Low cost secure network connectivity for a municipal organization

KRISHNA GUTTI

KTH Information and
Communication Technology

Master of Science Thesis
Stockholm, Sweden 2005

IMIT/LCN 2005-11

Low cost secure network connectivity for a municipal organization

Krishna Gutti
icss-kgu@fc.dsv.su.se

July 28 2005

Royal Institute of Technology
Department of Microelectronics and Information Technology
Stockholm, Sweden

Stokab AB
Stockholm, Sweden

Supervisors: Prof. Dr. Gerald Q. Maguire Jr.,
Royal Institute of Technology
Department of Microelectronics and Information Technology
Stockholm, Sweden

Johan Finnved
Systemingenjör, AB STOKAB
Stockholm, Sweden

Examiner: Prof. Dr. Gerald Q. Maguire Jr.,

Stockholm, Sweden

Abstract

Wireless Local Area Networks (WLANs) based on 802.11 technology were initially conceived with the aim of providing wireless connectivity to client devices in limited areas, such as office buildings, homes, etc. or in places where wires are too expensive to be placed. This 'anywhere' connectivity is said to have improved worker's productivity by allowing one to work flexibly from various places besides one's desk. Currently we are witnessing the growth of both public and private networks based on WLAN technology. Such hotspots are usually limited to the network owner's premises such as her office, campus, etc. This limits the total coverage area of this network. It is often not economically feasible for a network access provider to install Access Points at all places that a network user might go. This has become a problem for many network access providers; a sensible solution would be to collectively address the problem by entering into roaming agreements as is already done by most Wide Area Wireless Network providers. Such operator specific roaming agreements can provide nearly continuous coverage over a much wider area such as an entire city. One of the goals of this project was to study potential cost effective technical solutions that provide WLAN access to City of Stockholm's network based on 802.11 technologies; including evaluation from different technical aspects (e.g., capacity enhancements, improvements in handover latency, etc). Proper deployment and management strategies were also evaluated. Technologies permitting differentiated services for users, enabling provisioning of Voice over Wireless Local Area Network (VoWLAN) services and other interactive services were studied. Technologies for authentication, authorization and accounting were studied. Additionally technical means of providing secure access to the wireless network were investigated. Evaluation of architectures that allow inter-operator roaming were made.

Today's corporate users are increasingly mobile and there is a need to provide secure access to corporate data to these mobile users. The coverage offered by WLAN networks even with large roaming agreements would still have coverage gaps which can be reduced by relying on the 3G networks which are being widely deployed. Virtual Private Network technologies are successfully used for providing secure remote access to data and Mobile IP technology provides application persistence to mobile users even while switching between networks (e.g., WLAN to 3G). There is a need for them to co-exist in order to provide secure, mobile access to data. Such secure mobile access could also be provided without relying on the above, standardised solutions. A goal of this master's thesis was to evaluate the technical solutions to enable such secure, mobile access to data. Current products were evaluated and a suggestion of suitable products for the City of Stockholm was given.

The above solutions together would provide the City of Stockholm with secure wireless network connectivity

Keywords: Wireless LAN, Wireless LAN operator networks, WLAN operator roaming, Mobile VPN

Sammanfattning

Trådlös Lokal Areal Nätverken (WLANs) baserat på 802.11 teknologien var i början uppfattade med det sikta med av skaffande trådlös anslutning till klienten anordningen i inlemmat områdena , sådan som kontor byggnad , hemmen etc. eller på platsen var tråden är alltför dyr till vara placerat. Den här 'var som helst' anslutning är sa till har förbättrat arbetaren produktiv vid tillåt en till verk böjlig från olika ställen for resten en's skrivbord. Just nu vi er vittne växten av båda allmänhet och privat nätverken baserat på WLAN teknologien. Sådan hotspots är vanligtvis inlemmat till nätverken ägare lokalerna sådan som henne kontor, läger etc. Den här gränsen den räkna samman täckningen areal av de här nätverken. Den er ofta inte ekonomisk genomförbar till installera Tillträde Meningen i det hel tåt ställen så pass nätverken förbrukaren makt gå. Den här har bli ett problem för många nätverk skaffa; en förståndig lösande skulle bli till samlad adress problemet vid inlåtande in i att ströva avtalen så är redan gjort vid mest Vid Areal Trådlös Nätverken skaffa. Sådan operatör bestämd ströva avtalen kanna skaffa nästan kontinuerlig täckningen över en mycket vid areal sådan som en hel stor stad. En om målarna av det här projektet var till att studera potential kostnad effektiv teknisk lösandet så pass skaffa WLAN tillträde till Stor stad av Stockholm nätverken baserat på 802.11 teknologerna inklusive bedömningen från olik teknisk aspekterna (e.g., utrymme förstärkningarna , förbättringarna i handover latent tillstånd etc). Rätt spridandeen och företagsledning strategisk var också värderat ut. Teknologerna tillåt skilj tjänsten för förbrukaren, sättande i stånd till tillhandahållande av Röst över Trådlös Lokal Areal Nätverken (VoWLAN) tjänsten och annan interaktiv tjänsten var studier. Teknologerna för authentication, bemyndigandena och räkenskapen var studier. Ytterligare tekniskt medel av skaffande befästa tillträde till trådlös nätverken var undersöka. Bedömningen av arkitekturen så pass tillåta begrava - operatör ströva var gjord.

Idag gemensam förbrukaren är alltmer rörlig och där er en behov till skaffa befästa tillträde till gemensam datan till de här rörlig förbrukaren. Täckningen erbjudande vid WLAN nätverken evn med stor ströva avtalen skulle stilla har täckningen öppning vilken kanna bli nedsatte vid användande den 3G nätverken vilken er vida spridde. Verklig Privat nätverk teknologerna ni är lyckosam använd för skaffande befästa avlägsen tillträde till datan och Rörlig IP teknologien skaffar applicering hårdnackenheten till rörlig förbrukaren jämn fördriva tiden kopplande emellan nätverken WLAN till 3G). Där er ett behov för dem till tillpass - finnas for att skaffa befästa, rörlig tillträde till datan. Sådan befästa rörlig tillträde kunde också bli försynt utan tillit till den över, standardiserat lösandet. En målet av den här övervinna teorin var till att bedöma den teknisk lösandet till möjliggöra sådan befästa, rörlig tillträde till daton. Ström produkten var värderat ut och en förslagen av passande produkten för staden av Stockholm var givit.

Den över lösandet tillsammans skulle skaffa staden av Stockholm med befästa trådlös nätverken anslutning

Keywords: Trådlös LAN, Trådlös LAN operatör nätverken, WLAN operatör ströva , Rörlig VPN

Acknowledgements

I would like to thank Joackim Petersson and Tord Ingvarsson from Stokab AB for giving me the opportunity. I am thankful to Prof. Gerald Q. Maguire for accepting to supervise the thesis work, his guidance, good encouragement, being good source of inspiration and also his patience in listening to all my thoughts. It has been a great experience working with him. I am very glad to have worked with Johan Finnved from Stokab AB. I always enjoyed discussions with him. It has been wonderful experience working with him. I thank Camilla Borgelin and others in Stokab for their support during the project. I am happy to have worked with Jon Olov Vatn prior to this thesis work. He was good source of inspiration. I thank my parents and sister for providing me with everything that helped me reach this far.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Advancements in technology have enabled connectivity among computing devices, which has become a key element in improving productivity in modern business world. This connectivity has also provided a fundamentally new means of communication among people leading to new 'way of life'. Wireless and cordless telephony has lead to deeper penetration of telephony into the society and has facilitated more effective means of communications. Wireless the end user connectivity to computer networks; in particular the Internet would enable a significant leap forward in this information world. Connectivity to the Internet is often limited to wired devices, which are not suitable for the increasingly mobile users or too expensive when provided through current Wireless Wide Area Networks (especially cellular networks) due to their inherent support for relatively low data rates at high cost. Wireless Local Area Networks (WLANs) based on 802.11 [1] technology were initially conceived with the aim of providing wireless connectivity to clients in limited areas, such as office buildings, homes, etc. or in places where installing wires was too expensive. This has also reduced the cost of deploying networks as wiring costs can be reduced. These WLANs can provide wireless access to the Internet even when the client is mobile, although this technology alone only allows mobility which is limited to a sub-network.

As with many technologies, besides serving its intended purpose, WLANs have also come to serve another purpose by providing low cost wireless access networks on a large scale which is cheaper and sometimes more efficient than the current wired networks or WWANs. This ability has also recently drawn the attention of many investors in wide area wireless networks [2, 3, 4] and social activists who want to build wide area wireless access networks of their own [5]. Corporate wireless networks and wireless service provider Hotspots that are based on WLAN technology have been used to provide wireless access to corporate networks or to the Internet for the general public (respectively). The hotspots have proliferated in recent years. Although these provide a new way for the public to access the Internet; they don't provide a network with continuous wide area coverage, since hotspots are usually limited to a small coverage area and are often limited to customer of a given owner/operator. It is not economically feasible for one network owner to build hotspots in all places that their users might want wireless service. A similar problem is solved by wide area wireless network operators by negotiating roaming agreements. Such combined networks provide nearly continuous connectivity over wide area such as entire city.

Though 802.11 facilitates node movement, it is limited to a subnet (i.e., layer 2 mobility). But, the goal is to enable movement over a much wider area which usually encompasses several subnets/networks. Many network applications were written when the communicating computers had a fixed point of attachment, and these applications do not allow changes in the IP address during a session. However, emerging wireless technologies such as 802.11 and 3G aim to provide data services for users 'on the move' i.e., enabling them to be connected even as they move. This paradigm shift must occur without changing the applications, which are already widely deployed. Enabling node (computing device) movement to be transparent to applications is possible by Mobile IP technologies. Moreover, a WLAN network even with agreements between WLAN operators in a city would have coverage gaps; but these can be reduced by complementing the network with today's increasingly deployed 3G networks. MobileIP supports switching between the networks. In today's competitive business world providing access to corporate data from outside the corporate network is essential to improve productivity. Virtual Private Networks (VPNs) have proven themselves to be a solution for providing such secure remote access to corporate data. With VPNs enabling secure data access and Mobile IP enabling mobility and switching between networks there is a need to integrate these two to provide secure, mobile access to data. Alternatively, such secure, seamless mobile access could be provided without relying on the above standard technologies (e.g., using WTLS, UDP/TCP encapsulation). This thesis will explore these alternatives.

Chapter 2

Motivation and project proposal

The City of Stockholm [6] has several communities each of which has their own logical sub-networks. The goal of this work is to provide WLAN access to all these communities (WLAN access to the City of Stockholm (CoS) network) through a potentially cost effective technical solution. Operator roaming agreements with other wireless network providers should enable City's employees to access WLAN networks across the city. Another goal was to study potential technical solutions to enable such roaming agreements. Moreover, the presence of different sub-networks and multiple communities each with their own users is similar to the scenario faced by several Wireless Internet Service Providers (WISPs), thus the solution designed should be suitable for WISPs i.e., to allow users of one WISP roam to another providers' access network (domain) potentially without any services interruption. This could also facilitate multiple operators sharing access points.

In the highly data dependent competitive modern world the workforce increasingly needs access to data anytime, anywhere in order to significantly improve their competitiveness and hopefully their revenues. This same pressure to improve productivity is also being placed on municipal organisations. The City of Stockholm is looking for solutions that would enable smooth operation of network applications across different networks (GPRS, 3G, and WLAN) without breaking application connectivity while users (and their devices) roam across networks. There has been a lot of standardization work carried out to integrate services over these networks [2, 7] and maintain application session persistence for mobile nodes [8]. Access to corporate data from outside the corporate intranet poses the threat of exposing valuable corporate data since remote workers increasingly access corporate data via public network such as Internet and IPv4 doesn't provide any confidentiality or integrity services by default. VPN technologies have proven to provide secure remote access to corporate data. Today IPsec [9] based VPNs are widely used by the corporate world and also others (e.g. hospitals). IPsec by itself doesn't allow mobility (see section 6.1.2). There is work underway in IETF [10] to enable rapid mobility for IPsec. Within the existing standards, there is a need to integrate mobility, security to provide secure, seamless mobility. Security could be provided by technologies other than IPsec (e.g., TLS [11]), but each of these alternatives has its own advantages and disadvantages in a given situation. Today there are some third party solutions providing secure seamless connectivity [12, 13, 14]. A solution from Columbitech enabling smooth roaming when a user moves from one network to another is currently being evaluated by City of Stockholm. A goal of this project was to evaluate similar products. These solutions when combined should provide the City of Stockholm with an advanced networking solution, which is a step towards a fourth generation wireless communication system.

The best data rates provided by the current cellular architectures with 3G technologies are limited by the link layer speed (~350Kbps) and expensive compared to WLANs. WLANs provide high data rates ranging from 11Mbps to 54 Mbps. However, such WLANs are limited in coverage compared to 3G networks. It has been suggested by many [15] that future high-speed (with at least twice the data rates of today's 3G) wireless systems would be realizable by a combination of wireless technologies. The device manufacturers [3,4] have already announced plans to build mobile phone devices that work with such a combination of technologies. There is standardization work being carried out by standardization bodies [2,7] to enrich the experience of the end user, such that they can enjoy the best connectivity available (based on the priorities set in terms of bandwidth, cost, etc.) while the specific network being used is transparent to the user; thus enabling the user to carry fewer devices.

A long-term goal is to understand if widespread availability of hotspots with roaming between these hotspots combined with GPRS and 3G would reduce the need to install lots of new antennas for 3G in the City of Stockholm.

The figures below depict the aimed network connectivity. Figure 1 gives the network connectivity from the user's perspective; he can connect to the network (e.g., office network) through various networks (GPRS, 3G, Broadband, and Dial-up), network operators without perceiving much difference. Figure 2 shows the network coverage as a group of clouds through out the city, clouds with a particular outlined color representing a particular operator's network.

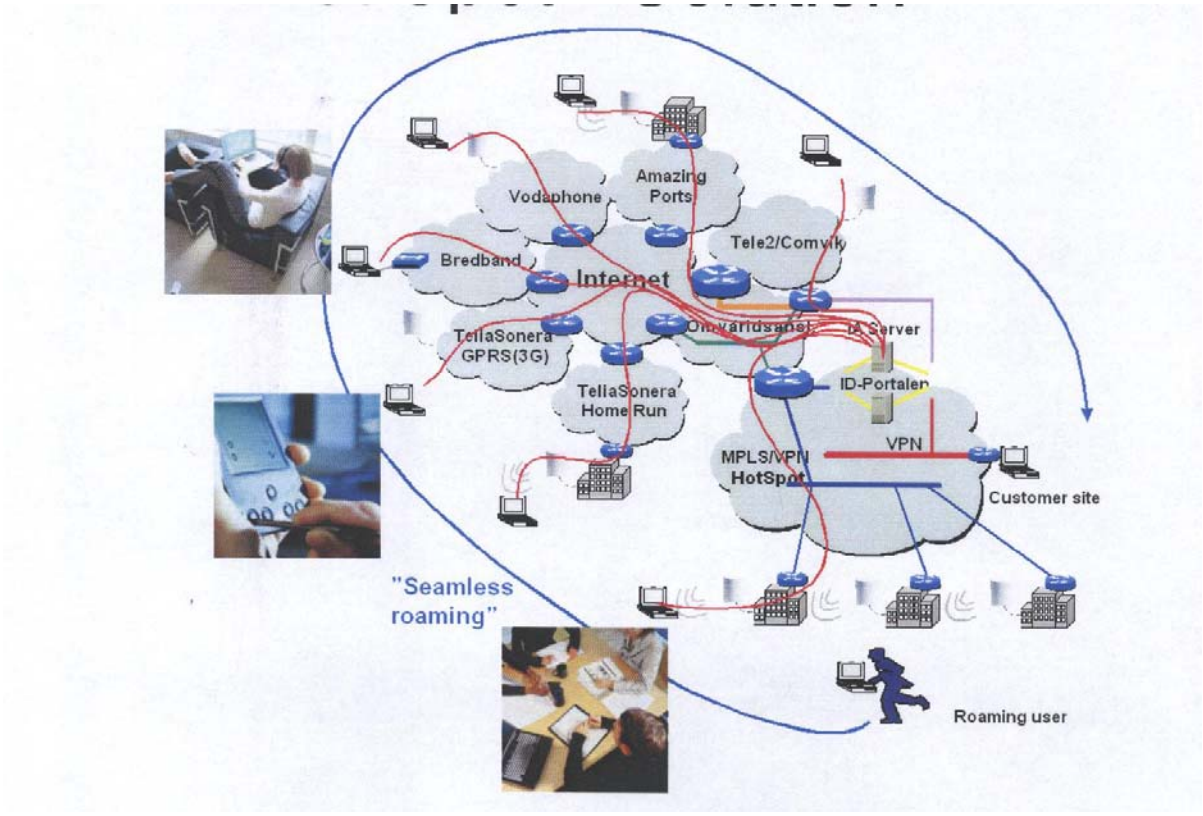

Figure 1. Wide area combined with Local area Network Connectivity[1]

[1] The picture is taken from Stutel project presentation by Joacim Pettersson, Stokab AB dated June 2004

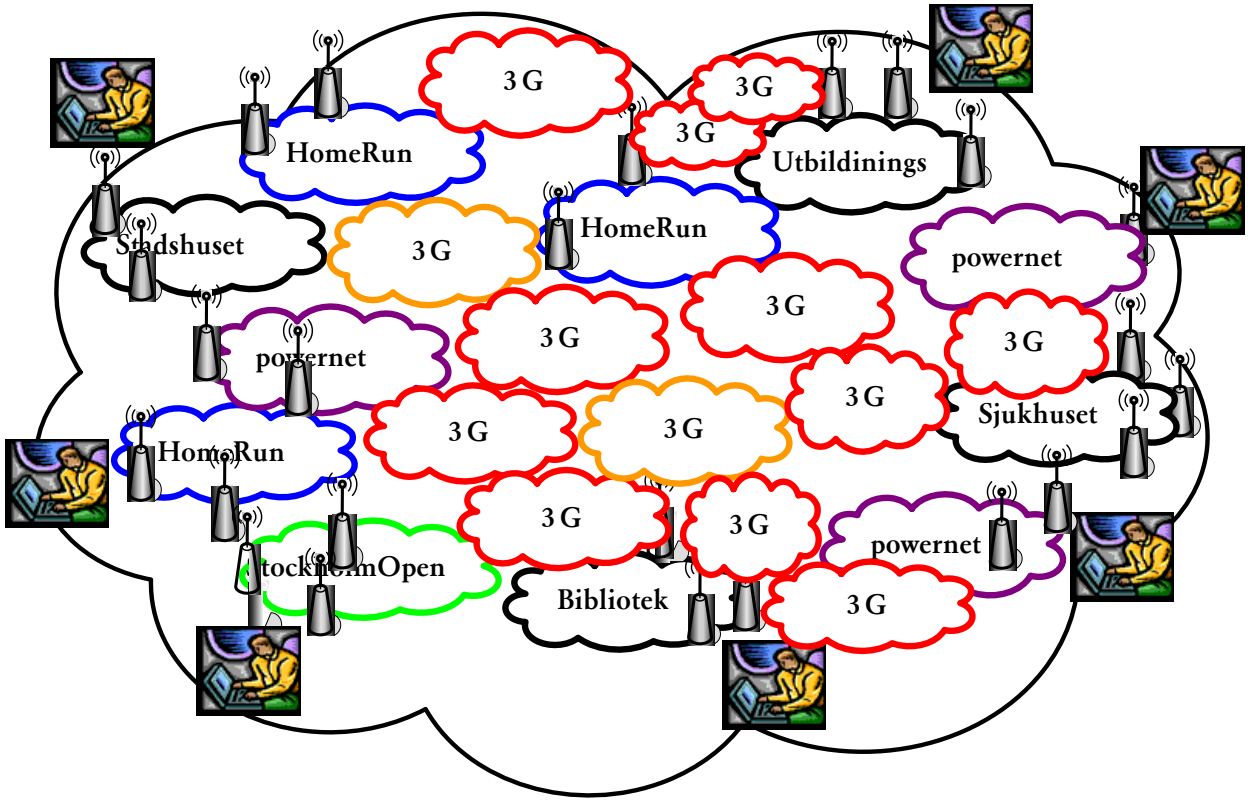

Figure 2. Target Network

Chapter 3

Previous work

Extensive WLAN deployments have been taking place since the late 1990's. They have been evolving since then and researchers have addressed many of the issues involved. Several campus network administrators [16, 17, 18] and operators [19] have produced reports on their strategies, problems faced, and other practical deployment issues related to channel selection, range etc. Other publications describe large-scale deployment strategies of 802.11-based WLANs [20]. These have provided insight into some of the practical issues concerning deploying and running of large WLANs. The thesis provides the technical requirements of the Wireless LAN solution and network designs suitable for Stokab's network; Enhancements proposed for the current standards for improvement of performance, usage of WLANs for low latency applications were studied. Researchers [21] have addressed the problems involved in global scale operator roaming solutions in WLAN networks; a framework [22] for implementing Wireless Internet Service Provider (WISPr) roaming were suggested. The thesis evaluates these works and suggests possible enhancements. Technologies for addressing the security of WLANs and WLAN roaming are suggested. There have been several problem statements and solutions [23 24] addressing Mobile VPNs, the thesis elaborates on these design analyses and provides results of the tests of the products based on the various designs analyzed.

Chapter 4

Wireless Local Area Networks

4.1 Evolution of Wireless LANs

Wireless technology has been evolving from the late nineteenth century. Telephony was a great technological achievement in the twentieth century. Wireless telephony was the next revolution in communication technologies that has provided great impetus for the penetration of telephones into people's lives. Telephone has changed the 'way of communication' among people. Internet has evolved from an experimental network aimed at providing robust network for defense purposes to a network of computing devices, which drives the business world today. The next revolution in networking would be in unwiring the Internet, particularly end-user connectivity. There has been demand in enterprises for wireless network connectivity that would enable the mobile workers on the move access to business information resulting in increased productivity. Several wireless data service providers (such as Ricochet) provided such wireless data services during the late 1990s. These were based on proprietary solutions thus requiring using their own devices and services. Moreover the data rates were limited to hundreds of Kilobits per second. The later 90's saw a new trend in providing high data rate services over wireless medium with the standardization of IEEE 802.11 [1], which is a Layer 1 and Layer 2 (in OSI reference model) specification that is limited to an range of hundred meters. This has later evolved into 802.11b [25], 802.11g [26] and 802.11a [27] standard, they differ in their physical layer from that of the original 802.11 standard. Initially, 802.11 was conceived with providing wireless connectivity to in-house networks (corporate intranets, home computers, etc).

There has been a lot of speculation on the future of 802.11-based networks. According to Gartner Dataquest, "shipments of WLAN enabled devices on the way were up to 31 million in 2004". Gartner Dataquest also tracks growth in WLAN access points, which they expect to top 10 million by 2005. IDC projects total WLAN shipments surging at a compound annual growth rate of 35% from 2001 through 2006."[28]

4.2 Basic WLAN network model

Wireless LANs operate in two different modes: Infrastructure mode and Ad-hoc mode.

4.2.1 Infrastructure mode

A client station equipped with a WLAN interface must be within the radio range (typically 50-150 meters) of an access point (AP), which serves as a base station providing the means of communicating with other devices (these could be similar WLAN device(s) or nodes attached to the wired network). All the information to be sent by the client station to any destination is sent to the AP, which then relays the information to the destination; the same occurs in other direction (destination→ AP→ client station). Infrastructure mode is preferred when majority of communication destinations of the wireless client are not within radio range of the client. The area covered by the radio range of an AP is called a Basic Service Set (BSS). Such BSS could be connected through some backbone network technology (e.g. Ethernet) to form an Extended Service Set (ESS). Thus an Infrastructure mode network could have an ESS extending through a large area such as a metropolitan city

4.2.2 Ad hoc mode

Ad hoc mode is preferred when the major part of communication destinations of the wireless clients are within radio range of the wireless clients. In ad hoc mode the stations intending to communicate form a dynamic network, thus communication occurs peer-to-peer. They do not need any central device i.e., no Access Points.

4.3 Functional requirements

Early on in this project I formulated a set of functional requirements. These requirements are spelled out in the sections below.
The keywords MUST, SHOULD, and MAY, when they appear in this document, are to be interpreted as described in RFC-2119 [29], that is:

1. MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation, which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

4.3.1 Supported radio interfaces: Client-AP interface- 802.11a/b/g

Most of the client cards currently are 802.11b compliant. The more recent 802.11g is backward compatible with 802.11b and many users are increasingly using 802.11g compatible devices. The presence of 802.11b clients causes 802.11g interfaces to fall back to 802.11b mode. Today APs built on an 802.11a/b/g chipset are increasingly available; their costs are expected to come down further. It should be noted that the range with 802.11a is less than 802.11b/g. 802.11b/g MUST be supported by APs to communicate with most client devices. The AP's SHOULD support 802.11a and as such devices operating at 5GHz, they MUST support IEEE standard 802.11h [30].

4.3.2 Compliance with Post & Telestyrelsen (PTS) regulations

The system MUST be compliant with the radio regulations of PTS for unlicensed spectrum.

4.3.3 Interoperability between devices

The system MUST work with standard client devices, i.e. while proposing possible enhancements to improve the system performance or to meet a specific goal no assumption should require changes to standard client devices. If off-the-shelf equipment is chosen, then APs from different vendors MUST be interoperable in most of their features. Other devices such as Access Controllers (AC) SHOULD be interoperable.

4.3.4 Channel selection

Proper channel selection is essential to reduce co-channel interference. This is important particularly when operating at 2.4GHz as this band provides only four usable channels (1, 5, 9, and 13) [19] based on their overlaps. Channel assignment could be hard in a wide scale deployment. Several approaches can be used. It's desirable for APs to have the capability to listen to all the channels and dynamically choose the channel to be used. For this Dynamic Frequency Selection MUST be supported. An AP SHOULD listen to all channels for any traffic in its surroundings and avoid using that channel. The APs MAY co-ordinate among themselves to select the channels they would use. Some products in the market already support this. Alternatively, a central device that knows the placement and coverage areas of APs MAY assign the channels to the APs. This is feasible only in a controlled environment such as a private campus, although at the edge of the campus there might be radio signals from other APs. Either they should use a channel which does not overlap with the neighboring AP or they should choose the same channel used by a neighbor AP. In the later case, when there are no non-overlapping channels with respect to neighbors, the AP should choose a channel used by a neighbor as this would lead to head-on collisions (rather than partial interference) if they try to transmit at the same time. The DCF (a MAC layer function which will be discussed in the following sections) will help reduce these collisions.

4.3.5 Ease of management

APs MUST provide for easy management. They MUST provide centralized management at least at each site. The management devices at each site SHOULD be accessible from a central location to enable centralized management of these devices, as this would be useful for an operator of a large network. They MUST support Simple Network Management Protocol Version 2 SNMPv2 [31] and MIB-II [32].

4.3.5.1 Remote configuration

The solution SHOULD provide for ease of management from several locations i.e. it SHOULD provide for configuration of access points and other access controllers from certain locations e.g. the APs SHOULD be configurable from a remote device as to their power levels, channels to be used, association data rates etc.

The central device SHOULD detect and report failure of an AP within a short period of time. In such case the central device MAY be able to adjust the adjacent APs to try to improve their coverage to reduce the coverage gap. The central device MAY judiciously give such instructions by assessing the current loads at the adjacent APs.

4.3.5.2 AP monitoring

The solution SHOULD include a component (hardware/software module) that would give a summary of the deployed access points regarding their usage levels and other parameters.

4.3.6 Load balancing

The AP's SHOULD support load balancing by proactively and dynamically distributing mobile clients among themselves.

4.3.7 External antenna connectors

The APs SHOULD have external antenna connectors or maximum power levels up to the PTS permitted output power for devices operating in the specific spectrum used.

4.3.8 Several VLAN mappings

The APs SHOULD allow for simultaneous operation of several VLANs segregating the traffic based on 802.1Q [33] each with different SSID i.e. to provide virtual APs.

4.3.9 Differentiated and bounded bandwidth services

The solution MAY provide differentiated bandwidth services to the users. The solution MAY provide bounded bandwidth service to users. The information for differentiating these users may be dynamically delivered to the APs each time a user authenticates to the AAA server (preferably RADIUS [34], RADIUS extensions [35] or Diameter [36]), the information MAY be provided by the assignment of each user to a VLAN

4.3.10 Mobility

The solution MUST support layer 2 mobility of the user by following IEEE Std 802.11F-2003 (IAPP) [37]. The solution SHOULD support layer 3 mobility of the user based on Mobile IP (Mobile IPv4 [38] or Mobile IPv6 [39]).

4.3.11 Security

The solution MUST provide for flexible security schemes. The solution MUST support several authentication mechanisms. The solution MUST enable secure exchange of AAA information among several operators, thus enabling user roaming across several operators' domains. The APs MUST support 802.11i [40].

4.3.11.1 Access control

The solution SHOULD provide for different levels of user access privileges based on the user classification information provided by the AAA server. The user classification could also be done based on the VLAN the user is mapped to.

4.3.12 Scalability

The solution SHOULD be scalable. This demands lower costs for adding, removing, replacing access points or other components.

4.3.13 Robust in varying climatic conditions

The APs MUST robust enough to bear cold climatic conditions with temperatures down to minus 35°c

4.3.14 Power over Ethernet

The APs MUST support Power over Ethernet (PoE) following the standard IEEE Std 802.3af-2003 [41]. This doesn't exclude powering the AP through traditional power supplies as some access points might be connected only to such power supply (when the backhaul data transfer is wireless).

4.3.15 Upgradeability and extensibility

The products SHOULD be upgradeable to extension standards as long as the extension standards permit such extension through a software or firmware upgrade. The solution SHOULD take into consideration possible future changes in the use of the wireless network and accordingly allow for easy transition.

4.3.16 End user Transparency

The solution SHOULD require zero configuration (as specified by the 'Zeroconf' working group of IETF) from the end user perspective. In other words it SHOULD be transparent to the user - making no demands on expert knowledge or requiring significant time to setup or maintain.

4.4 Deployment issues

Proper deployment strategies are important in efficiently using resources. Most of the issues relevant to the physical layer are related to practical issues such as proper placement of APs, coverage, etc. Ashish, et al. discussed the issues of RF propagation delay, access point positioning, cell dimensioning and channel allocation and they have given description of some of the commercial tools available in aiding the deployment process [20]. In a controlled environment such as a campus (e.g. corporate campus) it is possible to preplan things such as channel allocation, power levels, etc. and then proceed with deployment. Unfortunately, in a public place one does not have control of the channels or the specific power that can be used. So, these issues are dealt with as a local matter for each physical location.

Many of the deployment issues in WLAN networks are location specific, the most important being AP placement to ensure proper radio coverage achieving maximum capacity with a minimum number of APs, channel selection, etc. The issues are discussed further below.

4.4.1 Limitations of the spectrums

The spectrum chosen for 802.11 standards are at 2.4 GHz and 5 GHz. However these are already being used by several electronic systems such as Microwave ovens, Bluetooth, etc. Hence, these devices can cause significant interference to the WLAN signals. This interference to WLAN signals can be minimized only by minimizing the other devices operating in those spectrums. This is only possible in private places as in many regulatory domains these older devices enjoy precedence over 802.11 products.

4.4.2 AP placement

The number of APs required is determined by the total coverage area and the capacities that need to be provided at particular sites. The number of APs required should be kept to a minimum while meeting the requirements of both coverage and capacity. Penetration problems due to obstacles made of concrete, bricks, trees, etc. will affect the placement of APs. Proper signal coverage tests (RF site survey) should be done. There are several RF survey tools available in the market. Some vendors such as Cisco provide their WLAN customers with these tools. However, the low cost of an AP mitigates against spending a lot to optimize its placement.

4.4.3 Signal strength, Coverage and Capacity

Greater signal strength provides wider coverage but reduces the data rates at individual APs. The capacity of the APs also limits the coverage area perhaps even more than the signal strength of APs. In areas requiring greater capacity smaller cells are used to achieve higher data rates, by limiting the total number of users. There are additional limitations on these parameters in public places where there may be other APs and other devices operating at the same frequency.

4.4.4 Radio Range

802.11b/g operate in the 2.4GHz band (2.400-to-2.4835GHz, the exact boundaries are defined by the particular regulatory agencies). Signals at this frequency are susceptible to line of sight problems at long range.

4.4.4.1 Effect of increasing range on the throughput (or link speeds)

Lars et al in report on successful operation of links over a distance of 15km with stable connectivity and link speeds up to 3Mbps [17]. They have also reported variations in latency and maximum link speeds during the course of a day, possibly due to changes in weather conditions. Latency over a 3 km wireless link were around 10ms without contention, when another node was contending for the medium the latency rose up to 70ms due to frequent retransmissions. Studies of using 802.11b for even longer ranges were made by Pravin et al. [42].

4.4.4.2 Long-range solutions

Spatial reuse in high density areas is desirable. In low density areas greater range might be a better choice. Also, long range products with higher data rates would also be useful in connecting APs without wired backhaul to their counterparts with wired connection as it would remove the complexities involved in meshing. There are a few such products available in the market, these include products from vivato® [43].

4.4.5 Backhaul

Traditionally APs are connected to the backhaul through wires. However, it might not be feasible to install wires at all places so as to place AP's e.g. high expense. In such cases providing the backhaul through wireless media is a better choice. This could be done by 802.11 interface. As 802.11a is not widely used by client devices, this appears to be better choice. The backhaul in that case would contain one or more 802.11a interfaces. The extensive dark fiber network owned by the City of Stockholm helps avoid long-range wireless links and wireless backhaul as access points can generally be placed where they are needed and directly connect to the fixed network.

4.4.6 MIMO, 802.11n and higher speeds

The upcoming 802.11n [44] standard promises speeds up to 100Mbps. There are two primary proposals from two competing groups. They are incompatible. There are products already in the market based on each of these proposals. One vendor's products are not compatible with others. The compatibility with upcoming standards is also not assured.

4.5 802.11 MAC

IEEE 802.11, 802.11a/b/g standards recommend two different MAC functionalities, namely Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF is a required for any device claiming to be compliant with the 802.11 standard. PCF is optional. DCF utilizes Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). This is similar to Ethernet's (802.3) MAC functionality, which uses Carrier Sense Multiple Access/Collision

Detection (CSMA/CD). However, WLANs can't listen while transmitting making the Collision detection (CD) infeasible. Hence, they use CSMA/CA. Besides, there are some other key differences between wired and wireless medium which resulted in additional reliability measures in WLANs. First, wireless medium is unreliable compared to wired medium due to poor link qualities, possible interference from other devices particularly as 802.11a/g WLANs operate in unlicensed spectrum where many devices (e.g. other WLANs, microwave ovens etc) operate. This unreliability problem is addressed by the use of Acknowledgements (ACK) for each data frame exchanged over the wireless medium. The unacknowledged frames are retried for transmission until the corresponding retry limit is reached. Due to fuzzy boundaries in Wireless LANs there could be a situation where a node might not be visible to all the nodes in the same BSS. This is known as hidden node problem. It is addressed by the inclusion of 'Request To Send' / 'Clear To Send' RTS/CTS frames. Not all the data frames use RTS/CTS as it adds to the overhead thus affecting throughput. A threshold is set for the size of the data frame only above which RTS/CTS should be used. CSMA works as follows. When any STA needs to send data, the MAC layer learns about traffic in the medium. If the medium is idle the MAC Service Data Unit (MSDU) is passed on to the physical layer, which then transmits it along with its headers. If the medium is busy then the MAC layer waits until the medium becomes idle and waits for some more additional time specified by DCF Interframe Spacing (DIFS) and then performs a backoff algorithm to resolve contention between the STAs. The STA randomly chooses a number in the interval 0 to CW_{min} (predefined). It waits for this number of time slots (a time slot is physical layer implementation dependent) i.e. the contention time = random number * time slot. Any station that has successfully transmitted a frame also performs a backoff just after receiving the ACK for last fragment, so as to ensure that it doesn't get the channel right away without any contention for next transmission. When a collision occurs the interval is increased exponentially for each retry, i.e. the interval would now be $0 - (2^N * CW_{min} - 1)$ where 'N' is the number of the retry attempt, this decreases the probability of collision in a STA's next attempt to transmit. Such an exponential increase is performed until the upper bound of the interval reaches CW_{max} (predefined). The physical carrier sensing defines a virtual carrier sensing through the use of Network Allocation Vector (NAV). Most of the frames in 802.11 contain the duration for which the medium is expected to be busy. As every active STA (which is not in sleep mode) hears this value the NAV is updated with each frame. A station updates its NAV. Malicious users could exploit the use of NAV to get an unfair share of channel access, for a DoS (Denial of Service) attack; more on this will be discussed in section 4.11.

4.5.1 DCF

In this section a brief explanation of DCF is given along with some improvements suggested to improve throughput. The possibility of improving throughput by making changes in the AP alone is examined.

DCF is the mandatory part of the 802.11 standards. It is implemented in all the products. Several proposals have been made to improve the performance. Most of them focus on modifications to the contention window, specifically the binary exponential backoff procedure. The Contention Window (CW_{min} or CW_{max}) size represents discrete time points at which clients could transmit, the greater the number of clients the more discrete points ought to be available to reduce the probability of collision. At the same time it is an important factor in determining the throughput as it represents the time when the STA is idle during backoff. Several studies have been made on the performance analysis of 802.11 CSMA/CA, all proving performance increase by using adaptive CW_{min} depending on the number of clients [45]. In [47] the focus was the proper value for CW_{min}, which is critical in determining the time STA spends on backoff. They suggest adapting the CW_{min} value depending on the number of clients. In [46] sachin et al. demonstrate the increase in performance by choosing CW_{min} value depending on the number of clients. Anyhow they suggest using default CW_{min} = 31 if there are more than 2 clients. In [47 48 49 50] the authors proposed using a contention window whose value is determined dynamically (the number of clients being

one of the key parameters) together with a modified backoff algorithm. Others propose use of slow congestion window decrease [51]. In [52] the authors proposed improvements to throughput by reducing overhead by using concatenation of several frames and piggybacking. They prove that the performance can be increased by the use of their scheme; PCF has defined such frame types. Several other MAC improvements were suggested to improve overall performance. All these schemes require changes in the client devices (as each client chooses the CW_{min}, CW_{max} values by itself) that make it hard to implement the suggested changes. However some of these modifications might only be done at the AP. But the effect of implementing such a scheme at only the AP would result in unfair channel usage by AP further increasing the latency in channel gain by the clients, which is undesirable, so no gain is to be made by modifications to CW_{min} or exponential backoff method at the AP alone.

The value of the RTS threshold is also something that would be configured at the client device. As all the clients would be visible to the AP activating RTS/CTS (by reducing the corresponding threshold value) at the AP only would simply increase overhead.

Several other enhancements such as proposed in [53] were made to improve the performance of WLANs but they require a change in the hardware or a major change in the MAC protocol. These are not discussed here due to their apparent infeasibility for adoption, given the large installed base of existing client devices.

4.5.2 PCF

In PCF the AP allocates the channel to one station for a certain period of time. The stations can request a time slot from the AP. Although PCF provides a means to implement many features such as guaranteed QoS it is not supported in most client devices. Some Access Point products claim to attain high data rates by using PCF. This would often be desirable as the majority of the data transfers are often downstream (AP to Client).

4.6 802.11h

802.11a operates in the 5GHz band. In many parts of Europe this frequency band is also used by radar satellite applications. A solution for the co-existence of 802.11a with deployed systems working in 5GHz band was to use Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) services

4.6.1 Dynamic Frequency Selection (DFS)

The radar systems should be given priority in using the channel. The priority is provided by the AP pro-actively testing a channel for the presence of operating radar before using a channel and also while operating in a channel. The AP during association with the client would learn the channels supported by the clients. The AP can ask the clients to be quiet for some time to listen for the presence of any operating radar system. If such a system is detected the AP would select and advertise a new channel to the clients to migrate to a new channel thus giving priority to the radar systems.

4.6.2 Transmit Power Control (TPC)

The AP would associate with the client based on the STA's power capabilities. The local maximum transmit power level for the current channel is advertised. The power is constrained to the limitation set for that regulatory domain. The transmit power is adapted based on a range of information, including path loss and link margin estimates.

4.7 QoS

The Medium Access Control specification in 802.11 provides equal probability to get the channel on an attempt for all the nodes competing for the channel. So, it doesn't differentiate between the streams of data sent by the nodes. This means a stream of VOIP packets (requiring low latency) would be given the same priority as a stream of file transfer (where high latency is acceptable). It is desirable to give higher precedence to low latency data flows. IEEE 802.11e committee is looking at ways of providing such Quality of Service for such data flows. The standardization body has already produced draft standard and some products claim to be supporting the draft standard and claim upgradeability to the final standard once the standard is ratified.

Although the current MAC doesn't provide QoS, it is desirable to learn the impact of the lack of such support in running low latency applications. [54] explains the number of clients that can be supported by an AP when all the clients are simultaneously running VoIP solutions. Solutions from vendors competing for the standard show better performance.

4.8 Layer 2 mobility

4.8.1 Inter Access Point Protocol (IAPP)

The 802.11 MAC was initially conceived with the aim of providing wireless bridging connectivity to clients. Issues concerning a roaming client such as fast handoffs weren't initially looked into. The later 802.11F is aimed at enabling fast handovers when the client moves from one AP to an adjacent AP when both APs are within same layer 3 sub-network.

4.8.2 Handover Latency

Although 802.11F aims at enabling fast layer 2 handovers, the handover latencies as measured in many published experiments [55] [56] aren't low enough to be acceptable with a low latency application, such as VoIP. Many proposals have been made for enabling fast handovers. IEEE 802.11 Task group 'r' is looking at ways of improving handover performance. There are products claiming to support fast handoffs. However, products from different vendors don't usually provide such fast handoff's when used with each other i.e., interoperability is not assured. In [56] it has been shown the delay in handoff is more during detection phase (the phase in which the need for handoff is evaluated), but this is not the case in devices that evaluate such need based on signal strength (going down below a threshold) as assumed in [55] [57] [58]. Today most of the devices follow the later method. Arunesh et al. [55] has proved that around 90% of delay in handoff is due to probe delay (the delay due to search for and choosing proper AP to handoff). Several ideas have been proposed to reduce the probe delay. Shin et al. [57] have suggested the use of active scanning with selective channels using neighbor graph and use of caching with the aim of enabling fast handoff by limiting changes in infrastructure to the client devices. Here the handoff delay is not reduced at the 'learning phase' (initial stages where the adjacent APs' table is yet to be filled). A solution to this might be to query an external agent about the possible next AP's to handoff; such solution could also be used to perform dynamic load balancing as the external agent can choose not to advertise fully loaded APs (Assuming that the agent would be knowing the statistics of the APs by some means such as SNMP). Hector Velayos et al. [56] have suggested the idea of broadcasting the channels being used by the adjacent APs so that there would be less number of channels to be scanned. They have also suggested the usage of optimal values for 'Minchanneltime' and 'maxchanneltime'. Those effects combined together too don't provide desired handoff latency as shown in [55]. Arunesh et al. [59] have suggested the use of neighbor graphs, they differ with [57] as they propose the use of 'pruning' as neighbor graphs give all the APs adjacent to the current AP in all directions and as it is hard to take the direction of traversal of the client into consideration it's a good idea to use local Non-overlap graphs to reduce the number of AP's (sometimes channels)

to search for. As it was proven that the major contributor for the delay is the time for probing one other way of reducing the handover latencies would be to use two radios at the client where the second radio always probes the channels for available WLANs. The advantages of this include lower cost as radios are not high cost components. The downside is that the legacy client devices can not be used.

As said earlier in section 4.6 WLAN devices operating in 5GHz band must comply with 802.11h [30]. The standard facilitates the AP to inform an associated client to move to a new channel (when it finds that another device is operating in that channel). I propose an idea which exploits this facility to achieve near zero-latency layer 2 handoff. It goes as follows: An AP would be equipped with as many radios as there are adjacent APs (with same Extended Service Set Identifier (ESSID)) from which the client might handover to this AP. One of the radio is considered as primary radio which is used for associating with the clients (similar to legacy AP's). The other radios listen to the channels in which the adjacent APs are operating in. All the APs share same Basic Service Set Identifier (BSSID) i.e. they have same MAC from client's perspective. If an AP (B) listens to a new client on one of the secondary radios (it happens when the client starts to enter the overlapping region between the APs (A & B)[2]) it would request AP (A) working at that channel to handover the client to itself AP (B). If the AP (A) had been associated to the client it means that the client is moving towards the AP (B) as B has found the client only now. AP (A) could then instruct the client to shift to a channel used by AP (B) for communicating with the clients i.e., channel in which the primary radio of AP (B) is operating. If the AP (A) was not associated to the client (it could be the case for example when the client is associating with AP (A)) it would send an 'ignore' message to AP (B). If the client moves to an overlapping area where the handover is possible to more than one AP, there would be contention between AP's. The contention could be resolved for example by the holding AP (A) choosing the AP which made the most recent request for the handoff. One could also use the same channel with all the AP's, but this leads to inefficient use of available channels. The idea of using same MAC address for the AP's is earlier proposed by Douglas et al [60]. The advantage in the proposed idea is that it requires no change at the client side devices. The method is useful only to WLAN devices that are operating at 5 GHz (and following 802.11h) and not those operating at 2.4GHz. However, there are only three non overlapping channels, four usable channels (section 4.3.4) in 2.4GHz frequency band; if the current channel is not assumed to be used by the adjacent AP, there are at most three channels - hence only two other alternatives. However, in 5GHz band there are up to 12 non-overlapping channels where a fast handoff scheme would be crucial.

4.9 Security

4.9.1 MAC layer

The 802.11 MAC uses CSMA/CA to allocate the channel to a station. The decision of using a channel is based on physical carrier sensing and virtual carrier sensing through use of the Network Allocation Vector. A station can abuse this and gain the channel for longer or even all the time. The other stations wouldn't learn about the channel being available as they expect the channel to be used for the length of time specified in the NAV. This could be a potential problem

[2] Here the handoff process initiates only when some message (frame) is sent by the client (to AP (A)). This shouldn't be a problem even in the case where the data flow is only from the AP (A) to the client while the client is moving as the messages in 802.11 are acknowledged at layer 2. When the client is in sleep mode, the handoff doesn't begin until the client sends some message. This too shouldn't be a problem as there is no need for fast handoff when the client is in sleep mode and the data destined to the client, stored by AP (A) during its sleep mode can be relayed to AP (B) during the handover.

in public places such as hotspots. Raya et al. discussed the issue in length and suggested possible systems to detect such greedy users [61]. However, most of the techniques that are used at the MAC layer to detect a greedy user can be bypassed. In some cases log of the amount of data transfers of each user can help detect such greedy users. The above technique of abusing NAV can also be used to launch Denial of Service (DoS) attacks. Also, the MAC facilitates a station going to sleep, thus all the data destined to that station is stored at the AP and later relayed when the station wakes up. The instruction used by the station to tell the AP about its plans for sleep mode doesn't contain any authentication element. This can easily be abused to launch Denial of Service. Many such issues are discussed in [62].

4.9.2 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) as the name suggests was designed to provide a reasonable level of security but the term "reasonable" is often misleading. Today there are many free tools available via the Internet [63 64 65] that can be used to crack the WEP key. The strength of the algorithm depends on the key length chosen. A carefully chosen 104-bit key can be broken in a few hours. Additionally, it is one way authentication (Client to AP only) making it vulnerable to Man-in-the-Middle attacks.

4.9.3 Wi-Fi Protected Access

To provide better security than WEP, the IEEE working group 802.11i was formed. In the mean time Wi-Fi Alliance, a WLAN vendors group chose to come out quickly with an intermediate solution that can be used to replace WEP. WPA was ratified by the Wi-Fi Alliance to meet this goal. WPA was designed to be software upgrade for WEP based devices. So, the key component in WPA is still WEP. The main improvement though is Temporal Key Integrity Protocol which simply changes the key faster.

4.9.3.1 Temporal Key Integrity Protocol (TKIP)

TKIP was also designed to provide better security than WEP, but without requiring a hardware change to the devices (APs or Client Stations). TKIP improves security through use of temporal keys which are frequently changed (thus hopefully avoiding allowing the attacker to collect enough information to crack the key). The strength of TKIP as with any encryption depends on the use of properly chosen keys i.e., use of dictionary words or short keys are easy to crack and there are tools [66] available to do so.

4.9.4 EAP

Extensible Authentication Protocol (EAP) [67] provides a framework for multiple authentication methods. Advantages of EAP include support for multiple authentication mechanisms without having to pre-negotiate a particular one; an authenticating device need not understand all the authentication methods and can rely on a back-end server, which understands these methods. EAP typically runs over data link layers such as Point-to-point protocol (PPP) [68] as defined in [67], IEEE 802 as defined in IEEE 802.1x [69] and 802.11 as defined in IEEE 802.11i [70]; it doesn't require IP. The basic entities in EAP include

Authenticator: The end of the link initiating the EAP authentication. An Authenticator need not implement all the EAP methods; for those EAP methods it can act as a pass-through agent and rely on a backend authentication server.

Peer: The end of the link that responds to the authenticator

Backend Authentication server: A backend authentication server is an entity that provides an authentication service to an authenticator. When used, this server typically executes EAP methods for the authenticator.

There are four classes of messages: Request, Response, Success, and Failure. A basic EAP authentication exchange begins with Authenticator sending a Request. This request consists of type, Identity, One Time Password, etc. The peer then sends a response corresponding to the request type. Additional requests can be sent by the authenticator and corresponding responses by the peer, however, EAP is a 'lock step' protocol meaning that other than the initial request, a new request can not be sent without a valid response. The conversation ends if the authenticator cannot authenticate the peer (i.e., unacceptable responses to one or more requests) in which case it transmits a Failure. The authentication conversation can continue until the authenticator determines that a successful authentication has occurred, in which case the authenticator transmits a Success. An explicit NAK provides flexibility to choose different authentication

The EAP packet Format is shown in Figure 3

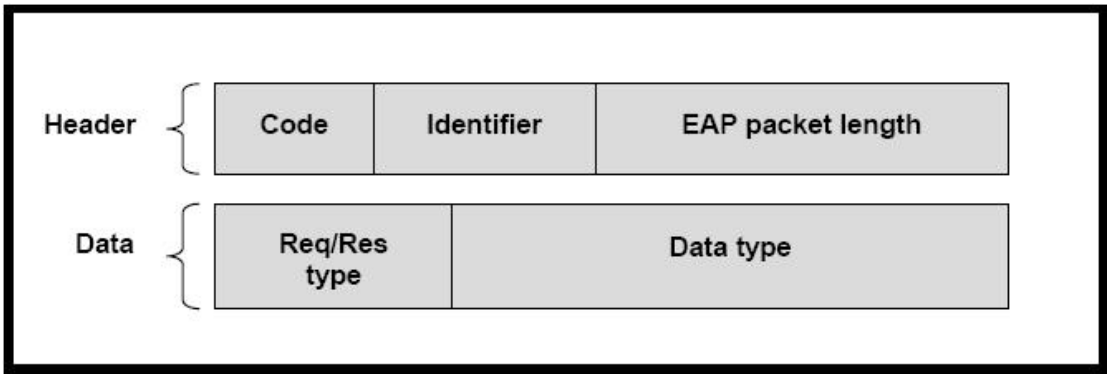

Figure 3. EAP packet format

Code

One octet in length, defined values:

Request
Response
Success
Failure

Identifier

One octet in length, aids in matching responses with requests

Length

Two octets in length, indicates length in octets of the EAP packet including the code, Identifier, Length and Data fields

Data

Zero or more octets, value depends on the code field value, for Code field values 1 and 2 (i.e., Request and Response) Data field consists of 'Type' – 'Type-data' fields

Request/
Response

Type One octet in length, indicates type of request or response
The types 1-4 (below) MUST be supported and type 254 SHOULD be supported.

1. Identity
2. Notification
3. Nak (Response only)
4. MD-5 challenge

254. Expanded types

Type-data
Zero or more octets, value depends on the 'Type' field

A generic EAP authentication is shown in Figure 4 and EAP-TLS timeline is shown in Figure 5.

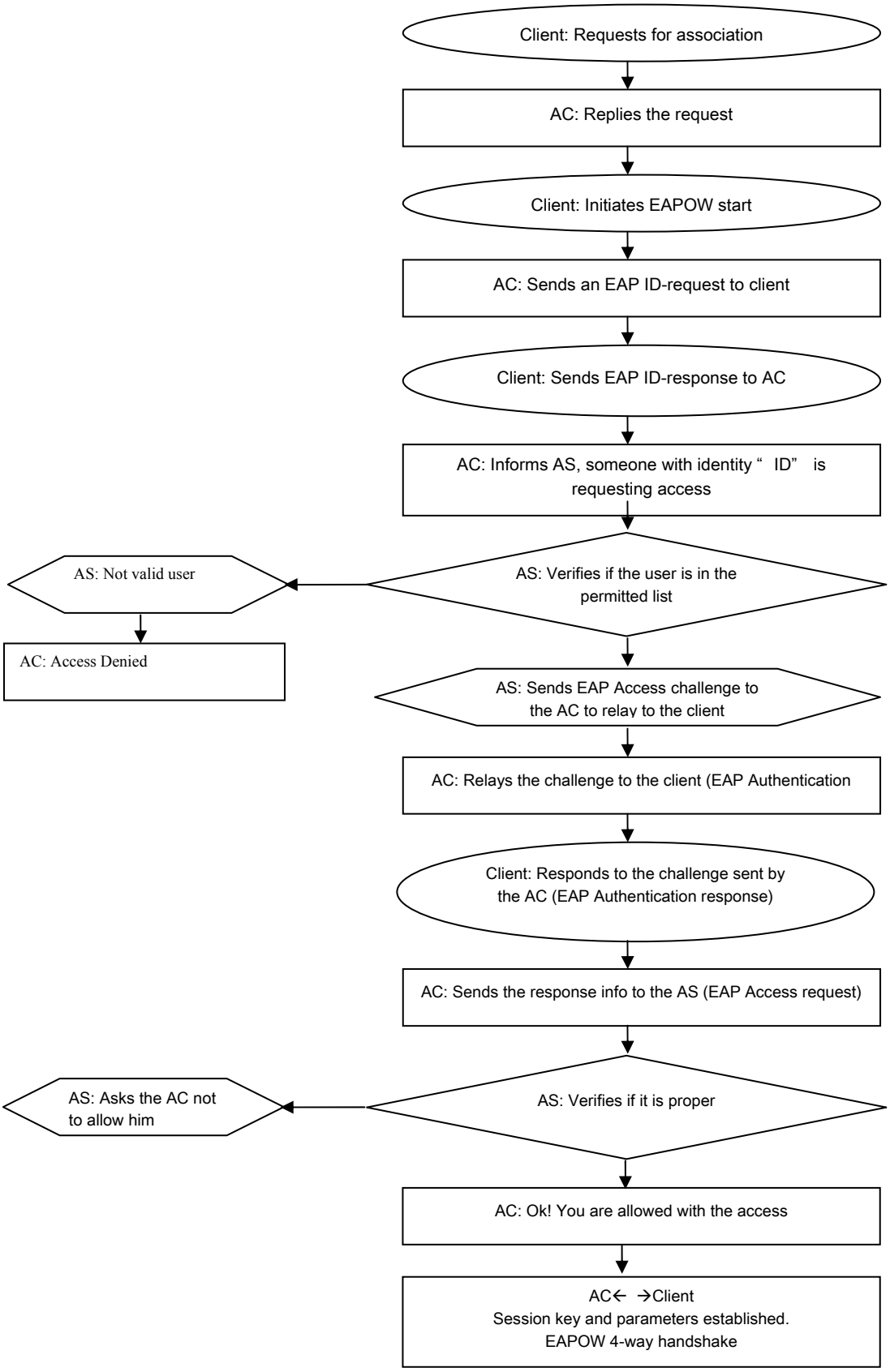

Figure 4. EAP based authentication

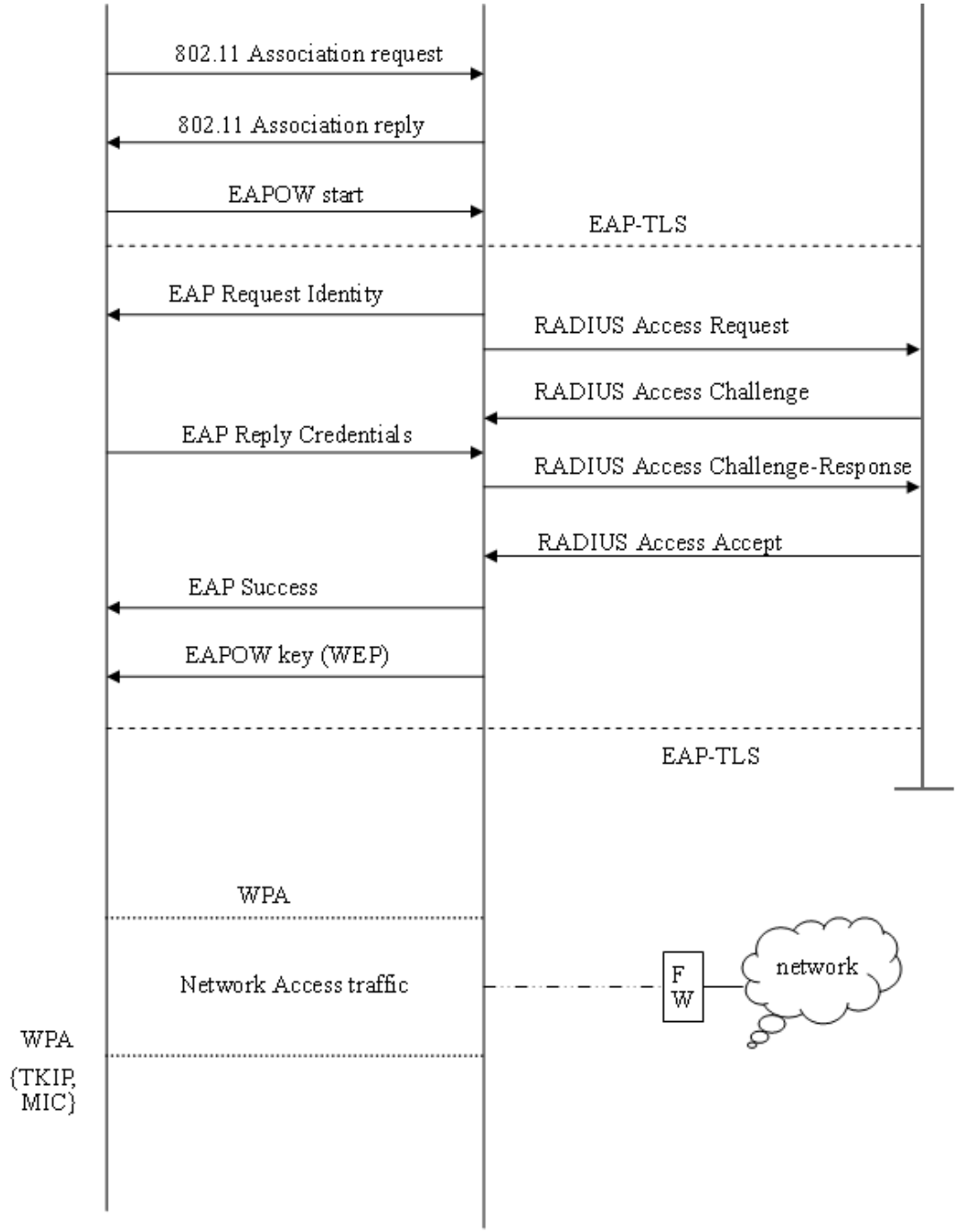

Figure 5. EAP-TLS based authentication

Sseveral EAP based authentication methods viz., EAP-MD5, LEAP, PEAP, EAP-TTLS, EAP-TLS facilitate authentication. Certificate based authentication is provided by EAP-TTLS and EAP-TLS. EAP-TTLS is one way certificate based authentication where the authenticating entity proves its identity through a certificate. If certificates are to be used by both ends EAP-TLS can be used; it tunnels EAP messages over TLS.

4.9.5 Remote Authentication Dial-In User Service (RADIUS):

RADIUS is an authentication, authorization, and accounting (AAA) protocol which provides a means of authenticating users through several ways. The model consists of a RADIUS client and RADIUS server. The typical RADIUS usage scenario is: The user tries to access a network or a resource which is guarded by an access controller (AC). The access controller acts as a RADIUS client. The RADIUS server which sits at a central location is called Access control server (ACS). The user either provides his authentication credentials to this AC or the access control server depending on the authentication method. If provided to the AC, the AC would relay them to the ACS using the RADIUS protocol. The ACS would reply whether the user should be provided access or not. If so, the resources he should be provided access to and other Authorization attributes are also provided. Two RADIUS servers could communicate with each other. This would be useful in cases where the user belongs to a different domain than where he is accessing the resource i.e., a domain different from the AC domain. The AC sends the access request to the ACS in its domain, depending on the user (e.g., based on Network Access Identifier [71] (NAI) which contains the domain name) the RADIUS server (ACS) can relay the request to the users home domain radius server. RADIUS runs on top of UDP/TCP.

4.9.6 802.11i

As stated in [16] the key component in WPA is WEP, although the ability to crack the key is mitigated through the use of TKIP. However, 802.11i defines two new types of networks, one is a Robust Security Network (RSN) and the other is a Transitional Security Network (TSN), the latter is defined to be backward compatible with the existing wide base of WEP based systems. Both RSN and WEP based systems can operate in parallel in TSN. RSN supports AES encryption which is supposed to be much stronger than WEP.

4.10 WLAN Architectures

The standards defined regarding 802.11 based WLANs permit several architectures relative to the placement of functions (802.11 defines the services Authentication, Association, De-authentication, Disassociation, Distribution, Integration, Privacy, Reassociation, MSDU delivery) either in the end radio device (Access point/Wireless Terminal Points [72]) or a centralised device operating on several end radio devices. This has lead to broadly two different architectures in the WLAN market today. One contains the stand alone Access point and other consists of Access Points with minimal functionality which utilize a central manager that performs most of the functions.

4.10.1 Stand alone AP's

These devices (Access points) provide the physical layer, MAC functions and security (802.1x, WEP, WPA or 802.11i) functions by themselves, e.g., Cisco Aironet 1200 series [73]. These products don't provide as much control of the operating environment/users as the switch based solution.

4.10.2 Switch based solution

Another class of device is a switch based solution that utilizes a central manager to which the end radio devices (Access points), also called Wireless Terminal Points are connected. Several functions are provided by the switch. These could be authentication (802.1x) and/or Encryption (WEP, WPA or 802.11i). The disadvantage of this architecture is that there is no standardisation yet. Several functions are based on proprietary implementations i.e., leading to interoperability problems with other vendors APs. But there are products (such as Trapeze networks) which claim to be supporting many other vendors APs

4.10.2.1 Centralized management (Control And Provisioning of Wireless Access Points)

With the proliferation of 802.11 based WLAN usage in large campuses such as enterprise or university campuses the number of APs operated by a network management group has increased tremendously. Such large-scale deployments are only realizable through some centralized control and management. Although 802.11 specifies the PHY and MAC layer services to be provided by the APs it doesn't specify a means of exchanging information needed to centrally control the environment (e.g. terminal devices (AP's) operating parameters). This has lead to proprietary implementations of such centralized control through 'Access Controllers' (ACs). A means of achieving such centralized control of the environment from several vendors would be desirable for providing users the flexibility in choosing their vendors. An IETF working group named 'Control And Provisioning of Wireless Access Points (capwap)' [74] was formed with the aim of solving this problem. Its initial work was studying the current architectures used by vendors. Basing on these architectures there were a few proposals, including a protocol called "CAPWAP Tunneling Protocol' [75] which enables several services required for remotely managing the 'Wireless Terminal Points'. Secure Light Weight Access Point Protocol (SLAPP) [76] and Light Weight Access Point Protocol (LWAPP) [77] are two other proposals in consideration at the time of writing.

4.11 Proposed Architectures

Stokab's network has several communities each with their own subnet. Stokab's customers range from various libraries, schools ... City hall. Two architectures are proposed for Stokab's customers.

4.11.1 Multiple SSID based architecture

In this architecture an access point operates several SSIDs simultaneously. Traffic in each SSID network is segregated using VLAN (802.1Q) tags. The traffic from each VLAN is mapped to an MPLS VPN which runs in the backbone. The traffic primarily ends at the Firewall which acts as AAA server. If a VLAN's traffic is destined to the VPN (which could very well be the case for staff of various communities) then the traffic can be directed to the Firewall which would then send it to the external interface of the VPN gateway. The VPN Routing and Forwarding tables have an entry pointing to the Firewall for the traffic destined to the outer interface of the VPN Gateway. This architecture is useful in cases where there are several classes of users and each class accesses resources that are subset of other class of users. Figure 5 depicts a case where there are several classes of users trying to get WLAN service from a single access point

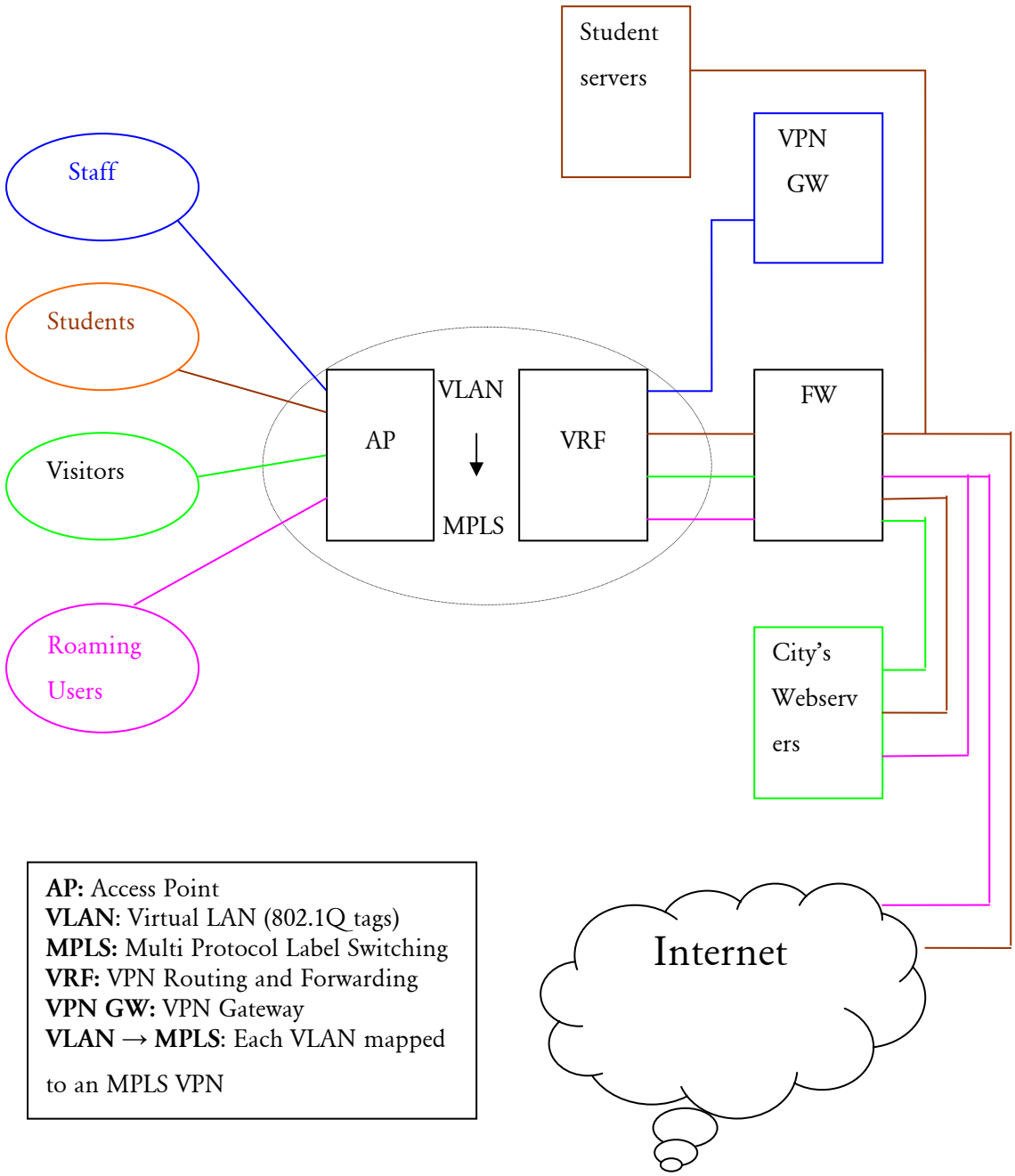

Figure 6. Multiple SSID based architecture

In this architecture the Access Point supports simultaneous operation of several SSIDs and can isolate the traffic from each SSID by using 802.1Q tags. These 802.1Q tagged VLANs are mapped to MPLS VPNs. The 'staff' SSID traffic is mapped to a MPLS VPN and all the traffic in this VPN is routed towards the VPN Gateway (through the Firewall). The 'Student' SSID traffic is mapped to a MPLS VPN and this traffic is routed to the Firewall. The visitors and Roaming Users traffic are placed in a two separate MPLS VPNs and the Routing entries in VPN Routing and Forwarding tables direct this traffic towards the Firewall. The Firewall redirects the traffic to the appropriate authenticator and does access control depending on the authorization information received from this authenticator.

4.11.2 Single SSID based architecture

In this architecture only one SSID is used. There is an access controller performing the gate keeper functionality. All users will be redirected to a webpage to choose the class they belong to and the corresponding authentication is carried out. It could also be that depending on the resource the user is trying to access the access controller could authenticate the user. Figure 6 depicts a scenario with the same classes of users as in the previous architecture, but using the single SSID architecture. Here only one SSID is used with each Access point. The Access Controller does act as authorizing and access control enforcer. It does the similar work done by the Firewall in the previous design. There are no separate MPLS VPN's for each class of user. Anyhow, the traffic in the back bone can be isolated by the access controller.

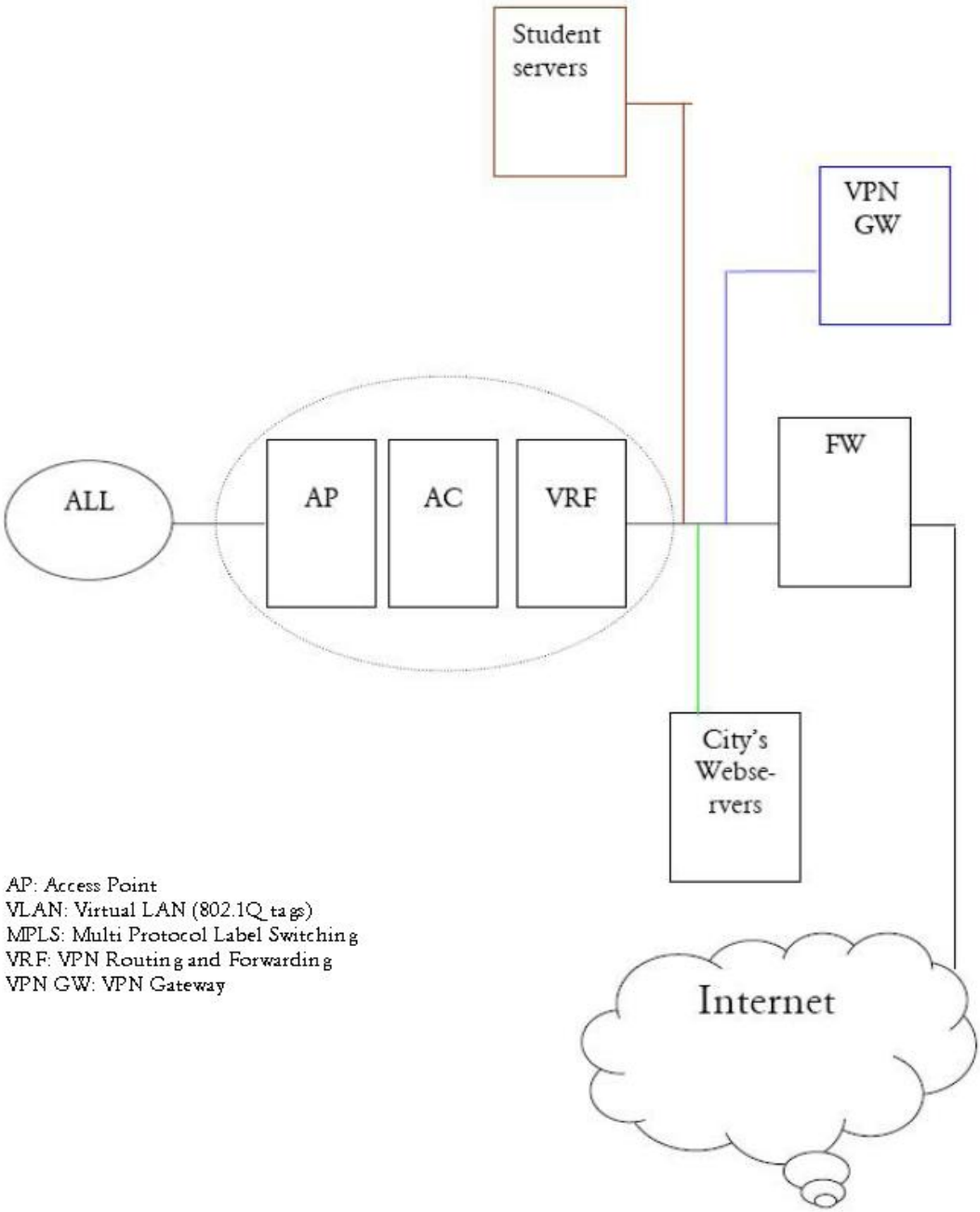

Figure 7. Single SSID based architecture

4.11.3 Comparison of these Architectures

Table 1 shows a comparison of these two architectures. As can be seen the former architecture provides more flexibility such as implementing various authentication schemes, easy sharing of infrastructure (could be as part of roaming agreements) where as the later architecture is simpler.

Table 1. Comparison of proposed architectures

Multiple SSID	**Single SSID**
Multiple Authentications supported e.g., EAP, Web-login Could easily segregate traffic in the backbone (as VLAN tagging is supported) which might be desirable In later stages it would easily allow sharing of Access Points	Less confusing for the user Limits to one authentication method (e.g., Web based authentication) Access controller must support some mechanism e.g., VLAN to segreagate traffic before sending it out to the backbone

4.12 Operator roaming

Today 802.11-based wireless networks are increasingly being deployed both in corporate and public places. The wireless networks of one operator are usually limited to a few geographical areas. According to a report from the market research firm IDC, "the number of western European wireless hotspots is expected to grow to more than 32,500 locations by 2007, generating total revenue of US$1.4 bn" [78]. In order to increase their service area thus revenues (direct or indirect), one of the business strategies is to work together with other operators by entering into roaming agreements. Here the technical issues involved in entering into such agreements are addressed. It is acknowledged that for commercial operators the business model and billing form the key for their business success. However, no suggestion or assumption of a business model is made; rather, possible technical means that can be used for many business models is provided. Also, compatibility in the technologies used (802.11a/b/g) by the users and different operators is assumed and will not be discussed further. One of the key technical issues in such roaming agreements is to securely implement Authentication, Authorization, and Accounting (AAA). Aboba and Zorn [79] provide the criteria for evaluating roaming protocols for dial-up Internet service roaming by stating the requirements to be met by the involved sub-systems. The architecture consists of three major subsystems: Phone book subsystem, Authentication subsystem, and Accounting subsystem. These concepts can be applied to WISP roaming with the exception that in WISP roaming there is no phone book sub-system; however an equivalent sub-system is an SSID list of the roaming networks and corresponding authentication methods. Although [79] provides generic requirements it does not specify the authentication methods, protocols, etc. to be used. Many have proposed architectures for user roaming across different operators' networks, not only 802.11 networks but also the widely used cellular based networks [80 81 82]. These architectures have APs with several radio interfaces capable of communicating with both WLANs and cellular networks. Issues related to inter operator roaming have been addressed by the cellular industry and some of the concepts, particularly network selection by a mobile phone in cellular operator roaming can be of use to WLAN operator roaming. A brief overview of network selection in cellular operator roaming is given in the following section. In the following sections the concepts of network selection,

authenticating to the network, authorization and accounting are examined. Confidentiality of the traffic is not discussed here. Several established technologies, e.g., IPsec or 802.11i can be used for providing this service.

Though there is no standard for operator roaming in 802.11 networks, the Wi-Fi Alliance, "a non-profit organization, composed of the leading manufacturers of wireless systems or of companies that provide Wi-Fi® services" [83]through the committee, 'WISPr' has published recommended practices for Wireless Internet Service Provider roaming [22]. This will be discussed in the following sections.

4.12.1 Requirements on the Operator roaming solution

I have formulated a set of requirements to be met by the operator roaming solution. They are:

1. The solution SHOULD use the existing authentication infrastructure for authenticating the users.

2. The solution MUST provide secure authentication of user. Secure authentication implies the authentication system must have sufficient strength to render it infeasible to derive the user credentials even when the authenticating media is accessible to the attacker.

3. The solution SHOULD be scalable.

4. The solution SHOULD work with standards based infrastructure at the roaming operator's end.

5. The roaming operator SHOULD NOT be a trusted entity. The authentication system SHOULD not hand over credentials to the roaming operator. The roaming operator SHOULD not be able to perform replay attacks.

6. The accounting MAY be reliable.

7. The solution MAY protect the roaming user's identity from being revealed in the roaming network.

8. The solution MAY work without requiring any client side software.

9. The solution should require zero configuration (as specified by 'Zeroconf' working group of IETF) from the end user's perspective. In other words it should be transparent to the user making no demands on expert knowledge or requiring significant time to setup or maintain.

4.12.2 Network selection

In GSM networks the Subscriber Identity Module (SIM) contains the list of networks in order as preferred by the home operator and the home network would normally have highest priority. There are two settings (manual or automatic) which affect the way in which the mobile phone connects to an operator. In manual setting, the user selects the network to connect from the list of available networks. With the automatic setting the network with highest priority in the list of available networks is selected. The SIM card is distributed to the users by the operators.

When working in Infrastructure mode typically 802.11 client devices scan for the presence of Access Points in all or selected channels and will try to associate with AP with best signal strength [54]. If the AP rejects this association request, then AP with next best signal strength is selected. Typically

the management of device connection is done either by operating system in the computing device or the driver provided with the WLAN client device. One problem to be handled is the naming of the networks, as there could be millions of hotspots worldwide there are high chances for the network names to be confused one for another if commonly used strings are used as ESSID, in such a case the device could mistake a network as a roaming network when it is not, even though this need not be a fatal error it would increase the delay, this can be avoided by taking some simple measures e.g., include a trademark string or unique string such as domain name in the ESSID. Standardization of SSID nomenclature would provide a scalable solution. Such standardization has been proposed [21]. Yui-wah et al. [21] have discussed this problem, explained various solutions, proposed their own solution, compared and contrasted the solutions. The various solutions involve use of a Roaming Table. This is claimed not to scale when the number of hotspots goes to the scale of millions. But, such a large number of organizations could realistically come into roaming agreements through some intermediaries, which would take up the task of aggregating the hotspots. In this case even if a particular hotspot owner decides to keep his SSID, he can simultaneously broadcast a common SSID used by the partners (as many APs today support multiple SSIDs). Moreover the storage capacities of today's mobile computing devices are increasing, even in a hotspot network of a million SSIDs the amount of memory with an SSID as a data type of maximum 32characters, it would require 128 bytes per SSID, less than 128MB for million entries (imagining UTF-16 coding which allows use of many non-English alphabets). The computation cycles (thus time) required to search the entry would increase. The processing powers today are at least in the order of a few hundreds of megahertz, which would be capable of performing a quick search in a table of a few million entries. The authors propose use of Roaming Information Code (RIC), which could either be transported as SSID or a new information element of the 802.11 standard. They claim the nomenclature is scalable to a scale of millions of hotspots

Here I propose another SSID nomenclature. As said earlier use of unused strings such as domain names would be a simple solution. The idea below leverages on that to provide a formal nomenclature.
Use of 32 bytes for the name is suggested.

Use 32 bytes
Flags 1 byte
Version 1 byte
Prefix- 2 bytes, could use 'country code- Top Level Domain' (ccTLD)
Postal code 3 bytes
Code 25 bytes (= string)

Where string could be any sequence of characters, I suggest using a unique string such as a domain name, since most hotspot owners are within some domain they can use this domain name as part of the string, for e.g. mydomain.com_rådmansgatan, or a string containing a trademarked word which would usually not be used by others, an email address, etc. One more method is to use the MAC addresses of the AP's as part of the list, the advantages include fast search as MAC address of the AP is included in all the frames sent by it which would take less time to be recognized. The disadvantages include use of multiple entries for each network as there could be several AP's in one network (this could be too expensive in cases where the network is of a large operator who for example has hotspots in a large country in which case there is only one ESSID). There are several other means that can be used to move this burden from the client to the AP. For example, one could include a broadcast instruction which requests if someone is in agreement with the client's operator for which the roaming visiting network AP can respond. However such solutions require change in the standard compliant legacy devices (clients and AP's).

4.12.3 Roaming Architecture

Wireless Internet Service Provider roaming was addressed by Wi-Fi Alliance. They have released a specification which provides a framework for authenticating, authorizing, and accounting users in inter-operator roaming networks. This framework is specified in [22]. The architecture suggested is shown below Figure 9. Each operator in the roaming network would have a RADIUS or Diameter server[3]. This AAA server would in turn communicate with the AAA server in the other operator's network. The user authentication could be done using several EAP methods viz., EAP-MD5, EAP-TTLS, EAP-TLS, etc. The architecture is similar to those used today in many of the public wireless access places (hotspots).

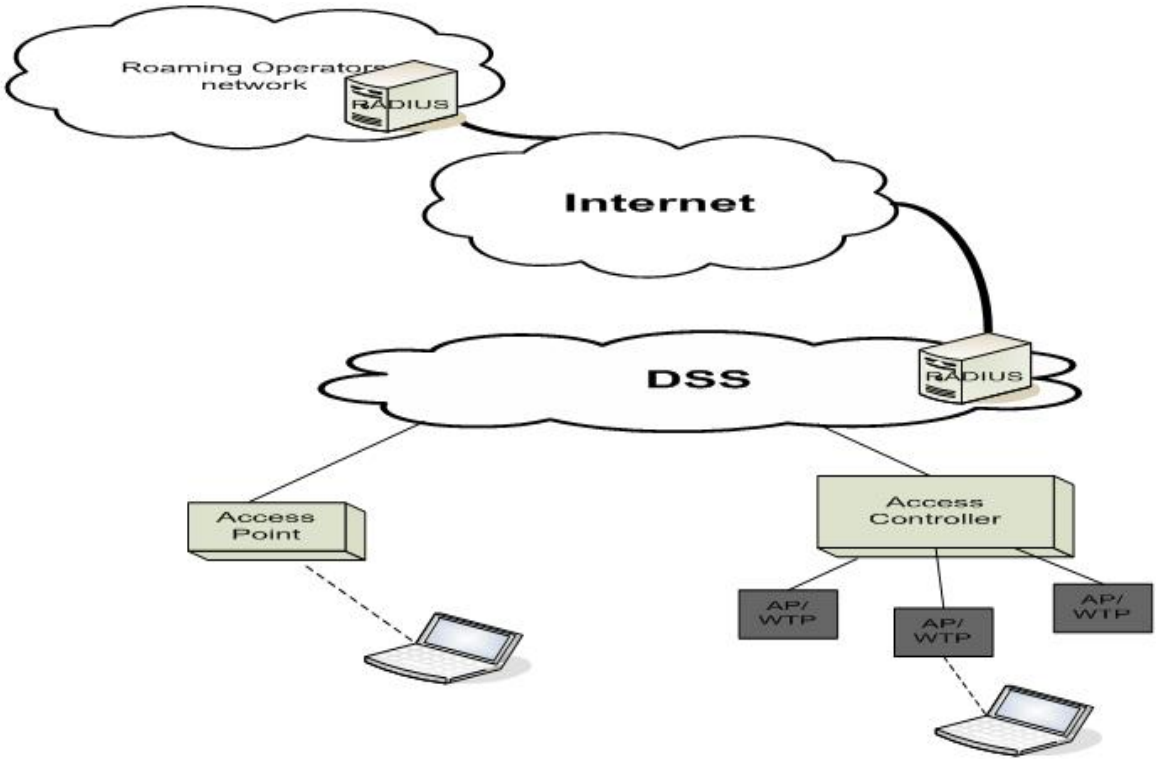

Figure 8. Operator roaming architecture

4.12.4 Authentication Scenario

When the user is near an Access Point in the roaming operator's network and tries to access a webpage. The user will be redirected to a roaming operator list page/login page. If a list of operators is given the user selects his home operator (e.g., via a drop down menu or a hyperlink, if the list is too long it could be categorized into sub-lists), this step can altogether be avoided if NAI [71] is used for username. The next page would be a login page where the user enters his username and password. The web login is protected by using SSL. The RADIUS server at the operator's network conveys these credentials to the user's home operator radius server. This authentication requires the user credentials to be handled by the roaming operator. This can be avoided by using EAP-TTLS or EAP-TLS where the authentication credentials are securely tunnelled to the end

[3] From here on in the current section RADIUS is used as a general term for both RADIUS/DIAMETER. So, RADIUS could be replaced by Diameter unless explicitly mentioned otherwise.

RADIUS server as shown in the below figure. (Using the web login authentication between the user and his home operators SSL server isn't easy to implement as there are problems in identifying the user by the roaming operator's RAIDUS server i.e., there wouldn't be an identity used by the home server to tell the roaming server that the user with this identity should be allowed access of this kind. This is because RADIUS works as request-reply process there must be a request sent by the roaming network server for a corresponding, 'allow the user' radius reply from the home server. One could think of using the user's IP-address as his current identity i.e., when the user chooses his home operator in the operator's list page a RADIUS request with the IP-address of the user as the username can be sent simultaneously with a redirection message to the home network. This is not practical in today's world where the users are often behind NAT or NAPT, thus the same IP address is used for many users. Use of two logins would solve the problem. In the first login the user is authenticated against the home server, and a page displaying a one time username and password is sent securely over the SSL tunnel which the user uses to login to the roaming server and normal radius transaction continues. However, such a design is not usually used, as the roaming networks are trusted). After a successful login, the Home operator's RADIUS server would send the 'successfully authenticated' message and appropriate authorization attributes, based on which the user is provided with the appropriate access e.g., to the internet. The RADIUS servers in the Operator and home network can start their accounting process once the user is authenticated. To avoid inappropriate accounting by the roaming network for long time, it is suggested to re-authenticate the user after a certain period of time at the home network if an authentication scheme which doesn't require handing over the user credentials to the roaming network such as EAP-TLS is used. Figure 9. shows EAP-TLS/TTLS based authentication process.

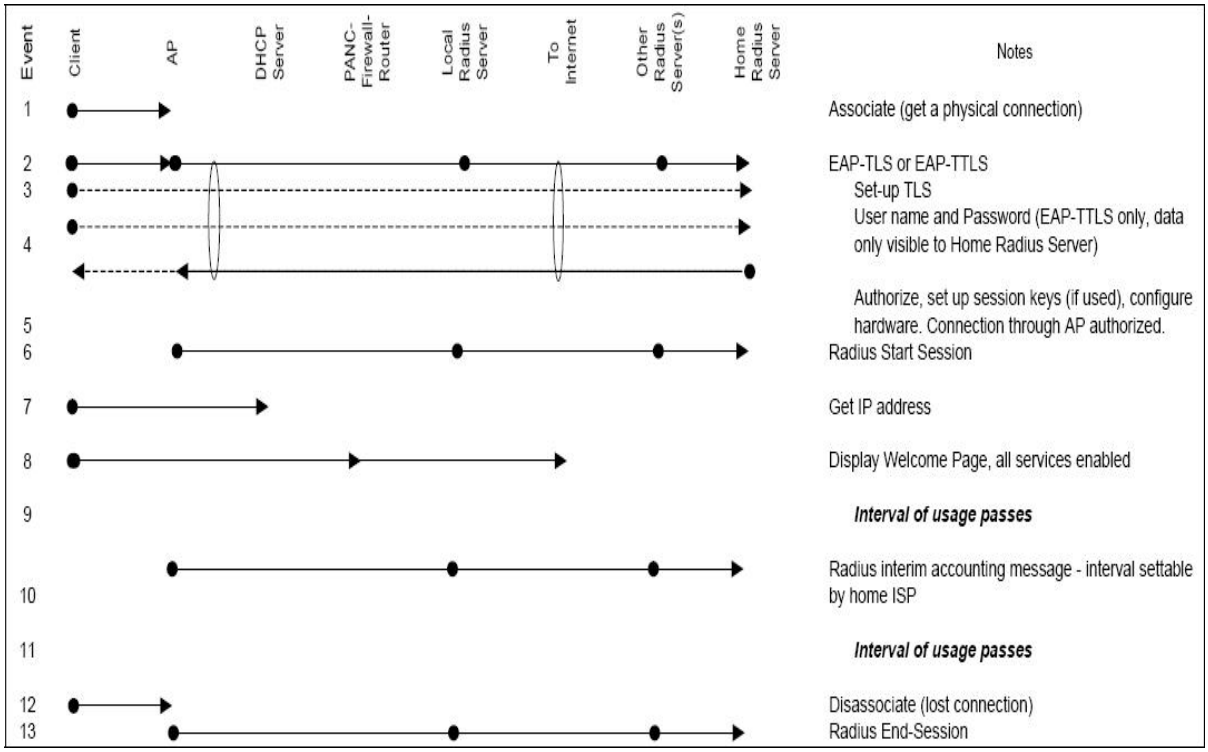

Figure 9. EAP-TLS/TTLS implementation

4.12.5 Authorization

WISPr [22] specifies various RADIUS authorization attributes that can be used by a WLAN operator in performing authorization functions. Vendor specific attributes can be used for custom attributes.

4.12.6 Accounting

WISPr [22] specifies various RADIUS accounting attributes that can be used by a WLAN operator in performing accounting functions. Vendor specific attributes can be used for custom attributes. The accounting requirements depend on the billing system used.

There could be several likely cases of billing between home operator-user, roaming operator-home operator.
Home operator to user:
The Home operator can charge the user in one of the following ways:

1. Based on the duration that the user is logged in
2. Based on the amount of data transferred to/from the client
3. Unlimited subscription (during a period, e.g., a month)
4. No charge (for e.g., home operator could be a corporate operating network for their staff).

Roaming operator to user's home operator

a. Based on the duration that the user is logged in to the roaming network
b. Based on the amount of data transferred to/from the client
c. Fixed charge.

Other billing systems are feasible, for e.g., the roaming operator could charge based on the number of times a specific home operator's users have logged in. I assume such billing schemes are very unlikely and thus do not consider them further.

Among the above cases all the combinations except 3-c and 4-c require detailed accounting. These cases, 3-c and 4-c don't require accounting and thus eliminate the related costs. The user only needs to be authenticated (to be provided access). There are two solutions that fit for all the remaining cases. Below I describe the solution and the solutions are mapped to the particular case in Table

Solution-1 (S1):

When the user credentials are passed to the roaming operator during the authentication process it is hard to ensure proper accounting if the roaming operator is not be a trusted party. If the authentication is done based on temporary credentials which are different each time the user authenticates e.g., one-time passwords, the user can be provided with a logout option (e.g., a hyperlink); when the user uses the option he could be redirected to the home operators logout webpage and at the same time the RADIUS server at the home operator can send the corresponding logout message for accounting purposes. The home operator's corresponding page would contain a message stating that the user is logged out. This method is not fool proof. The Home operator only knows that 'some' user logged out but should rely on the accounting information provided by the roaming operator to identify the user (for the user billing by the Home operator). But, this shouldn't be problem as it is very unlikely that a roaming operator would change one user to another while sending the accounting credentials to the Home operators RADIUS server.
If the credentials used during authentication can be reused (sufficient for successfully authenticating the user) then the authentication should be between the user and the home operator. This could be done through the use of EAP-TTLS or EAP-TLS. When this is used the user should be provided with the logout option as described above.

Solution-2 (S2):

There could be client side software which monitors the upload and download of data

during a session (between a login and a logout). When the user logs out the roaming operators RADIS server informs the user's data transfer details to the Home operator's RADIUS server. The client side software can at logout phase securely inform the data transfer details of that particular session to the server which resides at the Home operator's network.

One other option is to tunnel all the data destined to the client through the Home operator. This could for example be the case if the home operator offers VPN service and the users must access any source of information only through the VPN or the home operator is providing Mobile IP service and the user receives or sends data only through the home agent (i.e. always uses Mobile IP). Here both the network operators know the usage in real-time and can exchange and agree upon that information. Perhaps VPN server/Mobile IP Home Agent and radius server which can exchange such usage information with each other is to be custom built to meet this requirement.

Charging based on data transferred is expensive as it needs custom built software. The benefit of choosing this option must be weighed against the costs involved to implement this. The link speeds (between the client and AP) are high and WLAN infrastructure cost is not too high so charging based on this option is in most cases not required to make good profits.

Table 2. Accounting solutions

Case	1	2	3	4
a	S1	S2	S1	S1
b	S2	S2	S2	S2
c	S1	S2	NA	NA

NA: No accounting is needed. This saves the costs of implementing proper accounting

Chapter 5

Network Layer Mobility

The addressing scheme used by IP (both v4 &v6) to locate the end point where the node is attached is hierarchical. The interface's (IP) address is based on the network to which a node is attached. These networks have relatively stable addresses through which packets are routed by routers. So, if a node moves from one network to another it has to get a new IP address relevant its new network attachment point. The transport mechanism used for communications between applications running on two different nodes in the Internet rely on the IP address of the node (along with the port number related to the application) to deliver messages to the application[4]. So each particular communication session is valid only as long as the IP addresses of the nodes remains the same as used during connection establishment. As soon as a node's IP address changes the communication link is broken. A new communication link needs to be setup with the new address(s) of the node(s). Such a broken link may end the application session. Most applications need to be restarted to re-access the service. Although there was widespread use of portable computers that are capable of connecting to the various networks, they were mostly used for portable computing (i.e. restarting the applications at the new point of attachment). WLANs along with other emerging high-speed wireless data technologies have provide a means of being connected to networks 'on the move'. Proliferation of these technologies has driven the demand for mobile computing (i.e., applications running even while the nodes are changing their point of attachment). The IETF working group "IP Routing for Wireless/Mobile Hosts (mobileip)" [84] has been the key standardization body working to provide the technical means for enabling mobile computing within the frame work of IP, thus ensuring no changes to the existing IP infrastructure (routers, non-mobile nodes, etc.) were needed. Mobility in both IPv4 and IPv6 are addressed by the resulting standards [38] [39].

Several ideas [85, 86, 87] were proposed for addressing this problem. Most of the ideas are similar concerning the layer they chose for addressing the issue of mobility, the network layer (layer 3) [5]. Also, most of these ideas used basically two IP addresses for the mobile client; one that would be constant and the other IP address reflects the node's current point of attachment. There were also other proposals. Douglas E Comer et al. proposed using ATM as backbone technology in providing wireless access to mobile users in a large university campus [60]. The architecture proposes transparency of movement of node from one AP to another AP by using same Layer2 address for the APs from the nodes' perspective. The backbone can differentiate between two AP's by their distinct Layer2 address on the wired interface. The APs have to operate in the same channel. The advantages include near zero handoff delay. The downside is inefficient use of available bandwidth. A complete treatment of the topic can be found in [88, 89]. IP Mobility Support for IPv4 [38] is

---

[4] It is to be noted that in TCP/IP, nodes usually do not have any globally unique identity based upon which messages can be routed (although nodes can have fully qualified domain names they are not suitable for mobile clients as implementing highly dynamic DNS updates is not feasible for a network of computers of Internet scale) besides their attachment point address so the applications send messages using the attachment point address. This architecture was suitable in the early days of computing where the nodes were mostly non-mobile, thus allowing reuse of the attachment address as node's identity. In today's computing world, nodes are increasingly mobile leading to a paradigm shift. The IETF working group **"Host Identity Protocol (hip)"** is looking at ways of separating the location information from host identity.

[5] Lately, proposals were made for enabling mobility by addressing it at the application layer [http://www.ietf.org/html.charters/sip-charter.html]

the latest standard as of this writing to provide IP layer mobility in IPv4 networks. The Applicability of IP Mobility Support can be found in [90].

5.1 Basic Architecture

Figure 11 shows a mobile node (MN) communicating with the corresponding node (CN) while the MN is in the Home Network. Figure 12 shows the MN communicating with the CN through the Foreign Agent (FA). This figure illustrates the basic operation of Mobile IP for an IPv4 network. There are three main actors: MN, Foreign Agent (FA), CN (note that the CN need not be aware of Mobile IP on the MN side)

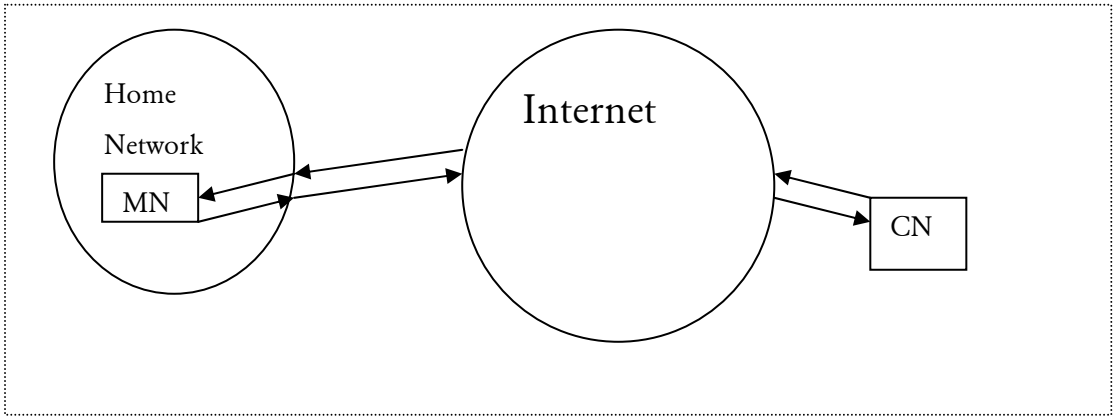

Figure 10. MN connected to its home network, communicating to the CN

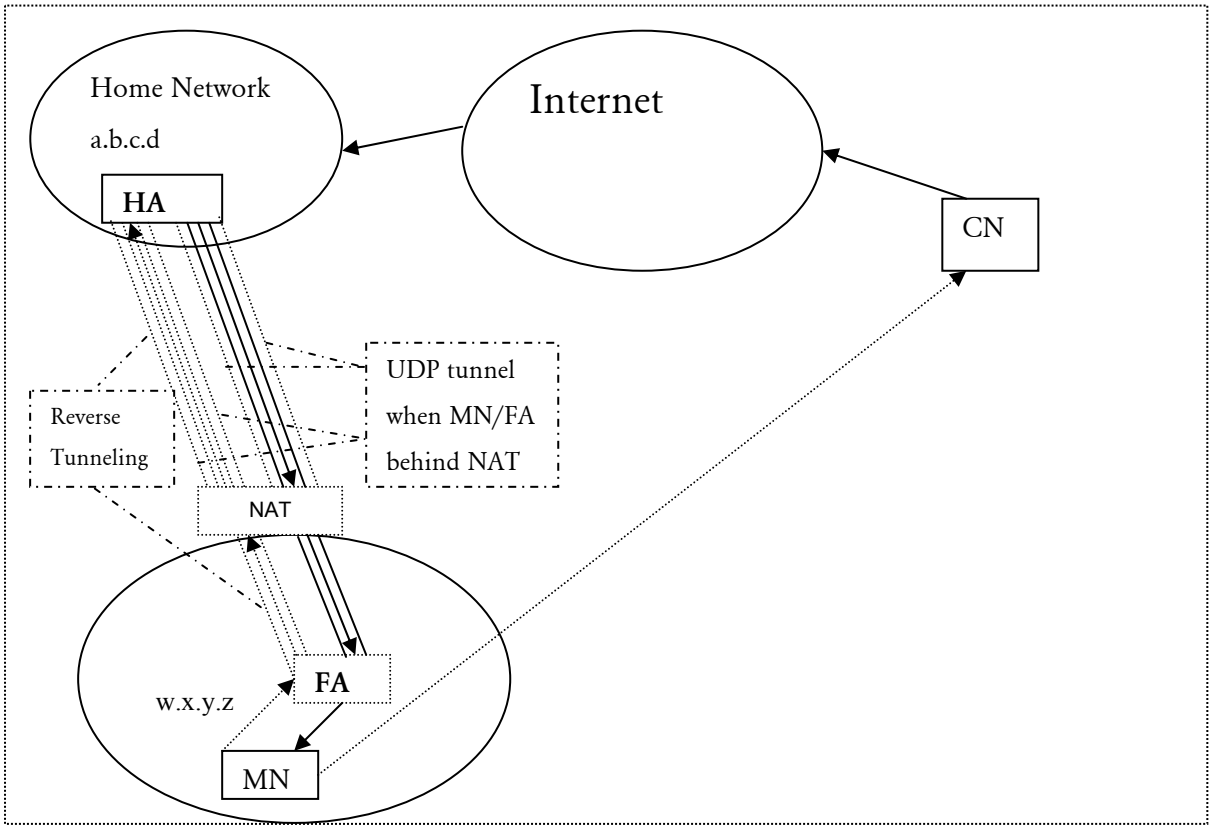

Figure 11. MN connecting via the foreign network, communicating with a CN through its HA.

Mobile Node (MN): This node can change its point of attachment to the Internet while maintaining its application layer connections. It has two addresses: a Home address that is constant and a care of address (CoA) that reflects its current point of attachment.

Corresponding Node (CN): This node is communicating with the MN. The CN could also be mobile; in that case it too should implement Mobile IP making its movement transparent to both the MN and MN's Home Agent (HA).

Home Agent (HA): This node (acts as a router) in the home network of the MN. It intercepts packets intended for the MN's home address. It too might be mobile in which case it would in turn have its own HA. To keep things simple we will assume that it has a fixed IP address.

Foreign Agent (FA): The Foreign Agent delivers packets in the foreign (visited) network to the MN. This function can be collocated within the MN.

5.2 ICMP Router advertisements/solicitation

Mobility agents (HA, FA) are configured to send advertisements indicating their presence and the availability of their service to the nodes in their network. These advertisements are ICMP router advertisements [91] extended to also carry a Mobility Agent Advertisement Extension and, optionally, a Prefix-Lengths Extension, and One-byte Padding Extension. These advertisements include the period (lifetime) for which the agent is willing to accept a registration request

5.3 Dynamic discovery of Home Agents

The MN should know the address of its own HA in order to register. If it doesn't know this address, a subnet directed broadcast address is used in place of the address of the HA. The HA then MUST reject the mobile node's registration and SHOULD return a rejection. The MN can use the source address of the rejection as the address of the Home Agent. Some routers change the subnet directed broadcast address to 255.255.255.255 before injecting them into a particular subnet. So, the Home Agents must be prepared to respond similarly to this address too.

5.4 Mobile IP Network Access Identifier Extension for IPv4

Mobile nodes must posses some identification information which can be used by the HA to perform authentication of registration messages (select the corresponding Security Parameter Index (SPI)). Clients are usually identified by their NAI [71], rather than by some other means (e.g., Home Address in the case of MN. Calhoun and Perkins [92] specify how such an NAI can be included in registration requests by the MN, when such an NAI is used, the Home Address field can be set to zero, the registration reply from the HA will then include the Home Address. To enable redundancy it is usual to include several Home Agents and AAA servers in the Home network. In such a case, the MN should specify to the Foreign Agent, to which AAA server in its Home network it would authenticate to. Also, the AAA server would have to be informed about the Home Agent the MN was previously bound to. Johansson and Johansson [93] specify how the NAI of these entities (AAA server, HA) is to be specified and dealt with.

5.5 Proxy and Gratuitous ARP

A link layer address is used to deliver packets to a node in its subnet. ARP is used to resolve the link layer address given the IP address of a node. A mobile node can not reply to ARP requests corresponding to its Home address when it is away from home, as these datagrams should

be delivered to the Home Agent so that the home agent can relay these packets to the mobile node's current location. To facilitate the above Proxy ARP and Gratuitous ARP are used. When a Mobile Node moves away from its home network and registers with the Home Agent, the Home Agent sends a Gratuitous ARP, which would be based on either an ARP request or reply messages. When a HA accepts registration of a mobile node which is away from the home network it sends a Gratuitous ARP, in which it sets the Sender and Target IP address to be the Home address of the mobile node and the Hardware address is set as the Hardware address of the Home Agent. In an ARP reply message the Target Hardware address is set to the link layer address of the Home Agent. These messages will cause the other nodes on this subnet update their ARP cache. When a node sends an ARP request corresponding to the IP address of the mobile node with is registered with the Home Agent and the mobile node is away from home, then the Home Agent will send an ARP reply with its own Hardware Address as the Hardware Address corresponding to the mobile node's IP address. This is known as Proxy ARP.

5.6 Network Address Translator (NAT)

As noted earlier, in IPv4 networks there is scarcity of Internet routable IP addresses. This has prompted network operators to use one of the private address pool specified in [94]. As these addresses can only be used internal to a routing domain these addresses can be used in many different routing domains. Such networks have Network Address Translators (NATs) [95] in between this private domain and the Internet so that the packets sent from nodes having a private address can be mapped to an Internet routable address. NATs perform mapping of these addresses in several ways. Hodrege et al. [96] describe the basic concepts related to NATs and various flavors of NATs.

5.7 Mobile IP traversal of NAT

A mobile IP packet is sent from the Home Agent encapsulated in another IP packet directly to the Mobile Node or indirectly via a Foreign Agent. This encapsulation hides the transport layer header as the next header following the new IP header is not a transport layer header, but rather an IP header in the case of IP-in-IP encapsulation, a Minimal Forwarding header in Minimal encapsulation, or a GRE header in the case of Generic Routing Encapsulation. However, NATs often use the transport layer header (to identify a session which is used as a key to its address and port mapping) to perform mapping of the address corresponding to a MN inside its network. If the MN/FA are behind an NAT[6], then the NAT will not be able to map the packet it received to the MN/FA inside its network. In this case Mobile IP doesn't work. To solve this problem, the tunneled packet is provided with a UDP header following the outer IP header to keep the tunneling transparent to the NAT. The Mobile IP Tunnel Data message header is also appended between the UDP header and inner IP header. This is used to differentiate the traffic using the UDP header (registration requests and replies are sent through the well known port 434) from encapsulated/decapsulated traffic. The packet is as shown below when IP in UDP encapsulation is used

Outer IP header	Outer IP header
IP header	UDP header
IP payload	MIP Tunnel Data Message Header
	IP header
	IP payload
MN/FA not behind NAT	MN/FA behind NAT

[6] There could also be more than one NAT, chained before the MN; however it doesn't make any substantial difference in the problem.

Other encapsulations such as Minimal encapsulation [112] and GRE [113] are done similarly. Reverse tunneling is performed similarly. In all these a UDP header (8 bytes) and a MIP Tunnel Data message header (4 bytes) add to the overhead. [97] specifies Mobile IP NAT traversal.

A new extension is defined for expressing the MN's UDP tunneling capabilities and requirements during registration with the HA. The extension (specified in section 3.1 [97]) is shown below:

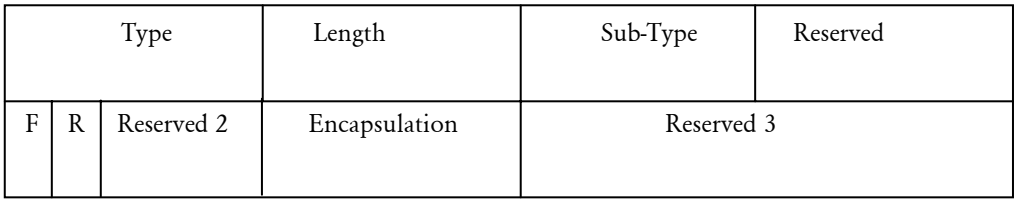

Figure 12. IP-in-UDP encapsulation

This RFC also specifies a UDP Tunnel reply extension (specified in section 3.2 of [97]) as below

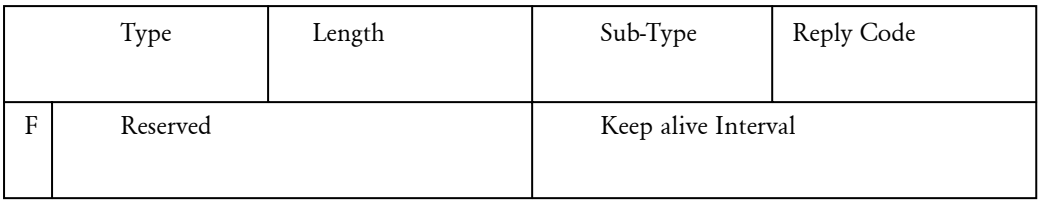

Figure 13. UDP Tunnel reply extension

There could also be a NAT before the CN, but this does not effect the mobile IP signaling. RFC 3519 [97] addresses NAT traversal of MoblieIP, but only when the MN/FA is behind NAT, not when the HA is behind NAT. However, it provides a means of placing an HA behind a NAT following some configuration as described next.

The HA could be behind a NAT, but in this case the NAT before the HA should use a public IP address and port 434 for the HA at all times so that the MN/FA can send registration requests to that address and port (i.e., using static port forwarding). Additionally, the MN/FA MUST always specify in its registration request, its capability to handle UDP tunneling by including the UDP tunnel request extension type: 144. If the HA detects that either the MN is behind a NAT (e.g. Presence behind NAT is detected when there is a mismatch in source address in outer IP header of the registration request packet and a care of address/co-located care of address field) or itself is behind a NAT, it should send a registration reply with UDP tunneling extension type: 44 whenever the request from MN/FA contains the UDP tunneling extension otherwise mobile IP wouldn't work.

5.7.1 Security considerations in UDP tunneling

Several security problems concerning traffic redirection exist when using UDP tunneling. The source address field in a UDP tunneled packet is filled by the NAT, thus it cannot be used in calculating an authentication extension and thus an intruder can use this for re-direction attacks. Using a low re-registration lifetime is suggested to reduce the redirection period. Although redirection of traffic cannot be prevented, the confidentiality of hijacked data can be achieved by using some data protection mechanism (e.g. IPsec).

Chapter 6

Mobile VPN

In the highly competitive business world the workforce increasingly needs to access data anytime, anywhere in order to improve competitiveness and hopefully revenues. However, access to the corporate data from outside the corporate intranet poses threats due to the risk of exposing valuable corporate data, since the channel often used by remote workers to reach corporate data is a public network such as Internet. Since by default IPv4 doesn't provide any security service, the data should be accessed by establishing a secure channel, e.g., by a Virtual Private Network. VPNs have enjoyed great success in providing location flexibility for the workforce while still enabling them to access corporate data.

6.1 Security services at various layers

VPNs can be of several types based on the technology used. Security can be provided at several layers of the protocol stack. The sections below introduce some of the types of widely used VPNs.

6.1.1 Link layer

Link layer encryption provides security for passing data across the link. At each link the data is decrypted and then encrypted before forwarding over the next link. Link by link encryption is not useful for remote users to access their corporate network, as it is not feasible nor in most cases it is economically reasonable to establish their own links and secure those link nodes. However, PPTP [98] and L2TP [99] are widely used VPN technologies that provide security at layer 2. These protocols treat the underlying links as just a single bit pipe hence they can provide end-to-end encryption.

6.1.2 Layer3

IPsec [100] provides security at the IP layer. IPsec provides access control, connectionless integrity, data origin authentication, limited protection against replays, confidentiality (encryption), and limited traffic flow confidentiality. In the following text the term VPN is used for IPsec VPN. IPsec provides security services through two protocols: Authentication Header (AH) [101] and Encapsulation Security Payload (ESP) [102]. Their usage is illustrated below (when ESP is used the Transport Layer header and Application layer header are encrypted as shown in field with diagonal line).

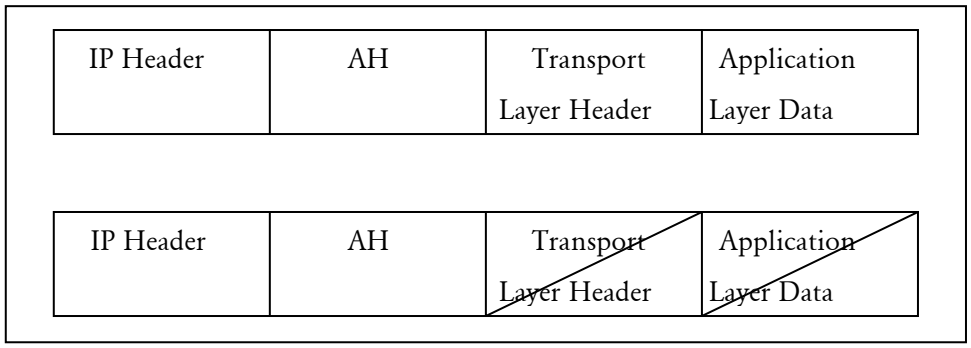

Figure 14. Transport mode (the fields with diagonal line represents encrypted fields)

Using AH provides connectionless integrity, data origin authentication, and an optional anti-replay service as specified in [101]. The AH is placed between the original IP header and the IP payload. While ESP provides all of these services along with data confidentiality (encryption) and limited traffic flow confidentiality as specified in [102]. For a VPN at least one of these header services is to be provided. This mode is called transport mode. The above mode of operation leaves the IP header exposed. If it is desirable to provide security (confidentiality and/or Integrity) to this header, or because it is convenient (e.g., in many situations where the VPN connection of the client is to a VPN Gateway sitting at the edge of corporate network) then the entire IP packet is encapsulated as the payload of another IP packet that contains the destination address of the VPN gateway. This is shown below. This mode of operation is called tunnel mode.

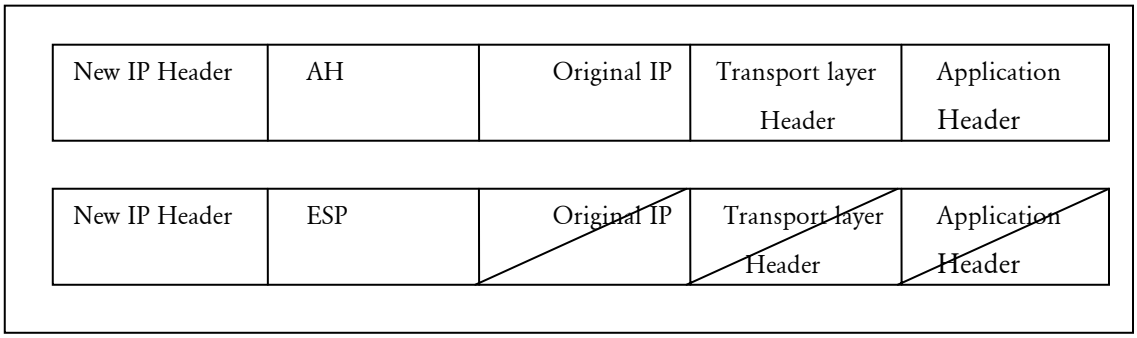

Figure 15. Tunnel mode (the fields with diagonal lines represent encrypted fields)

AH and ESP use both encryption and hashing algorithms to protect the data. Therefore before a VPN connection can be setup between two hosts they must agree upon the algorithms to be used and securely exchange the keys to be used with these algorithms. IKE [103] provides the framework for this key exchange.

A host might have VPN connections to several other hosts (or a security gateway) and a host need not require or use same security service and set of algorithms and keys for all these hosts. In fact, a host should use different security parameters for each of the several higher layer connections even while communicating with one host. This per host and per port security is provided through the concept of a "Security Association". Each "Security Association" is unidirectional and provides security services through AH or ESP (but not both). If both are to be provided for a communication, then two (or more) separate security associations are used. A security association is uniquely identified by a triple consisting of a Security Parameter Index (SPI), an IP Destination Address, and a security protocol (AH or ESP) identifier. There are two types of Security Associations: Transport mode and Tunnel mode (as explained above). A given communication might require a combination of AH and ESP services. In such a case the SAs are combined. Sections 4.3 and 4.5 of [95] describe several combinations that can be used; the document also describes the management of SAs along with other issues.

6.2 Mobile VPN architectures

Secure seamless access to data can be provided in several ways. However, there are two services to be provided: mobility and security. Not surprisingly there are many alternatives that have been proposed.

6.2.1 Proprietary bundling of Mobility and Security

There could be proprietary bundling of mobility and security as shown in figure 14. In this approach a server maintains the sessions for the mobile node and relays the data to its current

point of attachment using existing standards [38] or some proprietary protocol to provide mobility. The data could be encapsulated in several ways, based on standards e.g. [113] or in some other way e.g., via UDP/TCP encapsulation. The security can be provided at one of several possible layers layer-2, layer-3, layer-4 and higher layers. This approach is illustrated with two examples of commercial products.

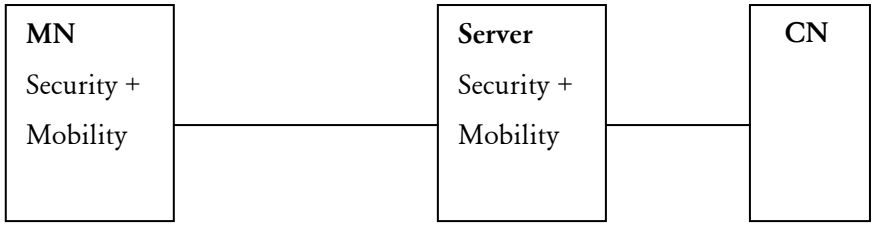

Figure 16. Security and Mobility bundled

6.2.1.1 Commercial Products

6.2.1.1.1 Columbitech

Columbitech utilize two key components: client side software and a server machine. Additionally there is an optional software component used for managing the servers, client configuration distributions etc. In their approach security is provided by Wireless Transport Layer Security (WTLS).

The Server acts as a relay point working at layer 4 (transport layer) for the client, i.e., when a client tries to open a port for a connection to CN, a port is opened at the server for making a connection to the CN, so the connection is now between CN and the server. The data received by the server on this port from the CN is sent to the client through TCP encapsulation. The software at the client side decapsulates the data and provides it to the application as if the data has arrived from the CN. While mobility is provided by TCP encapsulation the vendor claims that they address TCP's performance problem over wireless networks at the client side by continuously monitoring the current round-trip time in order to dynamically configure the TCP buffers for optimal transmission performance [104].

The advantages of the product are the use of transport layer security, which has the advantage that it works across NATs without increasing overhead. They implement compression above transport layer when there are recurrent patterns of data thus providing a better compression rates than attempting to apply compression at lower layers. The per-packet overhead is less than IPsec + Mobile IP (more on this calculation later). They provide connection persistence even when the client connectivity is lost for a while as the actual communication socket connects the CN and the server. They can improve performance of handoffs due to store and forward mechanism at the server. The disadvantages of this solution are that, it is not based on standardized products, thus it locks customers to their products. If an IPsec infrastructure is already in use then the solution doesn't make use of this existing infrastructure. There can be unnecessary retransmissions of data that should be dropped. This is because the solution bundles the data intended for the MN into a TCP packet even if the data belongs to a UDP connection (from the MN-CN perspective). Often a delayed packet belonging to this connection should be dropped rather than wasting resources retransmitting it (thus also adding unnecessary delay). Connection persistence is not always desired: e.g., it might be desirable for the application at CN to know that the MN is no longer reachable.

However, the server tries to maintain all the connections when the MN looses its connection to server.

6.2.1.1.2 Netmotion Wireless

This solution consists of two key components: client side software and server side software; along with an optional 'Policy management module', which can be installed on the server. In this approach security is provided through Roamable IPsec™. The vendor claims that an existing security infrastructure can be used, but it doesn't seem to work with existing IPsec infrastructure.

Mobility is provided by encapsulating the 'application data' into UDP packets. The product description seems to indicate that these packets are acknowledged. The server tries to maintain sessions with Corresponding Nodes by acknowledging packets when the client is unreachable for some time. The advantages and disadvantages of this product are more or less the same as with Columbitech. e.g., both provide data compression. The difference between the products is in the tunnelling they use. Columbitech uses TCP tunnelling while Netmotion uses UDP tunnelling.

6.2.2 IPsec + Mobile IP

IPsec based VPNs have been successful in the corporate world and are widely deployed. IPsec is more suitable for remote workers than mobile workers (i.e., workers who would like to access data 'on the move') as a mobile worker would usually pass through several sub-networks, each change in IP address would cause a new key exchange if IPsec is outside the Mobile IP header. This occurs because the VPNs SA is identified by the triple: Security Parameter Index, IP destination address, Security Protocol. So, when there is change in IP address of the associated node a new SA has to be established. This is time and resource consuming. However, IPsec facilitates smooth operation of the SA when a node changes its IP address. This support is provided when a node is behind a NAT and the NAT changes the address of the node before a session is broken. In such a case the node, which is not behind NAT, would use the last valid authenticated packet from the outer interface to determine which IP and port addresses should be used. So, when the node moves within the domain of an NAT, this can be used. Additionally, the presence of NAT can be emulated when the node is not behind a NAT. Here UDP tunnelling must be used even when the node is not behind a NAT. When this is not used, the time to re-establish the connection is often long enough to disrupt some applications and also some security policies require manual intervention (e.g., entering a key) before renegotiation of keys.

There were proposals for updating the SA when the node gets a new IP address. Byoung et al. [105] suggest using an update message to be sent to the VPN gateway whenever the MN moves to a new location and gets a new IP address. This would reduce the need for re-establishing the SA(s) whenever the MN moves to a new location. The scenario is illustrated in Figure 15 below.

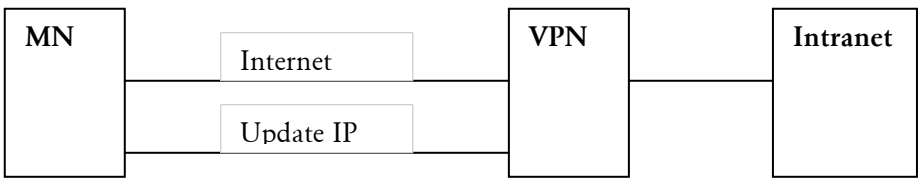

Figure 17. VPN Gateway enabling fast mobility

There are products in which a properly authenticated inbound packet received by the stationary peer causes the corresponding destination address (mobile peer care-of address) to be updated from the received packet. Though this allows for mobility without signalling it has some traffic redirection vulnerabilities [23].

IETF working group "IKEv2 Mobility and Multihoming (mobike)" is looking into ways to update SA when there is change in a node's IP address. MobileIPv4 is the proposed standard for solving the mobility problem in IPv4 based networks. The problem of security and mobility is solved as long as the communication is between a Home Agent (HA) and Mobile Node (MN). But communication occurs through a VPN.

There are several ways in which the Mobile IP and VPN could coexist. The problems of their coexistence and possible deployment scenarios are discussed in [23]. The following are the possible co-existence scenarios (many of the scenarios given are from [23], they illustrate the wide variety of potential situations. In each the environment consists of a Mobile Node (MN), which would either be inside the Intranet or outside of it. It is assumed that the MN requires mobility both inside and outside this Intranet. A VPN gateway is at the edge of the intranet.

6.2.2.1 Mobility outside the intranet

When mobility is not required inside the Intranet, the setup would be:

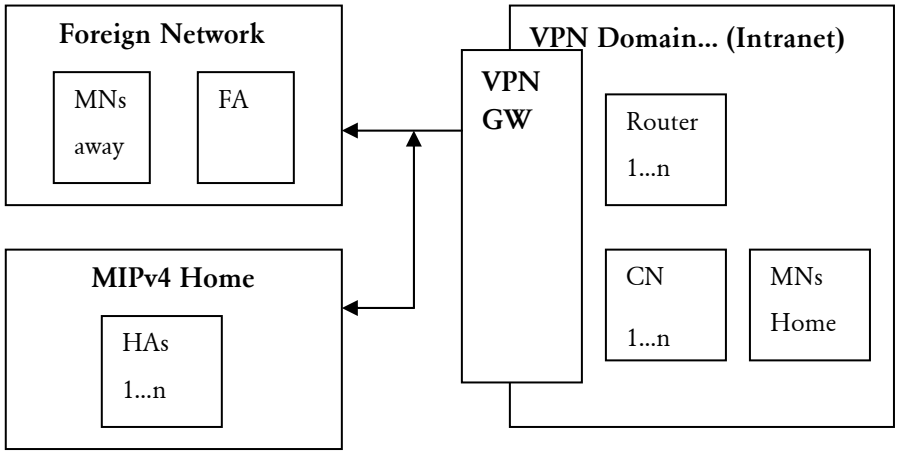

Figure 18. Mobility only outside the Intranet

This configuration could also be used when mobility is desired within the Intranet. Here a VPN tunnel is used between the Home Agent of MN and the VPN Gateway. Since the home address is stable there is no need to establish a new SA when the MN is assigned a new IP address.
The packet overhead can be computed for two cases:
When MN is not behind NAT, IP in IP encapsulation is used in Mobile IP, IPsec Tunnel mode with ESP with Authentication, for a cipher with 128-bit block e.g. AES, and worst case padding (padding could be greater if traffic flow confidentiality is desired)

IPv4 header + IP header Security protocol header(s)
= (20 bytes for new IP header)
+ (20bytes for new IP header
+ 4+4+16 bytes for SPI, sequence number, cipher initialization vector
+ 15+1+1 bytes for padding, padding length field, next header field
+ Authentication data depending on the algorithm used, 12 bytes for HMAC-MD5-96 or HMAC-SHA1-96)
= 93 bytes

When MN is behind NAT and another NAT sits between HA and VPN, there is additional overhead
UDP encapsulation for MIP
= 8 bytes of UDP header
+ 4 bytes of MIP tunnel data message header
= 12 bytes
UDP encapsulation of IPsec (work in progress)
= 8 bytes of UDP header
The total overhead in this case is 93 + 12+8 = 113 bytes

When mobility is desired both in the Intranet and outside, there could be several configurations described in the following sections

6.2.2.2 VPN Gateway at the edge of the Intranet

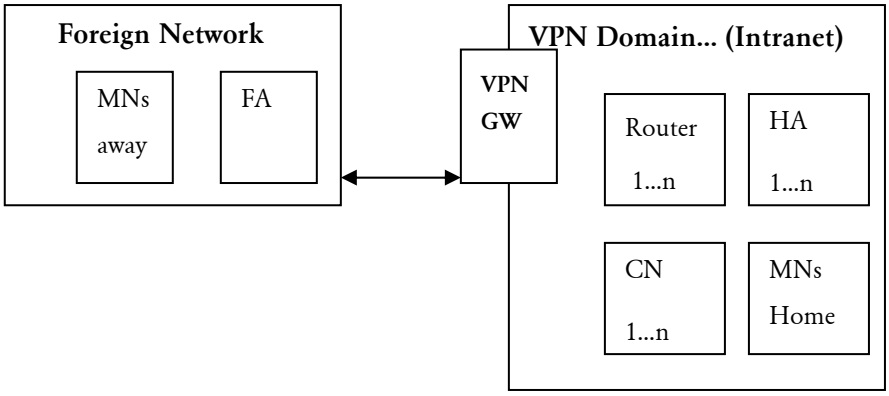

Figure 19. VPN Gateway at the edge of the Intranet

A VPN tunnel is formed through Security Associations (SA). When the destination IP address changes the SA would not be found in the Security Association Database (SAD) and the SA is to be re-established which is computationally intensive, hence time consuming. The application connections could be lost or some latency sensitive applications might suffer due to delay introduced during this re-negotiation. A Mobile IP HA can be added behind the VPN gateway for nodes requiring mobility support transparent to applications. Such a HA would also provide mobility to nodes moving inside the intranet and the internal traffic need not pass through the VPN. Unfortunately, there is no standardization for updating the nodes SA. However the IETF working group "IKEv2 Mobility and Multihoming (mobike)" is looking at ways to update SA when there is change in a node's IP address.
The Overhead is same as in section 5.2.2.1

6.2.2.3 VPN and HA co-located at the edge of the Intranet

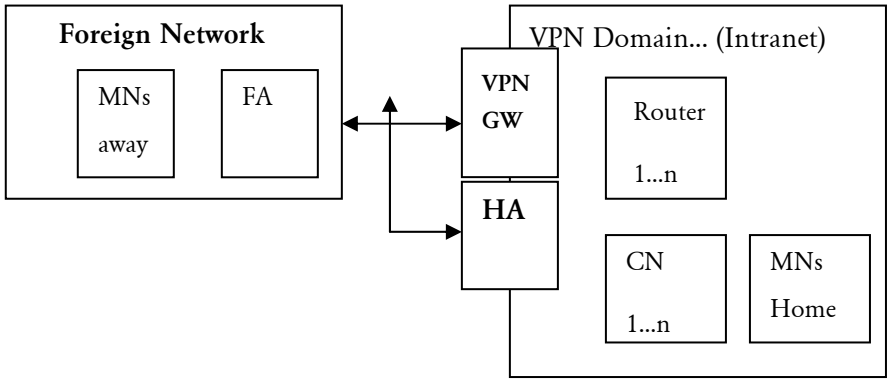

Figure 20. VPN and HA co-located at the edge of the Intranet

Here the combination could work either via a VPN tunnel inside a Mobile IP tunnel or a Mobile IP tunnel inside a VPN tunnel. The later has the problem of establishing a new SA when the MN is assigned a new IP address. So, the former, a VPN tunnel inside Mobile IP should be considered. Here the SA is between the VPN gateway and the MN using the MN's Home address. In this configuration, traffic needs to be routed either through the VPN or directly depending on the current location of the MN. However, the CN doesn't know this location (After all, the purpose of Mobile IP is to keep such changes transparent to CN). If the MN is inside the intranet the data would be sent without passing through the VPN. If the MN is outside the intranet then the traffic arriving at the HA for MN must be tunneled through VPN. This could be done in several ways, involving modifications to routing at the HA or VPN gateway, e.g., when the MN is outside the Intranet and the packet received is not through the VPN gateway, then the HA can forward the packet to the VPN gateway which would then tunnel it to the mobile nodes Home agent. Then the HA would tunnel it through Mobile IP and thus forward to the MN's current point of attachment.

The firewall at the outer edge of the intranet should be configured to allow incoming packets from:

i. Registration request addressed to the HA
ii. VPN tunneled packets which are in turn tunneled through to the HA
iii. VPN tunnel establishment packets sent through the HA

Outgoing packets, which are:

i. Registration replies from the HA
ii. VPN tunneled packets sent through the HA
iii. VPN tunnel establishment packets sent through the HA

The overhead is the same as in section 5.2.2.1

6.2.2.4 Combined VPN Gateway and Mobile IPv4 HA

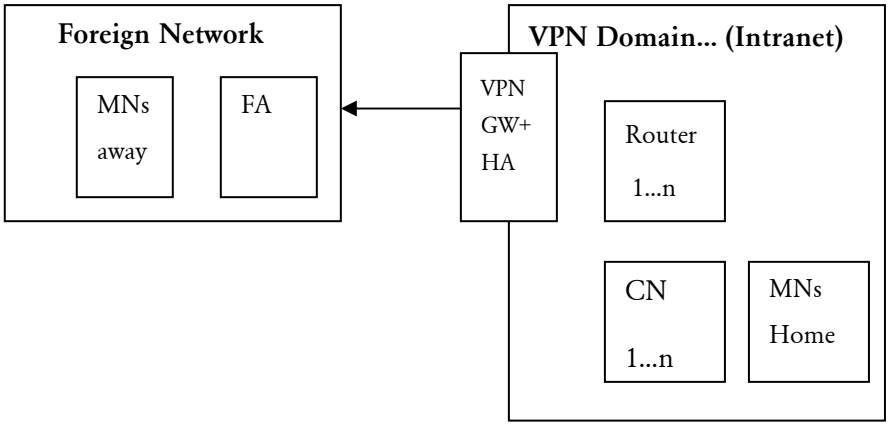

Figure 21. Combined VPN Gateway and Mobile IPv4 HA

This scenario is similar to the above scenario, with the advantage that there is no need for special routing. The drawback is that both VPN and HA are bundled in a single product, which doesn't allow the flexibility of choosing products from different vendors. Examples of products using this approach are given below.

Packet overhead:

Same as in section 7.2.2.1 except that there would be no NAT between VPN and HA thus overhead in that case would be 93 bytes + 12 bytes= 105 bytes.

6.2.2.4.1 IPunplugged

"Mobile VPN" from IPUnplugged [106] uses client software implementing MobileIP and IPsec. The server side consists of a Roaming Gateway which is both VPN and HA. There is an optional software component called Roaming Server that is useful in managing Roaming Gateways and clients distributing configuration files to the clients, which eliminates the need for manual configuration of each client. The Roaming server has RADIUS server component that provides AAA capability. The Roaming Gateway acts as Radius client.

An advantage of this product is its interoperability with third party Mobile IP products. However there is no such interoperability with third party VPN products, although the Roaming Gateway works with other VPN Gateways (e.g. site-to-site VPNs) with Open BSD Interoperability.

6.2.2.4.2 Netseal

MPN from Netseal [107] consists of client and server software. IPsec provides the security and MobileIPv4 provides mobility. No interoperability information was mentioned on their web.

6.2.2.5 Use of two Home Agents

In this scenario two Home Agents are used, one inside the Intranet and other outside the Intranet, VPN in between them. This configuration provides mobility both inside and outside the Intranet.

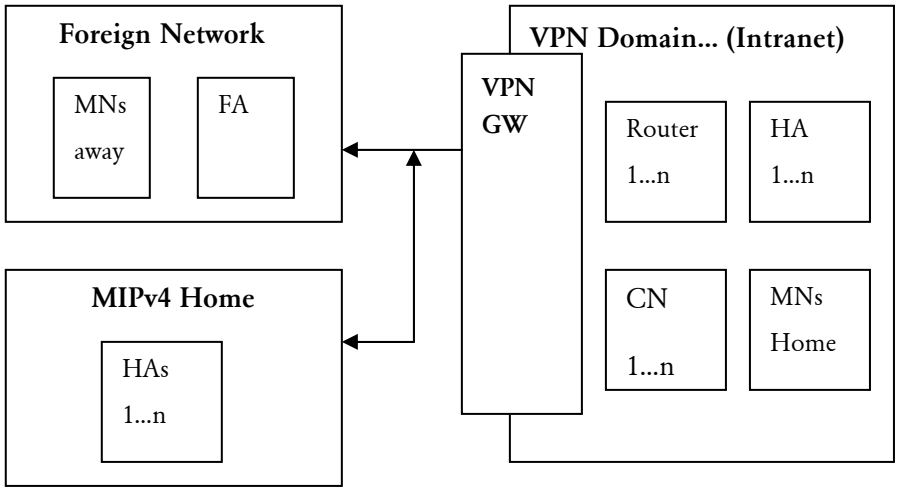

Figure 22. Use of two Home Agents

This solution works without any problems with existing Mobile IPv4 and IPsec VPN. The downside is that it would introduce one more tunnel, thus additional overhead. This solution is suitable for corporate environments where an investment has already been made in IPsec VPNs or Mobile IPv4. However, as noted due to repeated tunnelling the overhead affects the data transfer rates. Besides, this architecture contains two independent entities VPN infrastructure and MobileIP infrastructure and this increases management costs as the network scales. The advantage of this approach is that it requires only minimal changes in the existing VPNs or MobileIP. Furthermore, the changes are only required at the client.
There is a work in progress (proposed Internet draft) in IETF on providing standardisation of the client for the above environment [23]. The proposal discusses many issues including the secure detection of the internal network attachment along with performance issues among others.

There are two cases for calculating the packet overhead:

1) When the MN is not behind NAT and IP in IP encapsulation is used in Mobile IP, IPsec Tunnel mode, ESP with Authentication with a cipher with 128-bit blocks e.g. AES, worst case padding:
   IPv4 header + IP header Security protocol header(s) + IPv4 header
   = (20 bytes for new IP header)
   + (20bytes for new IP header
   + 4+4+16 bytes for SPI, sequence number, cipher initialization vector
   + 15+1+1 bytes for padding, padding length field, next header field
   + Authentication data depending on the algorithm used, 12 bytes for HMAC-MD5-96 or HMAC-SHA1-96) + 20

   = 113 bytes

2) When MN is behind NAT and another NAT sits between external HA - VPN, another NAT between VPN – Internal HA, overhead additional to the above
   UDP encapsulation for external HA MIP
   = 8 bytes of UDP header + 4 bytes of MIP tunnel data message header
   UDP encapsulation of IPsec (work in progress)
   = 8 bytes of UDP header
   UDP encapsulation for internal HA MIP
   = 8 bytes of UDP header

+ 4 bytes of MIP tunnel data message header

The total overhead is 113 + 12+ 8 + 12 bytes
= 145 bytes

Two examples of products using this approach are described in the next sections

6.2.2.5.1 Birdstep Technology

The 'Mobile IP' client from Birdstep Technology [108] claims to follow the above approach. They claim that their product works with standards based products (Mobile IPv4 & IPsec) from several vendors.

6.2.2.5.2 Secgo

Secgo claims that their 'Mobile IP' client and server (HA/FA) products are interoperable with VPN clients and HA/FA products from several other vendors [109]

6.3 Mobile VPN Solution Requirements

The City of Stockholm has a set of requirements to be met by a Mobile VPN solution.
The requirements are extracted from [110]

Summary of requirements

1. The VPN-system must use already existing authentication infrastructure (the ID-portal of the current Tacacs system)

2. The VPN-system must support authentication systems specified in [111].

3. The VPN-system must support using an external system for authorization data such as access rights and group assignment.

4. It would be suitable to use RADIUS/Tacacs or LDAP/LDAPS for authorization.

5. All events in the system that could have an effect on incoming or outgoing IP-traffic, such as logins and logouts, must be logged.

6. The log must clearly specify username for user-related events.

7. If any type of address translation or address assignment is used it must be clearly specified in the log files which IP-address that was assigned to which user at what time.

8. The IP-traffic between an end user device (PC) and the VPN-server must be protected by encryption.

9. The encryption used to protect the IP-traffic must be of sufficient strength to render it virtually impossible to decrypt the data without prior knowledge of the correct key.

10. The IP-traffic between the end user device (PC) and the VPN-server should use IPSec as VPN protocol.

11. The VPN-system must support some type of NAT-traversal.

12. The NAT-traversal should be UDP-encapsulated IPSec.

13. The VPN-system must support users of different groups that are logically separate from each other. No IP-traffic should pass between users of different groups.

14. The VPN-system must support sending traffic from different user groups to different local networks.

15. Groups and group assignment must be done using the authorization system.

16. User traffic must be delivered to the correct network using one of the techniques documented in [111] (separate ethernet interfaces, VLANs or MPLS).

17. All devices with the capability to remotely access the city network must be equipped with a personal firewall.

18. The personal firewall must be automatically activated at boot.

19. Normal users should not be able to disable the firewall.

20. When a user is connected to the internal city network, the firewall function should be disabled on the interface connected to the city network.

21. This (requirement 20) only applies to wired networking (Twisted Pair / TP).

22. The function that detect whether or not the user is on the internal network should not rely solely on the IP address.

23. The firewall function in the device must be active when the device is connected to an unknown network.

24. The rules for the firewall should be centrally administered.

25. The personal firewall must always be active on interfaces connected to external networks, especially if any other interface is connected to an internal network.

26. The personal firewall must not regulate traffic passing over the encrypted VPN-connection.

27. All mobile devices capable of remote access must be equipped with malicious code protection (antivirus).

28. The malicious code protection software must start automatically at boot.

29. It is preferable to use some type of anti-spyware software.

30. Selected anti-spyware and anti-virus software must support automatic updates of signature files.

31. In the event that a user has access to the Internet without activating the remote access, the antivirus software must be able to update its virus signature files over the Internet.

32. To protect sensitive data, all devices capable of remote access must be equipped with hard disk encryption software.

33. The encryption used to protect the hard disk must be of sufficient strength to render it virtually impossible to decrypt the data without prior knowledge of the correct key.

34. The software used for hard disk encryption must support some type of key escrow scheme.

35. All devices must be protected by a turn-on-password and a bios-setup-password.
36. At boot, and when a device returns from "suspension", the operating system must require the user to enter a username and a password.

37. All systems must have a password-protected screensaver or equivalent locking function.

38. It should be possible for the user to manually lock the device.

39. It must be possible for a user to log on to the device without access to the network.

40. The use of the remote access function must never require elevated privileges or "local admin".

41. The remote access service must be independent of IP-carrier (LAN, WLAN, GRPS and 3G).

42. The activation of remote access must be fully user initiated.

43. It must be clearly visible to the user when remote access is active.

44. The remote access connection must be automatically disconnected if the user is inactive.

45. When remote access is active, all traffic must go over the tunnel.

46. The VPN-client must never allow "split tunnelling"

47. A user connected to the internal network must never be dependent on the VPN-infrastructure.

48. It must be possible for a user to use the remote access service to access internal resources from any network within the city.

49. It would be appropriate if it were possible to active the remote access system even from the internal network.

50. The encryption software installed on mobile devices must protect configuration files and keys/fingerprints used by the VPN-client.

Besides the above requirements there are some additional general requirements as listed below:

51. The mobility part of the solution SHOULD be as compliant as possible with RFC3344. To that end,
    a. The client side software SHOULD work both with care of address and co-located care of address.
    b. There SHOULD be FA functionality.
    c. The HA/FA SHOULD be capable of sending agent advertisements.
    d. The client SHOULD be capable of sending advertisement solicitations.
    e. The Home address of the mobile node SHOULD be dynamically configurable.
    f. Reverse tunneling from mobile node to HA/FA MUST be supported.
    g. Mobile IP traversal of NAT device must be supported as specified in RFC3519 or later standards.

52. The HA/FA SHOULD be capable of working behind NAT.

53. The solution MUST securely detect existing connection to internal network. The amount of detection time of mobile nodes movement from internal network to external network MUST be at minimum so as to minimize the data sent unencrypted. This would not be difficult when data in all the wireless interfaces MUST always be tunnelled through VPN, as it only requires monitoring the wired connection to Intranet. It can take some time before the mobile client detects that it has moved from an external network to internal network but not many messages sent to/received from home network SHOULD be lost. The amount of signaling used to detect movement from internal to external network SHOULD be optimal such that it doesn't add much overhead to the data traffic.

54. The solution MUST be robust to failures by using fail-over components. The Mobile IP solution if not supporting failover HA usage SHOULD support dynamic discovery of HA.

55. The solution SHOULD be based on the Mobile IPv4 and IPsec standards. To that end the solution MAY be able to work completely (all functionalities) with a combination of standards based components from several vendors. There would broadly be four components: client side VPN, server side VPN, client side Mobile IPv4 and Mobile IPv4 HA/FA.

56. The solution on the client side MAY coexist with other vendors VPN and if another vendors VPN clients are used the solution MAY avoid need to login separately both for VPN and MobileIPv4 solutions.

57. The Mobile IPv4 HA/FA component SHOULD work with any other vendor's standards based client side software for Mobile IPv4. The client side software from the selected vendor SHOULD work with other vendor's standards compliant implementation of Mobile IPv4 HA/FA. The solution SHOULD support "Mobile IP Network Access Identifier Extension for IPv4" [92].

58. The solution SHOULD allow for flexible ways of prioritizing the network to be chosen based on different variables (e.g., power consumption, network access cost), available performance parameters (e.g., throughput Latency) and MAY depend on the application being run (i.e., application dictates the required connection speed and latency levels).

59. The solution SHOULD be easy to manage e.g. centralized server capable of distributing configuration information to the clients, through the central server it SHOULD be possible to tear down an established remote connection to the internal network.

60. The solution SHOULD provide log details of the users who attempt to connect or connect to the network. The log details SHOULD include the bandwidth, data transfer usage by the mobile user.

61. The solution SHOULD minimize handoff delays.

62. The solution SHOULD work with existing VPN infrastructure and MAY work with at least some other widely used VPN infrastructures.

63. The solution SHOULD be scalable.

64. The solution MAY not require modification of operating Systems TCP/IP stack.

65. The solution MAY support minimal encapsulation [112] and Generic Routing Encapsulation [113].

66. The solution MAY enable application persistence in the event of client being temporarily disconnected.
67. The solution MAY be capable of using more than one interface at a time when sufficient throughput is not available in one interface and the mobility agent MAY support simultaneous bindings.

6.4 Product summary

Table 3. Product summary

Product	Interoperability with other MobileIP products		Integration with other VPN products		Load balancing / Fail-over	NAT traversal	Integration with standard Radius server	Session persistence	Packet Overhead (bytes)
	Client side	Server side	Client side	Server side					
IPUnplugged	Yes	Yes	No	No	Yes	Yes	Yes	No	105
Birdstep	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	145
Secgo	Yes	Yes	Yes		Yes	Yes	Yes		145
Netmotion	NA	NA	No		Yes	Yes	Yes	Claims	Unknown
Ecutel	Unclear	Unclear	claims it can 'co-exist')			Yes	Yes	No	105
Columbitech	No	No	No		Yes	Yes		Yes	Unknown

6.5 Requirement compliance of products

Three products (Birdstep, Ecutel-Viatores, and IPUnplugged) were considered for testing as part of the thesis. Despite my best efforts I couldn't get Birdstep running. We have informed the vendor about the problem and asked for troubleshooting help. However, we haven't received reply as of this writing. The requirement compliance list was compiled based on the product design and feature list given in the information sheet.

The requirement compliance for Columbitech was taken from another project report in which the requirement compliance was given.

Table 4. Requirements compliance

Requirement	Birdstep	Columbitech	Ecutel- Viatores	IPUnplugged
1	NA, Possible, C1	YES	No	Yes
2	NA, Possible, C1	YES	No	Yes
3	NA, Possible, C1	Unknown Most likely	No	Unclear,C21
4	NA, Possible, C1	Unknown Most likely	No	Yes
5	NA, Possible, C2	Unknown	YES, C17	Yes, C22
6	NA, Possible, C2	Unknown	No	Yes, C22
7	NA, Possible, C2	Unknown	No	Yes, C22
8	NA, Possible, C1	YES	Yes	Yes
9	NA, Possible, C1	YES	Yes	Yes
10	NA, Possible,	NO	Yes	Yes
11	NA, Possible, C1	YES	Yes	Yes
12	NA, Possible, C1	NO	Yes	Yes
13	NA, Possible, C1	Unknown	No, C18	Yes
14	NA, Possible, C1	Most likely	No, C18	Yes
15	NA, Possible, C1	YES	No, C18	Unclear, C21
16	NA, Possible, C1	NO	No, C18	Yes
17	NA, Possible, C3	YES	No, C19	NA, Possible, C3B
18	NA, Possible, C4	Unknown	No, C19	NA, Possible, C3B
19	NA, Possible, C4	Unknown	No, C19	NA, Possible, C3B
20	NA, Possible, C4	Unknown	No, C19	NA, Possible, C3B
21	NA, Possible, C4	Unknown	No, C19	NA, Possible, C3B
22	Yes, C5	Unknown	Yes	Yes
23	NA, Possible, C4	Unknown	No, C19	NA, Possible, C3B
24	NA, Possible, C4	Unknown	No, C19	No
25	NA, Possible, C4	Unknown	No, C19	NA, Possible, C3B
26	NA, Possible, C4	Most likely	No, C19	NA, Possible, C3B
27	NA, Possible, C6	Most likely	NA, Possible, C6	NA, Possible, C6
28	NA, Possible, C6	Most likely	NA, Possible, C6	NA, Possible, C6
29	NA, Possible, C7	Most likely	NA, Possible, C7	NA, Possible, C7
30	NA, Possible, C8	Most likely	NA, Possible, C8	NA, Possible, C7
31	NA, Possible, C8	Unknown	NA, Possible, C8	Yes
32	NA, Possible, C9	YES	NA, Possible, C9	NA, Possible, C9
33	NA, Possible, C10	Unknown	NA, Possible, C10	NA, Possible, C10

Requirement	Birdstep	Columbitech	Ecutel- Viatores	IPUnplugged
34	NA, Possible, C10	Unknown	NA, Possible, C10	NA, Possible, C10
35	NA, Possible, C11	YES	NA, Possible, C11	NA, Possible, C10
36	NA, Possible, C12	YES	NA, Possible, C12	NA, Possible, C12
37	NA, Possible, C13	YES	NA, Possible, C13	NA, Possible, C13
38	NA, Possible, C14	YES	NA, Possible, C14	NA, Possible, C14
39	NA, Possible, C15	Most likely	NA, Possible, C15	NA, Possible, C15
40	YES	Unknown	YES	YES
41	YES	YES	YES	YES
42	YES	YES	YES	YES
43	YES	Unknown	YES	YES
44	YES, C16	Unknown	YES	YES
45	YES	YES	YES	YES
46	YES	YES	No, C20	YES
47	YES	YES	YES	YES
48	YES	YES	YES	YES
49	YES	Most likely	YES	YES
50	NA, Possible, C10	Most likely	YES C23	YES, C23
51	YES	NO	Partially, C24	YES
52	YES	Unknown	YES	YES
53	YES	Unknown	YES	YES
54	YES	YES	YES	YES
56	YES	NO	Partially, C26	Partially, C26
57	YES	NO	NO	NO
58	YES	NO	NO	NO
59	Partially, C27	NO	Partially, C27	Partially, C27
60	YES	YES	YES	YES
61	YES	Unknown	YES, C17	YES, C22
62	YES	YES	YES	YES
63	YES	NO	NO	NO
64	YES	YES	YES	YES
65	YES	YES	YES	YES
66	YES	NO	NO	NO
67	NO	YES	NO	NO
68	NO	NO	NO	NO

C1: The product is a Mobile IP client that integrates with the existing VPN and MobileIP infrastructure. The requirement compliance depends on the VPN chosen. The Cisco used in my

VPN tests at the time of writing supports these requirements.

C2. The product is a Mobile IP client that integrates with the existing VPN infrastructure. The requirement compliance depends on the VPN, Mobile IP HA chosen. Cisco VPN, HA in test at the time of writing supports these requirements

C3A: The product in itself doesn't contain any firewall. However, the product creates a virtual interface through which all the traffic is directed. The traffic coming from networks other than home network must pass the IPsec integrity check, this functionality offers protection from malcontent (e.g., traffic sent on wireless interface by a rouge user). Third party Firewalls can be used for this purpose.

C3B: The product in itself doesn't contain any firewall. However, the product places a virtual interface only through which all the traffic is directed. The traffic coming from networks other than home network must pass the IPsec integrity check, this functionality offers protection from malcontent (e.g., traffic sent on wireless interface by a rouge user).

C4: C3 applies here and the functionality is dependent on the Firewall chosen.

C5. The product in itself doesn't contain any firewall. However, the product creates a virtual interface only through which all the traffic is directed. The traffic coming from networks other than home network must pass the IPsec integrity check, this functionality offers protection from malcontent (e.g., traffic sent on wireless interface by a rouge user). The detection of Home network is not based on IP address but involves mobile IP authenticated registration

C6: The requirement compliance depends on the Anti-virus product chosen. The product co-exists with third party anti-virus software.

C7: The requirement compliance depends on the Anti-sypware product chosen. The product co-exists with an anti-spyware

C8: The requirement compliance depends on the Anti-virus / Anti-Spyware products chosen

C9: The requirement compliance depends on the Data encryption software chosen.

C10: The requirement compliance depends on the data encryption software chosen.

C11: The requirement compliance depends on the Bios system in the computer. Most of the computers today in the market support such password scheme.

C12: The requirement compliance depends on the Operating system in the computer. Most of the computers today in the market support such password scheme.

C13: The requirement compliance depends on the computers chosen. Most of the computers in the market meet the requirement.

C14: The requirement is not applicable to the product. Such protection feature is provided by most of the computers today in the market.

C15: The product meets the requirement. Mobile IP could be started up after the user logs into the computer. The same (startup after login) could be chosen with the VPN system.

C16: The requirement is dependent on the HA and VPN Gateway chosen. However, most of the

products (HA, VPN) in the market meet this requirement.

C17: The Viatores server runs on linux and user logins and logouts are written to Syslog. Unfortunately, the log doesn't provide details of the users' usage time or the IP address allocation if dynamically assigned. The company said that it is working on this feature.

C18: The version tested doesn't support this. But, the NxG version slated to be released seems to support this feature of classifying the users and assigning proper HA (viatores server).

C19. C3 applies here. Besides, the next version of the product is claimed to be including a Firewall.

C20. Split tunneling is possible. But, the feature is centrally administered and distributed to the client along with other policy information. This can be allowed only by the administrator. So, if the administrator chooses not to allow split tunneling, the user doesn't have privilege to get such access.

C21. The exact attributes supported by the Radius server in the product is not known. But, standard authorization attributes are expected to be supported. So, the requirement is possibly met.

C22. The IPUnplugged Gateway runs on OpenBSD linux and user logins and logouts are written to Syslog. A clear interface (e.g., web based interface) giving all the details of users login, usage etc would have been better.

C23. The client protects its own data with RFC2898 methods like key derivation, salt and iterative count.

C24. FA functionality is not provided.

C26. The client can not integrate with other vendors IPSec VPN gateways or MobileIP HA.

C27. The priority can be configured only based on the interfaces.

6.6 Product comparison

Table 5. Product comparison

	IPUnplugged	Viatores
Requirement compliance	46/50	30/50
Startup time connected at home	Less than 3 seconds	Average of 20sec in 10 trials
Startup time connected away	Less than 3 seconds	Average of 3min 10sec in 10 trials
WLAN-LAN Handover latency	11.3 milli seconds	8.7 milli seconds
LAN-WLAN Handover latency	1.1 sec	2.7sec
Performance problems	Had far less problems. When the client is in a hotspot environment and the wireless interface was off for sometime (e.g., power save), the VPN doesn't allow for re-authentication through web-login. This problem occurred several times	Had problems in network drive mapping even when NetBIOS over IP is used. Had to use Single Sign on (SSO) for the map driving to work. Also, had some other glitches like failure to find the Home Agent (HA) though the HA was reachable and working properly. Several times the delays in startup was abruptly varying and was too high.
Features	Gateway can act as Foreign agent as specified in [38]	Foreign Agent functionality is not supported

Chapter 7

Conclusions

We tried to test most of the Mobile VPN products (based on Mobile IP and IPSec) in the market. None of them worked right away after the installation even though the network was setup as required by the products. Those that worked had to be tweaked to some extent. It shows that the products are not mature and also the market isn't that big as there weren't many product references. However, we could get at least some products to work with reasonably good performance.

Today 802.11 based WLANs are cheaper means of providing end user connectivity than cellular networks. Data communication can be attained at reasonable costs by leveraging this technology; coverage can be improved by operators/owners collectively addressing the problem by entering into roaming agreements and also leveraging the wide coverage of 3G networks. Mobile IP provides session persistence even when the user is switching from one network to another. Data can be securely accessed by using emerging products based on both IPSec and MobileIP. Thus a proof of concept for showing secure network connectivity for the municipality has been shown to be possible with existing products.

Chapter 8

Future work

Our focus was to provide low cost network connectivity, the primary medium was wireless as mobility was a key requirement. Today WLANs provide low cost connectivity, but this technology wasn't initially conceived for mobile users and users of low latency applications. However, ways to adapt the technology to fulfill these requirements are under investigation and being considered by standardization committees. Also, the technology could be used in combination with other existing and emerging wireless technologies to provide improved data connectivity. As future work one should look into efforts being made for 3G to/from WLAN roaming. Relevant products are just emerging into the commercial market; a study of the performance of the products would be a good step to evaluate how heterogeneous communication technology may evolve towards 4G wireless networks, which could be a combination of several technologies (3G and its improvements, WLAN and some other wireless technologies)

None of the open source Mobile IP solutions were compliant with the latest RFCs. Thus another future work would be to update them to the latest standards, thus offering a low cost open source solution, probably work together with an open source IPSec VPN solution.

A survey of the economic issues of providing city wide WLAN access through various business models could be very much useful as we see much debate going on as of the writing in many cities on the issue [114][115][116][117].

Appendix

Abbreviations and Acronyms

3G	Third generation of mobile communications
4G	Fourth generation of mobile communications
802.11x	Any of the IEEE standards 802.11, 802.11a, 802.11b or 802.11g
AAA	Authentication, Authorization and Accounting
AC	Access controller
AP	Access Point
ATM	Asynchronous Transfer Mode
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CAGR	Compound Annual Growth Rate
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CoS	City of Stockholm
DCF	Distributed Coordination Function
DECT	Digital European Cordless Telephone
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
GPRS	General Packet Radio Service
IAPP	Inter-Access Point Protocol
IDC	International Data Corporation
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMIT	Department of Microelectronics and Information Technology
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
MAC	Medium Access Control
MIP	Mobile IP
MIT	Massachusetts Institute of Technology
OSI	Open Systems Interconnection
PHY	Physical Layer
PCF	Point Coordination Function
PTS	Post & Telestyrelsen
RADIUS	Remote Access Dial-in User Service
RF	Radio Frequency
RFC	Request For Comments
QoS	Quality of Service
TCP/IP	Transport Control Protocol / Internet Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network

Bibliography

[1] IEEE Std 802.11-1997 Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications, Nov 1997

[2] UMA Technology: Extending Mobile services to Unlicensed Spectrum
www.umatechnology.org, Oct 18 2004

[3] Motorola Seamless mobility: CN 620
http://www.motorola.com/wlan/solution_cn620.html, Oct 20 2004

[4] DoCoMo N900il
http://www.docomo.biz/html/product/cordless/, Oct 23 2004

[5] Free wireless networking projects
http://freenetworks.org/moin/index.cgi/WirelessNetworkingProjects, Nov 16 2004

[6] City of Stockholm, http://www.stockholm.se, May 21 2005

[7] 3GPP2 – WLAN Interworking -Stage 1 Requirements
http://www.3gpp2.org/Public_html/specs/S.R0087-0_v1.0_040723.pdf, Oct 18 2004

[8] IP Routing for Wireless/Mobile Hosts (mobileip), MobileIP IETF charter,
http://www.ietf.org/html.charters/mobileip-charter.html, Nov 20 2004

[9] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, November 1998

[10] IKEv2 Mobility and Multihoming (mobike), IETF Working Group- mobike

[11] Transport Layer Security (tls), IETF Working Group- tls

[12] Columbitech Wireless VPN
http://www.columbitech.com/Products/wvpn.asp, Nov 06 2004

[13] IPunpluged: MobileIP solution
http://www.ipunplugged.com/enterprise.asp?mi=2.1 Nov 08 2004

[14] Birdstep: Birdstep Intelligent MobileIP
http://www.birdstep.com/wireless_infrastructure/mobile_ip.php3, Nov 10 2004

[15] T. S. Rappaport, W. Nowlin and B. Nowlin, Convergence of Cellular and Wireless LAN: Hotspot Traffic Statistics and User Trends March 22, 2004
http://www.ece.utexas.edu/~wireless/Montage%20Meeting%20Minutes/CTIATalk_March04.pdf,
Dec 14 2004

[16] J. Martell, D.G. Michelson, S.G. Mair, and D. Zollmann

Deployment of Canada's largest campus wireless network at the University of British Columbia Information Technology: Research and Education, 2003. Proceedings. ITRE2003. International Conference on, 11-13 Aug. 2003 Pages:360 - 364

[17] L. G. Bjønnes, H. Bryhni, J. M. Evang and Stein Gjessing,
Wireless Experimental Metropolitan Area Network Using IPv6 in Norway
(WEMAN), Proceedings of the Thirty-second Annual Hawaii International Conference on System Sciences-Volume 8 - Volume 8 table of contents, 1999, ISBN:0-7695-0001-3

[18] A.Hills, Large-scalewirelessLANdesign, Communications Magazine, IEEE, Volume: 39, Issue: 11, Nov. 2001, Pages:98 - 107

[19] Y. Choi, J. Paek, Sunghyun Choi, G. W. Lee, J. H. Lee, H. Jung , Deployment and testbeds: Enhancement of a WLAN-based internet service in Korea,
Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots,San Diego, CA, USA SESSION: Deployment and testbeds
Pages: 36 - 45, 2003 ISBN:1-58113-768-0

[20] Ashish Raniwala Tzi-cker Chiueh, Deployment Issues in Enterprise Wireless LANs
Department of Computer Science Stony Brook, RPE report, September 2003,
http://www.ecsl.cs.sunysb.edu/tr/wlandeployment.pdf, 05 March 2005

[21] Y. Lee, Mobility, roaming, and handoff: Network selection and discovery of service information in public WLAN hotspots, October 2004 Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots.

[22] "WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming", http://www.wi-fialliance.org/opensection/downloads/WISPr_V1.0.pdf, Jan 18 2005

[23] S. Vaarala, (Ed.), Mobile IPv4 Traversal Across IPsec-based VPN Gateways, September 28, 2004 work in progress

[24] F.Adrangi and H. Levkowetz, Problem Statement: Mobile IPv4 Traversal of VPN Gateways, October 4, 2004, work in progress.

[25] Supplement To IEEE Standard For Information Technology- Telecommunications And Information Exchange Between Systems- Local And Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications: Higher-speed Physical Layer Extension In The 2.4 GHz Band, IEEE Std 802.11b-1999

[26] IEEE standard for information technology-telecommunications and information exchange between systems- local and metropolitan area networks- specific requirements Part II: wireless LAN medium access control (MAC) and physical layer (PHY) specifications, IEEE Std 802.11g-2003

[27] Supplement to IEEE standard for information technology telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: high-speed Physical layer in the 5 GHz band, IEEE Std 802.11a-1999

[28] Www.rsasecurity.com/products/securid/whitepapers/MSWLAN_WP_0803.pdf, August 2004, accessed on Nov 04 2004.

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

[30] IEEE Std 802.11h-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003)), 2003

[31] R.Presuhn, J.Case, K.McCloghrie, M. Rose and S. Waldbusser, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), RFC 3416, December 2002

[32] K. McCloghrie, M. Rose, Management Information Base for Network Management of TCP/IP-based internets:MIB-II, RFC 1213, March1991

[33] IEEE standards for local and metropolitan area networks: virtual bridged local area networks, IEEE Std 802.1Q-1998

[34] C. Rigney, S. Willens, A. Rubens and W. Simpson, Remote Authentication Dial In User Service (RADIUS), June 2000, RFC 2865

[35] http://www.ietf.org/html.charters/radext-charter.html, Nov 10 2004

[36] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, Diameter Base Protocol, September 2003, RFC 3588

[37] IEEE trial-use recommended practice for multi-vendor access point interoperability via an inter-access point protocol across distribution systems supporting ieee 802.11 operation Page(s): 0_1- 67, 2003

[38] C.Perkins, "IP Mobility Support for IPv4", RFC 3344, August 2002

[39] D. Johnson, C.Perkins and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[40] IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Std 802.11i-2004.

[41] IEEE Std 802.3af-2003 (Amendment to IEEE Std 802.3-2002, including IEEE Std 802.3ae-2002), 2003

[42] P. Bhagwat, B. Raman and D. Sanghi, Turning 802.11 inside-out
January 2004 ACM SIGCOMM Computer Communication Review, Volume 34 Issue 1

[43] Vivato™ product information, http://www.vivato.net/prod_tech_overview.html, Nov 02 2004

[44] IEEE P802 TGn, grouper.ieee.org/groups/802/11/Reports/tgn_update.htm, May 23 2005

[45] Y. C. Tay, K. C. Chua, A capacity analysis for the IEEE 802.11 MAC protocol, Volume 7 , Issue 2, Pages: 159 - 171, 2001 ISSN:1022-0038

[46] S. Garg, M. Kappes, and A. S. Krishnakumar, "On the Effect of Contention-Window Sizes in IEEE 802.11b Networks," Avaya Labs Research, June 2002

[47] G. Bianchi, L. Fratta and M.Oliveri, Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs, Personal, Indoor and Mobile Radio Communications, 1996. PIMRC'96., Seventh IEEE International Symposium on , Volume: 2 , 15-18 Oct. 1996 Pages:392 - 396 vol.2

[48] Y. Chen, Q. Zeng and D.P Agrawal, Performance analysis and enhancement for IEEE 802.11 MAC protocol, Telecommunications, 2003. ICT 2003. 10th International Conference on , Volume: 1, 23 Feb.-1 March 2003 Pages:860 - 867 vol.1

[49] F. Calì, M. Conti, and E. Gregori, Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit, IEEE/ACM Transactions on Networking (TON), Volume 8 Issue 6, December 2000

[50] L. Bononi, M. Conti, and L. Donatiello, Design and performance evaluation of a distributed contention control(DCC) mechanism for IEEE 802.11 wireless local area networks, International Workshop on Wireless Mobile Multimedia Proceedings of the 1st ACM international workshop on Wireless mobile multimedia, Dallas, Texas, United States Pages: 59 - 67, 1998, ISBN:1-58113-093-7

[51] J. Galtier, Optimizing the IEEE 802.11b Performance using Slow Congestion Window Decrease, France Telecom R&D

[52] Y. Xiao and J. Rosdahl, Performance analysis and enhancement for the current and future IEEE 802.11 MAC protocols, ACM SIGMOBILE Mobile Computing and Communications Review Volume 7 , Issue 2 (April 2003) SPECIAL ISSUE: Wireless home networks,Pages: 6 - 19,Year of Publication: 2003

[53] A.C.V. Gummalla and J.O. Limb, Design of an access mechanism for a high speed distributed wireless LAN, Selected Areas in Communications, IEEE Journal on , Volume: 18 , Issue: 9 , Sept. 2000, Pages:1740 – 1750

[54]V. R. Chimata, Performance Analysis of VoIP in 802.11b networks, http://www.cse.iitk.ac.in/users/venkatch/thesis/voip/, Mar 25 2005

[55] A. Mishra, M. ho Shin, and W. A. Arbaugh, `` An Analysis of the Layer 2 Handoff costs in Wireless Local Area Networks ," ACM Computer Communications Review , vol. 33, no. 2, pp. 93 - 102, 2003.

[56] H. Velayos and G. Karlsson Techniques to Reduce IEEE 802.11b MAC Layer Handover Time.
http://www.it.kth.se/~hvelayos/papers/TRITA-IMIT-LCN%20R%2003-02%20Handover%20in%20IEEE%20802.pdf , Dec 10 2004.

[57] S. Shin, A.Forte, A.Rawat and H.Schulzrinne, Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs. http://www.cs.columbia.edu/~ss2020/fastL2handoff_mobiWAC04.pdf, Dec 06 2004

[58] H. Kim, S. Park, C. Park, J. Kim, and S. Ko, Selective Channel Scanning for Fast Handoff in Wireless LAN using Neighbor Graph.
http://dali.korea.ac.kr/publication/int_pro/paper/IntPro085.pdf, Dec 02 2004

[59] M. Shin, A.Mishra, and W.A. Arbaugh, Communication over wireless LANs: Improving the latency of 802.11 hand-offs using neighbor graphs,June 2004, Proceedings of the 2nd international conference on Mobile systems, applications, and services MobiSys '04

[60] D. E. Comer, John C. Lin and Vincent F. Russo, An Architecture For A Campus-Scale Wireless Mobile Internet, Purdue CS Technical Report CSD-TR 95-058, Sept. 1995

[61] M. Raya, and J.P. Hubaux and I. Aad DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots, International Conference On Mobile Systems, Applications And Services archive. Proceedings of the 2nd international conference on Mobile systems, applications, and services, Boston, MA, USA, SESSION: Communication over wireless LANs, 2004

[62] W.A. Arbaguh, and J. Edney, "Real 802.11 Security, Wi-Fi Protected Access and 802.11i", First edition, Pearson Education, July 15, 2003

[63] Aircrack, http://www.cr0.net:8040/code/network, Apr 14 2005

[64] Airsnort, http://airsnort.shmoo.com, Feb 21 2005

[65]Kismet, www.kismetwireless.net, Feb 10 2005

[66] coWPAtty, WPA key (weak) cracker, http://www.remote-exploit.org/images/5/5a/Cowpatty-2.0.tar.gz, Apr 16 2005

[67] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004

[68] W. Simpson, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994

[69] IEEE Std. 802.1X-2004, IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control, 2004

[70] IEEE Std 802.11i-2004, IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, June 2004

[71] B. Aboba, and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999

[72] L. Yang, P. Zerfos and E. Sadot, Architecture Taxonomy for Control and Provisioning of Wireless Access Points(CAPWAP),draft-ietf-capwap-arch-06, November 18 2004

[73] CISCO AIRONET 1200 SERIES, http://www.cisco.com/en/US/products/hw/wireless/ps430/ , May 16 2005

[74] IETF Working Group, Control And Provisioning of Wireless Access Points (capwap) http://www.ietf.org/html.charters/capwap-charter.html, Nov 02 2004

[75] I.Singh, P.Francisco, K.Pakulski and F. Backes CAPWAP Tunneling Protocol, April 2005, work in progress, http://www.ietf.org/internet-drafts/draft-singh-capwap-ctp-01.txt, April 28 2005

[76] P.Narasimhan, D.Harkins and S.Ponnuswamy SLAPP:Secure Light Access Point Protocol, May 31, 2005, work in progress, http://www.ietf.org/internet-drafts/draft-narasimhan-ietf-slapp-01.txt , June 02 2005

[77] P.Calhoun, B. O'Hara, S.Kelly, R.Suri, M.Williams, S.Hares and N.Cam Winget, Light Weight Access Point Protocol (LWAPP), March 31, 2005, work in progress, http://www.ietf.org/internet-drafts/draft-ohara-capwap-lwapp-02.txt, Apr 22 2005

[78] W. Davies, A-roaming we will go: the wish of many IT managers is for seamless and secure roaming between different wireless networks. EAP SIM will help make that happen, Telecommunications International, Feb, 2004, http://www.findarticles.com/p/articles/mi_m0IUL/is_2_38/ai_n6354540, Jan 26 2004

[79] B.Aboba and G. Zorn, "Criteria for Evaluating Roaming Protocols", RFC 2477, January 1999

[80] Jun Li, Stephen B. Weinstein, Junbiao Zhang and Nan Tu, "Public access mobility LAN: Extending the wireless internet into the LAN environment", IEEE Wireless Communications, vol. 9, no. 3, June 2002 pp. 22-30

[81] Apostolis K. Salkintzis, "Interworking Techniques and Architectures for WLAN/3G Integration Toward 4G Mobile Data Networks", IEEE Wireless Communications, June 2004, pp. 50-61

[82] Design and implementation of a WLAN/cdma2000 interworking architecture Buddhikot, M.M.; Chandranmenon, G.; Seungjae Han; Yui-Wah Lee; Miller, S.; Salgarelli, L.; Communications Magazine, IEEE, Volume 41, Issue 11, Nov. 2003 Page(s):90 - 100

[83] Wi-Fi Alliance, http://www.wi-fialliance.org/OpenSection/index.asp, Jan 18 2005.

[84] "IP Routing for Wireless/Mobile Hosts (mobileip)" IETF working group http://www.ietf.org/html.charters/mobileip-charter.html Nov 02 2004

[85] J.Ioannidis, D.Duchamp and G.Q. Maguire Jr; IP-based Protocols for Mobile Internetworking, Proceedings of SIGCOM'91, ACM, September 1991, PP.235-245

[86] F.Teraoka, K.Claffy and M.Tokoro, Design, implementation, and evaluation of Virtual Internet Protocol, Distributed Computing Systems, 1992., Proceedings of the 12th International Conference on , 9-12 June 1992 Pages:170 – 177

[87] C.Perkins, Y.Rekhter, Support for Mobility with Connectionless Network Layer Protocols (Transport layer Transparency), draft RFC, January 1993.

[88] C. E. Perkins, Mobile IP Design Principles and Practices
Prentice Hall PTR, 1st edition (January 15, 1998)

[89] J. Solomon, Mobile IP the Internet Unplugged
Prentice Hall PTR; 1st edition (January 15, 1998)

[90] J. Solomon, “Applicability Statement for IP Mobility Support”, RFC 2004, October 1996

[91] S. Deering, , "ICMP Router Discovery Messages", RFC 1256, September 1991.

[92] P. Calhoun and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, March 2000

[93] F. Johansson, and T. Johansson, "Mobile IPv4 Extension for Carrying Network Access Identifiers", RFC 3846, June 2004

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

[95] P. Srisuresh and K. Egevang, ”Traditional IP Network Address Translator (Traditional NAT)”, RFC 3022, January 2001

[96] H. Hodrege and P. Sri suresh, , IP Network Address Translator (NAT) Terminology and considerations

[97] H. Levkowetz and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices", RFC 3519, May 2003

[98]K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little and G. Zorn,
Point-to-Point Tunneling Protocol (PPTP), RFC 2637, July 1999

[99] W.Townsley, , A..Valencia, A.. Rubens, G.Pall, G. Zorn and B. Palter,
Layer Two Tunneling Protocol "L2TP”, August 1999

[100] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998

[101] S. Kent and R. Atkinson, IP Authentication Header, RFC 2402, November 1998

[102] S. Kent and R. Atkinson, IP Encapsulating Security Payload (ESP)

[103] D. Harkins and D. Carrel, The Internet Key Exchange (IKE), November 1998

[104] Columbitech Wireless VPN™, Technical Description

http://www.columbitech.com/white_papers/ColumbitechWirelessVPNTechnicalDescription.pdf, Nov 10 2004

[105] K Byoung-Jo and S. Srinivasan, Simple mobility support for IPsec tunnel mode, 2003

IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No.03CH37484), 2003, pt. 3, p 1999-2003 Vol.3

[106] http://www.ipunplugged.com/, Nov 12 2005

[107] http://www.netseal.com/, Nov 15 2005

[108] http://www.birdstep.com/, Nov 10 2005

[109] Mobile IP product technical details, http://www.secgo.com/docs/secgo_mobile_ip_tech_details_datasheet_2004-07.pdf, Dec 02 2004

[110] T. Pettersson, Mobile VPN solution requirements, STOKAB AB, Nov 25 2005

[111] Draft ”Säkerhetsmålsättning för mobilt bredband”

[112] C. Perkins, "Minimal Encapsulation within IP", RFC 2004, October 1996.

[113] S. Hanks, T. Li, D. Farinacci, and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, October 1994

[114] How much does it cost to build an open source, open architecture muni network? http://www.muniwireless.com/archives/000755.html, 05 July 2005

[115] Philadelphia: Muni Wi-Fi’s Worst-Case Scenario http://www.eweek.com/article2/0,1759,1784105,00.asp, 05 July 2005

[116] Advanced IP Pipeline | Philly's Wi-Fi: Panacea Or Boondoggle? http://www.advancedippipeline.com/160702498, 05 July 2005

[117] Muni-Wireless: The Battle Continues http://www.eweek.com/article2/0,1895,1755328,00.asp, 05 July 2005

IMIT/LCN 2005-11

www.kth.se