Project Number:	**IST-2001-32603**
Project Title:	**6NET**
CEC Deliverable Number:	**32603/ULANC/DS/4.2.1/A1**
Contractual Date of Delivery to the CEC:	June 28th 2002
Actual Date of Delivery to the CEC:	July 29th 2002
Title of Deliverable:	IPv6 Wireless LAN Access Issues
Work package contributing to Deliverable:	WP4
Type of Deliverable*:	R
Deliverable Security Class**:	PU
Editors:	Martin Dunmore, Christopher Edwards
Contributors:	Njål T. Borch, Martin Dunmore, Piers O'Hanlon, Reinhard Ruppelt

* Type: P - Prototype, R - Report, D - Demonstrator, O - Other

** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Abstract:

This report investigates the major issues relating to IPv6 access over wireless LANs. Although 6NET is particularly concerned with IPv6, most of the issues in this report apply equally as well to the IPv4 case since the issues tend to be related to the properties of wireless LANs rather than the version of IP being deployed.

Keywords:

Wireless LAN, Access, 802.11, Bluetooth, Hiperlan, Mobile IPv6.

Executive Summary

Since the release of a wireless equivalent to the Ethernet standard, Wireless Local Area Network (WLAN) technology has experienced a widespread deployment and triggered an accelerated development of low-cost, interoperable products. The demand for WLAN access has surged dramatically over the past year. Users are beginning to favour WLAN access because it allows them to access their network and the Internet from anywhere in the workplace, without having to “plug in”. Administrators are attracted to WLANs because they are easier to install (no cable to pull through walls and ceilings), they are flexible (they can be installed in places that wired LANs cannot, and do not require rewiring when seating or office plans change), and, in part owing to this flexibility, they are less expensive to maintain over the long-term.

Installing a wireless LAN is deceptively easy. So much so, that it is not uncommon for departments within some organisations to deploy their own wireless LANs without the prior knowledge or consent of the relevant network administrator. In most cases, a wireless LAN can be deployed using the default settings of an access point to which corresponding clients will automatically connect. Thus, a simple wireless LAN capable of supporting tens of clients can be constructed in only a few minutes from receiving the equipment.

There is no shortage of vendors for wireless LAN access points and client network interface cards (NICs). These range from inexpensive 802.11b products requiring minimal configuration to more expensive ‘enterprise class’ products that offer greater functionality and often include vendor-specific features.

Thus it is no surprise that Wireless LAN ‘hotspots’ are becoming more prevalent worldwide. More and more network operators are considering building or buying WLAN hotspot networks to augment their 3G offerings. According to Cahners In-Stat [37], the number of public wireless LANs in the US is expected to reach 41,000 by 2006. According to industry analysts Frost and Sullivan, the number of access sites will jump from 155 in 2000 to more than 27,000 in Western Europe by 2005 [42]. A study by IDC [44] forecasts that worldwide there will be more than 100,000 hotspots spring up on airports, in hotels or conference centres in the next four years.

Despite the apparent increasing popularity of WLANs, there are many concerns regarding their capability to resist unauthorised access and protect data privacy. IEEE 802.11 does not provide sufficient security, even in consideration of recent attempts to enhance the current 802.11 MAC layer.

Even with IEEE 802.1x and individual keys the protocol remains weak. Therefore, it is recommended to place WLANs outside an organisation’s Internet firewall, not to trust any host connected via 802.11, and to use proven high security protocols, e.g. IPSec and AAA (cf. Annex AAA Protocols / Authentication Protocols).

Another limitation of WLAN deployment is the present lack of unified roaming between wireless ISPs. Currently, wireless ISPs do not have roaming agreements with each other and can therefore only offer islands of wireless connectivity. Users must subscribe to individual wireless ISPs in each area they wish to have connectivity. What we have at the moment is ‘static’ mobility. That is, a user may enjoy connectivity at a WLAN hotspot, but the ability to stay connected and roam between WLAN cells (either owned by the same provider or owned by different providers), is hampered by the lack of both hotspot continuity and Mobile IPv6 intelligence in the network.

Mobile IPv6 is an enabler for true user and service mobility in a multi-access environment. Mobile IPv6 provides connectivity over any wireless access type and supports seamless roaming between WLAN technologies (e.g. 802.11x, Bluetooth, HiperLAN etc.) and the more extensive geographic coverage of 2G, emerging 3G and future 4G access technologies. As such, it can be viewed as an overlay network for all the various types of wireless access networks that may be present and is therefore the primary candidate for global mobility management in the future mobile Internet.

Table of Contents

1 Introduction

The future Internet is likely to provide network services that operate over a great number of different access technologies. Traditionally, access to the Internet has been via wired network infrastructure such as Ethernet or Token Ring LANs, PPP dial-up, cable modems or xDSL. In recent years, there has been a significant increase in the number of users accessing the Internet via wireless links such as satellite, cellular networks and of course,Wireless Local Area Network (WLAN) technology. The tremendous growth in Internet usage means that many people now rely on Internet access for their business, educational, leisure and entertainment needs. Coupled with the global popularity of mobile cellular phones, PC notebooks and, more recently personal digital assistants (PDAs), people now demand Internet access through these portable devices, while they are on the move. The emergence of WLAN technologies such as IEEE 802.11 and Bluetooth, has brought this possibility of a ‘mobile Internet’ much closer to reality. WLAN technologies now offer high enough data rates that they can be a serious alternative to wired LANs in many scenarios. WLAN networking products such as access points and client interface cards are now readily available, easy to deploy, and can in many cases offer a lower cost per user than deploying a wired network for the same coverage.

This report investigates some of the issues relating to IPv6 access over WLANs. Although 6NET is particularly concerned with IPv6, most of the issues in this report apply equally as well to the IPv4 case since the issues tend to be related to the properties of WLANs rather than the version of IP being deployed.

The rest of this report is structured as follows. The next section looks at the different WLAN technologies that are available to choose from. Undoubtedly the most widely deployed is the ‘Wi-Fi’ 802.11b standard, although there are numerous alternatives. Section 3 investigates the issues involved in WLAN deployment. It looks at how easy it is to design and deploy a WLAN, what products are available and recent development in the deployment of public WLAN ‘hotspots’. Anybody reading about WLANs in the media could not have failed to notice the many security concerns attributed to WLANs. Section 4 details some of these security concerns in addition to access control and privacy issues. The problem of enabling users to roam between WLANs (also know as ‘handover’) is addressed in Section 5. The problems of both horizontal and vertical handovers are described in addition to their effects upon higher network layers. Related to this, section 6 looks at the effect upon quality of service (QoS) when a node roams between networks of different quality. Finally, the role of Mobile IPv6 in the future mobile Internet is discussed in section 7.

2 Wireless LAN Technologies

Since the release of an Ethernet equivalent standard, Wireless Local Area Network (WLAN) technology has experienced a widespread deployment and triggered an accelerated development of low-cost, interoperable products. Providing the flexibility to rapidly and wirelessly transfer large data files and high resolution images, access the Web, support videoconferencing, and rapidly reconfigure high-bandwidth sites; high-rate wireless technology promises not only to take Local Area Networks (LANs) to new heights competing with wired infrastructures but also to facilitate the convergence of data and cellular telephone networks.

This section gives a brief overview of the major current wireless network standards[1].

[1] Source: IEEE, Intersil, Intel and others

2.1 Wireless Ethernet (IEEE 802.11)

IEEE 802 is a set of local area network (LAN) standards from the Institute of Electrical and Electronic Engineers (IEEE). There are many individual standards under the 802 umbrella including 802.3 and 802.11.

The standard IEEE 802.3 for wired LANs originated in the late 1970s and is most commonly known as Ethernet. Initially, the standard specified data rates up to 10 Mb/s over coaxial cable or twisted copper pairs. Most LANs operate to this Ethernet standard and almost all networking hardware – routers, hubs, servers, network interface cards (NICs), and all types of modems/gateways – have Ethernet ports. Today, Fast Ethernet is up to 100 Mbps, Gigabit Ethernet is 1 Gbps and 10 Gigabit Ethernet (10GE, approved by IEEE in June 2002) supports data rates up to 1000 times of standard Ethernet. The Gigabit Ethernet is targeted toward wide area network (WAN) interconnects in which many channels are multiplexed for single pipeline distribution.

IEEE 802.11 defines and governs WLANs operating in the 2.4 GHz spectrum and was ratified in 1997. It can be compared to the IEEE 802.3 standard for Ethernet for wired LANs. The IEEE 802.11 specifications address both the Physical (PHY) and Media Access Control (MAC) layers. The original 802.11 standard specified operation at 1 and 2 Mbps using three different wireless technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and infrared (IR). The original standard ensures interoperability of communications equipment within each of these wireless technologies but not between the three technologies. Since then, several standards have been developed under the 802.11 umbrella that allow much higher data rates. The 802.11b standard allows operation up to 11 Mbps and the 802.11a standard defines operation at a higher frequency (5 GHz) and much higher data rates (up to 54Mbps).

2.1.1 High Rate Wireless Ethernet (IEEE 802.11b)

The extension 802.11b (also referred to as ‘Wi-Fi’) to the 802.11 standard, adopted in 1999, allows data rates of 5.5 and 11 Mbps in the 2.4 GHz spectrum and can currently be deemed as the ‘leading’ standard. This extension is backwards compatible to the original 802.11 standard (only DSSS systems; not FHSS or Infrared systems) but adopts a new modulation technique called Complementary Code Keying (CCK), which allows the speed increase. The 802.11b standard defines only one modulation technique for the faster speeds – CCK – unlike the original 802.11 standard that allowed DSSS, FHSS and IR. Because CCK is the only specified technique in the 802.11b standard, any equipment, regardless of the brand or make, will interoperate as long as it meets the 802.11b specification. This advantage is leveraged by the creation of the Wireless Ethernet Compatibility Alliance (WECA), an organization that has set up a certification lab to test 802.11b equipment. When such equipment is certified by WECA, it can carry the Wi-Fi brand on its packaging.

2.1.2 Data Rates to 54 Mb/s in the 2.4 GHz band (IEEE 802.11g)

IEEE 802.11g is a standard that defines a technology for operation at 2.4 GHz that offers higher data rates (up to 22 Mbps) using Orthogonal Frequency Division Multiplexing (OFDM), while remaining compatible to 802.11b. Even higher data rates are considered using two different methods (up to 33 Mbps using PBCC-DSSS and up to 54 Mbps using CCK-OFDM). For owners of existing Wi-Fi equipment, IEEE 802.11g provides a smooth migration path to higher data rates, thus extending the life of 2.4 GHz equipment. The 802.11g Draft Standard was adopted at the November 2001 IEEE 802 meeting.

2.1.3 5 GHz Wireless LAN/WAN (IEEE 802.11a)

IEEE 802.11a (aka Wi-Fi5) is the IEEE WLAN standard that applies to the 5 GHz Unlicensed National Information Infrastructure (UNII) band. This standard specifies the use of Orthogonal Frequency Division Multiplexing (OFDM) for data transmission at rates up to 54 Mbps. There is a European standard, which uses a very similar PHY to 802.11a, called HiperLAN2 (see more details below). Also related is work being done by the IEEE 802.11 Task Group H, which was formed to address the regulatory issues with 802.11a that prevent acceptance by European agencies. These issues are Dynamic Frequency Selection and Transmit Power Control. (DFS/TPC). Another 802.11 Study Group (the 5GSG) has formed to address interoperability between 802.11a and HiperLAN with an objective to make the two standards compatible and for 802.11a to become the global standard for the 5GHz band.

2.1.4 Enhancements to 802.11a/b

The IEEE is working on a number of enhancements to WLAN standards 802.11a/b. The most significant of these are:

802.11e to enhance the 802.11 MAC with a view to improve and manage Quality of Service and provide classes of service.

802.11f to develop recommended practices for an Inter-Access Point Protocol (IAPP) which will provide the necessary capabilities to achieve multi-vendor Access Point interoperability across a Distribution System supporting 802.11 WLAN Links.

802.11i to enhance the 802.11 MAC to with improved security and authentication mechanisms.

2.2 European 5 GHz Wireless LAN/WAN (HiperLAN)

HiperLAN was developed under the European Telecommunications Standardization Institute (ETSI) Broadband Radio Access Networks (BRAN) project. The current standard, HiperLAN/1, operates in the 5GHz spectrum at data rates of up to 24Mbps. The ETSI are currently developing a new Hiperlan/2 standard under the umbrella of the HiperLAN/2 Global Forum (H2GF). HiperLAN/2 is similar to IEEE 802.11a in that both operate in the 5 GHz waveband and both use Orthogonal Frequency Division Multiplexing (OFDM) to attain data rates as high as 54 Mbps. Differences between the two standards exist primarily in the medium access control (MAC) portion of the systems. Whereas the 802.11 standards are connectionless, HiperLAN/2 is connection oriented. Air connections are time division multiplexed (TDM). Each channel, or connection, can be assigned an appropriate quality of service (QoS) based on need (type of data being transmitted such as voice or video). Additionally, HiperLAN/2 will be capable of carrying Ethernet Frames, ATM cells and IP packets. Because of its broadband and channel diversity/QoS capabilities, HiperLAN/2 will first be used for major Wide-Area Network (WAN) interconnections between nodes. Currently, IEEE 802.11a does not offer channel diversity with variable QoS and is closely compared to wireless Ethernet whereas HiperLAN/2 is similar to wireless asynchronous transfer mode (ATM).

2.3 Wireless Personal Area Network (IEEE 802.15)

The 802.15 Wireless Personal Area Network (WPAN™) working group focuses on the development of consensus standards for Personal Area Networks or short distance wireless networks. WPANs are used for the wireless networking of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, and consumer electronics. The goal of this working group is to publish WPAN standards that have broad market applicability and deal effectively with the issues of coexistence and interoperability with other wired and wireless networking solutions.

2.4 Short Distance Device Interconnectivity (Bluetooth)

Bluetooth (BT) is a de facto standard established by a group of manufacturers. It was named after the 10th century Viking king, Harald Bluetooth who united his kingdoms of Denmark and Norway. In February of 1998, the Bluetooth Special Interest Group (BT-SIG) was formed to develop the standard. This standard is intended to complement, not compete with, IEEE 802.11b since BT is for personal area networking (PAN) while 802.11 applies to wide area and local area networking. BT is designed to allow laptops, PDAs, cellular phones, and other devices to exchange data in a close-range (10m max.) ad-hoc network. BT uses quick frequency hopping at 1600 hops per second in the 2.4 GHz band and a data rate of 721 Kbps. Transmitted power is limited to a very low 1mW. Bluetooth is intended to be a replacement for Infrared (IR) and cables. Since both Bluetooth and IEEE 802.11b operate in the same 2.4 GHz band, there can be interference between systems operating simultaneously and in close proximity. Typically, this interference will result in reduced performance of the affected systems.

2.5 HomeRF Wireless LAN

HomeRF is the banner name for a group of manufacturers that formed in 1998 to develop a standard for the wireless interconnection of home PCs and electronic devices. The resulting specification is called the Shared Wireless Access Protocol (SWAP). HomeRF was originally formed because these companies believed a full 802.11 radio would be too costly for home and consumer markets. In fact, this belief has been dispelled by the rapid adoption of 802.11 systems and an aggressive march down the cost curve. Furthermore, HomeRF's philosophy is that there does not need to be compatibility between home and work systems, a philosophy not shared by most systems providers. Systems based on 802.11 dominate the workspace and many believe that workers with 802.11-equipped laptops will want a compatible system at home. The original HomeRF SWAP protocol was capable of delivering only about 1.6 Mbp raw data rates. The adoption of IEEE 802.11b, with 11 Mbps as a top data rate, made HomeRF a hard sell. To address that, a new technique described in the HomeRF 2.0 protocol, employs what is called wide band frequency hopping (WBFH). Even so, most key supporters of HomeRF have now deployed 802.11b solutions and support for HomeRF has dwindled along with a declining market share.

2.6 Wide Band Frequency Hopping (WBFH)

Approved by the FCC in August of 2000, WBFH permits channel bandwidths as wide as 3 and 5 MHz instead of the prior 1 MHz in the 2.4 GHz band. This increased bandwidth allows data rates as high as 10 Mbps per channel as compared to the original 2 Mbps maximum per channel (roughly 2 Mbps per 1 MHz of channel bandwidth). HomeRF 2.0 products and other Frequency Hopping Spread Spectrum (FHSS) products benefit from this. However, Direct Sequence Spread Spectrum (DSSS) systems still dominate with 11 Mbps and possibly 54 Mbps modes. There is very limited support for WBFH technology among systems providers.

3 Wireless LAN Deployment

One of the most attractive features of deploying a WLAN is that there is no need to install metres upon metres of cabling to connect computer systems that are within a relatively short distance of each other. One utopian view might be that network racks bulging at the seams with patched cables will soon become a thing of the past, with only the wired uplinks for a small number of access points needing to be catered for. Certainly, one can picture the significant savings in time and money for many IT departments by removing the need to hire contractors to install cables, cable ducting, patch panels and other equipment and then connect everything together as required.

The demand for WLAN access has surged dramatically over the past year. Users are beginning to favour WLAN access because it allows them to access their network and the Internet from anywhere in the workplace, without having to "plug in". Administrators are attracted to WLANs because they are easier to install (no cable to pull through walls and ceilings), they are flexible (they can be installed in places that wired LANs cannot, and do not require rewiring when seating or office plans change), and, in part owing to this flexibility, they are less expensive to maintain over the long-term.

3.1 Ease of Deployment

Installing a WLAN is deceptively easy. So much so, that it is not uncommon for departments within some organisations to deploy their own WLANs without the prior knowledge or consent of the relevant network administrator. In most cases, a WLAN can be deployed using the default settings of an access point to which corresponding clients will automatically connect. Thus, a simple WLAN capable of supporting tens of clients can be constructed in only a few minutes from receiving the equipment.

However, the apparent ease of WLAN deployment does mask many important factors that should be taken into account by professional network administrators. One point that may be overlooked is that installing WLAN access points does require wiring. Often the access point will need to have an Ethernet cable attached in order to be connected to the wired network infrastructure of a particular organisation. In any case the access points will need to be connected to a power outlet, although some access points offer have the capability to be powered over the Ethernet cable. In addition to power and possible uplink to a wired infrastructure, many other factors need to be taken into account when designing a WLAN implementation and therefore, placement of access points. Probably the two most important factors are coverage range and desired throughput (data rate). Usually it is a trade-off between these two factors. The maximum throughput of a particular wireless access type is usually only obtainable within a vastly reduced coverage range from the stated maximum and in favourable environmental conditions. Most everyday objects and buildings will lead to attenuation (signal degradation) in the wireless network (see table). Thus, in most situations a compromise has to be made in favour of either throughput or desired network coverage.

Barrier	Effect on Attenuation	Example
Air	Minimal	Everywhere!
Wood	Low	Office partitions, desks
Plaster	Low	Inner walls
Synthetic material	Low	Office partitions
Asbestos	Low	Ceilings
Glass	Low	Windows
Water	Medium	Damp wood, water tanks, aquariums
Brick	Medium	Inner and outer walls
Marble	Medium	Inner walls, floors, worktops
Paper	High	Paper rolls, cardboard boxes
Concrete	High	Floors, outer walls
Bulletproof glass	High	Security areas
Metal	High	Desks, office partitions reinforced walls, pipes, warehouse shelving

Table 1 Attenuation Effects of Various Elements[1]

Areas with wide open spaces such as warehouses and some open office space offer the best scenario for WLAN deployment. Areas with many walls and other high attenuating materials will see a decrease in throughput. Thus there is some debate as to whether deploying WLANs as the de-facto network type in

[1] Source: [1]

general business environments is beneficial. It may be more prudent to deploy them in areas of most convenience such as meeting rooms, conference suites etc., and rely on traditional wired infrastructure to carry the bulk of business traffic. If a WLAN is to be deployed, a thorough site survey should be conducted to ascertain the number of access points required and their optimal placement within the area to be covered. Aside from contracting professional wireless network designers to conduct the site survey, a network administrator can utilise commonly available spectrum analysers (supplied with most notebook WLAN cards) and walk around the coverage site observing the signal strengths for various locations of access points. One important point here is that the same combination of access point/client cards intended to be deployed should be used in the site survey. It is not uncommon for different product combinations to display different throughput results for the same test conditions.

The type of wireless access protocol being deployed is a major factor to be taken into consideration when designing a WLAN. For example, 802.11b access points only have three non-overlapping channels that can carry user traffic. Placing too many 802.11b access points within close proximity to each other will cause these channels to overlap and significantly reduce the throughput of the LAN. Meanwhile, 802.11a access points have eight indoor channels plus four channels for outdoor usage. This allows more access points to be located within the same area to support more users, and at a higher bandwidth than 802.11b. The downside to 802.11a is that the higher frequency reduces effective coverage at the same output power levels. Thus, two to four times more 802.11a access points will be required to cover the same area with 802.11b.

A thorough site survey should also identify potential interference within the operating frequency of the WLAN type to be deployed. The licence-free 2.4Ghz band used by 802.11b, 802.11g and Bluetooth is prone to interference from devices such as microwave ovens, wireless phones and some even some light bulbs [55] that emit radiation within the same frequency band. The most damaging of these are 2.4 GHz wireless phones that people are starting to use in homes and some companies. If one of these phones is in use within the same area as an 802.11b access point, degradation in throughput can be expected. Microwave ovens operating within a couple of metres of an access point or wireless client will also cause throughput degradation. Bluetooth and 802.11b devices will also interfere with each other causing performance degradation especially if they are in close proximity to one another. This has an important implication for users who may have dual 802.11b and Bluetooth capability on their notebook or PDA. A node that has dual Bluetooth and 802.11b capability runs the risk of obliterating all communications on both RF interfaces if they try to operate simultaneously in areas where Bluetooth and 802.11b coverage overlap. Similarly, two different users enjoying separate 802.11b and Bluetooth access respectively, will see decreasing signal to noise ratio (SNR) as they get closer to each other.

Also, neighbouring 802.11 WLANs of the same type will cause interference with each other unless the selection of 802.11 channels between the two WLANs has been co-ordinated.

In the physical sense that higher frequency signals have a shorter range and are less able to penetrate barriers, interference in the 5Ghz band should not be as prevalent as in the 2.4Ghz band. The 5Ghz band is also less cluttered with radiating devices, although being an unlicensed band this situation will likely change in the near future as 5Ghz WLAN and possibly other 5Ghz radiating devices become more common.

It is worth mentioning that another important consideration when thinking of deploying WLANs is the issue of network security and data privacy. In wireless network design security has to be considered at an early stage due to the inherent security vulnerabilities associated with wireless transmission (security is discussed in more detail in section 4). Depending upon the requirements of the organisation, security can range from simple enabling of WEP encryption to more intensive authentication and encryption via authentication servers, VPNs and other higher layer security mechanisms. If full security is a pre-requisite, WLAN deployment becomes more expensive with the addition of firewalls, authentication and VPN servers not to mention the administrative complication of maintaining software on the servers and updating all the clients.

3.2 Availability of Hardware/Software Products

There is no shortage of vendors for WLAN access points and client network interface cards (NICs). These range from inexpensive 802.11b products requiring minimal configuration to more expensive 'enterprise class' products that offer greater functionality and often include vendor-specific features. Such features may include tweaks to obtain higher throughput than standard products by using proprietary radio interfaces. However, because these proprietary techniques are not part of the relevant standard, they can often cause interoperability problems with products from different manufacturers

Most of the major notebook computer manufactures now ship products that have embedded 802.11 NICs. Some flavours of notebooks may also ship with embedded Bluetooth NICs. Even for those notebooks without embedded WLAN support, PCMCIA, USB or PCMCIA adapters for WLAN protocols are readily available worldwide.

The Microsoft Windows XP Operating system has embedded Wi-Fi capabilities. Windows XP automatically searches for a Wi-Fi access point and, if one is present, asks the user if they would like to connect to it. Practically all 802.11 NICs come with Windows 2000/XP drivers, while a good number of them also have Linux drivers available.

The majority of WLAN products available today are for the 802.11b (Wi-Fi) standard which has a maximum data rate of 11Mbps. In the future, products based on the 802.11g standard will offer data rates of up to 54Mbps. Furthermore, the 802.11g standard is backwards compatible with 802.11b so that an 802.11g access point will support both 802.11g and 802.11b clients. However, products complying with the 802.11g standard are not expected to ship until mid-2003 at the earliest. Currently, there are products available for the 802.11a standard, which also offers maximum rates of 54Mbps. However, the drawback is that 802.11a products are not interoperable with 802.11b products. Furthermore, the higher frequency range of 802.11a equates to a shorter range of coverage. In addition, current prices are such that 802.11a NICs are around 50% more expensive than their 802.11b counterparts and 802.11a access points are around 35% more expensive. Thus, network managers searching for a higher data rate alternative to 802.11b have the dilemma whether to implement a more expensive 802.11a solution which would not be compatible with any existing 802.11 equipment, or wait until 802.11g products become available. Fortunately, some WLAN product manufacturers are now offering dual-mode 802.11a/b chipsets for access points and client NICs so that they can select whichever access type is available. On the downside, employing dual-mode access points makes network design more complicated. If the 802.11b component of a dual-mode access point has significantly longer range than the 802.11a component, careful planning of access point placement is needed to avoid 'gaps' or 'holes' in the 802.11a area coverage.

3.3 Public Hotspots

WLAN 'hotspots' are becoming more prevalent worldwide. More and more network operators are considering building or buying WLAN hotspot networks to augment their 3G offerings. While the United States has about 4,100 hotspots today, according to Cahners In-Stat [37], the number of public WLANs in the US is expected to reach 41,000 by 2006. According to industry analysts Frost and Sullivan, the number of access sites will jump from 155 in 2000 to more than 27,000 in Western Europe by 2005 [42], in locations as diverse as hotel conference centres, airports, restaurants and shopping malls. A study by IDC [44] forecasts that worldwide there will be more than 100,000 hotspots spring up on airports, in hotels or conference centres in the next four years.

Specific events driving the growth in public access include [36]:

- falling cost of WLAN-enabled laptops, increasing availability/penetration in the enterprise,
- growing acceptance of remote work environments,

- emerging OEM-provider relationships, such as the Boingo-HP partnership to enable HP notebooks with Boingo client software,
- provider-provider relationships that allow for virtual expanded footprint and introduction of users to network, and
- new discussion and standardisation forums.

Below are a few examples that illustrate the exploding growth of the hotspot networks.

Japan

On April 25, 2002 NTT Communications Corporation (NTT Com) announced that on May 15 it will launch the Hotspot[1] WLAN service for mobile access to the Internet via PCs and PDAs, marking the start of the world's first commercial WLAN service to be compatible with IEEE 802.11a (5.2 GHz band) and IEEE 802.11b (2.4 GHz band) standards.

Compatible with both the high-speed 802.11a standard and widely used 802.11b standard, Hotspot is available in best-effort connection speeds of 36 Mbps (802.11a) or 11 Mbps (802.11b, Wi-Fi1 compatible products).

Hotspot enables PC and PDA users to enjoy broadband Internet access in wireless environments. Users simply require a WLAN card and WLAN-compatible terminal to use the service.

Hotspot started in about 200 locations ("hotspots") in the 23 wards of Tokyo, including cafes, hotels and public areas. NTT Com hopes to increase the service locations to about 1,000 within this year. 802.11a service, limited initially, will expand to all Hotspot service locations by 2002.

General Features:

- Usable with standard mobile devices.
- Provider-free online access (no need to subscribe to an ISP).
- Adaptable as corporate IP-VPN by providing global IP addresses.
- 802.11b and 802.11a compatible. 802.11a/b dual-band access points, which incorporate chipset developed by NTT Access Network Service Systems Laboratories, enable use of multi-vendor WLAN equipment.

Security Features:

- Extended service set identifier (ESSID) and wired equivalent privacy (WEP).
- ID and password protected authentication (protected by secure socket layer (SSL)) for logging in.
- Support of IC cards for ID verification when accessing corporate networks. Also, Hotspot will be combined with NTT Com's Safety Pass Business for IPsec-based highly-secure intranet access and with NTT's OCN (Open Computer Network) Business Pack to offer leased VPN equipment and OCN network.

Japan Telecom Co. Ltd. is running trials based largely around hotspots at railway stations and wireless network operator NTT DoCoMo plans to use its network of existing cellular towers to install a WLAN network.

[1] Hotspot is a registered trademark of NTT Communications Corporation.

Stockholm

Aptillo Networks [59] recently launched the public Hotspot network project Streetwise in Stockholm, Sweden. Streetwise is a full-scale wireless network test bed open to the general public. It involves the retailers and restaurants at the shopping street Biblioteksgatan, and altogether 14 companies with different expertise in wireless infrastructure and mobile services. Streetwise aspires on making maximum use of today's possibilities with mobile Internet. The heart of the network consists of Aptilo's Mobile Access Server and Access Point Controller in combination with access points for WLAN (802.11). The network covers the entire shopping street Biblioteksgatan including indoor's at the eight shops and restaurants taking part in the Streetwise project. On top on offering local mobile services users can also via credit card pay for ad hoc wireless Internet access.

Compaq/Aptilo

Compaq and Aptilo Networks, a Swedish provider of mobile network solutions announced a strategic pan-EMEA (Europe, Middle East and Africa) partnership on May 2, 2002, to deliver wireless broadband solutions in public locations. The two companies also announced their first customer, Spanish service provider, Kubi Wireless [60], which will deploy a large number of hotspots throughout Spain over the next two years. Starting in April 2002 in Barcelona, customers visiting the Hotel Majestic and Hotel Monte Carlo will be able to surf the web, send emails and conduct online transactions - all using high-speed wireless technology.

Starbucks

T-Mobile Wireless Broadband provides high-speed wireless Internet access in the US in convenient public locations such as airports, airline clubs and selected Starbucks (~650 hotspots) coffeehouses . The network is made for speed with a full T1 connection at every location using either a laptop or handheld that is Wi-Fi 802.11b wirelessly-enabled.

British Telecom

BT plans to install about 400 wireless local area networks (LANs) across the UK by June 2003, in places like coffee shops, hotels, railway stations, airports and bars. By June 2005, BT wants to provide the hotspots at more than 4,000 locations, including airports, train stations, motorway service stations and cafes [41].

Pass-One

On June 14, 2002, over 50 leading WLAN companies convened in Boston at the Founding Meeting of Pass One [61], a new international association formed by wireless Internet service providers (WISP). The goal of the new organization is to facilitate "barrier-less roaming" between wireless networks. The participants agreed in principle to establish a global service as a recognizable indicator of quality wireless connectivity. More than 20 WISPs (including many of the major North American cellular carriers) and 30 WLAN equipment vendors agreed on an action plan to deliver to the market a globally accepted service level standard.

Cebit

On Cebit 2002 Mobilcom and Cisco presented the largest WLAN hotspot worldwide[1]. Approximately 200 access points covered about 300,000 square meters providing wireless Internet access for almost all exhibition halls.

[1] If one would spread wireless access points uniformly over the whole geographical area of Germany keeping the same density as for Cebit 2002 one would need a total of 237,940,000 base stations. If you plan to deploy just as many Airport access points you have to spent roughly the same amount of money as was to be paid in 2000 for the UMTS licenses in Germany.

Cisco

Cisco, in collaboration with national telcos, mobile operators and wireless ISPs, has equipped 19 airports across Europe with WLAN hotspots based on the 802.11b standard [57]. Cisco is also in negotiations with 100 other airports across Europe, the Middle East and Africa to install similar WLAN hotspots. These hotspots have generally been free to access to begin with, although some airports have begun to charge for access with prices ranging from 1 to 22 Euros.

3.4 Legal and Sociological Issues

When thinking of deploying a WLAN, it is important to consider the legal restrictions of the corresponding country. The 802.11a standard offers eight non-overlapping channels compared to the three channels of 802.11b and 802.11g. The more channels that are available makes it easier to avoid interference with neighbouring LANs by configuring the channels usage. According to Atheros [57] in dense WLAN deployments, the extra channels available in 802.11a give up to 14 times more throughput than 802.11b networks. However, the regulatory bodies in the Netherlands and the UK (the first countries in Europe to approve 802.11a) have approved the usage of only four channels in 802.11a, thus greatly reducing the potential throughput of 802.11a leaving little gain over that of 802.11b. Conversely, in Japan 802.11b is restricted to using only one channel. One possible workaround is to deploy dual-mode WLANs (e.g. 802.11a/b or 802.11a/g) to maximise the number of channels available for the country in question.

There are also some sociological factors of deploying WLANs that are worth considering. One question is will deploying a WLAN necessarily make a workforce more productive? It is not difficult to envisage users at a meeting equipped with a wireless access point, constantly checking their email, surfing the web and sending instant messages, rather than focusing on the actual meeting. Yet when one considers the potential benefits of having the ability to quickly access information relevant to the meeting, it is probably a risk worth taking.

Health concerns regarding prolonged exposure to radio waves in WLANs is another sociological issue. WLAN devices (access points and client NICs) emit electromagnetic radiation at the frequencies in which they operate. However, the low power of WLAN transmissions means that it is widely accepted by organisations concerned with radio frequency safety (e.g. the National Radiological Protection Board in the UK, and the International Radiation Protection Association) that exposure to WLAN radiation poses no particular health risks.

"*Measurements have shown that routine exposure of users and other persons to low power portable and mobile transceivers and cellular telephones do not induce rates of [radio frequency] absorption that exceed any of the maximum permissible rates of energy absorption defined by these guidelines. Therefore, based on present knowledge, the exposures from low-power transceiver are considered to be without risk for the users and the public*"[1].

Furthermore, there are reasons why 802.11 WLAN devices can be considered safer than cellular telephones. In 802.11, only one device can transmit at any point in time, therefore the total radiation emitted by a network is equivalent to the total radiation emitted by a single device. However, in cellular networks, stations are transmitting simultaneously, increasing radiation emissions as network size increases. Moreover, the typical operating power of a WLAN device is less than that of a typical cellular phone (e.g. 50mW compared to 600mW).

[1] Quoted from the IEEE USAB Entity Position Statement Human Exposure to Radio frequency Fields from Portable and Mobile Telephones and other Communication Devices, December 2, 1992.

4 Access Control, Security and Privacy

Wireless working presents a new medium for connectivity. In traditional wired LANs, access is provided via the (wired) connection to an Ethernet port, thus access control to the LAN is governed by the actual physical access to the LAN ports. In contrast to the wiring of classical local area networks predefining a network membership, in a WLAN environment, the data is transmitted using radio frequencies (RF). Since the RF medium has the ability to penetrate walls and ceilings, any WLAN client is able to receive the ubiquitously existent RF signal, intentionally or unintentionally, if it is within range.

Precisely because of this lack of a physical barrier to restrict a system within radio range to be a member of a wireless network, wireless networking, more than any other networking technology, needs highly efficient authentication and access control mechanisms.

4.1 Security Threats

Protecting computers, network resources, and information against unauthorized access, modification, and / or destruction generally involves the following four topics:

Confidentiality
The property of communicating such that the intended recipients know what was being sent but unintended parties cannot determine what was sent.

Authentication
The property of knowing that the data received is the same as the data that was sent and that the claimed sender is in fact the actual sender.

Integrity
The property of ensuring that data is transmitted from source to destination without undetected alteration.

Non-repudiation
The property of a receiver being able to prove that the sender of some data did in fact send the data even though the sender might later desire to deny ever having sent that data.

Computer systems and communications channels face security threats that can compromise these qualities. The most common threats are:

- *Denial Of Service* occurs when a bad guy[1] causes a system or a network to become unavailable to legitimate users or causes services to be interrupted or delayed. Consequences can range from a measurable reduction in performance to the complete failure of the system. A wireless example would be using an external signal to jam the wireless channel.
- *Interception* has more than one meaning. A user's identity can be intercepted leading to a later instance of masquerading as a legitimate user or a data stream can be intercepted and decrypted for the purpose of disclosing otherwise private information. In either case, the bad guy is attacking the confidentiality or privacy of the information that is intercepted. An example would be eavesdropping and capturing the wireless interchanges between a wireless device and the network access point. Since wireless systems use the radio band for transmission, all transmissions can be readily intercepted. Therefore, strong authentication and encryption is necessary in order to keep the contents of intercepted signals from being disclosed.
- *Modification* means that data has been inserted, deleted, or otherwise modified on a system or during transmission. This is an attack on the integrity of either the data transmission or on the data stored on a system. An example would be the insertion of a Trojan program or virus on a user device or into

[1] cf. Kaufman, C., Perlman, R., and Speciner, M:, "Network Security: Private Communication in a Public World", Prentice Hall, 1995

the network. Protection of access to the network and its attached systems is one means of avoiding modification.

- *Masquerading* refers to the act of a bad guy posing as a legitimate user in order to gain access to a wireless network or a system served by the network. For example, a user with inappropriate access to a valid network authenticator could access the network and perform unacceptable functions (e.g., break into a server and insert malicious code, etc.). Strong authentication is required to avoid masquerade attacks.
- *Repudiation* is when a user denies having performed an action on the network. Users might deny having sent a particular message or deny accessing the network and performing some action. Strong authentication of users, integrity assurance methods, and digital signatures can minimize the possibility of repudiation.

4.2 802.11 Techniques for Access Control and Privacy

IEEE 802.11b group specifies two mechanisms for ensuring both privacy and access control, “Service Set Identifiers (SSID) and Wired Equivalent Privacy (WEP). Another mechanism to ensure privacy through encryption is to use a virtual private network (VPN) that runs transparently over a WLAN. Because the use of a VPN is independent of any native WLAN security scheme, VPNs are not discussed in this context.

SSID

One commonly used WLAN feature is a naming handle called an SSID, which provides a rudimentary level of access control. An SSID is a common network name for the devices in a WLAN subsystem; it serves to logically segment that subsystem. The use of the SSID as a handle to permit/deny access is dangerous because the SSID typically is not well secured. An access point, the device that links wireless clients to the wired LAN, usually is set to broadcast its SSID in its beacons.

Most wireless access points employ a second tool to overcome the weaknesses inherent in the SSID system to offer security of data travelling on the wireless network and computers on the network:

WEP

Since the ratification of the IEEE 802.11b standard in September 1999, WEP has been the primary mechanism by which organizations encrypt WLAN traffic. The IEEE 802.11b standard stipulates an optional encryption scheme, that offers a mechanism for securing WLAN data streams. WEP uses a symmetric scheme where the same key and algorithm is used for both encryption and decryption of data. The IEEE802.11 security claims include confidentiality (only stations which possess the shared key can read WEP-protected messages), data origin authentication / data integrity (modifications of WEP-protected messages can be detected) , and access control to prevent unauthorized users, who lack a correct WEP key, from gaining access to the network and privacy to protect WLAN data streams by encrypting them and allowing decryption only by users with the correct WEP keys.

Although WEP is optional, support for WEP with 40-bit encryption keys is a requirement for Wi-Fi certification by WECA, so WECA members invariably support WEP. Some vendors implement the computationally intense activities of encryption and decryption in software, while others, like Cisco Systems, use hardware accelerators to minimize the performance degradation of encrypting and decrypting data streams.

The IEEE 802.11standard provides two schemes for defining the WEP keys to be used on a WLAN. With the first scheme, a set of as many as four default keys are shared by all stations—clients and access points—in a wireless subsystem. When a client obtains the default keys, that client can communicate securely with all other stations in the subsystem. The problem with default keys is that when they become widely distributed they are more likely to be compromised. In the second scheme, each client establishes a "key mapping" relationship with another station. This is a more secure form of operation because fewer stations have the keys, but distributing such unicast keys becomes more difficult as the number of stations increases.

Various research work on WLAN security have pointed out that current WEP implementations are vulnerable to certain attacks against the encryption algorithm in use [5]. Specifically, there is a weakness in the key scheduling algorithm of RC4 that can be used to mount an attack on communication protected by WEP [5]. Only few days after the theory had been published the first Crack Tool was provided as an OPEN SOURCE project (cf. AirSnort[1]_[12], wepcrack [13]). It must be concluded that 802.11 WEP is totally insecure. R. Rivest comments on this [15], "Those who are using the RC4-based WEP or WEP2 protocols to provide confidentiality of their 802.11 communications should consider these protocols to be broken".

Authentication

A client cannot participate in a WLAN until that client is authenticated. The IEEE 802.11b standard defines two types of authentication methods, "Open System Authentication and Shared Key Authentication. The authentication method must be set on each client, and the setting should match that of the access point with which the client wants to associate. With open authentication, which is the default, the entire authentication process is done in clear-text, and a client can associate with an access point even without supplying the correct WEP key. The 802.11 specification, section 8.1.1 says, "Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm." Shared Key authentication supports authentication of STAs as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in the clear; however, it does require the use of the WEP privacy mechanism. With shared key authentication, the access point sends the client a challenge text packet that the client must encrypt with the correct WEP key and return to the access point. If the client has the wrong key or no key, it will fail authentication and will not be allowed to associate with the access point. Therefore, this authentication scheme is only available if the WEP option is implemented. The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11.

Concluding, IEEE 802.11 does not provide sufficient means for authentication in truly mobile environments. As a result of the missing key management very often Open System Authentication is used.

Some WLAN vendors support authentication based on the physical address, or Media Access Control (MAC) address, of a client. An access point will allow association by a client only if that client's MAC address matches an address in an authentication table used by the access point.

4.3 IEEE 802.11 Does Not Provide Sufficient Security

The purpose of the Task Group I of the 802.11 Working Group is to "enhance the current 802.11 MAC to provide improvements in security". Although the need for additional wireless security is recognized, the Task Group's conclusions and recommendations have raised concerns. A motion to remove WEP2 (May meeting 2001, Orlando, Florida), which improves on WEP but does not completely address the need for easy, strong encryption, failed. While WEP is acknowledged to have serious problems, WEP2's sliding window algorithm makes cracking/disclosing more difficult for attackers. WEP2's improvements include 128-bit encryption keys and better encryption algorithms. But since it's based on the same RC4 encryption and key system as WEP, it's vulnerable to the same attacks, i.e. WEP2 not significantly more secure than WEPv1.0

With the exception of Ericsson's 'High Security Solution' most alternative improvements to standard WEP offered by manufacturers do not offer maximum security:

[1] AirSnort is a WLAN tool, which cracks encryption keys on 802.11b WEP networks. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

Security Solution	AirSnort Attack	Known-Plaintext-Attack	Authentication	Data Integrity	Encryption Algorithm	Key Management	Downward Compatibility
WEPplus (Agere Systems)	+	–	–	–	–	–	+
FPK (RSA)	+	+	–	–	–	–	**n/a**
EAP (Cisco)	+	+	+	–	–	+	–
Kerberos (Symbol Technologies**)**	+	+	+	–	–	+	–
IPsec (Ericsson)	+	+	+	+	+	+	–

Table 2 WEP alternatives compared[1]

4.4 IEEE802.1x

For wireless clients running Windows XP, a stronger alternative is available, "IEEE 802.1x. 802.1x defines a generic framework for port-based authentication and key distribution. By using the Extensible Authentication Protocol (EAP), an "authenticator" (an Ethernet switch or a wireless access point) authenticates a "supplicant" (an Ethernet or wireless NIC) by consulting an authentication server (RADIUS or Kerberos). 802.1x can be implemented with different EAP types, including EAP-MD5 for Ethernet LANs and EAP-TLS for 802.11b WLANs. 802.1x also provides a carrier for secure delivery of session keys used to encrypt traffic between the supplicant and authenticator, addressing another serious omission in the WEP standard. For example, session keys might be created "on the fly" by the access point or supplied by a RADIUS server. If a war driver[2] with AirSnort recovered keys from WEP session traffic, the keys would be of no value for other sessions.

4.5 Conclusions

Summarizing one has to admit that IEEE 802.11 does not provide sufficient security, even in consideration of recent attempts to enhance the current 802.11 MAC layer. Major weaknesses are:

- Missing key management
- Use of keys shared by all stations
- Key length too small
- Lack of keyed MIC
- Lack of replay protection
- Linear integrity function (linear properties of CRC32) allows to forge ICVs
- Access control can be circumvented with known plaintext [5], [5]
- Crypto-analysis of shared keys

[1] c't magazine 04/2002, p. 178-180

[2] Hackers who operate out of moving vehicles are known as war drivers.

Even with IEEE802.1x and individual keys the protocol remains weak. As countermeasures it is recommended to place WLANs outside the Internet firewall, not to trust any host connected via 802.11, and to use proven high security protocols, e.g. IPSec, AAA (cf. Annex AAA Protocols / Authentication Protocols).

5 Support of Roaming Between Wireless Networks (Handovers)

One of the biggest challenges to the realisation of the future mobile Internet is the present lack of unified roaming between wireless ISPs. Currently, wireless ISPs do not have roaming agreements with each other and can therefore only offer islands of wireless connectivity. Users must subscribe to individual wireless ISPs in each area they wish to have connectivity. This is not only an unworkable model from the point of view of ‘always-on’ persistent mobility, it is also economically unattractive to the user. Thus the industry needs to agree on a business model in which wireless ISPs can determine who gets paid, and how much, when an end user roams from one WLAN to another. Until such a business model is put in place, wireless ISP ‘aggregators’ such as Boingo, are bringing together WLANs from multiple ISPs to create wireless services that cover larger geographic areas but present the same brand name to the end user.

Yet wireless ISPs have a variety of wireless access technologies to choose to deploy. Many different wireless technologies already exist and they differ significantly in terms of physical layer properties (frequency, modulation, bandwidth, latency, error rate), medium access control protocols employed and area of applicability. For instance WLANs offer a bandwidth up to tens of megabits per second, cover small geographical areas and emulate Ethernet network adapters, while wireless Wide Area Networks (WWAN), such as GSM/GPRS, have a line rate of some tens of kilobits per second, cover large geographical areas and provide modem functionality. Regardless of these physical layer properties, the need to provide seamless and persistent communication between heterogeneous access networks is paramount. Seamless roaming between wireless networks is achieved by *handover*, the transferring of a mobile host from one network to another.

5.1 Handover Types

Different types of handover can be distinguished. First of all there is the *horizontal handover*, which takes place at the link layer when the mobile terminal moves from one access point to another as a result of physical movement. With a horizontal handover, the two access points are of the same network type (e.g. two 802.11b access points). A horizontal handover can also occur when the mobile node, still connected to the same *type* of network, requires changes at the network layer (i.e. a change of the IP address). This can occur when roaming between ISPs who require re-registration at the network (IP) layer even if the two networks employ the same wireless access technology.

Conversely, *vertical handover* is defined as the process of performing handover between different types of network, such as between 802.11a and 802.11b access points. Vertical handover also refers to the case when a mobile node roams between a WLAN and a 2G/3G cellular network employing GPRS or UMTS. Vertical handover typically involves change of the mobile node’s IP address and the change of the administrative domain to which it is connected.

In the context of today’s radio communication networks, with GPRS networks widely deployed and an increasing number of WLAN hotspots available, vertical handover between these access technologies appears as an area of particular interest. It enables joining the large geographical mobility offered by the GPRS technology with the much better bandwidth/cost ratio WLAN technology can offer within limited public areas. The overall picture can further be enlarged with a number of other emerging access technologies, out of which Bluetooth for instance has already drawn much attention.

Without deployment of protocols able to transparently handle such dramatic network layer connectivity changes, vertical handover would become unattractive, therefore limiting the options of mobile users.

Fortunately, Mobile IP is a protocol, which inherently supports perpetuation of the data connection beyond the changes of the IP addresses produced by vertical handovers. Mobile IP is also able to offer the required interface to authentication and authorization infrastructures, which provide the administrative access control framework. As such it is the chief candidate for providing the global mobility management functions required the future mobile Internet. The role of Mobile IP in providing global mobility managements is discussed in section 7.

5.2 Impact on higher layer protocols

Despite the fact that vertical handovers typically perform with little delay with respect to the data traffic, higher layer protocols may experience performance degradation. This is because higher layer protocols have been designed in the framework of wired network infrastructures, which are characterised by constant bandwidth and small error rates. In such an environment, packet loss is in general an indication of traffic congestion, to which transport protocols like TCP respond by activating specific algorithms. Wireless infrastructures however, are in general characterised by a bandwidth which often varies over time, may be asymmetric with regard to traffic direction and in any case exhibits a much higher error rate. Furthermore, wireless media are themselves very different from one another in terms of bandwidth, latency and error rates. As a result, a vertical handover between different wireless networks can see these parameters vary significantly.

5.2.1 TCP problems with handover

Various research work has shown that inter-technology hand-offs impact the higher layers, and TCP, the most used transport protocol in the Internet, is not well suited for handoffs between access technologies with different characteristics.

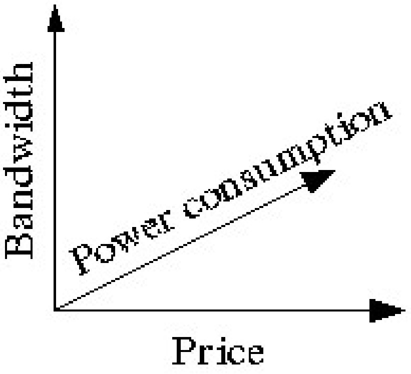
Gurtov [47] has shown that TCP does not react well to large delays (several times the usual RTT) suddenly occurring. Normally the latency of WWAN links is typically close to a second, which is several times higher than on a typical route in the wired Internet. TCP adapts well to this type of more or less constant delay. This is because the TCP retransmission timeout is updated dynamically based on the smoothed mean and variance of RTT samples of the connection. However, without a chance to adapt its retransmission timer to a suddenly occurring large delay, TCP has to assume that outstanding segments were lost and retransmits them.

Thus future research work in this area has to include examination of delay sources in the GPRS and UMTS wireless networks, as well as designing new algorithms to improve the response of TCP to long sudden delays due to drastic changes of network QoS.

5.3 Roaming policies

When roaming across a choice wireless technologies occurs, a demand for roaming policies is needed. In a future mobile Internet having multiple network access technologies available, selecting one or more of them is a non-trivial issue. It is not simply a question of better or worse, it is a multi-dimensional matrix or graph of network properties. Examples of such properties are bandwidth, power consumption, price, latency and hand-off time.

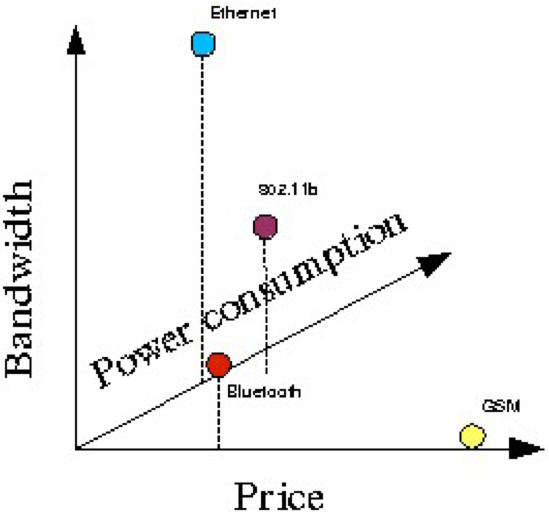
The different available network technologies must then be described within this graph. It will then be possible both for the application and the user to specify policies in a clean way.



5.3.1 An example scenario:

In our example scenario, four technologies are available: 100Mb Ethernet (cable), 802.11b (wireless), Bluetooth (short range wireless) and GSM (long range wireless). The Ethernet has no usage fee, just a subscription. The 802.11b WLAN has a higher bandwidth than Bluetooth, but uses more power. The GSM network has the better range of all systems, although the lowest bandwidth and highest price.

Gathered in the property graph, we get the graph to the right.



The user can now inform the system of her preferences, by weighting the different network properties. The user weights power consumption 3, bandwidth 1 and price 2. In other words, we want to use little power without paying large money. Bandwidth is of less importance. Then, the system must calculate a priority list in order to select network technology. Let us use a simple formula, such as (bandwidth * weight) - (power consumption * weight) - (price * weight). In words, more bandwidth is better, more power consumption and higher prices are worse.

Technology	*Bandwidth (1)*	*Power (3)*	*Price (2)*	*Total*
Ethernet	100	3	0	91
802.11b	11	4	3	-7
Bluetooth	1	1	2	-6
GSM	0	1	40	-83

This gives us the priority list:

1. Ethernet
2. Bluetooth
3. 802.11b
4. GSM

Using such a solution, it is possible for a novice user to easily supply wishes regarding complex matters. As well, it leaves room for applications to influence the choice of technology. If the operating system is allowed adjustments of, say, 10% the weight of the user, the applications and operating system might cooperate with the user to serve well. In our example, Bluetooth and 802.11b are very similar in total score. If we allow the operating system to add the software's wishes, it might give weights bandwidth: 0.3, power 0.2, price 0. If we adjust the numbers above, we get:

Technology	*User*	*Operating System*	*Total*
Ethernet	91	29.4	120.4
802.11b	-7	2.5	-4.5
Bluetooth	-5	0.1	-4.9
GSM	-83	-0.2	-83.2

Here we see that as the operating system has applications in need of bandwidth, 802.11b is granted precedence of Bluetooth. If the operating system notices that the battery is running low, it might switch priorities to be: power: 0.3, bandwidth 0.2 and price 0. We would then get:

Technology	User	Operating system	Total
Ethernet	91	19.1	71.9
802.11B	-7	1	-6
Bluetooth	-5	-0.1	-5.1
GSM	-83	-0.3	-83.3

Now, we switch back to using Bluetooth over 802.11b, due to the power restrictions.

In this solution, the user is only presented with a very simple interface, namely to prioritise the different parameters. Using a simple formula, the mobile IP sub-system can create a prioritised list of network technologies to use, based on a dynamically changing policy. When such a list exists, the system will select the highest available technology. By allowing applications to supply wishes to the operating system, a common policy can be created based on the system and the application needs. This policy is weighted less than the user, hence the user policy will not be overridden by the system.

6 Quality of Service

When a mobile node changes between different network technologies, it is expected that the networks might not have the same properties. For example, roaming from a cable based 100Mbps network with no packet loss to a wireless 11Mbps network with very variable packet loss. Mobile IP will only hide the fact that we changed network, it cannot hide the fact that the network can provide far less bandwidth.

In order for an application to provide a good level of service to a user, some mechanisms might be necessary. Both the issues of moving to a lower and higher quality network, is discussed below.

6.1 Roaming to a Lower Quality Network

When a node roams to a lower quality network, network applications may experience problems. If the node only transfers bulk data, such as email or files, the only visible effect might be a difference in throughput. The impact can however be much more visible if the node is streaming real-time data, say a video stream. If a video stream demands a certain amount of bandwidth, it might be useless if the network cannot support these demands. Worse, it may also block other access to the network both for itself and its neighbours. Mobility here might give a worse user experience, as it is currently not expected that a video stream continues to play when a user unplugs the Ethernet cable. When mobility is added, it is expected that the stream should continue without interruption.

If the application receives a notification when the network changes combined with network characteristics, it might be possible for it to adapt according to the user's wishes. Some possible actions can be:

1. Ignore the change (as is done today) - the service might continue if the network improves
2. Abort the operation cleanly due to missing network capabilities
3. Try to reconnect with different quality of service parameters. An example is to request a video stream of lower quality.
4. Try to dynamically change the service according to the user's policy. An example is to change to black & white mode, or show the video interlaced. It is also possible to solve such adaptation problems by creating specialised data formats that support graceful degradation. For example, the SPEG format [52], which prioritises packets internally, and drops low priority packets when the network is unable to supply sufficient bandwidth. The resulting stream will then provide the maximum quality that the network can support. It is important to see though, that it is the provider of the service that specifies the policy for data degradation. Providing multiple streams might of course allow the user some freedom as to what is preferred (black & white video versus interlaced

video). The brilliance of this solution is of course that the player does not necessarily need to know about network quality at all. The problem is that the network bandwidth is the limiting factor, making it necessary to include other means to reserve only parts of the bandwidth. For example, a user can be watching CNN while waiting for a file download to finish. It is possible that the user would prefer a lower quality video stream in order for the file download to finish earlier. This gives a 5th issue:

5. Use special data formats that allow prioritising data, allowing the service to automatically degrade gracefully.

6.2 Roaming to a Higher Quality Network

If a node roams to a network with better capabilities, it is not a problem of the same magnitude as roaming to a lower quality network. Specifically, the new network will have no problem supporting the service provided by the lower quality network. It might however be in place for the application to increase the QoS it provides to the user. For example, a video in black & white might switch to colour, or a mono IP telephone conference might switch to stereo mode. This is possibly only wanted if the application can change its parameters dynamically, without interrupting the user experience.

Here are some possible actions that map together with the list for actions for a quality degradation above:

1. The service might be able to continue as before the degradation took place, possibly by pre-buffering some data first.
2. The service was aborted, hence can no longer adapt.
3. Try to reconnect with different quality of service parameters if the user wants to.
4. Dynamically adapt to the user's policy, for example to re-enable colours in a video stream.
5. As the data format is prioritised, it will automatically also improve when the network improves.

6.3 Conclusion

As mobile networks provide transparent networking of various qualities, it seems evident that applications must be somewhat adaptive to this new environment. Both support for variable quality in file formats, as well as dynamically changing quality parameters seem likely in the future. It is important that not only degradation of quality is supported, but also that an increase in network quality is reflected by the applications.

It is important to see that the reason for wanting such adaptation is to provide a better experience for the users of a service. Therefore, it is vital that adaptive applications and systems allow users to prioritise the quality parameters in question. It is also important that this prioritising must not be to punch "strange" parameters into text boxes (bits/sec, pits/pixel, frame types), but rather to create abstractions (smaller size, less colours, worse frame rate). Only when the average user is able to present her wishes to the application, the application can start the job of pleasing her.

7 IPv6 and the Mobile Internet

There are numerous WLAN technologies that a service provider (or even an end user) may decide to deploy. As described in section 2 these WLAN technologies use different frequency bands, have different spread spectrum methods, provide different data rates and possess different medium access (MAC) protocols. There is a clear need for communicating systems to operate with all of the major WLAN access technologies in the future mobile Internet. The ideal scenario is that end users will not need to care about which WLAN technology they are using at their current location, whether it is one of the 802.11 flavours, HiperLAN, Bluetooth or another access type. Furthermore, there is also a need for wireless communicating systems to operate with 2G and 3G mobile network technologies. The growth of the Internet coupled with the popularity of mobile phone usage has led to a convergence of the two networks. The demand for data access over the Internet via mobile phone handsets has led to the specification and standardisation of the General Packet Radio Service (GPRS) to deliver enhanced data services for current GSM 2G mobile phone networks. The provision of data access for mobile handsets has also been a major driver for the specification of the IMT-2000/UMTS 3G mobile network. Although 2G and 3G mobile networks offer a lower data capacity compared to WLAN technologies, they have a more widespread geographic coverage. Hence, in the mobile Internet mobile users should be able to make use of the relatively fast data access of WLAN hotspots when they are available, and fall back to global 2G/3G data access rates in other areas.

For a true mobile Internet we therefore need multi-access communication systems that can operate with not only the various WLAN technologies but also the 2G/3G mobile phone networks. The key factor in the future mobile Internet will be the mobility between the different wireless access technologies available. In other words, it must be possible for a user terminal to seamlessly roam between different wireless access types for the true vision of the mobile Internet to be realised. One can envisage future mobile handsets, notebooks or PDAs that contain several radio interfaces within the same device, thus enabling the possibility of roaming between wireless access types.

From a hardware point of view this is a particularly difficult challenge. Developing the communicating interfaces that will operate in multiple frequency bands, using different modulation and spectrum spreading techniques is fraught with problems. Nevertheless, hardware manufacturers are beginning to roll out their first generation of multi-protocol WLAN interfaces, with more sophisticated models promised in the near future. Perhaps the thought of a NIC that operates with *all* of the major WLAN access types is a little optimistic for the foreseeable future. However, techniques such as Software Defined Radio (SDR) offer much promise towards this goal.

Furthermore, as yet there are no common radio interface management or mobility management techniques between the different wireless access types. Thus, it is not possible to perform handovers or roam between WLAN and 2G/3G systems [53].

However, from a network layer point of view, the challenge is a little more straightforward. Mobile IPv6 [53] places all the mobility management functionality at the network (IPv6) layer. It enables user devices (e.g. mobile handsets, PDAs, notebooks etc.) to be constantly addressable by their home address regardless of their current location within the Internet. By placing all mobility management functionality in the IPv6 layer, Mobile IPv6 exhibits two important benefits:

1. host mobility is transparent to protocol layers and applications above the IPv6 layer
2. the mobility of a host between different wireless access types can be achieved without the need for specific interworking mechanisms between the different wireless access types.

Vertical handovers are handled in Mobile IPv6 by initiating an inter-domain registration, which is a time consuming process, taking into account the propagation paths incurred and the additional authentication and authorization related operations. On the other hand, by the time the handover is taking place the mobile node is able in principle to access at least two different access networks. The mobile node can therefore update the network layer parameters to reflect the “new” location only upon reception of a successful reply and continue to use the “old” access medium until then.

Taking these characteristics into account MIPv6 seems to be the most promising candidate to provide the universal mobility in the next generation IP based telecommunication systems.

It is worth noting that Mobile IP (IPv4) [55] exhibits these same characteristics as Mobile IPv6. However, Mobile IPv6 is a much more efficient and streamlined protocol than its IPv4 counterpart. In any case, there are not enough IPv4 addresses available to assign to mobile handsets with respect to current numbers, let alone enough addresses for the anticipated future mobile Internet. Only IPv6 has enough address space to assign unique addresses (or even address blocks) to every device within the future mobile Internet. Thus, Mobile IPv6 is the only realistic mechanism for handling host mobility in the multi-access environment of the mobile Internet.

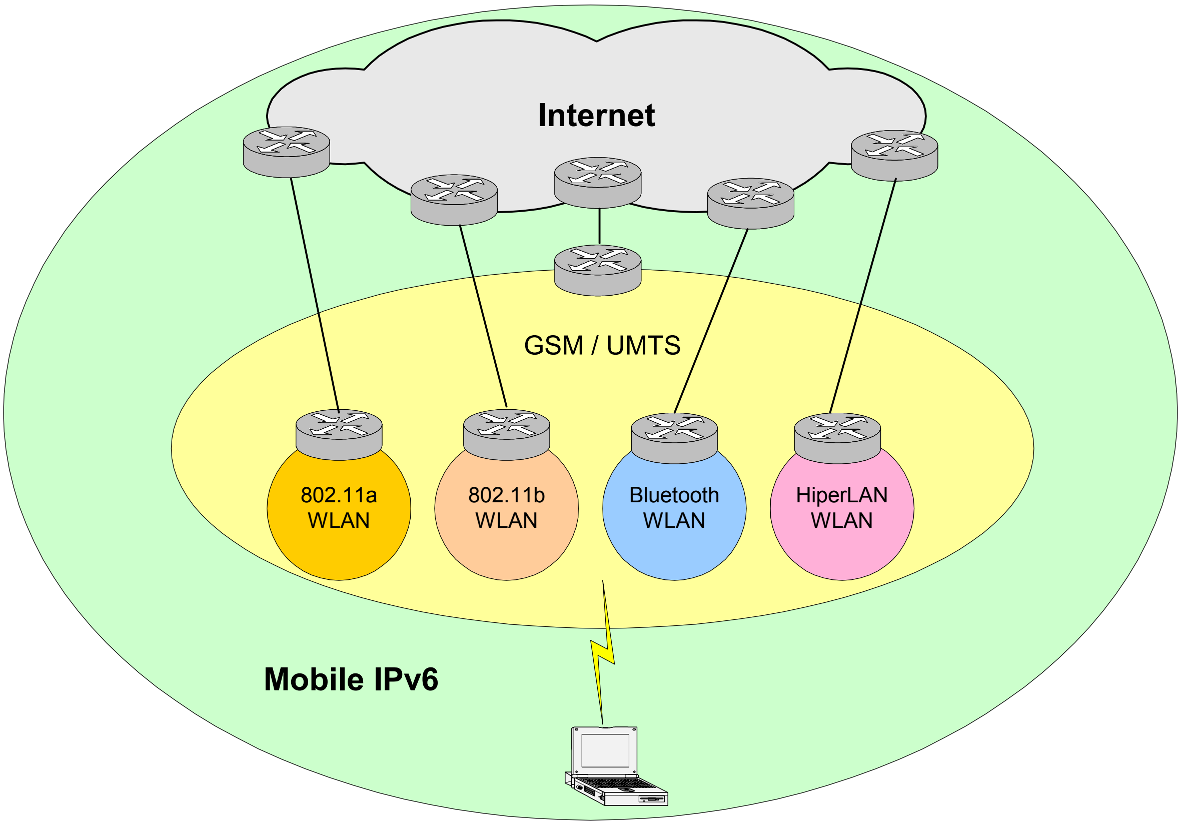


Figure 1 Mobile IPv6

Mobile IPv6 is an enabler for true user and service mobility in a multi-access environment. Mobile IPv6 provides connectivity over any wireless access type and supports seamless roaming between WLAN technologies (e.g. 802.11x, Bluetooth, HiperLAN etc.) and the more extensive geographic coverage of 2G, emerging 3G and future 4G access technologies. As such, it can be viewed as an overlay network for all the various types of wireless access networks that may be present in the future mobile Internet (see figure).

8 Conclusions

This report has investigated the major issues pertaining to WLAN access for IPv6 mobile nodes. We have shown how the deployment of WLANs holds many advantages over a wired network infrastructure and looked at the recent growth in WLAN deployment worldwide. However, this does not show that there is currently:

- little IPv6 deployment in wireless networks
- few ISPs giving out IPv6 address space to users
- even less MIPv6 deployment allowing users to roam between WLANs while achieving a persistent connection at the transport layer

Hence, assuming a user can achieve WLAN access at a corporate or public ‘hotspot’, this does not necessarily mean that he/she has access to the IPv6 Internet (either native or via a transitioning mechanism) Nor does it mean that the user can roam between WLAN hotspots. What we have at the moment is ‘static’ mobility. That is, a user may enjoy connectivity at a WLAN hotspot, but the ability to stay connected and roam between WLAN cells (either owned by the same provider or owned by different providers), is hampered by the lack of both hotspot continuity and Mobile IPv6 intelligence in the network.

WLANs give the home or office user the ability to deploy a network (home network or small Intranet) without the need to install cabling. However, access to the Internet through an ISP is a more interesting problem. At the time of writing the majority of access to the Internet offered by ISPs is via wired infrastructure such as PPP dial-up modem, cable modem, or xDSL. Furthermore, obtaining IP address space can be a significant problem. Most ISPs will provide only one static or dynamic IPv4 address per end user, meaning that some form of NAT is required at the user end premises to provide simultaneous Internet access to multiple hosts on the user network. Of course, it is possible to purchase multiple IP addresses from an ISP, but usually at significant cost. IPv6, with its 128-bit address space removes the need for ISPs to place as much value to assigning address blocks to end customers. Unfortunately, finding an ISP to provide your organisation with an IPv6 prefix for your network is currently not an easy task.

The problems with WLAN security are well documented. Certainly, any wireless medium is by definition, more vulnerable to attack than a wired alternative. Yet, no network administrator would dare assume that simply because his network is physically wired, that it was by definition totally secure from attack. Instead, authentication and encryption methods are employed in the higher layers of the protocol stack to achieve a more confident level of security and privacy from network intruders. This fact is somehow mysteriously overlooked by many who seek to ridicule the security features of WLANs. For optimum security, one must assume the communication channel is insecure, whether wired or wireless, and employ methods to overcome this.

Regarding a wireless network as insecure is probably the most prudent solution for a network administrator as it demands that other security methods must be clearly defined. It is simply not enough to rely on the security mechanisms at the link-layer of a wireless network. Thus, suitable security measures should established in the higher protocol layers for different kinds of data (such as IPsec for document sharing, PGP for email etc.), and public information (such as web pages) can be left unsecured. This will minimise the overhead of security, at the same time as it will provide the correct level of security for each application.

References

[1] Geir, Jim, “Wireless LANs”, Second Edition, SAMS Publishing 2002.

[2] Schiller, Jochen, “Mobile Communicatons”, Addison Wesley, 2000.

[3] Stallings, William, “Wireless Comunications and Networks”, Prentice Hall, 2002.

[4] Intersil, “Wireless and Related Network Standards and Organizations”, 2001.

[5] Fluhrer, S., Mantin, I., and Shamir, A. “Weaknesses in the Key Scheduling Algorithm of RC4“, http://www.crypto.com/papers/others/rc4_ksaproc.ps, 8. Annual Workshop on Selected Areas in Cryptography, August 2001.

[6] Stubblefield, A., Ioannidis, J., Rubin, A. D., “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”, http://www.cs.rice.edu/~astubble/wep/wep_attack.html , AT&T Labs Technical Report TD-4ZCPZZ, Revision 2, August 21, 2001.

[7] The Unofficial 802.11 Security Web Page, http://www.drizzle.com/~aboba/IEEE/ .

[8] Security of the WEP algorithm, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html .

[9] Arbaugh, W. A., Shankar, N., and Wan, Y. C. J., “Your 802.11 Wireless Network has No Clothes”, http://www.cs.umd.edu/~waa/wireless.pdf , March 2001.

[10] Borisov, N., Goldberg, I., and Wagner, D., “Intercepting Mobile Communications, The Insecurity of 802.11”, http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf , 2000.

[11] Walker, J., R., “Unsafe at any key size; An analysis of the WEP encapsulation”, http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip , October 2000.

[12] Airsnort homepage, http://airsnort.shmoo.com/ .

[13] Wepcrack homepage, http://sourceforge.net/projects/wepcrack/ .

[14] The Hacker’s Choice, http://www.thehackerschoice.com/releases.php .

[15] Rivest, R., “RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4”, http://www.rsasecurity.com/rsalabs/technotes/wep.html , August 2001

[16] R. Atkinson, “Security Architecture for the Internet Protocol”, IETF RFC 1825, August 1995

[17] Cisco Systems, Inc., “Wireless LAN Security”, white paper, http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm ,2001.

[18] ISP Planet, ”Improving WLAN Security”, http://www.isp-planet.com/fixed_wireless/technology/2001/better_wep.html , November 2001.

[19] Schäfer, G., “Network Security, “Security of Wireless Local Area Networks”, Technical University of Berlin, TKN – Telecommunication Networks Group, 2001.

[20] Mahan, R., E., “Security in Wireless Networks”, November 2001.

[21] Blunk, L., Vollbrecht, J., “PPP Extensible Authentication Protocol (EAP)”, IETF, RFC 2284, March 1998.

[22] Calhoun, P. et al, “Diameter Framework Document”, draft-ietf-aaa-diameter-framework-01.txt, IETF work in progress, March 2001.

[23] Calhoun, P. et al, “Diameter Base Protocol”, draft-ietf-aaa-diameter-07.txt, IETF work in progress, July 2001.

[24] Crocker, D., Overrell, P., “Augmented BNF for Syntax Specifications”, RFC 2234, November 1997.

[25] Droms, R., “Dynamic Host Configuration Protocol”, IETF, RFC 2131, March 1997.

[26] Droms, R., W. Arbaugh, “Authentication for DHCP Messages”, Internet Draft, work in progress, draft-ietf-dhc-authentication-16.txt, January 2001.

[27] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners-Lee, T., “Hypertext Transfer Protocol -HTTP/1.1”, IETF, RFC 2616, June 1999.

[28] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., Stewart, L., “HTTP Authentication, “Basic and Digest Access Authentication”, IETF, RFC 2617, June 1999.

[29] Lloyd, B., Simpson, W., “PPP Authentication Protocols”, IETF, RFC 1334, October 1992.

[30] Rigney, C. et al, “Remote Authentication Dial In User Service (RADIUS)”, RFC 2865, June 2000.

[31] Rigney, C., “RADIUS Accounting”, RFC 2139, April 1997.

[32] Simpson, W., “PPP Challenge Handshake Authentication Protocol”, IETF, RFC 1994, August 1996.

[33] IST-2000-25394 Project Moby Dick, “AAAC Design”, 2001.

[34] An 802.11 hotspot location directory, http://www.80211hotspots.com/ .

[35] Boingo Wireless, high-speed wireless Internet service in hot spot locations, http://www.boingo.com/index.html

[36] Streetwise, http://www.bluegrid.se/streetwise .

[37] In-Stat/MDR, “The Hotspot Market”, http://www.instat.com/infoalert.asp?Volname=Volume%20%2320#item2 , May 2002.

[38] Airpath Wireless, http://www.airpathwireless.com/ .

[39] IP3 Networks, http://www.ip3networks.com/ .

[40] Pronto Networks, http://www.prontonetworks.com/ .

[41] BBC News, http://news.bbc.co.uk/hi/english/business/newsid_1920000/1920551.stm , April 10, 2002.

[42] Frost and Sullivan, “World Wireless LAN Markets”, #5781-74, 1999.

[43] Frost and Sullivan, “Market Engineering Research for the Wireless Home Networking Market 1998-2005”, #5547-74, 1999.

[44] IDC, “Wireless LANs: Worldwide Market Review and Forecast, 1997–2003”, 1998.

[45] Global Sources, “LMDS, MMDS making slow progress in the United States, http://www.telecom.globalsources.com/MAGAZINE/BB/0205/LMDS01.HTM , March 2002.

[46] VDC, “Outlook for WLAN systems remains strong despite continued standards speculation”, http://www.vdc-corp.com/autoid/press/02/pr02-03.html , 2001.

[47] Gurtov, A., “Effect of Delays on TCP Performance”, Proceedings of IFIP Personal Wireless Communications 2001, August 2001.

[48] Kuhlberg. P., “Effect of Delays and Packet Drops on TCP-based Wireless Data Communication”, Master Thesis, University of Helsinki, Department of Computer Science, Series of Publications C, No. C-2001-7. February 2001.

[49] Sarolahti, P., “Performance Analysis of TCP Enhancements for Congested Reliable Wireless Links”, Master Thesis, University of Helsinki, Department of Computer Science, Series of Publications C, No. C-2001-8. February 2001.

[50] Sanmateu, A., et al, “Using Mobile IP for provision of seamless hand over between heterogeneous access networks”, Eurescom, P1013, FIP-MIP, 2001.

[51] Charles Krasic, Jonathan Walpole, “QoS Scalability for Streamed Media Delivery”, ftp://www.cse.ogi.edu/pub/tech-reports/1999/99-011.ps.gz .

[52] Aki Yokote, Alper Yegin, Muhammad Tariq, Carl Williams, Atsushi Takeshita, Internet Draft: Mobile IP API, http://search.ietf.org/internet-drafts/draft-yokote-mobileip-api-00.txt .

[53] Nokia White Paper, “Mobile IPv6 – an enabler for service mobility in a mult-access environment”, April 2002.

[54] Johnson, D., Perkins, C., Arkko J., “Mobility Support in IPv6”, IETF Internet Draft draft-ietf-mobileip-ipv6-18.txt, June 2002.

[55] Perkins C., “IP Mobility Support for IPv4”, IETF RFC 3220, January 2002.

[56] Stroh, S., “RF Lighting A Potential ‘Extinction Level Event’ for Communicating Users of the 2.4 GHz Band”, http://www.strohpub.com/0701feat.htm .

[57] Atheros Communications, http://www.atheros.com/ .

[58] News article from http://www.silicon.com, July 2002.

[59] Aptillo Networks, http://www.aptillo.com .

[60] Kubi Wireless, http://www.gruporodania.com/uk/company_n.htm .

[61] Pass One, http://www.pass-one.com/home.php .

Abbreviations

AAA	Authentication, Authorization and Accounting
ATM	Asynchronous Transfer Mode
AVP	Attribute Value Pairs
CCK	Complementary Code Keying
CHAP	Challenge Handshake Authentication Protocol
DFS/TPC	Dynamic Frequency Selection and Transmit Power Control
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ETSI	European Telecommunications Standardization Institute
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FPK	Fast Packet Keying
FTP	File Transfer Protocol
IEEE	Institute of Electrical and Electronic Engineers
HTTP	Hyper Text Transfer Protocol
ICV	Integrity Check Value
IPsec	IP Security Protocol
IR	Infrared
ITU	International Telecommunications Union
IV	Initialisation Vector
LAN	Local Area Network
LMDS	Local Multipoint Distribution Service
MAC	Medium Access Control
MD5	Message Digest 5
MIC	Message Integrity Check
MMAC-PC	Multimedia Mobile Access Communications Systems Promotion Council
MMDS	Multichannel Multipoint Distribution Service
NAS	Network Access Server
NASREQ	Network Access Server Requirements
NIC	Network Interface Card
OFDM	Orthogonal Frequency Division Multiplexing
PAN	Personal Area Network
PAP	Password Authentication Protocol
PBCC	Packet Binary Convolution Coding

PHY	Physical Layer
POP	Post Office Protocol
PPP	Point-to-point Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
ROAMOPS	Roaming Operations
SCTP	Stream Control Transmission Protocol
SLIP	Serial Line IP
SSH	Secure Shell
SSID	Service Set Identifiers
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TLS	Transport Layer Security
UDP	User Datagram Protocol
UNII	Unlicensed National Information Infrastructure
VPN	Virtual Private Network
WAN	Wide Area Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wireline Equivalent Privacy
WEP2	The first enhancement to the WEP protocol
Wi-Fi	Wireless Fidelity
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WLANA	Wireless Local Area Networking Association
WPAN	Wireless Personal Area Network

Appendix A

Organisations

ETSI – European Telecommunications Standards Institute

ETSI is a non-profit organization whose mission is to produce the telecommunications standards that are used throughout Europe. Based in Sophia Antipolis, ETSI unites about 800 members from 52 countries inside and outside Europe, and represents administrations, network operators, manufacturers, service providers, research bodies and users.

FCC – Federal Communications Commission

The FCC was established by the Communications Act of 1934 as an independent United States government agency directly responsible to Congress. The Act, which has been amended over the years, charges the Commission with establishing policies to govern interstate and international communications by television, radio, wire, satellite and cable. In other words, the FCC regulates all forms of electronic communications both within and going out of the United States. The FCC works with the International Telecommunications Union (ITU), the European Telecommunications Standards Institute (ETSI) and other organizations to establish international regulation.

IEEE – Institute of Electrical and Electronics Engineers

The IEEE is a non-profit, technical professional association of more than 350,000 individual members in 150 countries. Through its members, the IEEE is a leading authority in technical areas ranging from computer engineering, biomedical technology and telecommunications, to electric power, aerospace and consumer electronics, among others. Through its technical publishing, conferences and consensus-based standards activities, the IEEE produces 30% of the world's published literature in electrical engineering, computers and control technology, holds annually more than 300 major conferences and has more than 800 active standards with 700 under development.

ITU – International Telecommunications Union

The ITU, headquartered in Geneva, Switzerland, is an international organization within which governments and the private sector coordinate global telecom networks and services. The ITU is divided into three main sectors: ITU-R Sector is responsible for all work in the field of Radio communications. ITU-T Sector ensures an efficient and on-time production of high quality standards covering all fields of Telecommunications except radio aspects. ITU-D Sector facilitates and enhances telecommunication development worldwide by offering, organizing and coordinating technical cooperation and assistance activities.

MMAC-PC – Multimedia Mobile Access Communications Systems Promotion Council

The Multimedia Mobile Access Communication Systems Promotion Council (MMAC-PC) was formed in Japan in 1996 in cooperation with users, carriers, manufacturers as well as academia. The objective of the Council is to propose a high performance wireless system to allow any person to communicate "at anytime and any place". The Promotion Council's goal is to realize MMAC as soon as possible through investigations of system specifications, demonstrative experiments, information exchanges and popularization activities that contribute to the efficient use of the radio frequency spectrum. MMAC involves indoor and outdoor broadband high data rate communications tied together via both wireless and fiber optic systems.

WECA – Wireless Ethernet Compatibility Alliance

The Wireless Ethernet Compatibility Alliance (WECA) is a non-profit organization formed in 1999 to certify interoperability of Wi-Fi (IEEE 802.11b) products and to promote Wi-Fi as the global, WLAN standard across all market segments. WECA has instituted a test suite that defines how member products are tested to certify that they are interoperable with other Wi-Fi-certified products. When a product successfully passes the test, the company is granted the Wi-Fi seal of interoperability and may display the Wi-Fi logo on that product and its corresponding collateral material. This testing assures that products bearing the Wi-Fi logo will work with each other. Membership in WECA is open to all companies who support the Wi-Fi standard, including any member manufacturer that would like to submit its Wi-Fi-based product for interoperability testing. WECA now comprises 155 members.

WLANA – Wireless Local Area Networking Association

The Wireless LAN Association is a non-profit educational trade association, comprised of the thought leaders and technology innovators in the local area wireless technology industry. Through the vast knowledge and experience of sponsor and affiliate members, WLANA provides a clearinghouse of information about wireless local area applications, issues and trends and serves as a resource to customers and prospects of wireless local area products and wireless personal area products and to industry press and analysts.

Appendix B

B1 Characteristics of Different Wireless LANs

	IEEE 802.11	IEEE 802.11b	IEEE 802.11g	IEEE 802.11a	ETSI Hiperlan/2[1]
Frequency [GHz]	2.4	2.4-2.4835	2.4-2.4835	5-5.25 (50 mW) 5.25-5.35 (250 mW) 5.725-5.825 (1 W)	5.15-5.35 5.47-5.725
Modulation scheme	DSSS, FHSS, IR	DSSS/CCK	Mandatory CCK and OFDM, optional PBCC (allows data rates ≤22 Mb/s) and CCK/OFDM	OFDM	OFDM
Data rate at L2	1 and 2 Mb/s	≤11 Mb/s	1.1 Mb/s, 5.5 Mb/s, 11 Mb/s, 22 Mb/s, 54 Mb/s	≤54 Mb/s	Speeds from 6 to 54 Mb/s
Data rate at L3	≤1.2 Mb/s	≤7 Mb/s	≤25 Mb/s	≤32 Mb/s	3-25 Mb/s
Compatibility	interoperability within each of these wireless technologies but not between the 3 technologies	compatible with 802.11 DSSS 1 and 2 Mb/s systems but not with 802.11 FHSS, IR and HomeRF	Compatible with 802.11b but not with 802.11 FHSS, IR and HomeRF	not compatible with 802.11, 802.11b, HomeRF and Hiperlan/2	not compatible with 802.11, 802.11b, 802.11g and HomeRF
Operating range		11 Mb/s:30-50m 5.5Mb/s: 40-50m 2Mb/s:80-120m	≤19m	≤12m	
Applications		all LANs (wireless Ethernet)		Wide Area Networks and Local Area Networks (data, voice, video)	WAN/LAN, packetized voice, video, data
Approval	worldwide	worldwide	worldwide, ratified 11/2002	US, JP, approval pending in Europe	approved for use in EC
Comments		De facto standard; Recently, Wireline		increased total cost of ownership; lack of a global	compatible with several core networks

[1] Source: Ericsson

		Equivalent Privacy (WEP), a security protocol implemented for 802.11b, had been broken.		standard; emergence of competing standards (i.e., 802.11g) lack of backward compatibility with 802.11b.	including Ethernet, IEEE1394[1] (Firewire, i.Link) and ATM; combines data with voice and video
Products		all major manufacturers, (WECA has certified more than 320 Wi-Fi products)	U.S. Robotics 22 Mbps wireless family	Intel® PRO/Wireless 5000 LAN family of products, Proxim's Harmony dual mode product family, (supports multiple WLAN standards, including 802.11a and 802.11b) Cisco Aironet 1200 series simultaneously supports for both 2.4 GHz and 5 GHz radios. Agere's Orinoco Access Point AP-2000 5 GHz Kit also supports dual mode networks operating on either the Wi-Fi 2.4 GHz (11 Mb/s) or 5 GHz (54 Mb/s) frequencies.	

[1] A recent direction the development of 1394 technology has taken is in providing a wireless solution for the transmission of 1394 protocols over IEEE 802.11. The basic idea is to implement 1394 as a Protocol Adaptation Layer (PAL) on top of the 802.11 radio hardware and Ethernet protocols, bringing together a convergence of these important technologies. This protocol adaptation layer enables the PC to function as a wireless 1394 device. (Look here for further information.)

B2 Comparison of IEEE802.15, Bluetooth, HomeRF and WBFH

	IEEE 802.15	Bluetooth	HomeRF	WBFH
Frequency [GHz]	2.4-2.4835	2.4-2.4835	2.4-2.4835	2.4-2.4835
Modulation scheme	FHSS		FHSS	FHSS
Data rate at L2	V1.1 – 721 kbps, V1.2 – 10 Mb/s	≤1 Mb/s	1.6 Mb/s 10 Mb/s	0.8 Mb/s, 1.6 Mb/s, 5 Mb/s, 10 Mb/s, (20 Mb/s by2002)
Data rate at L3				
Compatibility	Not compatible with any other WLAN standard			Not compatible with 802.11, 802.11b,802.11g, 802.11a and Hiperlan/2
Operating range	≤10 m	≤10 m	≤45 m	≤150 m
Applications	Hands-free wireless phone, PDAs, Laptops, PANs			Home LAN, Home networking of all electronic appliances
Approval	worldwide	worldwide		
Comments			voice support, enhanced telephone features, low power consumption	
Products			Proxim's Symphony™ Product Family	

Appendix C

This section gives a brief overview on the major AAA and authentication protocols[1] as described in [33].

C1 AAA Protocols

RADIUS

Radius is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server - which desires to authenticate its links - and a shared Authentication Server. By managing a single "database" of users, which allows for authentication (verifying user name and password) as well as configuration information detailing the type of service to deliver to the user (for example, SLIP, PPP, telnet, rlogin) it is provided administrative support for AAA.

RADIUS Features

As they are given mainly in [30] and [22], here we present the key features of RADIUS (Remote Authentication Dial-In User Service):

- Widely implemented and used
- For authentication of dial-in users. Roaming between different companies was not specifically considered in the protocol (while it is a must for new AAA protocols)
- Client/server model. NAS (Network Access Server) operates as a client of RADIUS.
- RADIUS servers are responsible for receiving user connection requests, authenticating the user.
- Client and server have a shared secret (hop by hop model.
- Sensitive information must be protected by MD5. RADIUS provides authentication mechanisms, using MD5 hash calculated over a stream of octets, including the shared secret between pairs.
- Transport layer uses UDP. Radius considers the transport layer unreliable and implements its own mechanisms to provide itself a reliable deliver.
- Silent discarding of packets.
- RADIUS' Messages are based on AVPs (Attribute Value Pairs) with alignment to 32 bits.

RADIUS Drawbacks

- In this section the main drawbacks of the protocol, as they appear in [22] are presented:
- Strict limitation of attribute data.
- Strict limitation on concurrent pending messages.
- Inability to control flow to servers.
- Limited server failure detection and silent discarding of packets.
- Inefficient server fail-over.
- Inefficient use of servers in proxy environments.

[1] IST-2000-25394 Project Moby Dick, "AAAC Design", 2001

- No unsolicited messages.
- Hop by hop security.
- Mandatory shared secret.

RADIUS Session Concept

A RADIUS session is defined as follows, "Each service provided by the NAS to a dial-in user constitutes a session, with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended. A user may have multiple sessions in parallel or series if the NAS supports that. For accounting purposes a session ID is generated [31]. RADIUS generates accounting records at the start and the stop of a session.

DIAMETER

With the arrival of newer NAS AAA requirements it has been concluded that RADIUS is ill-suited for inter-domain purposes. The Diameter protocol is a follow-on to the RADIUS protocol; it addresses the RADIUS deficiencies, and is intended for use with the NASREQ, ROAMOPS and Mobile IP application space.

Architecture

Consists of a base protocol and a set of protocol extensions. Common functionality is implemented into the base protocol, while application-specific functionality may be provided through the extension mechanism.

Base Protocol

The base protocol must be supported for all Diameter applications, and defines the basic PDU format, a few primitives and the basic security services offered by the protocol. Despite the fact that RADIUS and Diameter do not share a common PDU, migration from RADIUS is possible by reserving RADIUS codes in Diameter's numbering space. All data delivered by the protocol is in the form of an AVP. The base protocol provides the minimum requirements needed for an AAA transport protocol. It is not intended to be used by itself, and must be used with an application specific extension. Its key features are ([23]):

- Peer-to-peer communication model.
- Session oriented protocol.
- Proxy support.
- Redirect support.
- Based on SCTP (Stream Control Transmission Protocol)

Extensions

- *Strong Security* The base protocol allows Diameter servers to communicate securely using hop-by-hop authentication. This extension defines a set of extensions to the base protocol that provide authentication, confidentiality and non-repudiation.
- *Mobile IP* These extensions provide the ability for a Diameter server to authenticate, authorize and collect accounting information for services rendered to a mobile node.
- *NASREQ* This extension is used for AAA in a PPP/SLIP Dial-Up and Terminal Server Access environment. It defines a set of authentication/authorization commands, which can be used for CHAP (PPP Challenge Handshake Authentication Protocol), PAP (PPP Authentication Protocols) and EAP (PPP Extensible Authentication Protocol.
- *Accounting* The Diameter accounting extension is designed to allow accounting information to be sent across administrative domains.

- *Resource Management* This extension provides the messages that are required for a node to maintain state information.

DIAMETER Session Concept

DIAMETER has a session ID for binding the different AAA transactions together.

C2 Authentication Protocols

Authentication protocols are widely used in establishing a data-link layer connection, mostly a dial-up connection between an end-user's host and the Network Access Server (NAS), but also for switched lines. In general, they allow a peer to transmit authentication information to the authenticator until the authenticator acknowledges the peer. Some protocols are application-independent and some are integrated into an application.

- PAP (Password Authentication Protocol)
- PAP shows the following major characteristics:
- defined as one of PPP authentication protocols [29]
- use a 2-way handshake
- use a pair of user name and password
- passwords are sent in plain text (it is however possible to avoid sending plain text passwords by using one-way transformation, but the authenticator has to implement the same algorithm)
- no replay protection
- frequency and timing of the authentication process is determined by the peer to be authenticated

CHAP (Challenge Handshake Authentication Protocol)

CHAP shows the following major characteristics:

- Defined as one of PPP authentication protocols [29] and [32]
- Use a 3-way handshake
- Use a pair of user name and password
- Supports a challenge response mechanism controlled by the authenticator
- Supports replay protection
- Use one-way hash function to protect authentication information

EAP (Extensible Authentication Protocol)

EAP shows the following major characteristics:

- Defined as one of PPP authentication protocols [21]
- Supports authentication based on different mechanisms, identity-and challenge-based, but also using One Time Passwords or Generic Token Cards.
- These protocols are often integrated in the protocols at the transport level, which implement authentication-based authorization, such as RADIUS and DIAMETER.

DHCP (Dynamic Host Configuration Protocol)

DHCP [25] provides no methods to authenticate clients requesting configurations. In [26] mechanisms of authentication of the source and contents of DHCP messages are added, which allows for the authorization of clients also.

HTTP Authentication

Part of the Hypertext Transfer Protocol (HTTP/1.1) [27] is a framework for a basic access authentication scheme. [28] specifies a basic and a digest authentication scheme. Applying these mechanisms, the access to Web pages can be authorized.

SSL (Secure Socket Layer)

The Secure Socket Layer (SSL) protocol is created by Netscape Communications Corporation to protect information being transmitted through the Internet. The protocol is located on top of the transport layer and offers applications using protocols like HTTP, File Transfer Protocol (FTP), or Post Office Protocol (POP) to authenticate the server and client and to build a secure connection providing, confidentiality, integrity and authenticity. SSL 3.0 is part of Transport Layer Security (TLS) [24].

SSH (Secure Shell)

Secure Shell (SSH) is a client-server application, which offers the authentication of users and machines establishing a terminal connection between client and server using TCP/IP (Transmission Control Protocol/IP). It is used for encrypted remote logins instead of insecure rlogin or telnet applications.