Eidgenössische
Technische Hochschule
Zürich

Ecole polytechnique fédérale de Zurich
Politecnico federale di Zurigo
Swiss Federal Institute of Technology Zurich

Departement Informationstechnologie & Elektrotechnik
Professur für Technische Informatik
Professor Dr. Bernhard Plattner

Nicolas Cedraschi, D-ITET
Daniel Grob, D-ITET

Mobile WLAN Access Point for the ETH Shuttle Bus

Semester Thesis SA-2002.47
28.8. - 17.10.2002

Tutors:
Vincent Lenders
Károly Farkas

Supervisor:
Prof. Dr. B. Plattner

Institut für Technische Informatik und Kommunikationsnetze
Computer Engineering and Networks Laboratory

Acknowledgements

This report documents the work on a semester thesis accomplished at the *Computer Engineering and Networks Laboratory (TIK)*[1] of the *Swiss Federal Institute of Technology Zurich (ETHZ)*[2] during autumn 2002.
The authors would like to thank their tutors Vincent Lenders and Károly Farkas, PhD students at TIK, for their dedicated and competent support in various aspects and Karl Auer, Armin Brunner and Derk-Jan Valenkamp from the *Informatikdienste*[3] of the ETH Zürich for their expended time and their remarkable engagement. Finally, we thank Prof. Dr. Plattner for his assistant inputs.
We would also like to mention *Fujitsu-Siemens*[4] who contributed two laptops at favorable conditions. We benefited from an excellent infrastructure provided by TIK. Thus, we were allowed to focus on the important tastks.

Zurich, 7th November 2002

Daniel Grob, Nicolas Cedraschi

[1] http://www.tik.ee.ethz.ch
[2] http://www.ethz.ch
[3] http://www.id.ethz.ch
[4] http://www.fujitsu-siemens.com/

Abstract

The goal of this semester thesis was to develop a mobile *Access Point* for *Wireless LAN (IEEE 802.11b)*, applicable in the shuttle bus that connects the two campi ETH Zentrum and ETH Hönggerberg. A proper large range wireless connection system was evaluated. The bridge between the two systems and the Access Point were implemented on an embedded device. The system characteristics were tested and evaluated.

The access to this service must be granted for users with a n.ethz account and should be transparent, i.e. authentication and access procedure are the same as on the fixed Access Points in the ETH WLAN. There are two authentication concepts:

- *Old Access Concept:* The user authenticates via SSH connection on a validation server. The validation server unlocks the IP of the user on the gateway firewall.
- *New Access Concept:* The user authenticates on a VPN-server and sets up a VPN-tunnel to it, whence he can access the ETH LAN and thence the Internet.

To realize the Access Point, two different system concepts were developed and evaluated. *System Concept I* was implemented as a prototype. It supports the new access concept only. *System Concept II* supports the old access concept as well, yet is more sophisticated and therefore more difficult to implement. It is theoretically presented and discussed.

The work and studies within the scope of this thesis realized a mobile Access Point, but also revealed difficulties and limitations. The large range wireless system (GPRS) that connects the bus to the ETH WLAN, forms a bottleneck concerning data rate and delay.

Kurzfassung

Das Ziel dieser Semesterarbeit war es, einen mobilen Access Point für Wireless LAN (IEEE 802.11b) zu entwickeln, der im Shuttlebus, der zwischen den Campi ETH Zentrum und ETH Hönggerberg verkehrt, eingesetzt werden kann. Eine geeignete Technologie zur drahtlosen Verbindung zum ETH Netz wurde evaluiert. Das Konzept wurde als eingebettetes System realisiert. Die Systemeigenschaften wurden getestet und evaluiert.

Der Zugang zu diesem Dienst soll für den User mit einem n.ethz Account möglich sein und gleich ablaufen wie bei fest installierten Access Points an der ETH. Dafür stehen dem User zwei Authentisierungsverfahren zur Verfügung:

- *Altes Authentisierungsverfahren:* Der User authentiziert sich über eine SSH Verbindung auf dem Validierungsserver. Dieser schaltet die IP des Users auf einer Gateway-Firewall frei.
- *Neues Authentisierungsverfahren:* Der User authentiziert sich bei einem VPN-Server und baut zu diesem einen VPN-Tunnel auf, von wo er Zugang zum ETH WLAN und zum Internet erhält.

Für die Realisierung des Access Points wurden zwei Systemkonzepte entworfen und analysiert. Das erste Konzept wurde als Prototyp implementiert; es unterstützt nur das neue Authentisierungsverfahren. Das zweite Konzept bietet auch das alte Authentisierungsverfahren an, ist jedoch deutlich aufwendiger zu implementieren. Dieses wurde theoretisch aufgezeigt und diskutiert.

Der Prototyp zeigt, dass mit bestehender Technologie ein mobiler Access Point realisiert werden kann. Es hat sich aber auch herausgestellt, dass die für die Verbindung zwischen Bus und Internet in Frage kommenden drahtlosen Technologien (hier GPRS) den Flaschenhals bzgl. Durchsatz und Verzögerungszeit bilden.

Schedule

	Activity	Milestones
Week 1	• Setting up working Environment • HW Evaluation & Ordering • Comparing different Technologies • Literature Studies	
Week 2	• Collecting Information • Developing System Concept I	
Week 3	• Setting up Laptops with Linux • Integrating GPRS & WLAN HW • Starting Report	GPRS IF working
Week 4	• Developing System Concept II • Implementing System Concept I	WLAN HostAP
Week 5	• Implementing System Concept I & II	System Concept I working
Week 6	• Implementing System Concept II	
Week 7	• Preparing Presentation • Preparing Report	Presentation
Week 8	• Finishing Report	

Contents

List of Figures

Chapter 1

Introduction

These days, the *Internet* enters a new stage of expansion as more and more Internet-enabled devices are being deployed in various contexts. The common perspective foresees that millions of various devices and machines are going to be connected to the Internet, building its capillaries.

With the mingling of computers and telephones into sophisticated portable devices, the Internet disperses from its current realm of classical wired desktop applications (WWW and e-mail) to mobile location independent applications on handheld devices, that allow to provide location based realtime information, e.g. train schedules or weather forecasts[1].

A first step towards mobile networking (Internet access) has already been taken with the adapting of mobile communciation technologies like *Global System for Mobile Communications (GSM)* or *General Packet Radio System (GPRS)*. However, the data rates of GSM/GPRS are not competitive to the IEEE 802 standards, e.g. the Ethernet. The *Universal Mobile Telecommunication System (UMTS)* is announced as competitive to these standards and as a general solution for all mobile applications. The promised performances for UMTS concerning data rates and coverage are very ambitious and although researchers and telecommunication corporations all over the world have made huge efforts to overcome all technical difficulties, the actual implementation of the technical specification currently appears to be too expensive and lacks useful applications for the broad market so that its launch has been postponed.

In the recent years various wireless LAN technologies have been intro-

[1] http://mobile.sunrise.ch/wap/wap_lcl.htm

duced, e.g. the *802.11* standards by the IEEE or *HiperLAN* by the ETSI (see Section 2.1). These are about to partly fill this gap. Within the frame of this report the expression *WLAN* (Wireless Large Area Network) hence refers to the IEEE 802.11b standard. The original purpose is to give users mobility within a certain area and to get rid of the rather bothersome wiring. The usage of the licence free *Industrial, Scientific, Medicinal (ISM)* frequency bands as transmission media makes these technologies applicable for a broad commercial deployment.

Although WLAN is "only" a wireless technology, and although it does not offer the same degree of mobility range as UMTS or GPRS, it has many benefits such as its comparatively high data rates and its low setup costs that make it a serious competitor to mobile communication technologies, like UMTS, especially in urban environments and highly frequented locations.

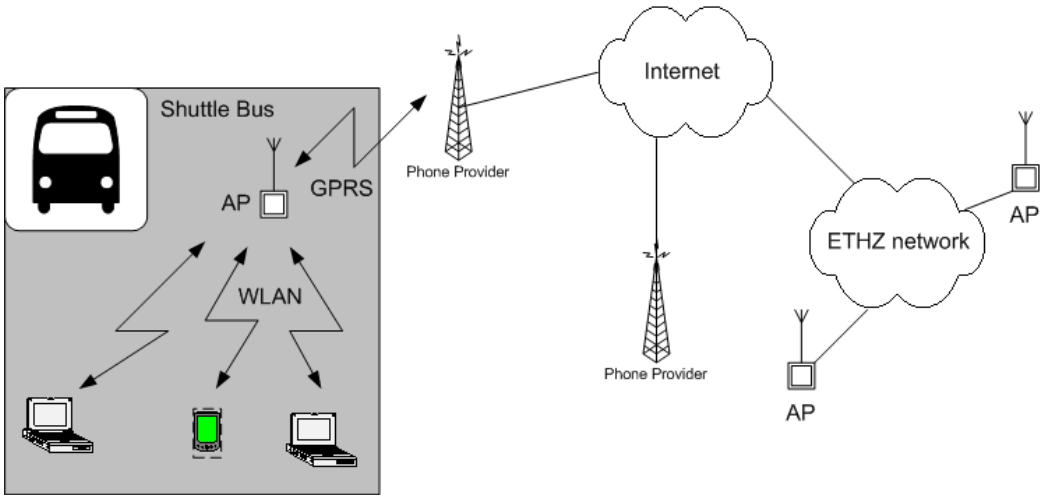

Figure 1.1: The Access Point (AP) on the ETH Shuttle Bus Connects to the ETH Network over GPRS

1.1 Motivation

Within the scope of the ETH World project [2] as a step towards creating *"a universal virtual communication and cooperation platform"* called *virtual*

campus, it is scheduled to integrate a WLAN infrastructure to provide access to the ETHZ infostructure and thence to the Internet. The deployment of the network is making good progress, so that currently most of the buildings of the campi (ETH Zentrum and ETH Hönggerberg) are covered by a network of IEEE 802.11b *Access Points (APs)*. However, the area between the two campi is not covered by APs. Therefore taking the shuttle bus to change campus inevitably results in connection loss.

The goal of this thesis is to provide WLAN connectivity in the bus just as on the campi. The concept is to set up an AP for the bus, that is connected to the WLAN of the ETH over a GPRS connection (see Figure 1.1). This connection has to be transparent, i.e. the user on the bus should be able to connect to the ETH WLAN subnet, as if he was on one of the campi. A WLAN-GPRS bridge has to be developed (and deployed) that transparently provides access to the ETH WLAN subnet. From this subnet the user can then access the entire ETH LAN and thence the Internet.

Chapter 2

Technology Review

2.1 Wireless LAN

WLAN [3, 4] is a flexible data communication system implemented to extend or substitute a wired LAN within a building or a campus. Using electromagnetic waves rather than a cable infrastructure, it minimizes the need for wired connections and therefore drastically reduces the cost-intensive pulling of cables through walls and ceilings. Moreover, systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Topologies are easily changed and range from peer-to-peer networks, suitable for a small number of users, to full infrastructure networks.

Due to considerable progresses in the fields of radio transmisson and fast integrated electronics, WLAN has seen a remarkable performance increase concerning the data rate. It is now already competitive to its older wired predecessor, the 10Mbit-Ethernet. WLAN gives way for new applications adding a new flexibility to networks.
Today's working environment is characterized by an increasingly mobile workforce. Users are equipped with notebook computers and spend more of their time working in teams that cross functional, organizational and geographic boundaries. WLAN systems provide LAN users with seamless access to real-time information within a campus, regardless of location or hardware configuration.

2.1.1 WLAN, the 802.11 Standard

The IEEE 802 committee has established the 802 standards that have driven the LAN industry for the past two decades. In 1997, after seven years of work, the IEEE published 802.11, the first internationally sanctioned standard for WLAN. In September 1999 they ratified the 802.11b "High Rate" amendment to the standard, which added two higher data rates (5.5 and 11 Mbps) to 802.11.

Like all IEEE 802 standards, the 802.11 standards focus on the bottom levels of the ISO communication standard, the physical layer and data link layer (see Figure 2.1). The basic architecture, features, and services of 802.11b are defined by the original 802.11 standard. The 802.11b specification affects only the physical layer, improving data rates and providing more robust connectivity.

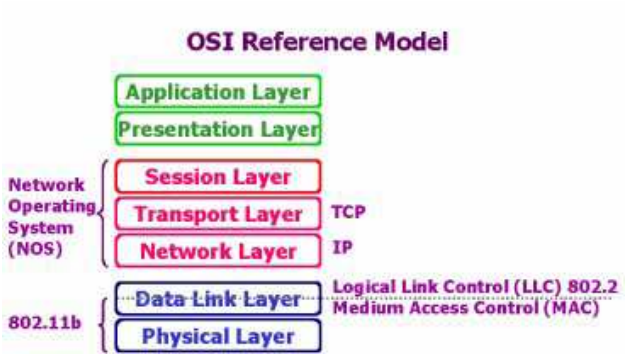

Figure 2.1: 802.11 Standards within the ISO Standard

Operating Modes

802.11 defines two pieces of equipment, a *wireless station*, which is usually a mobile device equipped with a wireless *Network Interface Card (NIC)*, and an AP, which acts as a bridge between the wireless and the wired network. An AP usually consists of a radio, a wired network interface (as defined e.g. in IEEE 802.3), and bridging software conforming to the 802.1d brigdging standard. The AP acts as *Base Station (BS)* for the wireless network, aggregating access for multiple wireless stations onto the wired network.
The 802.11 standard defines two modes: *Infrastructure* mode and *Ad hoc*

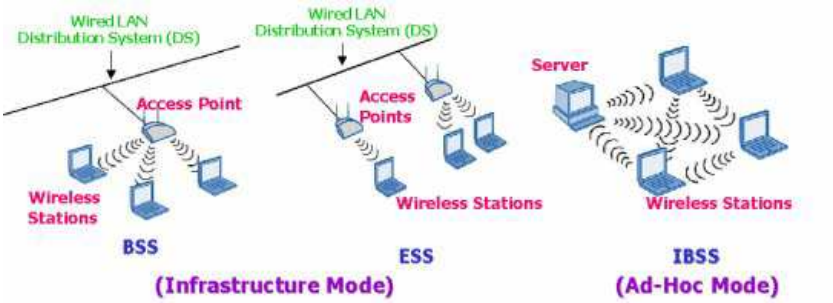

Figure 2.2: The Different Modes of 802.11

mode (see Figure 2.2). In the infrastructure mode, the wireless network consists of at least one AP connected to the wired network infrastructure and a set of wireless clients. This configuration is called *Basic Service Set (BSS)*. An *Extended Service Set (ESS)* is a set of two or more BSSs forming a single subnetwork. Since most corporate WLANs require access to the wired LAN for services they will operate on *Infrastructure* mode. The *Ad hoc* mode (also called peer-to-peer mode or *Independent Basic Service Set (IBSS)*) is simply a set of wireless stations that communicate directly with one another without using an AP or any connection to a wired network.

The Physical Layer

The three physical layers originally defined in the 802.11 standard included two spread-spectrum radio techniques and a diffuse infrared specification. Spread-spectrum techniques, in addition to increase reliability, boost throughput, and allow many unrelated products to share the spectrum without explicit coorporation and with minimal interference.

The original 802.11 wireless standard defines data rates of 1 Mbps using *Frequency Hopping Spread Spectrum (FHSS)* or *Direct Sequence Spread Spectrum (DSSS)*. It is important to note that FHSS and DSSS are fundamentally different data transfer mechanisms and will not interoperate with one another.

Using FHSS, the 2.4 GHz band is divided into 75 1-MHz subchannels. Each conversation between a sender and a receiver within the 802.11 network occurs over a different hopping pattern, and the patterns are designed to minimize the chance of two senders using the same subchannel simultaneously. In contrast, the DSSS technique divides the 2.4 GHZ band into 14 22-MHz

channels. Adjacent channels overlap one another partially, with three of the 14 being completely non-overlapping. Data is sent across one of these 22 channels.
The key contribution of the 802.11b addition to the WLAN standard was to standardize the physical layer support of two new speeds, 5.5 Mbps and 11 Mbps. To accomplish this, DSSS had to be selected as the sole physical layer technique for the standard.
To support very noisy environments as well as spatial range, 802.11b WLAN use *Dynamic Rate Shifting (DRS)*, allowing data rates to be automatically adjusted to compensate for the changing nature of the radio channel.

The Data Link Layer

The *Data Link Layer (DLL)* of 802.11 consists of two sublayers: *Logical Link Control (LLC)* and *Medium Access Control (MAC)*. 802.11 uses the same 802.2 LLC and 48-bit addressing as other 802 LANs, allowing for very simple bridging from wireless to wired 802 LANs, but the MAC is unique to WLAN.
The 802.11 MAC is very similar in concept to 802.3, in that it is designed to support multiple users on a shared medium by having the sender sense the medium before accessing it. 802.3 Ethernet LAN use *Carrier Sense Multiple Access with Collision Detection (CSMA/CD)* as MAC. In a 802.11 WLAN, collision detection is not possible due to antenna limitations; a station must be able to transmit and listen at the same time, therefore it can not hear a collision. To account for this difference, 802.11 uses a slightly modified protocol known as *Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)* or the *Distributed Coordination Function (DCF)*. CSMA/CA works as follows. A station whishing to transmit senses the air and, if no activity is detected, waits an additional, randomly selected period of time and then transmits if the medium is still free. If the packet is received intact, the receiving station issues an ACK frame that, once successfully received by the sender, completes the process. If the ACK frame is not detected by the sending station, a collision is assumed to have occured and the data packet is transmitted again after waiting another random amount of time.
CSMA/CA thus provides a way of sharing access over the air. This explicit ACK mechanism also handles interference and other radio related problems very effectively. However, it does add some overhead to 802.11 that 802.3 does not have, so that an 802.11 LAN will always have a lower data rate than

a wired LAN.
Another MAC-layer problem specific to wireless is the *hidden node* issue, in which two stations on the opposite sides of an access point can both sense activity from an AP, but not from each other, usually due to distance or an obstruction. To solve this problem, 802.11 specifies an optional *Request to Send/Clear to Send (RTS/CTS)* protocol at the MAC layer.
Finally, the 802.11 MAC layer provides two other robustness features: *Cyclic Redundancy Check (CRC)* and packet fragmentation. Each Packet has CRC checksum calculated and attached to ensure that the data is not corrupted in transit.

Association and Roaming

When an 802.11 client enters the range of one or more APs, it chooses an AP to associate with, based on signal strength and observed packet error rates. Once accepted by the AP, the client tunes in to the radio channel to which the AP is set. Periodically, it surveys all 802.11 channels in order to assess whether a different AP would provide it with better performance characteristics. If it determines that this is the case, it reassociates with the AP, tuning to the radio channel to which that AP is set. If two APs are in range of one another and are set to use the same or partially overlapping channels, they may cause some interference for one another, thus lowering the total available bandwith in the area of overlap.

Security

802.11 provides MAC layer access control and an encryption mechanism, known as *Wired Equivalent Privacy (WEP)*, with the objective of providing WLANs security equivalent to their wired counterparts. For the access control, the ESSID (also known as WLAN Service Area ID) is configured into each AP and is required knowledge in order for a wireless client to associate with an AP. In addition, there is provision for a table of MAC addresses called an *Access Control List* to be included in the AP, restricting access to clients whose MAC addresses are on the list.
For data encryption, the standard provides for optional encryption using a 40-bit shared-key algorithm from RSA Data Security[1]. Beyond Layer 2, 802.11 WLANs support the same security standards supported by other 802 LAN

[1] http://www.rsasecurity.com

for access control (such as network operating system logins) and encryption (such as IPsec or application-level encryption).

2.1.2 Wireless LAN Concept of ETH World

As mentionned in the introduction, the WLAN concept of ETH World [5] implies the deployment of a set of APs on the two campi. In the early stage of the ETH WLAN, there was only one subnet of public IPs for all WLAN users. This allowed roaming between the buildings, but as the number of users grew and more buildings were equipped with APs, the ETH WLAN subnet exceeded a critical size, which reduced its performance and made it increasingly difficult to administrate. Therefore, in a second stage the ETH WLAN has been divided into several subnets for different buildings with corresponding routers and DHCP relays (see Figure 2.3). However, as a consequence of this, roaming between the different buildings is no longer possible.

Currently over a hundred APs are deployed in most of the ETH buildings, all physically and virtually connected together to the ETH WLAN subnet and explicitly separated from the rest of the ETH LAN. The DHCP relays of the different buildings forward DHCP requests to a central DHCP server, which manages the IPs of all WLAN subnets.
If a user connects to one of these APs, he broadcasts a DHCP request into his subnet, which will be forwarded by the corresponding router to the central DHCP server. The DHCP server in turn assigns him an internal IP of the corresponding subnet. At this point the user can network with all the other WLAN clients, who are in the same subnet, but he cannot access the rest of the ETH network or the Internet. In order to do so, he needs to authenticate. This is done in two different ways, as depicted below in the following two sections. The first access concept is older and does not require any special software for users, but it brings some security issues with it. The second access concept is just about to be introduced and is planned to replace the first access concept in the long run, since it deploys a higher degree of security.

The Old Access Concept

As mentionned above, the WLAN network of the ETH is separated from the rest of the ETH LAN or any other network. The only connection between

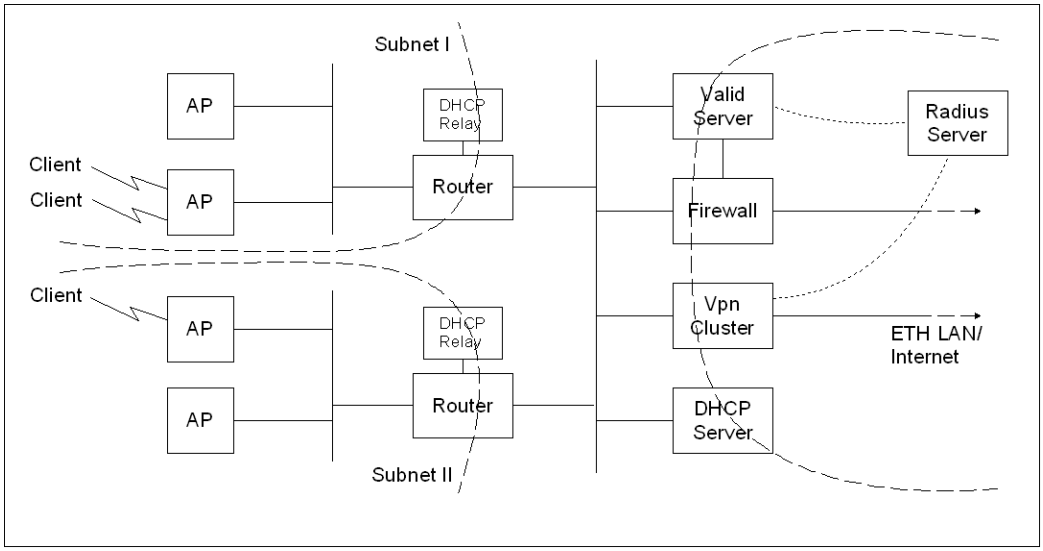

Figure 2.3: The Wireless LAN Concept of ETH World

the ETH WLAN subnet and the ETH LAN is a firewall. To get access, a user has to authenticate himself on the *Valid server*. If the authentication is successful, the user's IP is unlocked on the firewall and he is allowed to access the ETH LAN. The authentication is effectuated by a SSH or telnet login on the authentication server (Valid server).
This method introduces some security holes: First of all, the traffic of all other users in the same subnet can be sniffed and overheard over the air interface. The second problem is that the firewall does not re-lock the corresponding IP when a user logs out. It keeps the IP unlocked for at least 12 hours. So after an IP has been left it can be adopted by intruders to unauthenticatedly get access.

The New Access Concept

The new access concept is based on a *Virtual Private Network (VPN)*. VPN is a concept that allows a set of computer systems to communicate "securely" over a public network. Security features include encryption, strong authentication of remote users or hosts and mechanisms for hiding or masking information about the private network topology from potential attackers on the public network.

The ETH uses a software based VPN-application whose client software is downloaded and installed on the user machine. This software connects the user to a dedicated VPN-server in the WLAN network, that acts as gateway to the rest of the ETH LAN. After a successful authentication on this VPN-server, the client receives two public IPs for the two sides of the connection, and a VPN is set up between the client and the server. This method is more secure than the first one, since packets are encrypted by the client and can not be overheard over the transmission medium. It is as if the users device was physically wired to the VPN-server.

2.2 Large Range Wireless System

The expression *Large Range Wireless System* refers to wireless systems providing ranges of more than one kilometer. In this section, available and upcoming technologies are presented and compared in a general overview. The most favorable system for this project is evaluated and described.

The impressive growth of cellular mobile telephony as well as of the number of Internet users promises an exciting potential for a technology that merges both: *cellular wireless data services*. Within the next few years, there will be an extensive demand for wireless data services.
There are several major *second-generation (2G)* digital cellular standards used throughout the world. The most widespread are the *Global System for Mobile Communication (GSM)*, the *Code Division Multiple Access (CDMA)* standard called *cdmaOne*, *Time Division Multiple Access (TDMA)*, and *Personal Digital Communication (PDC)* which is mainly used in Japan. In order to comply with the upcoming extensive demand for wireless data services, there will be a transition to 3G technologies that, in addition to voice services, will add support for *always on* packet data access and eventually, new multimedia types of wireless services. GPRS (2.5G) is a first step into this direction, but based and working on the same infrastructure as GSM. Figure 2.4 depicts the Wide Area Cellular Network evolution towards 3G.

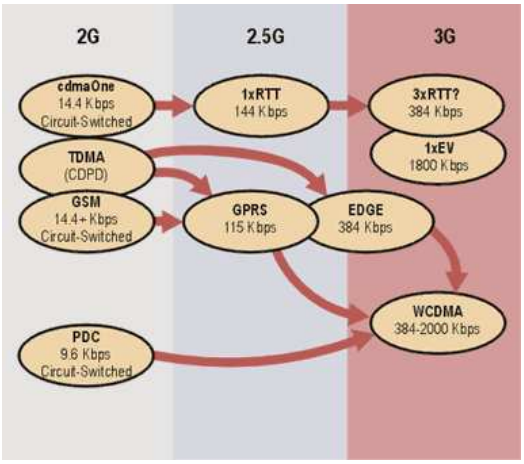

Figure 2.4: Wide Area Cellular Network Evolution

2.2.1 Comparison

Five large range wireless systems are compared[2]:

- *HSCSD: High Speed Circuit Switched Data* is an extension of GSM. It bundles GSM timeslots, and thus achieves theoretical rates of up to 57,6 kbit/s (four timeslots of 14.4 kbit/s each). The obtained data rates are about 35-40 kbit/s. A HSCSD connection is billed per time unit. The network coverage corresponds to the coverage of the GSM network.

- *GPRS: General Packet Radio System* is described in detail in the next section. It is another extension of GSM that offers data rates of 30-50 kbit/s. A GPRS connection is billed per data unit. The network coverage corresponds to the coverage of the GSM network.

- *EDGE: Enhanced Data rates for GSM Evolution* is an upcoming evolution of GSM, allowing bit-rates of 48 kbit/s per timeslot, i.e. 384 kbit/s in total. It is packet switched and requires relatively small changes to network hardware and software since it uses the same frame structure and bands as the existing GSM. At the moment no provider is planning on deploying EDGE in Switzerland in the near future.

- *UMTS: Universal Mobile Telecommunication System* is a wide band CDMA technology of *third-generation (3G)* mobile networks, introducing data rates of up to 2 Mbit/s under ideal circumstances, but realistic values are expected to be around 300-400 kbit/s. Its launch is ahead, but with much lower performances in the beginning. Swisscom is about to build a UMTS network which is going to operate with data rates of 64 kbit/s in a first phase.

- *Satellite Systems:* There are several technologies and providers that provide mobile connectivity over satellite, e.g. Iridium[3]. The performances for a handheld set are rather modest with 9.6 kbit/s. The technology is very expensive and not conceived for data transfer. There are satellite systems, which provide higher data rates, but these require expensive equipment, e.g. parabole reflectors, that must be continuously re-directed. This technology exceeds the scope of the present project.

Technology	Data Rate	Coverage	Billing
HSCSD	57.6 kbit/s	good	per time unit
GPRS	53.6 kbit/s	good	per data unit
EDGE	384 kbit/s	none	per data unit
UMTS	384 kbit/s	under construction	per data unit
Satellite Systems	9.6 kbit/s	global	per time unit

Table 2.1: Large Range Wireless Systems in Comparison

In Table 2.1 an overview of the properties of the above mentioned Large Range Wireless Systems is given. As seen in this table, the choice is reduced to either HSCSD or GPRS, since all the other technologies are either too expensive (Satellite Systems) or not (yet) deployed in Switzerland.

Among these two, GPRS meets the requirements for the mobile AP better, since it is packet switched, i.e. it only uses a channel, if there actually is data to transmit. This corresponds to the fluctuating traffic that the clients of the AP are expected to produce when surfing the Internet.

2.2.2 General Packet Radio System GPRS

GPRS [6, 7] is a bearer service for *Global System for Mobile Communication (GSM)* that greatly improves and simplifies wireless access to packet data networks, e.g. the Internet. It applies a packet radio principle to transfer user data packets in an efficient way between GSM mobile stations and external packet data networks. Packets are directly routed from the GPRS mobile stations to packet switched networks. Networks based on the *Internet Protocol (IP)* and X.25 networks are supported in the current version of GPRS.

Users of GPRS benefit from shorter access times and higher data rates. In conventional GSM, the connection setup takes several seconds and rates for data transmission are restricted to 9.6 kbit/s. In practice, GPRS offers

[2]This overview reflects the current state as of the Orbit '02 (October 2002, Basel)
[3]http://www.iridium.com

session establishment times below one second and ISDN-like data rates up to several ten kbit/s.
Moreover, GPRS packet transmission offers a more favorable billing for data traffic than circuit switched services, which is billed per time unit and is *always on*. The latter is unsuitable for applications with bursty traffic. The user pays for the entire airtime, even for idle periods when no packets are sent (e.g. when the user reads a Web page). For packet switched services, on the other hand, billing can be based on the amount of transmitted data.

To sum up, GPRS improves the utilization of the radio sources for data traffic, offers data based billing, higher transfer rates, shorter access times, and simplifies the access to packet data networks. A downside is that GPRS packets have lower priorities than speech packets, so the performance is dependent on the traffic load in the local cell.

GSM/GPRS Network Overview

GPRS uses the same physical layer as GSM, which uses a combination of *Time Division Multiple Access (TDMA)* and *Frequency Division Multiple Access (FDMA)* for medium multiplexing. Two frequency bands have been reserved for GSM operation: 890 - 915 MHz for uplink connections, and 935 - 960 MHz for the downlink connection. Each of these bands of 25 MHz width is divided into 124 single carrier channels of 200 kHz width with a gross data rate of 270 kb/s. A certain number of these frequency channels is allocated to a *Base Transceiver Station (BTS)*, i.e. to a cell. Each of these 200 kHz frequency channels carries eight TDMA channels by dividing each of them into eight time slots. The eight time slots in these TDMA channels form a TDMA frame. Each time slot of a TDMA frame lasts 156.25 bit times and, if used, contains a data burst. The time slot lasts 15/26 ms = 576.9 μs; so a frame takes 4.613 ms. The recurrence of one particular time slot defines a physical channel.

A GSM mobile station uses the same time slots in the uplink as in the downlink. The channel allocation in GPRS is different from the original GSM. GPRS allows a single *Mobile Station (MS)* to transmit on multiple slots of the same TDMA frame (multislot operation). Therefore, the channel allocation is very flexible: one to eight time slots per TDMA frame can be allocated for one MS. Moreover, uplink and downlink are allocated separately, which efficiently supports asymmetrics data traffic. Using 8 time

slots results in theoretical data rates of up to 171 kBit/s. However, GPRS packets have a lower priority assigned than GSM packets. Therefore, GPRS performace depends on the number of active GSM users in the same cell. The current GPRS devices are limited to use up to 4 time slots. This results in an actual data rate of about 30-50 kb/s. In conventional GSM, a channel is permanently allocated for a particular user during the entire call period (whether data is transmitted or not), whereas in GPRS the channels are only allocated when data packets are sent or received, and they are released after the transmission. For bursty traffic, this results in a more efficient usage of the scarce radio resources.

Internetworking with IP Networks

A GPRS network can be interconnected with an IP-based packet data network, such as the Internet or intranets. GPRS supports both IPv4 and IPv6. From outside, i.e. from an external IP network, the GPRS network looks like any other IP subnet. A special piece of equipement, the *Gateway GPRS Support Node (GGSN)* acts as an interface between the GPRS backbone network and the external packet data networks (see Figure 2.5). Each registered user who wants to exchange data packets with an IP network gets an IP address. The IP address is out of the address space of the GPRS operator.

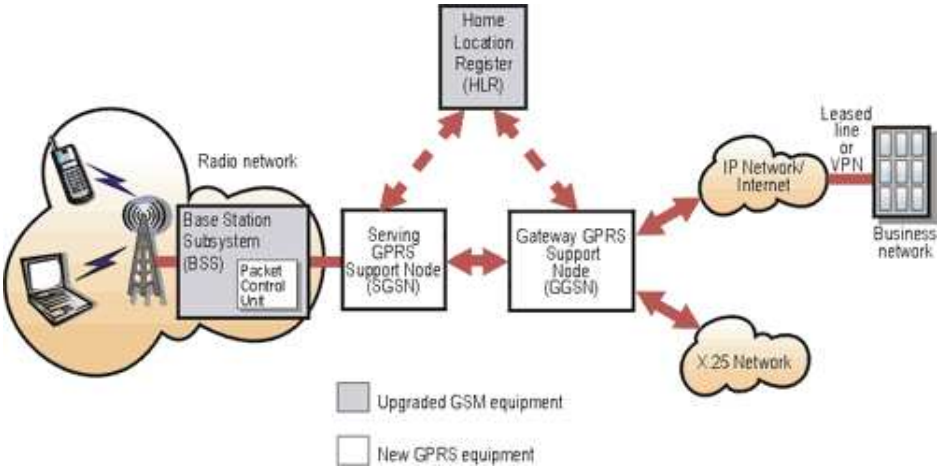

Figure 2.5: GPRS Network

Chapter 3

Related Works & Technologies

3.1 Related Works

Despite of intensive investigations on the Internet, only two comparable projects on mobile 802.11b APs were found.

A company that offers a comparable system is *Icomera*[1]. Yet, information and technical details are sparse on their homepage. The Icomera *Train Gateway*^{TM} system [8] consists of a hub on the train and the Train Gateway that is placed within the target network. These two support various wireless technologies (GPRS, Satellite etc.) to get connected. The choice of the *Large Range Wireless System* is left to the client.

A different approach is taken by *Wireless Train System*[2] (WTS) with their *Wireless Train Service Architecture (WTSA)* concept, where the whole roadway of the train is covered by APs and repeaters along the track. The APs are connected to the Internet, e.g. via ADSL.
Both concepts are expensive, either because of the costly Large Range Wireless System or an enormous infrastructural effort. Icomera's solution emanates from a rather simple concept, but to offer comfortable data rates for a number of users, several large range wireless connections have must be cascaded to widen this bottleneck. These technologies are very expensive. GPRS for example is about CHF 0.10 per kByte traffic[3]. The solution of WTS is less cost intensive to run, but the costs of the equipment and espe-

[1] http://www.icomera.com
[2] http://www.wirelesstrain.net
[3] http://swisscom-mobile.ch/sp/FDAAAAAA-de.html

cially their setup and installation are very expensive, since a whole physical network has to be built along the track and the APs and repeaters have to be supplied with power.

3.2 Related Technologies

3.2.1 MobileIP

MobileIP [9] is an extension of the IP protocol. It deals with the problem of handling a large number of mobile stations moving fast between different radio cells (Handoff) by using two addresses: The *home address* and the *care -of address*. The home address is static, whereas the care-of address changes at each new point of attachment. Moreover, MobileIP defines two entities to provide mobility support: a *Home Agent* (HA) and a *Foreign Agent* (FA) (see Figure 3.1).

The *Mobile Station (MS)* sends packets to a host. On their way back to the MS, the answer packets of the host are routed to the HA, since the MS is attached to the foreign network with its care-of address and not its home address. The HA redirects the answer packets through an IP tunnel to the FA by adding a new header with the care-of address as destination. The FA unwraps these packets and forwards them to the MS.

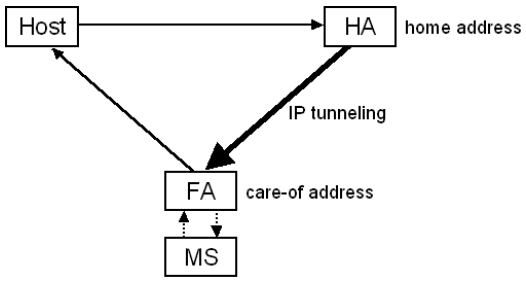

Figure 3.1: MobileIP

3.2.2 CellularIP

CellularIP [10] is a new protocol for mobile hosts that is optimized to provide access to a MobileIP enabled Internet with support of fast moving wireless hosts (see Figure 3.2). It inherits cellular systems principles for mobility

management, passive connectivity and handoff control. The central components of a CellularIP network are the *Base Station (BS)* and a gateway router. Mobile hosts attached to the network use the IP address of the gateway as their care-of address. Figure 3.2 illustrates the path of the packets addressed to a mobile host. The gateway "detunnels" packets and forwards them toward the BS. Inside the CellularIP network, mobile hosts are identified by their home addresses and data packets are routed without tunneling or address convertion.

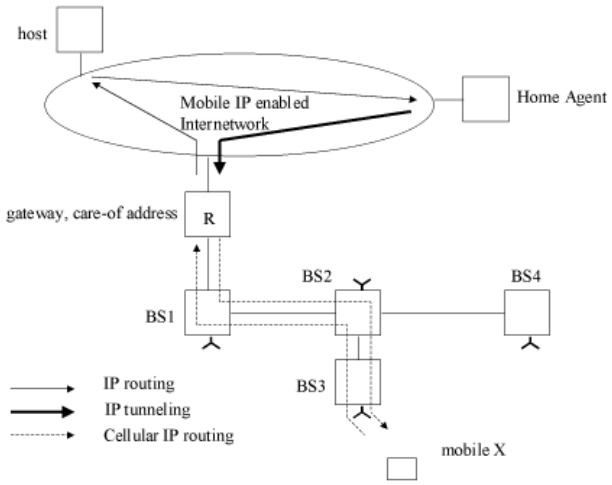

Figure 3.2: CellularIP

3.3 Wireless LAN Business Models

Currently a number of companies and unversities provide wireless LAN to allow employees or students an ubiquitous internet access within their buildings. Moreover, a number of companies have started to setup APs in highly frequented public places, so-called *Hot Spots*. Among these companies are the classical Telecom companies like Swisscom[4], but since the setup of a WLAN network is comparatively inexpensive and there is no licence fee for the usage of the frequencies, there are also new companies (e.g. Monzoon[5])

[4]http://www.swisscom-mobile.ch/sp/9DAAAAAA-de.html
[5]http://www.monzoon.ch

entering this promising market. However, the WLAN providing business is still "under construction", many problemes lack elegant solutions e.g. billing and authentication.

Since the launch of UMTS has been delayed, there are now efforts to get the best out of the existing technologies. Nokia offers a PCMCIA-card (D211[6]) that combines both technologies (GPRS & WLAN) and allows seamless roaming between them.

[6]http://www.nokia.com/phones/nokiad211

Chapter 4

The Access Point

We now turn to the discussion of the "Shuttle Bus WLAN Access Point" as it has been conceived and implemented within the scope of this thesis.

The first section of this chapter lists the requirements the AP has to meet. The second section deals with the AP hardware and its interfaces, followed by the presentation of the two system concepts that were developed and investigated in this thesis. Of these, the first was actually implemented and evaluated.

4.1 Requirements

The AP has to meet many criteria:

- *Performance:* The AP should provide several users on the bus with comfortable data rates and delay time.
- *Embedding:* The whole system should run on an embedded platform, more precisely, on a Set Top Box, which is ideal for this kind of purposes, since it is small, compact, silent and has a low power consumption.
- *Transparency:* Altough the AP is not physically connected to the ETH WLAN subnet, but routed through the Swisscom network and the Internet, the AP should act just like any regular AP on the campus to the user. Access and authentication should work like on the campus, though all traffic crosses the Internet before reaching the ETH network.

- *Security:* The AP should suffice the same security standards as any other AP of the ETH WLAN subnet.
- *Power Supply:* The AP should be embedded on the bus, i.e. it should not be depending on any dedicated power supply systems, but be integrated into the bus' power supply. Moreover, it should also work when the motor of the bus is turned off. Thus, it has to be equipped with an rechargeable battery that is charged while the motor of the bus is turned on.
- *Automatic Maintence:* The AP must be fail safe. An exception handling mechanism must cope with routine errors.

4.2 The AP Hardware

The prototype is based on a Fujitsu-Siemens Laptop, operated by Debian Linux (Kernel 2.4.19). Besides other interfaces, it has an Ethernet port, an integrated WLAN card and two PCMCIA slots.

For the usage on the bus, the system should be ported to the Set Top Box STB3036N by GCT Allwell[1] (See Appendix A.3). This box is an embedded PC, composed of standard PC components, with passive cooling. The processor is a GEODE GX1 (32-bit x86, with MMX compatible instruction set support). The Set Top Box provides one PCI slot, which can be equipped with a PCMCIA-Adapter (e.g. P222 by Elan Digital Systems[2]), which offers two PCMCIA slots. Moreover, it has an integrated Ethernet port and two IDE slots.

4.2.1 Large Range Wireless Interface

As pointed out in Section 2.2, GPRS is chosen for the *Large Range Wireless System*. It meets the above-mentionned requirements best, since it is packet switched and available on the route between the two campi.

As GPRS interface a GPRS/GSM card (*Globetrotter*, see Appendix A.2) by Option[3] is used. Using one of the PCMCIA slots and the *serial_cs* kernel module, it is adressable like a serial device.

[1] http://www.allwell.com.tw/
[2] http://www.elan-digital-systems.co.uk/adapter/data.php
[3] http://www.option.com

4.2.2 The WLAN Interface

To avoid the incorporation of a dedicated hardware AP, i.e. to keep the system compact, the AP interface is realized as a software AP. The HostAP Driver[4] by Jouni Malinen, enables every commercial WLAN card, that is based on the Prism Chipset 2/2.5/3, to act as an AP. The HostAP drivers are loaded as Linux kernel modules. Moreover, HostAP supports a number of other features, e.g. AP bridging, monitor mode, and support for wireless tools.

[4] http://hostap.epitest.fi

4.3 System Concept I

In the following sections two system concepts to achieve the aforementionned requirements are presented and investigated. The first of these was implemented and tested, whereas the second is theoretically presented and discussed.

The first system concept is based on a firewall on the AP and supports the New Access Concept (see Section 2.1.2) of the ETH WLAN only. The setup of System Concept I is depicted in Figure 4.1.

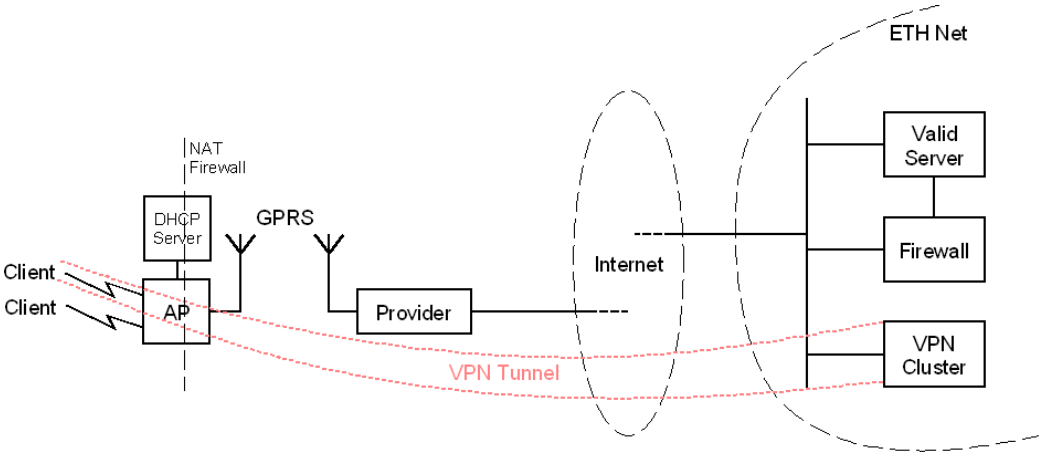

Figure 4.1: System Concept I

The mobile AP manages and operates a dedicated ETH-subnet of private IPs (172.30.199.0/24). The IP addresses are assigned by the DHCP-server on the AP. This subnet cannot be reached from outside, since these private IPs are not routed in the Internet. A *Network Address Translation (NAT)* gateway on the AP translates the private AP-subnet IPs to the IP of the GPRS point-to-point connection.
To access the ETH WLAN subnet, the client has to run a software *VPN-client*, provided by n.ethz[5]. The VPN-client connects to the VPN-server of the ETH and sets up an IPsec tunnel, through which the entire traffic of the client is routed. The address of the VPN-server is pre-configured in the

[5]http://n.ethz.ch/

VPN-software. Since the AP is connected to the ETH network via GPRS, i.e. it includes provider internal NAT, the VPN-client has to be configured to set up a TCP connection and NAT must be enabled. To avoid that a user accesses the Internet without passing the authentication on the VPN-server, the firewall (see Appendix B.2) allows traffic of the mobile AP to the following sites only:

- *VPN-Server of ETH WLAN:* Gateway to the ETH WLAN, where all users must authenticate and set up a VPN-connection to get to the ETH network and thence to the Internet.
- The n.ethz homepage, where a client gets the VPN-client software.
- The *Domain Name Server* of the GPRS Provider. To enable the user to resolve the names of the VPN-server and the n.ethz homepage.

A dedicated IP-address (172.30.199.240) is reserved for maintenance reasons, and thus not assigned by the DHCP server.

Pros & Cons of this System Concept

+ The authentication happens on the VPN-server, which queries the central Radius-server. Therefore, it suffices to have a n.ethz account and the above-mentioned VPN-client software.
+ Smooth incorporation into the ETH WLAN without any modifications of the existing infrastructure.
+ Embedded system with no further components or outstations. It is thus easy to maintain.
– The Old Access Concept via valid server is not implemented, since the user traffic cannot be routed via GPRS connection and the ETH-firewall.

4.4 System Concept II

As mentioned in 2.1.2, the ETH WLAN is separated from the rest of the ETH network by a dynamic firewall or the VPN-server. To extend System Concept I and to enable the Old Access Concept as well, the entire traffic of all the AP clients must be explicitely routed into the ETH WLAN subnet by the AP. This is achieved by setting up a tunnel (VPN) to a dedicated server within the ETH WLAN subnet.

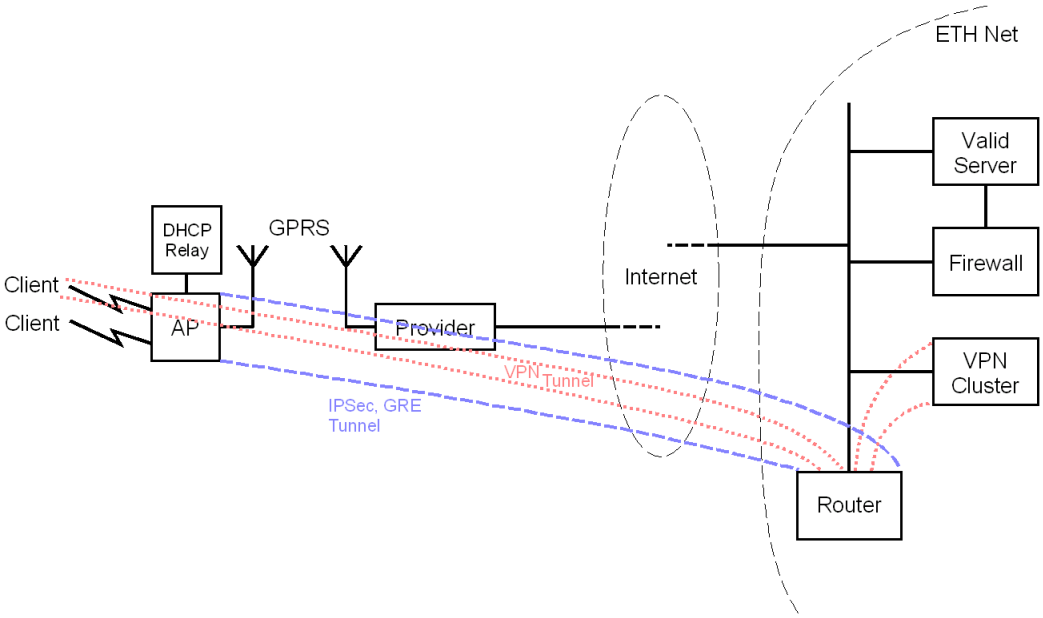

Figure 4.2: System Concept II

Intensive investigations revealed two feasible approaches to set up a tunnel. These are presented in the following two sections.

4.4.1 SSH-PPP-VPN

With the *Point-to-Point Protocol (PPP)* the TCP packets are converted into a character stream, which is then encrypted and transmitted via SSH connection. This enables forwarding between different subnets [11].

Pros & Cons

+ Easy to install and to set up.
+ No mucking with firewalls: If the SSH protocol traverses the connection, then PPP over SSH traverses as well.
+ PPP-SSH VPN's have no problems with dynamic IP addresses.
– If the SSH TCP connection is broken for any reason, the VPN goes down hard and takes all tunnelled TCP-connections with it.
– Works well with moderate loads over a reliable connection, but might cause some scalability problems. Has to be tested.
– Requires a dedicated router within the ETH WLAN subnet.

4.4.2 IPsec

IPsec[6] grants two choices of security services [12]:

- *Authentication Header (AH)* [13], which supports access control, connectionless message integrity, authentication and antireplay protection.
- *Encapsulating Security Payload (ESP)* [14], that supports access control, connectionless message integrity, authentication, antireplay protection and confidentiality.

In this scenario ESP has to be used, because the IPsec AH protocol incorporates a crytographic checksum including the IP addresses in the IP header. Since masquerading changes those IP addresses and since the cryptographic checksum cannot be recalculated by the masquerading firewall, the masqueraded packets will fail the checksum test and will be discarded by the remote IPsec gateway. Therefore, IPsec VPNs that use the AH protocol cannot be successfully masqueraded. ESP with authetication can be masqueraded.

Both AH and ESP support two modes of use:

1. The *transport mode* mainly provides end-to-end protection, where the IP packet payload is encrypted.

[6] http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

2. The *tunnel mode* encapsulates the entire IP packet (including the header) within a new IP packet to ensure that no part of the original packet is visible or may be changed as it is forwarded through a network.

For the present scenario, the tunnel mode is required, since an entire subnet must be routed through the tunnel.

NAT Implications

Generally, the use of NAT is quite troublesome in conjunction with IPsec, since the latter either hides private IP addresses through encryption and thus lets them escape translation, or integrity violations are experienced as a consequence of the NAT manipulating protected IP addresses.
For the present scenario, NAT happens in two different places:

1. The AP combines both IPsec and NAT functionality in the same box. By placing the NAT before the encryption of IPsec and the IPsec endpoint into the public address space of the GPRS connection, the coexistence of IPsec with NAT does not raise any compatibility problems. The packet address is translated before it is encrypted, i.e. no bothering with encryption and checksum of IPsec [15].

2. Within the provider's network, there are various potential sources for errors:

   - Incompatibility between IPsec authentication and NAT (as above)
     ⇒ solution: ESP instead of AH
   - Incompatibility between TCP checksum and NAT
     ⇒ TCP checksums have to be disabled or ignored
     ⇒ UDP encapsulation, instead of TCP encapsulation[16]

   - Incompatibility between IKE address identifiers and NAT
     ⇒ The *Internet Key Exchange (IKE)* (default IPsec method for secure key exchange) must be employed in AM (Agressive Mode), because it deploys identification data instead of IP adresses for end-node authentication. The same authentication method should also be used during the quick mode of IKE negotiation.

By additionally setting up a *Generic Route Encapsulation (GRE)* tunnel through either of these tunnels (SSH-PPP-VPN or IPsec) dynamic routing (e.g. OSPF) is applicable.

A word on the dedicated router: The tunnel has to be set up from both sides, thus it is favorable if both sides are based on the same technology and use the same implementation (tests with a Linux Box running Zebra[7] and Freeswan[8] on one side and a Cisco router on the other, i.e. an asymmetric setup turned out to be very problematic).

Pros & Cons

+ Stable implementions and widely used configurations are available
+ Additional features, e.g. GRE tunnel ⇒ dynamic routing
– Difficult to set up (see NAT implications above)
– Requires a dedicated router within the ETH WLAN subnet

4.4.3 Conclusion

System Concept II routes users on the bus directly into the ETH WLAN network, as if the mobile AP was physically connected to it. Thence, they are free to either authenticate on the valid server and cross the firewall or build up a VPN-tunnel to the VPN-server. The required transparency is created, but in return an additional router must be set up and maintained within the ETH WLAN.

4.5 The AP Software

The prototype is operated by Debian Linux. For the Set Top Box a dedicated slim Linux distribution for routers and firewalls is anicipated. Thus, in both cases routing and firewalling is provided by the kernel. Automation and maintenance routines are programmed as scripts. For further details see Chapter 5 and Appendix B

[7] http://www.zebra.org
[8] http://www.freeswan.org

Chapter 5

Embedding of the Access Point

5.1 Porting System to Box

The Set Top Box is described in detail in Appendix A.3. By using a PCI -PCMCIA adapter with two PCMCIA slots, the same hardware prerequisites as in the prototype are given. The rest of the hardware and software configuration are analogous to the prototype and are accordingly set up. The Ethernet port is used to access the box (via SSH) and for maintenance.

5.2 Automation & Maintenace

5.2.1 Automation

The AP automatically sets up all interfaces, starts the GPRS connection and the necessary daemons and programs. Moreover, a periodically invoked cron job, checks the connection and configures and restarts them, in case they are not working properly. The state diagram in Figure 5.1 on the next page illustrates the application flow of the script.

5.2.2 Maintenance

The dedicated server for System Concept II (see Section 4.4) is planned to run a daemon that sends out e-mail messages, whenever the connection to the mobile AP fails.

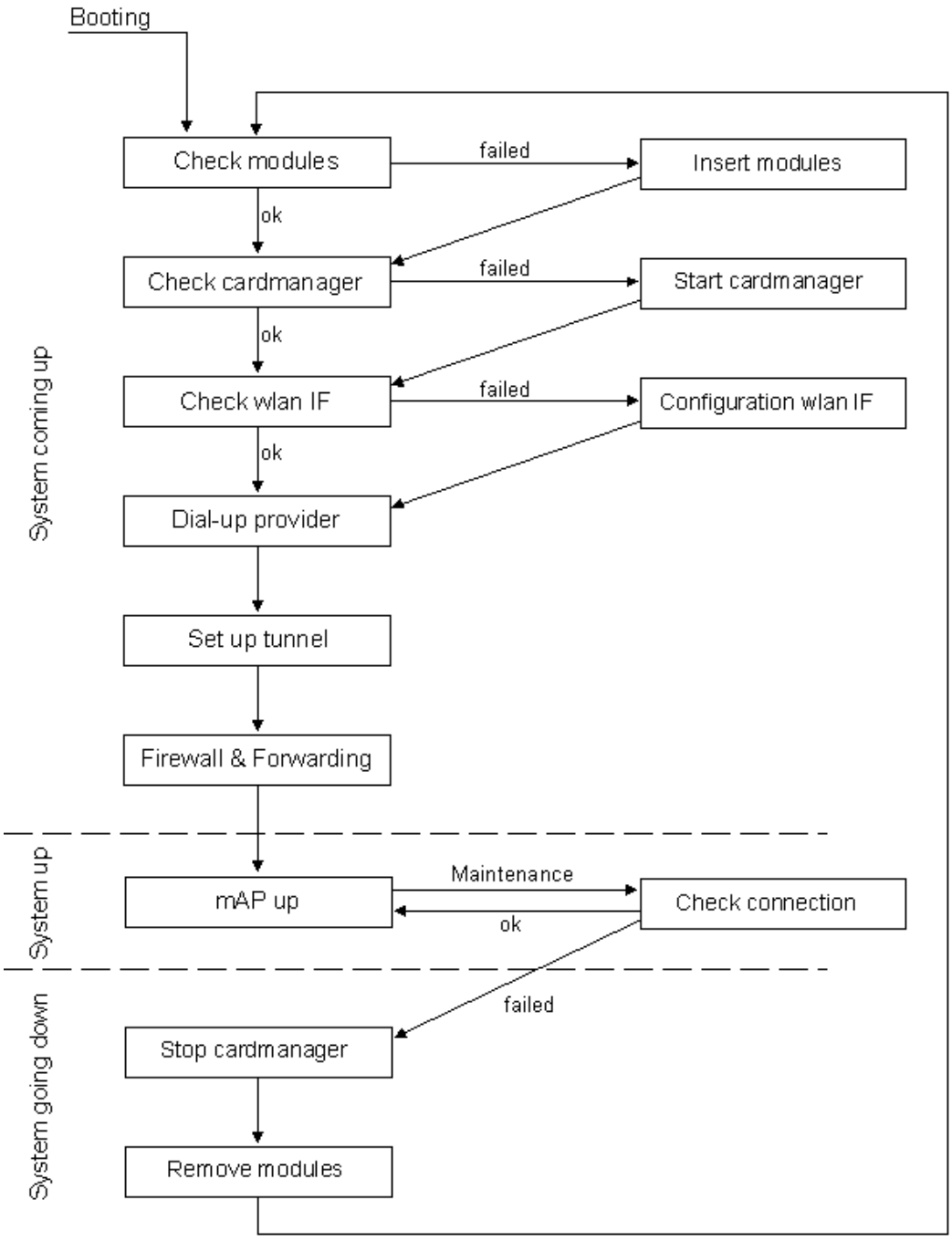

Figure 5.1: Stateflow of the Automation of the mobile Acess Point (mAP)

Chapter 6

Testing

To evaluate the implemented prototype on the route between the two campi, three metered values were chosen to describe its performance. These are presented in the following sections and the received values are discussed. Since it is obvious that the deployed GPRS connection is the bottleneck for the whole system, the performance evaluation focuses on the GPRS connection.

6.1 Signal Strength

In a first serie of tests the strength of the received signal on the route was measured. The GPRS card features a function (*at+csq*) that outputs the current signal strength in dBm. The range of the measurement runs from $-111dBm$ to $-51dBm$. dBm is converted to mW according to the following formula:

$$P_{mW} = 10^{(\frac{P_{dBm}}{10})}$$

Figure 6.1 illustrates the mean values of the series. It shows that the values at the stations *Schaffhauserplatz* and *Weihersteig* are above average and that the signal strength gets weaker leaving the densely populated area (between *Im Wingert* and *Hönggerberg*) and stronger again approaching *ETH Hönggerberg*. These characteristics are confirmed by the data rates of Figure 6.2.

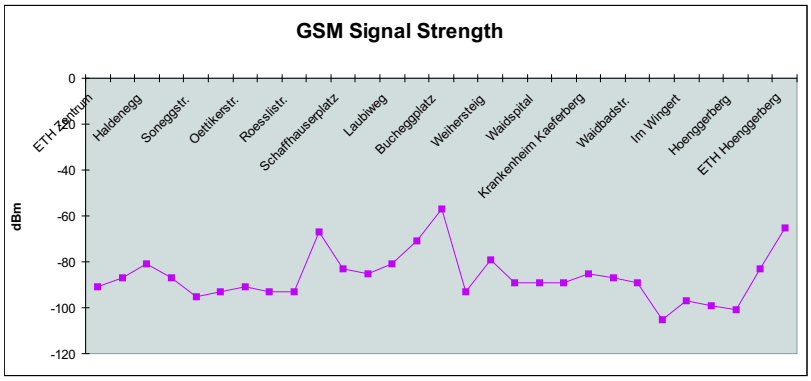

Figure 6.1: GSM Signal Strength during the Bus Ride

6.2 Data Rate

Figure 6.2 displays the data rates measured with *Netperf*[1]. This program generates a TCP stream of $16kBytes$ messages to determine the data rates of a connection. The results are depicted in Figure 6.2 in $10^3 bits/s$. The resulting average is about 1.3 kB/s. Moreover, there is a connection gap around *Hönggerberg*.

The Test with Netperf is problematic, since the results of the measurements are clearly below the expectated values of 30 - 50 kbits/s. Practical tests showed that the data rate must be higher. The download of a testfile with the a browser resulted in a mean data rate of about $4kB/s$.

6.3 Request/Response Time

The round-trip time was measured with *ping*. The illustrated values are the mean of a serie of measurements. The measuring unit is ms. This results in a round-trip average latency in a range between one and two seconds.

The larger part the time is spent within the GPRS network as seen in the following listing of a traceroute from the AP to a server within the ETH LAN. The first three columns show the results of three different measurings. Each value represents the time to the gateway (his adress is noted in the last column) and back to the testing host.

[1] http://www.netperf.org/netperf/NetperfPage.html

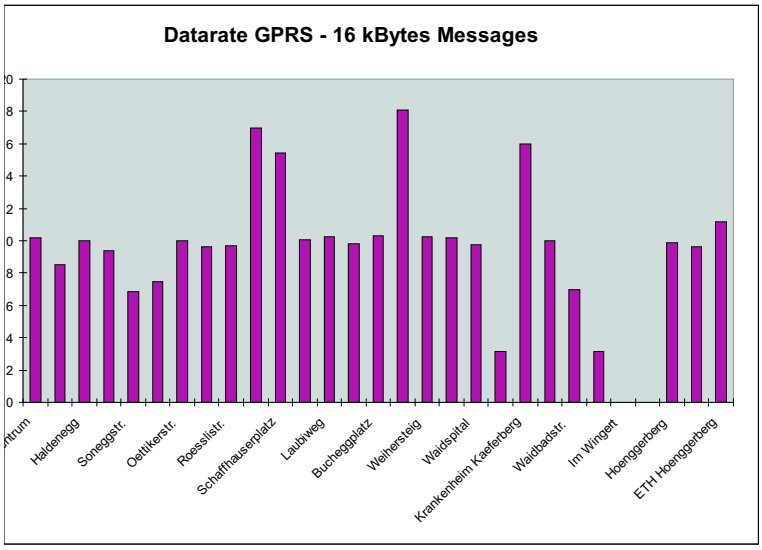

Figure 6.2: Data Rate of TCP over GPRS. Measured with Netperf

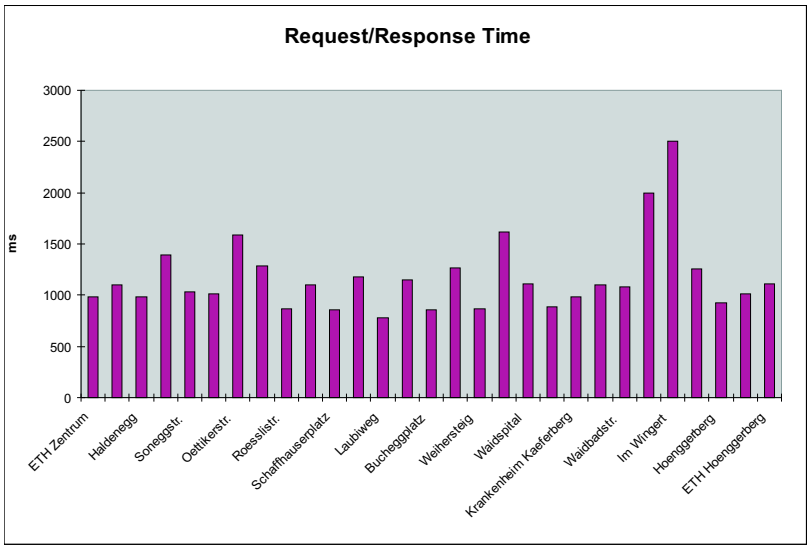

Figure 6.3: Request/Response Time. Measured with Ping

Since all values are over $700ms$ the conclusion is drawn that about 600-$700ms$ are spent within the GPRS network.

traceroute to pc-3298.ethz.ch [129.132.57.118], 30 hops max:

1	762 ms	1069 ms	900 ms	10.141.200.254
2	935 ms	1027 ms	1051 ms	10.141.200.254
3	1040 ms	870 ms	860 ms	192.168.177.65
4	1260 ms	1040 ms	1027 ms	172.25.145.2
5	1103 ms	862 ms	1419 ms	172.25.145.9
6	983 ms	867 ms	871 ms	192.168.177.85
7	1692 ms	859 ms	848 ms	192.168.19.13
8	917 ms	1051 ms	859 ms	138.188.101.249
9	1378 ms	1047 ms	1044 ms	192.168.8.10
10	979 ms	1050 ms	860 ms	192.168.10.1
11	1031 ms	859 ms	1388 ms	194.209.131.132
12	886 ms	1027 ms	871 ms	164.128.83.1
13	1006 ms	859 ms	848 ms	i71lzw-010-FastEthernet2-0.ip-plus.net [164.128.84.254]
14	1039 ms	1050 ms	860 ms	i79zhb-015-ser5-1-1.ip-plus.net [164.128.33.201]
15	721 ms	863 ms	1028 ms	zhb-005-GigEth8-0.ip-plus.net [164.128.33.33]
16	861 ms	862 ms	848 ms	i79tix-005-GigEth1-2.ip-plus.net [164.128.34.146]
17	1213 ms	1028 ms	1050 ms	Switch-1.ip-plus.net [164.128.33.118]
18	861 ms	863 ms	848 ms	swiEZ2-G3-2.switch.ch [130.59.36.249]
19	930 ms	847 ms	1051 ms	rou-eth-switch-1-giga-to-switch.ethz.ch [192.33.92.1]
20	1185 ms	1050 ms	1040 ms	rou-etx-1-mega-transit.ethz.ch [129.132.99.79]
21	841 ms	848 ms	1050 ms	pc-3298.ethz.ch [129.132.57.118]

Chapter 7

Conclusions & Further Perspectives

The efforts and studies within the scope of this thesis, to build a mobile AP for the ETH Shuttle Bus, produced a working prototype, but also revealed difficulties and limitations.

7.1 Results

A mobile AP for the Shuttle Bus is realizable with the existing technologies and infrastructure. But the *Large Range Wireless System*, which determines the data rate and the data unit price, forms a considerable bottleneck. As for related works, only two related project were found (see Section 3.1).

7.1.1 Large Range Wireless System

The comparison of different *Large Range Wireless Systems* (see Section 2.2.1) evinced GPRS to be the proper technology for the present system, since it provides very good network coverage and is accounted per data unit. Nevertheless, data rates are limited to some ten kbit/s at a price of approximately 10 sFr. per Megabyte.

7.1.2 Access Concepts

An important functionality of the AP is the provision of transparent access to the ETH WLAN. It turned out that the New Access Concept (see Section 2.1.2) is easier to implement, since the user himself sets up a VPN tunnel to a dedicated router, where he has to authenticate, i.e. no supplementary routing by the AP is required. This so-called *System Concept I* (see Section 4.3) was successfully implemented and tested. It allows the users on the shuttle bus to connect to the VPN-Server via WLAN interface and thence access the ETH LAN.
To support both access concepts, a second concept was designed and studied. This *System Concept II* (see Section 4.4) is based on a tunnel to a dedicated server within the ETH WLAN subnet. The tunnel virtually embedds the AP subnet into the ETH WLAN subnet.

7.1.3 Testing

The tests described in chapter 6 confirm that the *Large Range Wireless System* is the bottleneck. With maximum data rates of about $4kB/s$ or less, the performance is combarable with an analog modem.
The round-trip times are high in comparison with other technologies. Thus, the system is not reasonable for terminal applications or streaming. The connection gap is not very problematic for applications other than the aforementioned. It is geographically limited and therefore neglectable for a best effort system as the Internet.

7.2 Further Perspective

- *System Concept II:* The above-mentioned System Concept II is to be implemented and tested. Attempts showed that the setup has to be symmetric, (the same technologies at both ends of the tunnel). Thus, it is recommended to use a Linux box as outstation.

- *Porting to the Set Top Box:* The current Debian Linux on the Set Top Box should be replaced by *Linux Embedded Appliance Firewall (LEAF)*[1]. At boot time, this operating system is decompressed from a

[1] http://leaf.sourceforge.net/

Flash Card and loaded into a RAM disk, where it is executed. This solution works without any movable components, the system is therefore less vulnerable to concussions.

- *Cascading of several GPRS connections:* The cascading of several GPRS connections might improve the data rates. Studies and tests must be performed to reveal whether and how scalable a cascading is, e.g. by using a cellular phone for first tests. Channel balancing is an important issue in such a set up. There are tools for this kind of traffic adaption, e.g. bacp[2]. These have to be investigated and if useful, applied.

[2]http://www.networksorcery.com/enp/protocol/BACP.htm

Appendix A

Used Hardware

A.1 WLAN Access Point

In this section the hardware and the configuration used for the WLAN interface are described.

A.1.1 PC Card

Instant Wireless Network PC Card WPC11, Linksys[1] (Figure A.1).

Figure A.1: WPC11 by Linksys

[1] http://www.linksys.com

A.1.2 Configuration

A.1.3 Kernel Configuration for PCMCIA Support

PCMCIA/CardBus support:	m(odule)
CardBus support:	y(es)

Modules

yenta_socket.o :	PCI-to-CardBus
ds.o :	Driver Service
serial_cs.o :	PCMCIA Serial Port Driver
hostap_cs.o :	HostAP PCMCIA
hostap_pci.o :	HostAP PCI

Mapping PCMCIA Card to Driver

in /etc/pcmcia/hostap_cs.conf

```
...
...
card "EMTAC A2424i 11Mbps WLAN Card"
   manfid 0xc250, 0x0002
#   cis "cis/Emtac.dat"
   bind "hostap_cs"

card "Linksys WPC11 11Mbps WLAN Card"
   version "Instant Wireless ", " Network PC CARD", "Version 01.02"
   bind "hostap_cs"

card "Linksys WPC11 Ver 2.5 11Mbps WLAN Card"
   manfid 0x0274, 0x1612
   bind "hostap_cs"
...
...
```

Wireless Tools

The Wireless Extension[2] is a generic API allowing a driver to expose to the user space configuration and statistics specific to common Wireless LANs.

iwconfig :	Similar to ifconfig, but for wireless interfaces
iwevent :	Display Wireless Events
iwgetid :	Report ESSID, NWID or AP/Cell Address
iwlist :	Get Wireless statistics
iwpriv :	Configure optional parameters

Configuration

If the setup was succesfully, the output of *iwconfig* should look like the following listing or similar. The *ESSID* is set to *public* and the *Mode* to *Master*. From now on the device can be configured like an ethernet device with *ifconfig*.

```
wlan0     IEEE 802.11-b  ESSID:"public"
          Mode:Master  Frequency:2.422GHz  Access Point: 00:03:2F:03:20:FF
          Bit Rate:11Mb/s   Tx-Power:-4 dBm   Sensitivity=1/3
          Retry min limit:8   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

[2] http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

A.2 GPRS Modem

A.2.1 PC Card

GlobeTrotter Tri-band GPRS/GSM PCMCIA Modem by Option[3] (Figure A.2).

Figure A.2: GlobeTrotter Universal Tri-band GPRS/GSM PC-Radio Card

A.2.2 Configuration

Kernel Configuration for Modem Support

PPP support :	m
PPP filtering :	y
PPP support for sync tty ports :	m
PPP Deflate compression :	m
PPP BSD-Compress compression :	m

Scripts

Pon is used for dial-up. The scripts for pon are in /etc/ppp/peers.

[3] http://www.option.com

/etc/ppp/peers/swisscom :

```
noauth
crtscts
user gprs
connect '/usr/sbin/chat -v -f /etc/ppp/chatdata'
/dev/ttyS1
115200
noipdefault
defaultroute
bsdcomp 0,0
debug
```

/etc/ppp/chatdata :

```
'ABORT' 'BUSY'
'ABORT' 'ERROR'
'ABORT' 'NO CARRIER'
'ABORT' 'NO DIALTONE'
'ABORT' 'Invalid Login'
'ABORT' 'Login incorrect'
'' 'ATZ'
'OK' 'AT+CGDCONT=1'
'OK' 'AT+CGDCONT=1,"IP","gprs.swisscom.ch"'
'OK' 'AT+CPIN="xxxx"'
'OK' 'ATD*99***1#'
'CONNECT'
```

A.3 Set Top Box

In this section the Set Top Box STB3036N (see Figure A.3) by Allwell[4] is presented.

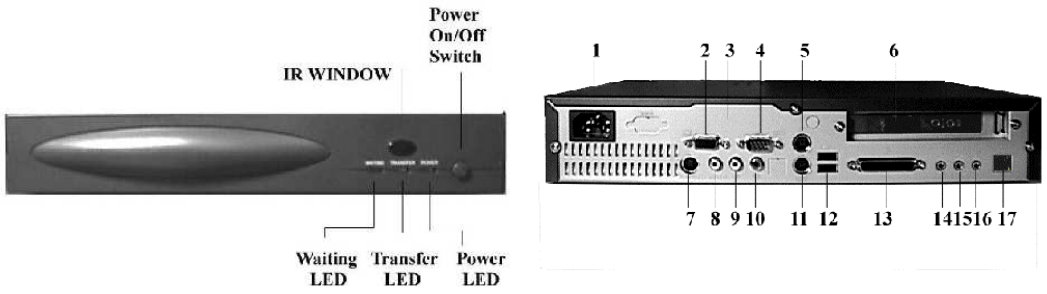

Figure A.3: Settop Box STB3036N, Allwell

Legend

1	AC Power	10	Audio out R
2	VGA Port	11	Keyboard
3	Optional (Scart)	12	USB
4	RS-232	13	Parallel port
5	PS/2	14	Line out
6	Exp. Slot PCI	15	Line in
7	S-Video	16	Microphone
8	Composite Video	17	RJ-45 LAN
9	Audio out L		

A.3.1 Features

- Geode GX1 CPU 266 up to 333MHz 32-bit x86, with MMX compatible instruction set support
- Integrated Floating Point Unit (FPU)

[4] http://www.allwell.com.tw

- Two 168-pin DIMM sockets (max of 256MB)
- Support M-System DOC from 16-144MB
- Support 40 pin IDE interface Flash Module from 16-256MB
- 2 x Ultra DMA/33 for up to four IDE devices
- 10/100Mb Ethernet Controller
- EISA type slot support PCI and ISA add on
- One PCI 104 socket
- Board Size: Dimension 242 x 235 mm
- APM 1.2 compliant
- Award BIOS with APM and PnP
- Power Supply: 45W, 5V/3A, 12V/2A, -12V/0.3A, 90-264V Auto switching or
- Optional add-on: Smart card reader, Compact Flash card

Appendix B

Used Software

B.1 Software Versions

Linux

Debian[1] Linux 3.0 with Kernel 2.4.19

HostAP

HostAP[2] driver for Intersil Prism2/2.5/3, Release 2002-10-12

Wireless Tools

Wireless Tools[3] for Linux, Version 25

Cisco VPN-Client

VPN-Client[4] for Windows and Linux, Release 3.6

[1] http://www.debian.org
[2] http://hostap.epitest.fi/
[3] http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html
[4] http://www.cisco.com/en/US/products/sw/secursw/ps2138/index.html

B.2 Firewall & NAT

To set up the firewall and NAT for the Approach I as mentioned in 4.3, the following script is used:

```
#!/bin/sh
#
# rc.firewall-2.4-stronger
FWVER=0.80s

# Log:
#   0.80s - Addapted for mAP
#   0.73s - Added comments in the output section that DHCPd is optional
#           and changed the default settings to disabled
#   0.72s - Changed the filter from the INTNET to the INTIP to be
#           stateful; moved the command VARs to the top and made the
#           rest of the script to use them
#   0.70s - Added a disabled examples for allowing internal DHCP
#           and external WWW access to the server
#   0.63s - Added support for the IRC module
#   0.62s - Initial version based upon the basic 2.4.x rc.firewall

$
echo -e "\nLoading rc.firewall - version $FWVER..\n"

# The location of various iptables and other shell programs
IPTABLES=/sbin/iptables

LSMOD=/sbin/lsmod
DEPMOD=/sbin/depmod
INSMOD=/sbin/insmod
GREP=/bin/grep
AWK=/usr/bin/awk
SED=/bin/sed
IFCONFIG=/sbin/ifconfig

#Setting the EXTERNAL and INTERNAL interfaces for the network
EXTIF="ppp0"
INTIF="wlan1"

# Determine the external IP
EXTIP="‘$IFCONFIG $EXTIF | $GREP ’inet addr’ | $AWK ’{print $2}’ | \
$SED -e ’s/.*://’‘"
```

```
# Assign the internal TCP/IP network and IP address
INTNET="172.30.199.0/24"
INTIP="172.30.199.1"

# Setting a few other local variables

UNIVERSE="0.0.0.0/0"

#Swisscom DNS 1
SCDNS1="164.128.36.34"

#Swisscom DNS 2
SCDNS2="164.128.76.39"

#vpn-cluster ethz
VPN1="129.132.99.161"
VPN2="129.132.99.162"
VPN3="129.132.99.163"
VPN4="129.132.99.171"

#n-ethz.ch
NETHZ="129.132.97.10"

#Address for Maintenance
SERVICE="172.30.199.14"

# Need to verify that all modules have all required dependencies
$DEPMOD -a

#Load the main body of the IPTABLES module - "ip_tables"
if [ -z "‘ $LSMOD | $GREP ip_tables | $AWK {’print $1’} ‘" ]; then
   $INSMOD ip_tables
fi


#Load the stateful connection tracking framework - "ip_conntrack"
if [ -z "‘ $LSMOD | $GREP ip_conntrack | $AWK {’print $1’} ‘" ]; then
   $INSMOD ip_conntrack
fi

#Load the FTP tracking mechanism for full FTP tracking
if [ -z "‘ $LSMOD | $GREP ip_conntrack_ftp | $AWK {’print $1’} ‘" ]; then
   $INSMOD ip_conntrack_ftp
fi
```

```
#Load the IRC tracking mechanism for full IRC tracking
if [ -z "‘ $LSMOD | $GREP ip_conntrack_irc | $AWK {’print $1’} ‘" ]; then
   $INSMOD ip_conntrack_irc
fi

#Load the general IPTABLES NAT code - "iptable_nat"
#  - Loaded automatically when MASQ functionality is turned on
if [ -z "‘ $LSMOD | $GREP iptable_nat | $AWK {’print $1’} ‘" ]; then
   $INSMOD iptable_nat
fi

#Loads the FTP NAT functionality into the core IPTABLES code
echo -e "ip_nat_ftp"
if [ -z "‘ $LSMOD | $GREP ip_nat_ftp | $AWK {’print $1’} ‘" ]; then
   $INSMOD ip_nat_ftp
fi

#Enable IP forwarding
echo "  Enabling forwarding.."
echo "1" > /proc/sys/net/ipv4/ip_forward

echo "  Enabling DynamicAddr.."
echo "1" > /proc/sys/net/ipv4/ip_dynaddr

#############################################################################
#
# Enable IP forwarding and Masquerading

# Clearing any previous configuration
echo "  Clearing any existing rules and setting default policy to DROP.."
$IPTABLES -P INPUT DROP
$IPTABLES -F INPUT
$IPTABLES -P OUTPUT DROP
$IPTABLES -F OUTPUT
$IPTABLES -P FORWARD DROP
$IPTABLES -F FORWARD
$IPTABLES -F -t nat

# Flush the user chain.. if it exists
if [ -n "‘$IPTABLES -L | $GREP drop-and-log-it‘" ]; then
   $IPTABLES -F drop-and-log-it
fi
# Delete all User-specified chains
$IPTABLES -X
# Reset all IPTABLES counters
```

```
$IPTABLES -Z

#Configuring specific CHAINS for later use in the ruleset
echo "  Creating a DROP chain.."
$IPTABLES -N drop-and-log-it
$IPTABLES -A drop-and-log-it -j LOG --log-level info
$IPTABLES -A drop-and-log-it -j DROP

######################################################################
# INPUT: Incoming traffic from various interfaces.  All rulesets are
#        already flushed and set to a default policy of DROP.

# loopback interfaces are valid.
$IPTABLES -A INPUT -i lo -s $UNIVERSE -d $UNIVERSE -j ACCEPT

# local interface, local machines, going anywhere is valid
#$IPTABLES -A INPUT -i $INTIF -s $INTNET -d $UNIVERSE -j ACCEPT

# remote interface, claiming to be local machines, IP spoofing, get lost
$IPTABLES -A INPUT -i $EXTIF -s $INTNET -d $UNIVERSE -j drop-and-log-it

# Allow any related traffic coming back to the MASQ server in
$IPTABLES -A INPUT -i $EXTIF -s $UNIVERSE -d $EXTIP -m state --state \
ESTABLISHED,RELATED -j ACCEPT

#Maintenance Port SSH
$IPTABLES -A INPUT -i $INTIF -s $SERVICE -d $INTIP -j ACCEPT

# DHCPd
$IPTABLES -A INPUT -i $INTIF -p tcp --sport 68 --dport 67 -j ACCEPT
$IPTABLES -A INPUT -i $INTIF -p udp --sport 68 --dport 67 -j ACCEPT

# Catch all rule, all other incoming is denied and logged.
$IPTABLES -A INPUT -s $UNIVERSE -d $UNIVERSE -j drop-and-log-it

######################################################################
# OUTPUT: Outgoing traffic from various interfaces.  All rulesets are
#         already flushed and set to a default policy of DROP.

# loopback interface is valid.
$IPTABLES -A OUTPUT -o lo -s $UNIVERSE -d $UNIVERSE -j ACCEPT

# local interfaces, any source going to local net is valid
$IPTABLES -A OUTPUT -o $INTIF -s $EXTIP -d $INTNET -j ACCEPT
```

```
# local interface, any source going to local net is valid
$IPTABLES -A OUTPUT -o $INTIF -s $INTIP -d $INTNET -j ACCEPT

# outgoing to local net on remote interface, stuffed routing, deny
$IPTABLES -A OUTPUT -o $EXTIF -s $UNIVERSE -d $INTNET -j drop-and-log-it

# anything else outgoing on remote interface is valid
$IPTABLES -A OUTPUT -o $EXTIF -s $EXTIP -d $UNIVERSE -j ACCEPT

# DHCPd
$IPTABLES -A OUTPUT -o $INTIF -p tcp -s $INTIP --sport 67 \
-d 255.255.255.255 --dport 68 -j ACCEPT
$IPTABLES -A OUTPUT -o $INTIF -p udp -s $INTIP --sport 67 \
-d 255.255.255.255 --dport 68 -j ACCEPT

# Catch all rule, all other outgoing is denied and logged.
$IPTABLES -A OUTPUT -s $UNIVERSE -d $UNIVERSE -j drop-and-log-it

##############################################################################
# FORWARD: Enable Forwarding and thus IPMASQ

echo "     - FWD: Allow only existing/related connections in"
$IPTABLES -A FORWARD -i $EXTIF -o $INTIF -m state --state ESTABLISHED,RELATED \
-j ACCEPT

# some adresses are open:
# Swisscom DNS
$IPTABLES -A FORWARD -i $INTIF -s $INTNET -d $SCDNS1 -j ACCEPT
$IPTABLES -A FORWARD -i $INTIF -s $INTNET -d $SCDNS2 -j ACCEPT
# vpn-cluster.ethz.ch
$IPTABLES -A FORWARD -i $INTIF -s $INTNET -d $VPN1 -j ACCEPT
$IPTABLES -A FORWARD -i $INTIF -s $INTNET -d $VPN2 -j ACCEPT
$IPTABLES -A FORWARD -i $INTIF -s $INTNET -d $VPN3 -j ACCEPT
$IPTABLES -A FORWARD -i $INTIF -s $INTNET -d $VPN4 -j ACCEPT
# n.ethz.ch
$IPTABLES -A FORWARD -i $INTIF -s $INTNET -d $NETHZ -j ACCEPT

# Catch all rule, all other forwarding is denied and logged.
$IPTABLES -A FORWARD -j drop-and-log-it

echo "     - NAT: Enabling SNAT (MASQUERADE) functionality on $EXTIF"
$IPTABLES -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE

##############################################################################
echo -e "\nStronger rc.firewall-2.4 $FWVER done.\n"
```

Bibliography

[1] IEEE Std 802.11, The Institute of Electrical and Electronics Engineers Inc, 1997.

[2] ETH World, *http://www.ethworld.ethz.ch*, 2002.

[3] IEEE 802.11b Wireless LANs, Wireless Freedom at Ethernet Speeds, 3Com Corporation, 2000.

[4] Introduction to Wireless LANs, WLANA Inc, 1999.

[5] Wireless LAN Konzept ETH, *http://www.wireless.ethz.ch/files/ETHZ_WLAN_Konzept_2002.pdf*, April 2002.

[6] Christian Bettstetter, Hans-Jörg Vögel, and Jürg Eberspächer. GSM Phase 2+ General Packet Radio Service GPRS: Architecture, Protokols and Air Interface, IEEE Communications Survey vol.2 no.3, 1999.

[7] Alan Sicher and Randall Heaton. GPRS Technology Overview, White Paper, Dell, 2002.

[8] Icomera Train Gateway v1.1, *http://www.icomera.com/downloads/pdf/IcomeraTrainGateway_11.pdf*

[9] Inge Gronboek. Cellular and Mobile IP: Overview and Enhancements, Project Paper, 1999.

[10] Comet Group. CellularIP, Columbia University N.Y., 2002.

[11] Scott Bronson. PPP-SSH MiniHOWTO, *http://www.linux.org/docs/ldp/howto/mini/ppp-ssh/index.html*, 2002.

[12] Christos Xenakis, Evangelos Gazis, and Lazaros Merakos. Secure Deployment in GPRS Mobile Networks, Proceedings, 2002.

[13] S. Kent and R. Atkinson. IP Authentication Header, RFC 2402, Nov 1998.

[14] S. Kent and R. Atkinson. IP Encapsulating Security Payload, RFC 2406, Nov 1998.

[15] Bernard Adoba. IPsec-NAT Compatibility Requirements, Internet Draft, draft-ietf-ipsec-nat-reqts-02.txt, August 2002.

[16] A. Huttunen. UDP Encapsulation of IPsec Packets, Internet Draft, draft-ietf-ipsec-udp-encaps-03.txt, June 2002.