and adopted by ITU-T in recommendation E.860.	http://www.itu.int http://www.eurescom.de
RADIUS	Remote Authentication Dial-In User Service	An authentication and accounting system used by many (W)ISPs. When logging in to a public Internet service you must enter your user name and password. This information is passed to a RADIUS service, which checks that the information is correct, and then authorize access to the WISP. The RADIUS specification is maintained by a working group of the IETF.	http://www.ietf.org/
RAM	Random Access Memory	A type of data store used in computers that allows the stored data to be accessed in any order, that is, at random.	
RF	Radio Frequency	Any frequency within the electromagnetic spectrum normally associated with radio wave propagation.	
RFID	Radio Frequency Identification	Radio Frequency IDentification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag is a small object that can be attached to or incorporated into a product, animal, or person. RFID tags contain antennas to enable them to receive and respond to radio-frequency queries from an RFID transceiver. Passive tags require no internal power source, whereas active tags require a power source.	
RGW	Residential Gateway	A hardware device that connects a home or small office network to the Internet. The residential gateway provides port translation (NAT) and allows all the computers in a small network to share one IP address and Internet connection. The residential gateway may sit between the modem and the internal network, or a DSL or cable modem may be integrated into the residential gateway. A residential gateway often combines the functions of an IP router, multi-port Ethernet switch and Wi-Fi access point.	
RSVP	Resource Reservation Protocol	A protocol designed to reserve resources across a network for an integrated services Internet. RSVP provides receiver-initiated set-up of resource reservations for multicast or unicast data flows with scaling and robustness. It is specified in IETF RFC 2205.	http://www.ietf.org http://tools.ietf.org/html/rfc2205
RTS	Request To Send	RTS/CTS (Request to Send / Clear To Send) is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem and exposed node problem. A node wishing to send data initiates the process by sending a Request to Send frame (RTS). The destination node replies with a Clear To Send frame (CTS). Any other node receiving the CTS frame should refrain from sending data for a given time (solving the hidden node problem). The amount of time the node should wait before trying to get access to the medium is included in both the RTS and the CTS frame. Any other node receiving the RTS frame but not the CTS frame is permitted to transmit to other neighboring nodes (solving the exposed node problem). This protocol was designed under the assumption that all nodes have the same transmission range.	http://www.ieee802.org/11
RU	Residential User	A user which is a member of the household where the Residential Gateway is placed.	
SAP	Service Access Point	An identifying label for network endpoints used in OSI networking. The SAP is a conceptual location at which one OSI layer can request the services of another OSI layer. Service access points are for example used in IEEE 802.2 Logical Link Control in Ethernet and similar data link layer protocols.	
SAP	(Bluetooth) SIM Access Profile	A Bluetooth profile which allows devices such as car phones with built-in GSM transceivers to connect to a SIM card in a phone with Bluetooth, so the car phone itself does not require a separate SIM card.	https://www.bluetooth.org
SGSN	Serving GPRS support node	The SGSN is an exchange which performs packet switching functions for mobile stations located in a geographical area designated as the SGSN area.	http://webapp.etsi.org/Teddi/
SIFS	Short Interframe Space	Used in IEEE 802.11 for the highest priority transmissions enabling stations with this type of information to access the radio link first. Examples of information which will be transmitted after the SIFS has expired include RTS (Request To Send) and CTS (Clear To Send) messages in addition to positive acknowledgements.	

ISSN 0085-7130 © Telenor ASA 2006

Acronym/ Term	Definition	Explanation	Web-resources
SIM	Subscriber Identity Module	A subscriber identity module (SIM) is a logical application running on a UICC smartcard. Although the terms UICC and SIM are often interchanged, UICC refers to the physical card, whereas SIM refers to a single application residing in the UICC that collects GSM user subscription information. The SIM provides secure storing of the key identifying a mobile phone service subscriber but also subscription information, preferences and storage of text messages. The equivalence of a SIM in UMTS is a Universal Subscriber Identity Module (USIM).	
SIP	Session Initiation Protocol	An IETF Protocol used to set up voice calls over an IP network. Also the name of the IETF WG developing the protocol. SIP is defined in IETF RFC 3261.	http://www.ietf.org http://tools.ietf.org/html/rfc3261
SIR	Signal to Interference Ratio	Also called C/I – Carrier to interference ratio. The power ratio between the useful signal level (S) and interfering signals (I). Often expressed in dB.	
SLA	Service Level Agreement	A contract between a provider and a customer that guarantees specific levels of performance and reliability at a certain cost. This contract should also precisely define what could be penalties and back-up solutions in case of problems. SLA is especially important to define when an important part of your system or activity relies on third party providers. SLA is also a very good approach for services provided internally to your organisation where you should also have a customer approach concern. A definition is found in IETF RFC 3272.	http://www.ietf.org http://tools.ietf.org/html/rfc3272
SMS	Short Message Service	A service available on most digital mobile phones and other mobile devices that permits the sending of short messages, also known as text messages between mobile phones, other handheld devices and even landline telephones. The term text messaging and its variants are more commonly used in North America, the UK, and the Philippines, while most other countries prefer the term SMS. SMS was originally designed as part of GSM, but is now available on a wide range of networks, including 3G networks.	
SO	Site Owner		
SOHO	Small Office, Home Office	Refers to a local area network as used in a small office / home office business.	
SSID	Service Set IDentifier	A code attached to all packets on a wireless network to identify each packet as part of that network. The code consists of a maximum of 32 alphanumeric characters. All wireless devices attempting to communicate with each other must share the same SSID. Apart from identifying each packet, SSID also serves to uniquely identify a group of wireless network devices used in a given "Service Set". There are two major variants of the SSID. Ad-hoc wireless networks that consist of client machines without an access point use the BSSID (Basic Service Set Identifier); whereas on an infrastructure network which includes an access point, the ESSID (E for Extended) is used instead. Each of these different types may be referred to in general terms as SSID. A network's SSID is often referred to as the "network name" and is commonly set to the name of the network operator, such as a company name. An extremely weak form of wireless network security is to turn off the broadcast of the SSID: to the average user there does not appear to be a network in use; it is however still readily available to hackers using the appropriate tools.	http://www.ieee802.org/11
STA	Station	Term used to denote user terminals and access points in a Wi-Fi Wireless LAN.	http://www.ieee802.org/11
SWAP	Shared Wireless Access Protocol	The SWAP (Shared Wireless Access Protocol) specification was developed by the Home Radio Frequency Working Group (Home RF) for a broad range of interoperable consumer devices. SWAP is an open industry specification that allows PCs, peripherals, cordless telephones and other consumer devices to share and communicate voice and data in and around the home without wires. The SWAP specification provides voice and data communications in the 2.4 GHz ISM band.	http://www.palowireless.com/homerf/
TCP	Transport Control Protocol	Transport layer protocol defined for the Internet by Vint Cerf and Bob Kahn in 1974. A reliable octet streaming protocol used by the majority of applications on the Internet. It provides a connection-oriented, full-duplex, point-to-point service between hosts. Currently described in IETF RFC 793.	http://www.ietf.org http://tools.ietf.org/html/rfc793
TGS	Ticket-Granting Server	A server that issues service tickets to clients that possess a Ticket-Granting Ticket.	
TGT	Ticket-Granting Ticket	A ticket issued by an Authentication Server that enables the recipient to request service tickets from a Ticket Granting Server. A Kerberos function.	
TXOP	Transmission Opportunity	Part of the IEEE 802.11e Enhanced Distributed Channel Access (EDCA) method. A bounded time interval during which a station can send as many frames as possible (as long as the duration of the transmissions does not extend beyond the maximum duration of the TXOP). If a frame is too large to be transmitted in a single TXOP, it should be fragmented into smaller frames. The use of TXOPs reduces the problem of low rate stations gaining an inordinate amount of channel time in the legacy 802.11 DCF MAC.	http://www.ieee802.org/11

Acronym/ Term	Definition	Explanation	Web-resources
UDP	User Datagram Protocol	UDP is an unreliable protocol used as an alternative to TCP. UDP does not support retransmission of lost packets. It is used for media transport because voice and video transmission is delay sensitive. Currently defined in IETF RFC 768.	http://www.ietf.org http://tools.ietf.org/html/rfc768
UMA	Unlicensed Mobile Access	UMA provides an alternative access to GSM and GPRS core network services via IP-based broadband connections. In order to deliver a seamless user experience, the specifications define a new network element and associated protocols that provide for the secure transport of GSM/GPRS signaling and user traffic over IP. The caller can automatically switch from GSM to IP-based networks and back again without interruptions.	http://www.3gpp.org
UMTS	Universal Mobile Tele-communication System	The European member of the IMT 2000 family of 3G wireless standards. UMTS supports data rates of 144 kb/s for vehicular traffic, 384 kb/s for pedestrian traffic and up to 2 Mb/s in support of in-building services. The standardisation work began in 1991 by ETSI but was transferred in 1998 to 3GPP as a corporation between Japanese, Chinese, Korean and American organisations. It is based on the use of WCDMA technology and is currently deployed in many European countries. As of October 2006 there are more than 90 million subscribers worldwide. The first European service opened in 2003. In Japan NTT DoCoMo opened its "pre-UMTS" service FOMA (Freedom Of Mobile multimedia Access) in 2000. The system operates in the 2.1 GHz band and is capable of carrying multimedia traffic.	http://www.3gpp.org http://www.umts-forum.org
U-NII	Unlicensed National Information Infrastructure	Part of the US NII initiated under the Clinton administration. It was a proposed, advanced, seamless web of public and private communications networks, interactive services, interoperable hardware and software, computers, databases, and consumer electronics to put vast amounts of information at users' fingertips. The U-NII defines the wireless frequency bands allowed for e.g. IEEE 802.11 WLANs, Bluetooth operation and similar.	
USAID	United States Agency for International Development	A US government organization responsible for most non-military foreign aid. It is an independent federal agency, receiving overall foreign policy guidance from the US Secretary of State and seeks to "extend a helping hand to those people overseas struggling to make a better life, recover from a disaster or striving to live in a free and democratic country ..." (mission quote).	http://www.usaid.gov
UWB	Ultra Wideband	A technology for transmitting information spread over a large bandwidth that should, in theory and under the right circumstances, be able to share spectrum with other users. The FCC and ITU-R define UWB in terms of a transmission from an antenna for which the emitted signal bandwidth exceeds the lesser of 500 MHz or 20% bandwidth. Thus, pulse-based systems, wherein each transmitted pulse instantaneously occupies a UWB bandwidth, or an aggregation of at least 500 MHz worth of narrowband carriers, for example in orthogonal frequency-division multiplexing (OFDM) fashion can be regarded as UWB systems.	
VCC	Voice Call Continuity	A function of the IP Multimedia Subsystem (IMS).	http://www.3gpp.org
VDSL	Very High Speed Digital Subscriber Line	VDSL transmits data up to 26 Mb/s over short distances of twisted pair copper wire. The shorter the distance, the faster the connection rate. Specified by ITU-T G.993.1. Second generation, VDSL2, supports up to 100 Mb/s data rate either symmetric or asymmetric in the range of 1-3 km. Specified in ITU-T G.993.2.	http://www.itu.int
V-LAN/ VLAN	Virtual LAN	A method of creating independent logical networks within a physical network. Several VLANs can co-exist within such a network.	
VoIP	Voice over Internet Protocol	Voice over Internet Protocol is the routing of voice conversations over the Internet or any other IP-based network. The voice data flows over a general-purpose packet-switched network, instead of traditional dedicated, circuit-switched voice transmission lines. Several standards exist to support VoIP, like H.323 from ITU-T and SIP (IETF RFC 3261).	http://www.itu.int http://www.ietf.org
VoWLAN	Voice over WLAN	Voice over IP over a Wi-Fi network.	
VPN	Virtual Private Network	A VPN is a private communications network usually used within a company, or by several different companies or organizations, to communicate over a public network. VPN message traffic is carried on public networking infrastructure (e.g. the Internet) using standard (often insecure) protocols, or over a service provider's network providing VPN service guarded by well defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider.	
VU	Visiting User	A temporary (alien) user attached to a Residential Gateway.	
WAN	Wide Area Network	A network that provides data communications to a large number of independent users spread over a larger geographic area than that of a LAN (Local Area Network). It may consist of a number of LANs connected together.	

Acronym/ Term	Definition	Explanation	Web-resources
WAP	Wireless Application Protocol	Wireless Application Protocol (WAP) is an open international standard for applications that use wireless communication, for example Internet access from a mobile phone. WAP was designed to provide services equivalent to a Web browser with some mobile-specific additions, being specifically designed to address the limitations of very small portable devices. It is now the protocol used for the majority of the world's mobile internet sites, otherwise known as wap-sites. The Japanese i-mode system is the other major competing wireless data protocol. The latest version is WAP 2.0. It is specified by the WAP Forum.	http://www.wapforum.org
Wi-Fi	Wireless Fidelity	A term for certain types of wireless local area network (WLAN) that use specifications in the 802.11 family. The term Wi-Fi was created by an organization called the Wi-Fi Alliance, which oversees tests that certify product interoperability. A product that passes the alliance tests is given the label "Wi-Fi certified" (a registered trademark).	http://www.wifialliance.org
WiMAX	Worldwide Interoperability for Microwave Access	A specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture. Based on the IEEE 802.16 WMAN. Published on April 8, 2002, the standard defines the use of bandwidth between the licensed 10 GHz and 66 GHz and between the 2 GHz and 11 GHz (licensed and unlicensed) frequency ranges and defines a MAC layer that supports multiple physical layer specifications customized for the frequency band of use and their associated regulations. 802.16 supports very high bit rates in both uploading to and downloading from a base station up to a distance of 50 km to handle such services as VoIP, IP connectivity and TDM voice and data.	http://www.ieee802.org/16 http://www.wimaxforum.org/
WISP	Wireless Internet Service Provider	A commercial provider of WLAN services in public places.	
WLAN	Wireless Local Area Network	This is a generic term covering a multitude of technologies providing local area networking via a radio link. Examples of WLAN technologies include Wi-Fi (Wireless Fidelity), 802.11b and 802.11a, HiperLAN, Bluetooth and IrDA (Infrared Data Association). A WLAN access point (AP) usually has a range of 20 –300 m. A WLAN may consist of several AP's and may or may not be connected to Internet.	
WMM	Wi-Fi MultiMedia	A subset of the 802.11e standard from the Wi-Fi Alliance	http://www.ieee802.org/11
WPA	WiFi Protected Access	An improved version of WEP (Wired Equivalent Privacy). It is a system to secure wireless (Wi-Fi) networks, created to patch the security of WEP. As a successor, WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared.	http://www.ieee802.org/11 http://www.wifialliance.org
WPAN	Wireless Personal Area Network	A generic term covering different technologies to provide short range wireless networks. Best known are the Bluetooth, ZigBee and IEEE 802.15 WPAN standards.	https://www.bluetooth.org http://www.ieee802.org/15 http://www.zigbee.org
WWAN	Wireless Wide Area Network	A generic term covering different technologies to provide wide area wireless networks.	
xDSL	(Any) Digital Subscriber Line	Various configurations of digital subscriber line: X = ADSL – asymmetric, VDSL – very high speed, SHDSL – single pair high speed, SDSL – symmetric, HDSL – high speed.	
ZigBee		A specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs). The ZigBee 1.0 specification was ratified on December 14, 2004. ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in the USA and 2.4 GHz in most jurisdictions worldwide. The radios use direct-sequence spread spectrum coding (DSSS). Binary Phase Shift Keying (BPSK) is used in the 868 and 915 MHz bands, and orthogonal Quartenary Phase Shift Keying (QPSK) that transmits two bits per symbol is used in the 2.4 GHz band. The raw, over-the-air data rate is 250 kbit/s per channel in the 2.4 GHz band, 40 kbit/s per channel in the 915 MHz band, and 20 kbit/s in the 868 MHz band. Transmission range is between 10 and 75 metres (33~246 feet), although it is heavily dependent on the particular environment. The maximum output power of the radios is generally 0 dBm (1 mW).	http://www.zigbee.org