Wireless access in the Kista - IT University

Alberto Escudero, aep@flyinglinux.net
Björn Pehrson, bjorn@it.kth.se
Enrico Pelletta, enrico@it.kth.se
Jon-Olov Vatn, vatn@it.kth.se
Pawel Wiatr, pawel@it.kth.se

Royal Institute of Technology KTH
Department of Microelectronics and Information Technology IMIT
Electrum 204
S-164 40 Kista - Sweden

17 March 2001

Abstract

The wireless internet access of the Kista - IT University network started out in October 1999 as a research project - "The FlyingLinux project" - in the Telecommunication Systems Lab at the Department of Teleinformatics at KTH (Sweden).

The research main objective was to study the possibility of adopting MobileIPv4 and standard DHCP-based wireless access as part of the IT University network infrastructure. The result of that work was that a *IEEE 802.11b based* environment was available for one hundred users during the 2G1303 project course that was held from March to May 2000.

After that experience a new *environment* was conceived to offer internet access for the two hundred students and researchers of the IT-University study programme. Each student or researcher uses a IEEE 802.11b compliant PCMCIA card to get wireless connectivity using a set of access points available in three different buildings and common areas. Mobility is supported between the radio cells using link level handover or MobileIP when roaming between IP networks. The wireless access allows students to attend lectures with their laptops, take notes and see online documentation while their mail arrives in their laptop mailboxes. The Kista-IT University wireless network is proud of being one the biggest wireless academic network in the world which supports MobileIP.

This paper gives an overview of the new wireless environment available at KTH IT-University as of winter 2001. The paper focuses on design and functional issues and introduce the network using a top-down approach, that is, describing the big functional blocks and then the details of the implementation.

1 Background

1.1 KistaOpen

KistaOpen is an umbrella for a number of different internetworking projects in the Kista borough in Stockholm. KistaOpen includes the *campus network* of KTH Kista, the *student dormitory network* "KistaIP"[1] , the *Sweden Silicon Valley Link network* "SSVL" connecting the KTH campus and the Stanford University campus in California (USA) and the *Internet exchange* "KistaIX".

Other projects being discussed under the KistaOpen umbrella include:

1. Expansion of the Kista access network to other housing than student dormitories.

[1] KistaIP project aims to be the first step towards a *city network* for Kista.

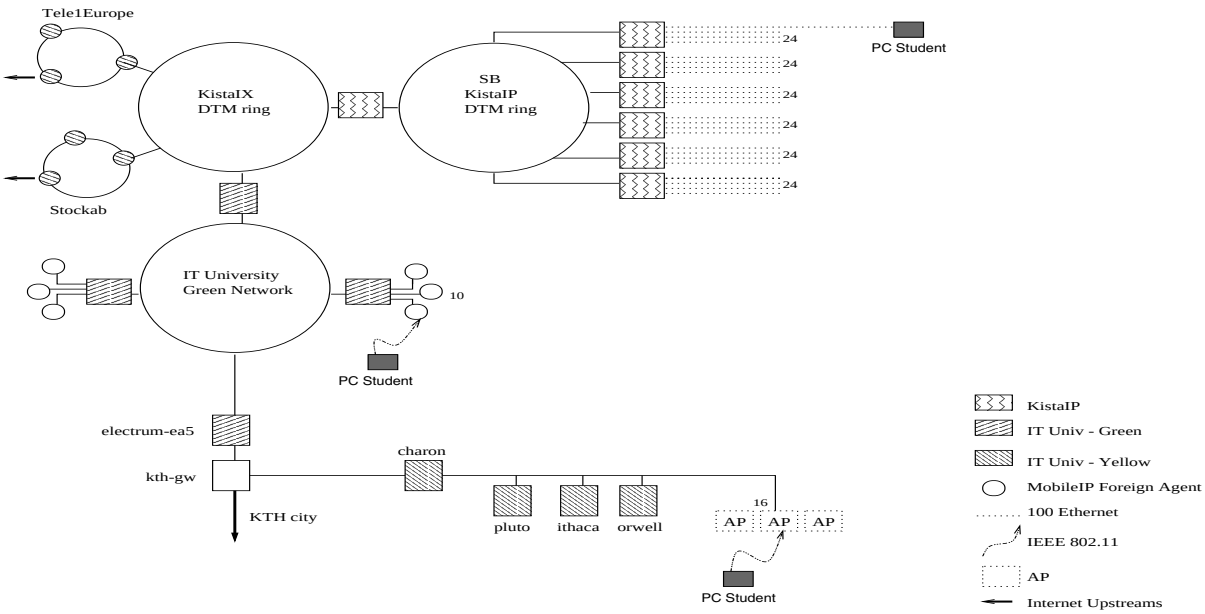

Figure 1: KistaIX, KistaIP, IT University (Green & Yellow) networks

2. Mobile IP-based roaming between different wireless networks, including wireless LANs, GPRS, UMTS, Bluetooth.

3. Introduction of (M)IPv6 in all networks.

4. QoS and resource sharing services.

5. Traffic measurement, modeling and analysis.

1.2 IT University

In 1999, KTH formed a new school of Information Technology located on its Campus in Kista. Since some of the activities of the new school are organized in cooperation with the University of Stockholm and Karolinska Institute, it is also called the IT-University. In fall 2000, a new diploma engineering program in Information technology was launched. The admission in the year 2000 was 150 students and will in the year 2002 increase to 300 students so that the fully expanded program includes some 1500 students.

The school also offers a three year applied engineering program including some 1800 students, graduate education in computing and systems sciences, teleinformatics and electronics. Continuing education is also offered, both on campus and via KTH Online .[2] . Including programs offered by the University of Stockholm and Karolinska Institute, the total number of students will be around 6000 within the next four years.

The IT-University has decided to provide their students with a campus network beyond state of the art, including wireless access supporting roaming and a number of novel services.

1.3 KistaIP

For the students studying on the Kista campus, there is student housing provided by Svenska Bostäder (SB) on a former sports ground called KistaIP. SB is a housing company and a subsidiary of the City of Stockholm. SB has decided to use KistaIP as one of their testbeds for how to offer their tennants network services. There is a fiber pair to each apartment, which initially is used to deliver 100 Mbit/s ethernet connections. One router port is available for each apartment and a 2Gbit/s uppstreams connection to the Internet Exchange (KistaIX). A service that SB wants to provide their tennants is the free choice of upstreams service provider.

[2]KTH Online `http://www.online.kth.se`

1.4 SSVL

The Sweden Silicon Valley Link was first established in 1995 to explore the impact of the global information infrastructure on the future of academic life. It currently consists of a dedicated leased T1-line connecting two Gigabit/s rings, one connecting the main buildings on the KTH-Kista campus and one connecting a few strategic laboratories at Stanford University. SSVL is organized as a public AS (8973) and is peering with Stanford, KTH, Tallinn Technical University (via a dedicated E1 connection Kista Tallinn) and the Technical University of Blekinge in Karlskrona, Sweden.

1.5 KistaIX

The Kista Internet eXchange (KistaIX) is designed to exchange traffic between the KistaIP student housing network, the KTH campus network, commercial ISPs and other IXes. This will make it possible for the students to develop commercial services which are not allowed in the academic network and for KTH to share redundant connections between the networks on its different campuses. There is also a discussion about moving the SSVL link to connect KistaIX and PAIX in Palo Alto, to which Stanford is also connected, to increase the utilization of the link and make it possible to enhance its capacity. The first commercial ISP to be conected is Tele1Europe and the first other IX to be connected is the Stokab IX in downtown Stockholm.

2 IT University Network

2.1 Network topology

The Kista - IT University network is divided into three functional networks called *Red, Yellow,* and *Green.* The *Red* network hosts the computer infrastructure of the administration and financial departments. The *Yellow* network [Fig.2] is a class C subnet in which each student and teacher has an allocated IP address. The *Green* network is composed of different IP subnets in which IP mobility is supported via the Mobile IPv4 protocol [1].

In the *Yellow* network mobility is supported at the "link level" thanks to a set of access points that cover: the Electrum building, IBM Forum lecture halls and Glasgatan (a common area with restaurants, library and meeting rooms). The wired network is based on a gigabit ethernet [2] backbone and is attached to Cisco 3524 switches. These swiches are connected to 100Mbps subnets which in turn connect to 10Mbps access points [Fig.3].

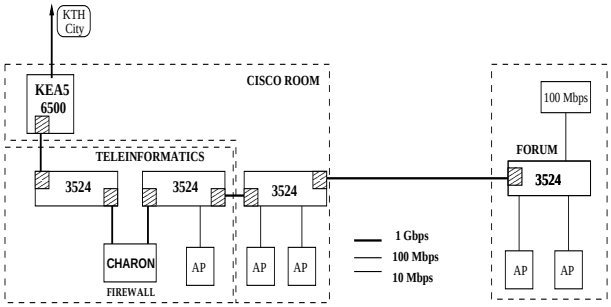

Figure 2: Yellow Network backbone scheme

New security measures [Fig.4] have been introduced in this network to allow only authorized personel to get wireless connectivity.

In the *Green* network, wireless access is available through a set of *MobileIPv4 Foreign Agents* [3] that provide IP level mobility. Mobile IP supports transparency above the IP layer, including the maintenance of active TCP connections and UDP port bindings. These Foreign Agents allow *"roaming"* in other networks by enabling the mobile nodes to keep the same IP address (based on their Home IP network address). The Authorization mechanisms to access the *Green* network rely on those provided by MobileIPv4.

2.2 Yellow network: wireless access overview

Before giving a more detailed description of the wireless access in the *"yellow network"* we will consider as our example, all the steps necessary to publish a page on the schools's web server, from a student's laptop (i.e. a wireless node) running the Flyinglinux distribution. This example was choosen because it will help us introduce the *Yellow* network design to the reader and shows all the security mechanisms involved.

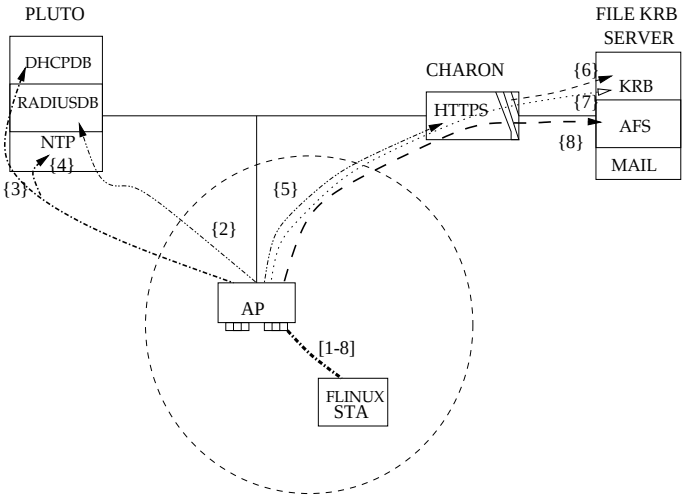

Figure 4: Yellow network at the KTH IT-University. Wireless authentication.

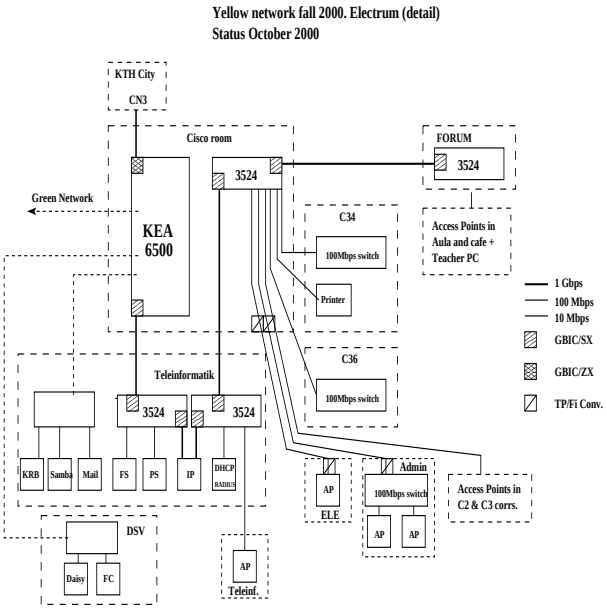

Figure 3: Yellow network (detail).

2.2.1 IEEE 802.11b association

The access points (AP) in the *Yellow* network support the IEEE 802.11b standard [4] that provides speeds of 1,2, 5.5 and 11 Mbps in the 2.4-2.5 GHz band.

Before the mobile station (STA[3]) is allowed to send a data message via an access point (AP), it must first become associated with the AP. The STA learns what APs are present and then send a request to establish an association. An *association request* includes the network name (ESSID) as one of the information items (parameters).

The *association* ensures that the distribution system (DS)[4] knows in which access point a certain station (STA) is attached and hence the traffic will be delivered to the access point correctly.

2.2.2 IEEE 802.11b authentication

The IEEE 802.11b standard defines two subtypes of authentication mechanisms: *Open System* and *Shared Key*. The subtype invoked is indicated in the body of the *authentication management frames*. The stations (STA) use *Open System* authentica-

[3] Any device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM).

[4] The distribution system is used to interconnect a set of basic service sets BBSs and integrated local area networks (LAN) to create an extended service set (ESS). In this case fifteen access points provide access to the Yellow network.

tion subtype to send an authentication request to the AP. Once the STA is authenticated with an AP the data frames sent by the STA are bridged through the AP.

KTH/IT University wireless infrastructure uses Lucent's access points. The Lucent's APs are configured to run a *"Radius-based authentification"*. The MAC address of the STA, that was included in the *Open System management frame,* is used by the radius client implemented in the access points to build an authentication request against a radius server. The radius server *'pluto'* contains a database of MAC addresses permitted for each access point. This data is configured when the users receive their wavelan card.

2.2.3 Configuring network interface via DHCP protocol.

Data frames can now reach the DHCP server through the AP. The next step is to configure the network interface, the default gateway, and DNS servers to be used by the STA.

By running a DHCP client on the STA a DHCP request is sent to the broadcast address 255.255.255.255. The DHCP server *'pluto'* answers that request by returning a fixed IP address statically associated with the MAC address of the dhcp request.

2.2.4 Set the date and time by NTP.

We use the NTP protocol for date and time synchronization. *ntpdate* sets the local date and time by polling the Network Time Protocol (NTP) server(s) in order to determine the correct time.

Three NTP servers are available to provide NTP time syncronization to the wireless stations. The server's names are *"pluto", "ithaca"* and *"charon"*. The later also works as the firewall of the *Yellow* network.

2.2.5 Firewall authentication.

The firewall *'charon'* stops all outgoing traffic until authentication is completed. The authentication is done via a web form hosted at `https://charon.it.kth.se`. This is a secure web server where the user's name and password information is "posted" to a *cgi-bin* program.

The firewall is between the *Yellow* network backbone and the gigabit connection to main KTH .

2.2.6 Kerberos user verification and netfilter IP forwarding

The user name and password information is processed by a *cgi-bin* program that queries the IT.KTH.SE kerberos [8] domain controller (KDC) to verify the password provided by the user. A successful result changes the rules in the firewall allowing outgoing and incoming traffic from/to the mobile station.

2.2.7 Getting granting tickets as well as AFS ticket and tokens.

The next step is to retrieve a Kerberos ticket granting ticket (TGT) and a Andrew Filesystem System [9] ticket and token for our AFS cell */afs/it.kth.se.*[5]

Now that the user can reach the other side of the firewall and has both Kerberos and AFS tickets, the user will be able to access its *public_html folder* on the AFS server. For each user account there is a `/afs/it.kth.se/home/it00/<user>/public_html` folder which is writable only by the <user>.

This *"web publishing folder"* is the place in which the web server will look when trying to find URLs of the form `http://www.it.kth.se/~user`.

2.2.8 Updating web pages

As the user can now write in the `/afs/it.kth.se/home/it00/<user>/public_html` folder, the user can edit and update the pages remotely.

2.3 Yellow network AFS access

The remote accounts of the IT University's users are available in a IBM Transarc AFS server. Linux or other Unix variants can use arla [5], an open source AFS clone, to access the filesystem. Windows users can access their AFS files either using a *non-free* Windows AFS client or through the Samba Server *'polka'*. The main idea was to provide an alternative method to access the AFS server from Windows that using the commercial

[5] Linux users running KTH implementation of Kerberos can get both by running *kauth.*

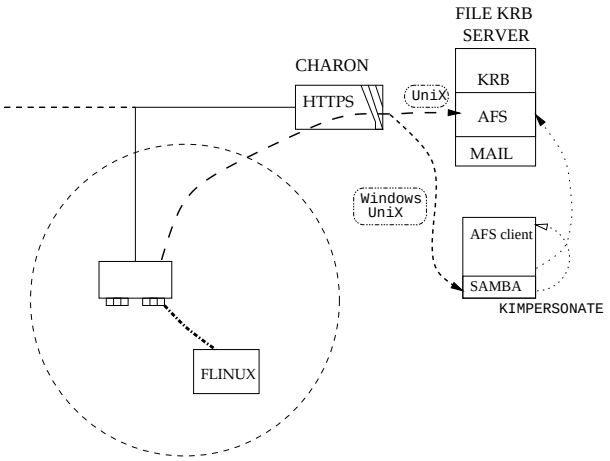

Figure 5: AFS server access through a *patched* samba server which impersonates the AFS tocken.

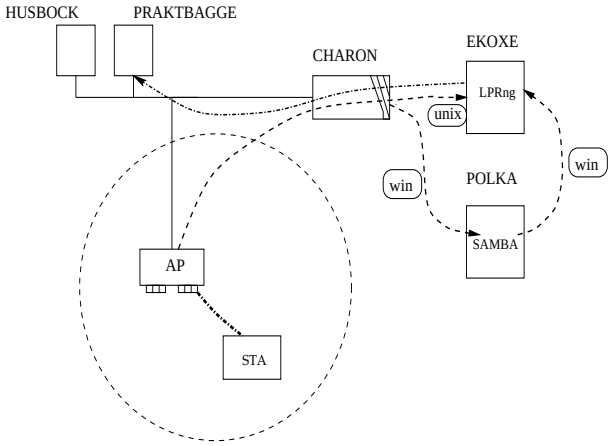

Figure 6: Authenticated Printing services

AFS client. This is done via a *patched* samba server, that also runs an AFS client and uses *kimpersonate* [6] in the samba *"preexec"* option to create a AFS "fake" tocken.

As shown in [Fig.5] Unix clients access the AFS server using the AFS client (arla) while Windows clients access the AFS server via the Samba Server (polka). When the Windows clients access the samba server, *kimpersonate* is called to provide an *"impersonated"* Kerberos ticket to the AFS client.

2.4 Yellow network Printer services

Unix users send their printers jobs to the *LPRng* daemon running on `ekoxe.it.kth.se`. The printer server only accepts printer jobs coming from the *Yellow* network range of IP addresses and the network printers only accept jobs coming from the printer server.

Windows users send their print jobs through the Samba Server `polka.it.kth.se` that in turn uses `ekoxe.it.kth.se` as its printer server.

ekoxe handles two network printers: *husbock* and *praktbagge*. These printers are inside of the firewall.

As shown in [Fig.6] the printer jobs sent by the the STAs' (either running Linux or Windows) need to pass through the firewall in order to reach the printer server. An authentication as the one described in [3.1.2] is required.

2.5 Green Network: MobileIP support

The *Green* network backbone is a 1.6 Gbit Dynamic synchronous Transfer Mode (DTM) ring. The DTM routers are situated in IT University Forum (former IBM Forum Building), Teleinformatics Department (Electrum Building) and the Video Room (Electrum Building). Each DTM router handles a set of subnets allocated for different research purposes including IPv6, Multicast, and Digital Video transmission.

In each of the subnets a set of MobileIPv4 [Fig.7] Foreign Agents are configured to provide mobility between the different IP networks.

The *Foreign Agents* are manufactured by Lifix[7] and run a GNU/Debian Linux based distribution that includes the Dynamics MobileIP implementation.

IT University users, whose statically assigned IP addresses are in the *Yellow* network (home network), can roam in the *Green* Network's subnets (foreign network) while keeping their home network IP configuration.

The Home Agent *'ithaca'* is located in the *Yellow* network inside of the firewall and is setup to support triangle and bidirectional tunneling.

[6] Kimpersonate has been written by Love Hörnquist-Åstrand `lha@stacken.kth.se` and it is a part of Heimdal (KTH Kerberos V implementation)

[7] Lifix `http://www.lifix.fi`

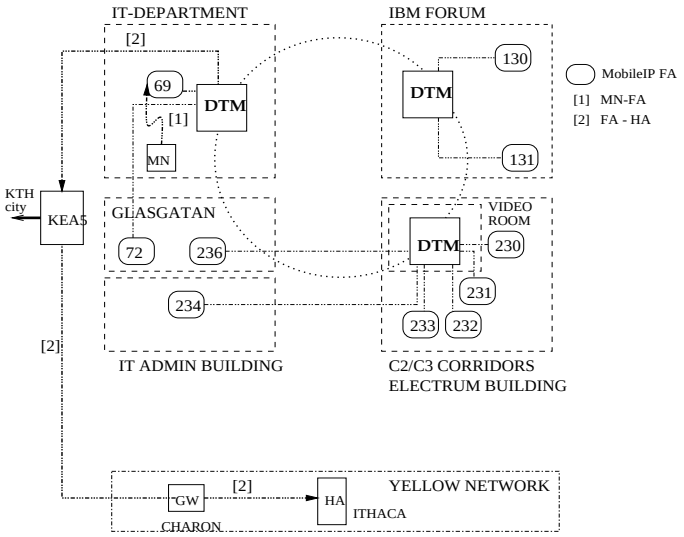

Figure 7: Green Network. MobileIP FA layout.

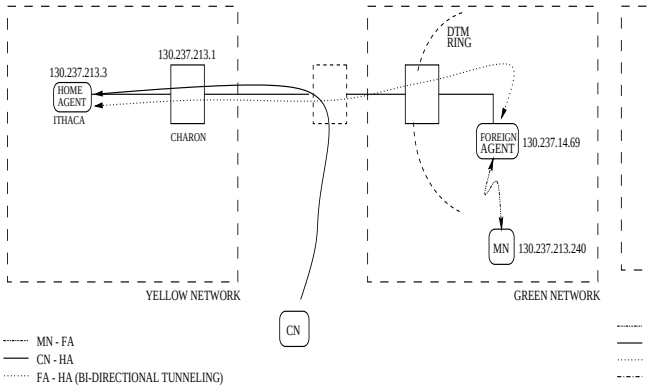

Figure 8: MobileIP bidirecctional tunneling

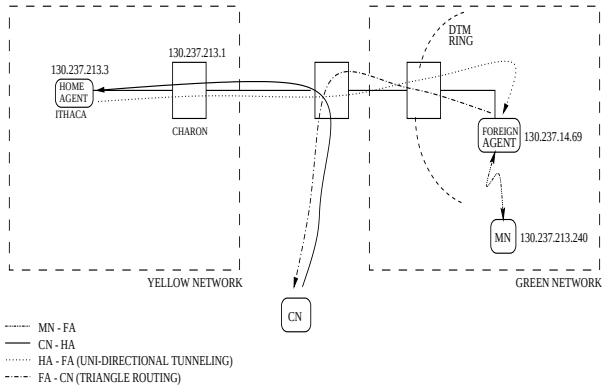

Figure 9: MobileIP triangle routing

2.6 Green Network: Firewalled MobileIP Home Network

When using MobileIP with Foreign Agent Care-of-address, the FA can deliver the MobileNode traffic to the correspondent node by:

- Bi-direcctional tunneling: [Fig.8]

1. The Foreign Agent establishes a tunnel to the Home Agent. The Home Agent establishes a tunnel to the Foreign Agent.
2. The traffic from the Mobile Node to the Correspondent Node is first tunneled back to the Home Agent.
3. The traffic from the Correspodent Node to the MobileNode is tunneled in the Home Agent.

- Triangle Routing: [Fig. 9]

1. The Home Agent establishes a tunnel to the Foreign Agent.
2. The Foreign Agent routes the traffic from the Mobile Node to the Correspondent Node via its default route interface. [8]

[8] The Foreign Agent routes the traffic via the device that handles the destination address encoded in the IP header. The Foreign Agent will try to match the destination address with its routing table.

Mode	In	Out	Ingress Filters
Triangle	YES	NO	DISABLE
Bidirectional	YES	YES	-

Table 1: Firewall forwarding rules for the MobileIP environment

3. The traffic from the Correspodent Node to the MobileNode is tunneled via the Home Agent.

Hence, if the mobile node uses bidirectional tunneling the firewall must permit packet forwarding in both directions, as follows:

1. The CN sends traffic to the IP address of the MN (forward accepted for packets with MN's IP destination header).
2. The MN sends traffic to the CN by tunneling the packets first to the HA (forward accepted for packets with MN's IP source header).

and, if the mobile node uses triangle routing the firewall must permit packet forwarding only in the outside-inside direction (incoming), as follows:

1. The CN sends traffic to the IP address of the MN (forward accepted for packets with MN's IP destination header).
2. The MN sends traffic to the CN via the FA (outgoing-traffic forwarding from MN's IP is not required in the firewall)[9]

A solution that can be adopted is to allow by default incoming traffic to the *Yellow* network and deny the outgoing. When Mobile Nodes use triangle routing this kind of solution does not require of them extra authentication in the firewall [3.1.2] while MobileIP nodes using bidirectional tunneling must also get authenticated in the firewall. This solution is far from being desirable (for example: TCP SYN, "smurf" or "land" attacks do not involve packets being returned).

Our solution was to include in the Home Agent implementation the capability of changing the *firewall forwarding rules* depending on the Mobile Node registration status (registered, unregistered, tunnel expired).

[9]The FA routes the packets to the CN using MN's IP source header. The routers from the FA to the CN can prevent routing packets with *"non-expected"* source header by *ingress-filtering* mechanisms. It is not possible to know in advance if triangle routing could be used.

3 Server descriptions

The following servers are part of the IT university wireless infrastructure:

3.1 Charon

The basic functionalities of Charon are:

- Gigabit support
- Routing and firewall
- Kerberos Login Authentification (through an Apache SSL cgi-bin)

3.1.1 Gigabit support.

One of the design requirement was to have a Gigabit backbone network connecting to the main KTH network and the Stockholm City network. Charon serves as a geteway between the *Yellow* network and the Cisco 6500 that connects the IT-University network with KTH City. This host is connected via two 3Com985 gigabit controllers one to the Cisco 6500 and another the Cisco 3514 switch of the *Yellow* network.

In order to provide gigabit ethernet support we choose Jes Sorensen's aceNIC driver based on Alteon Tigon chipset [2].

3.1.2 Routing and Firewalling

Charon provides routing and firewall functionality for all the *"flinux nodes"*[10] attached to the wireless (and wired) infrastructure in the so called "Yellow network". Each packet coming from the 130.237.213.0/24 subnet to the Internet is filtered using Linux iptables netfilter (packet filtering code available in the 2.4 kernels) against a set of fixed and dynamic rules. The kernel has been compiled with Netfilter support [6].

The following computers and services are inside of the Yellow network:

[10]The "flinux nodes" have a set of IP addresses reserved for students and teachers in the 130.237.213.0/24 subnet. This is often abbreviated as the *213* network.

Name	IP	Services	OS	Network
Charon	130.237.213.1 130.237.203.240	Firewall, IP-klogin	Linux	Yellow
Pluto	130.237.213.2	DHCP,Radius,NTP	Linux	Yellow
Ithaca	130.237.213.3	Mobile Home Agent	Linux	Yellow
Orwell	130.237.213.7	Monitor System	Linux	Yellow
Polka	130.237.212.16	Samba Server	Linux	212 net
Ekoxe	130.237.203.37	Printer Server	Linux	203 net
Garbage	130.237.212.33	AFS server	SunOS	212 net
FA<n>	130.237.14.n	MobileIP Foreign Agent	Linux	Green

Table 2: Server list at the IT university infrastructure.

1. NTP, Radius, and DHCP Server (pluto: 130.237.213.2)
2. MobileIP (IPv4) Home Agent (ithaca: 130.237.213.3)
3. Network Printers (husbock: 130.237.213.6 and praktbagge: 130.237.213.7)
4. Flyinglinux clients (student and teacher wireless laptops) (130.237.213.10/130.237.213.170)

After booting the router/firewall, the *fixed netfilter rules* are:

1. **Primary policy:** Drop off all packets whose source **or** destination is not the router/firewall (forwarding denied).
2. **DNS availability policy:** The DNS servers provided by the DHCP server need to be reachable through the firewall (udp port 53 accept).
3. **NTP Server policy:** The NTP server that is inside of the firewall *(130.237.213.2)* must be able to send and receive traffic through the firewall (udp port 123 accept).
4. **MobileIP Home Agent policy:** The MobileIP Home Agent that is inside of the firewall *(130.237.213.3)* needs to be able exchange registration requests and replies through the firewall (udp port 454 accept) and be able to setup and receive IPIP tunnels.
5. **Printers policies:** The printers (*husbock: 130.237.213.6* and *praktbagge: 130.237.213.7*) that are inside the firewall must to be able to talk with the printer server that is outside the firewall *(ekoxe: 130.237.203.37)* (tcp port 515 accept).

The *dynamic netfilter rules* are created in accordance with the mobile clients status in the firewall. By default no traffic from any client can cross the firewall unless an authentification has been performed. How this authentication works is described in the following section [3.1.3].

3.1.3 Kerberos Login authentification

Each of wireless nodes included in the range of IP addresses that goes from 130.237.213.10 to 130.237.213.170 can not send traffic to or receive traffic from the outside world (except the exceptions mentioned in [3.1.2]. By default the router/firewall drops all packets with source and destination from/to the "flinux-nodes".

In order for the flinux-nodes are able to send and receive traffic from the outside world, each node have to validate its IP address. This is done by a user-login Web Form which invokes a *C cgi-bin* [Fig. 10][11] in which the node need to authentificate providing the *user* and *password*. The communication between the client browser and the Web server is done with HTTPS.

Those user and password values are used by the *cgi-bin* in the function:

```
res=krb_verify_user(user,inst,realm,pwd,0,NULL);
```

in where:

[11] IP-kerberos-login (release 1.3) is based on the IP-login code released at Sveriges Lantbruksuniversitetet (SLU) and Uppsala Universitet (UU) for their Nomad service. The initial version of IP-login developed by <robert.olsson@data.slu.se>uses a TACACS+ client instead of Kerberos to perform the authentification. IP-klogin has been modified by Alberto Escudero <aep@it.kth.se> to support authentication against Kerberos Domain Controllers (KDC).

realm=IT.KTH.SE

inst=""

user=<extracted from the WWW form>

pwd=<extracted from the WWW form>

The *krb_verify_user* function checks the authentification values against the specified Kerberos REALM and returns 0 when the authentification is correct.

if(res == 0) do_IP_kerberos_login();

do_IP_kerberos_login() calls a second *C* program call *IP-klogin <IP>*. IP-klogin has three basic functions:

- Add a forwarding rule for the specified IP address that has successfuly performed the Web-based authentification.
- Check that the node is still online by sending periodic ARP-requests.
- Remove the forwarding rule for the IP address when the number of arp-request without answer reach a fixed value *probe-drop-threshold (PDT)*.

Using *IP-klogin* in a wireless network introduced limitations that were not expected as link layer connecitivity is not as reliable.

What level of security does IP-klogin provide?

An attack on the authentication method can be performed by hijacking the victim's IP address during the time that the victim stops answering the ARP-requests and when the firewall deletes the forwarding rule for that IP address. Unfortunatelly we can not reduce this *"non active client time to close"* as much as we would like. When working in a wireless environment the link level is not as reliable as we might desire thus making the *"time to close"* very small will lead to the users having to re-login too frequently.

IP-klogin does not prevent DoS (Denial of Service) attacks or IP/MAC-hijacks [Fig. 11](the capability of an attacker to configure their computer with the same IP/MAC address). The main purpouse of introducing *IP-klogin* was to make sure that the connectivity to the IT-University network could not be obtained "by mistake" while not annoying users with complicated authentification mechanisms or introducing significant traffic overhead.

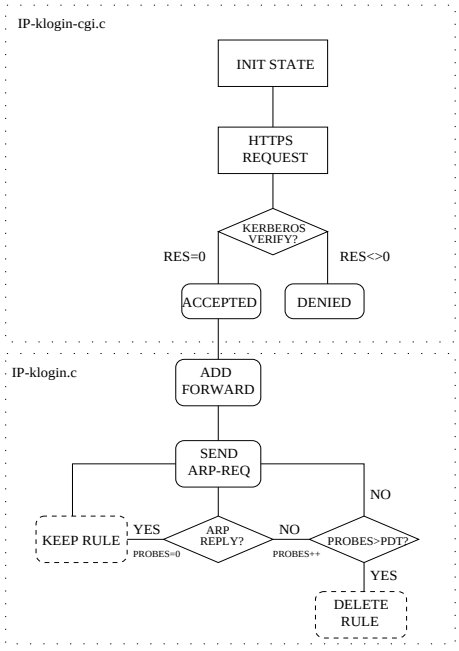

Figure 10: IP-klogin-cgi checks user and password against the KDC and calls IP-klogin to keep IP forwarding.

Figure 11: The figure shows the period of time available for a potencial attacker to hijack the IP address of the victim before the router deletes the forwarding rule for the authenticated IP address.

3.2 Pluto

Pluto [12] provides:

- DHCP service.
- Radius service.
- FTP service.
- NTP service.

3.2.1 DHCP Server

Pluto provides mobile nodes with a fixed IP address based on the MAC address of the DHCP REQUEST. Each student can use a wired interface (10/100 Mbits) or a wireless interface (Lucent "Orinoco" Silver IEEE 802.11b) PCMCIA card in order to attach to the network. The *DHCP Request* includes either the wired MAC_{wired} or the wireless $MAC_{wireless}$. The *dhcpd.conf* configuration file includes a common entry for all the mobile nodes in the *213* network:

```
subnet 130.237.213.0 netmask 255.255.255.0{
range 130.237.213.10 130.237.213.254;
option domain-name "it.kth.se";
option domain-name-servers 130.237.72.201,
    130.237.212.6, 130.213.15.187;
option broadcast-address 130.237.213.255;
option routers 130.237.213.1;
}
```

and a for each user's IP two entries, one for the *"wireless device"*:

```
host it00_aep {
hardware ethernet 00:60:1D:D2:D2:B8;
fixed-address 130.237.213.243;
}
```

and also another entry for the *"wired device"*:

```
host it00_aep {
hardware ethernet 00:01:02:AC:AD:92;
fixed-address 130.237.213.243;
}
```

[12] Pluto has one satellite named Charon [SHAR-on], named after the boatman in Greek mythology who operated the ferry across the River Styx to Pluto's realm in the underworld.

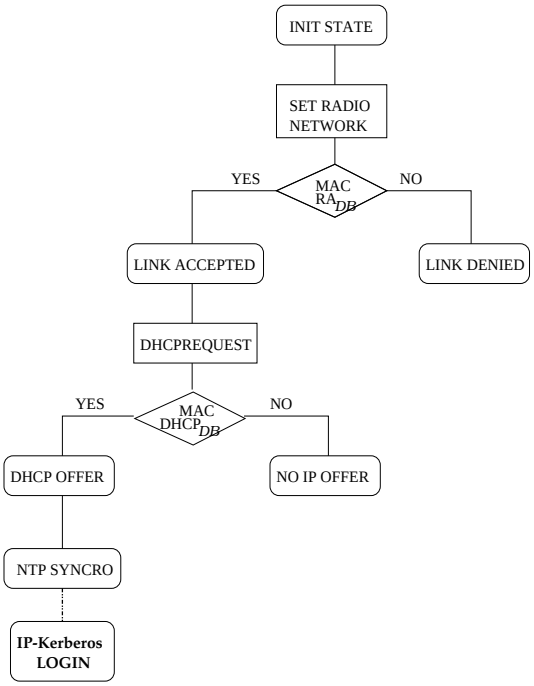

Figure 12: Set the radio network, obtain an IP address and syncronize the time. Next step IP-kerberos Login.

3.2.2 Radius Server

Pluto runs Livingston Enterprises, Inc.'s Radius Server release 2.1. Each of the Lucent Access Points runs a radius client with a common shared secret with the Radius Server. Each time a *flinux node* associates with an access point an authentication process is executed by the radius client in the Access Point. The access point queries the radius server to check if the MAC address of the *flinux node* can send data frames.

The *flinux nodes* do not need to run any authentification software because the information needed by the Radius Client is extracted from the Open System authentification management frames[13]. In order to avoid the traffic exchange between the access points and the radius server being sniffed we utilize a private subnet (192.168.10.0/24) with the following configuration:

Using the $Radius_{MAC} - based$ authentification we can determine in which access points we allow a certain $MAC_{wireless}$ address to send data frames (Class 3).[14]

If for example we want the MAC address 00:02:2D:00:82:B9 to be allowed in access points 192.168.10.101 and 192.168.10.102 the raddb configuration files for the radius server will look like:

/etc/raddb/users:

```
00022d-0082b9 Password = "superqw-
    erty"
DEFAULT Auth-Type = Accept
```

/etc/raddb/clients:

```
192.168.10.101  superqwerty
192.168.10.102  superqwerty
```

3.2.3 FTP Server

FlyingLinux can be installed via the network. FlyingLinux also includes *"wireless support"* on the boot floppy that allow users to install/upgrade the full distribution via their wireless link. Due to the fact that the *"flinux nodes"* can not get through the firewall unless they perform an authentication through a Web Form (HTTPS), an ftp server hosting the distribution is available inside the firewall.

[13]IEEE 802.11 defines two subtypes of authentification services: Open System and Shared Key. The subtype invoked is indicated in the body of the authentification management frames.

[14]This kind of authentification does not stop the wireless client from receiving data frames. Setting up the wireless device in promiscous mode will enable the interface to listen to all frames corresponding to the configured ESSID.

3.3 Ithaca

3.3.1 MobileIP Home Agent

Ithaca *(130.237.213.3)* is the Home Agent of the *Yellow* network. Ithaca runs Dynamics MobileIP implementation release 0.7.1 available at [7].

The Home Agent code has been modified in order to provide two new features:

1. **Reload configuration:** A new API called *API_RELOAD_CONFIG* has been added. This call allows the home agent daemon *(dynhad)* to reload the Security Parameter Index (SPI) and Shared Secrets into the home agent configuration without destroying the bindings.

2. **Change firewall rules depending of MN's Registration Status:** A hook inside of the home agent can change the filtering rules in a remote firewall depending on the registration status of the mobile node. The code has been modified to be able to run remote commands in the firewall. Open-SSH is used as command transport.

- When the mobile node *registers* against the home agent a command is excuted in a remote firewall machine (*charon*) and creates a new forwarding rule for the Mobile Node's IP.

- When the mobile node *deregisters* or the *tunnel expires* a remote command removes the forwarding rule for the Mobile Node's IP.

3.4 Polka

The basic functionalities of Polka are:

- Sun U1. Solaris 2.6 Transarc AFS client.

- Kimpersonate Samba Server

Polka runs a hacked 2.0.7 samba server. The hack allows to the samba server to read and write into a remote AFS server. *Polka* that also runs an AFS

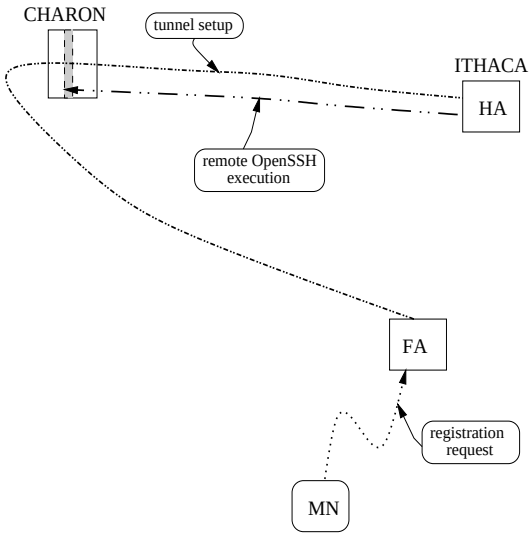

Figure 13: remote command execution between the Home Agent (Ithaca) and the firewall (Charon)

client uses *kimpersonate* in the *"preexec"* option to create a "fake" ticket using the service-key of the service.

In order to setup the Kimpersonate Samba server the following steps need to be followed:

3.4.1 Modify the Samba source code (smbd)

server.c: The function *open_ sockets* of the samba server (2.0.7) has been patched with:

```
[root@themess smbd]# diff server.c server.c~
245,247d244
<     if (k_hasafs())
<     k_setpag();
```

3.4.2 Add a *preexec* entry in the samba configuration file

smb.conf: The samba configuration file includes the following entry:

```
# for gettting afs-token root preexec = /opt/local/samba/tools/gettoken %u
```

3.4.3 Configure the gettoken script properly

gettoken: A shell script that calls kimpersonate as follows:

```
/opt/local/samba/tools/kimpersonate
-4 –no-krb5 \
–server=afs/it.kth.se@IT.KTH.SE \
–client="$user"@IT.KTH.SE \
–expire-time=$expiretime \
–keytab=AFSKEYFILE:"$keyfile"\
# push ticket to token
/usr/athena/bin/afslog -c it.kth.se
```

3.4.4 Install kimpersonate

kimpersonate: a C program that impersonates a user when there exist a srvtab, keyfile or KeyFile. Kimpersonate is part of Heimdal, a Kerberos V implementation from KTH.

4 Clients and Client configuration

The clients available for students and teachers during the academic year 2000-2001 are mainly laptops, according to a subsidized leasing model. There are also also a few desktops to provide a choice and redundancy for laptop repairs. It turns out that all students have chosen the laptop solution. The laptops run a double boot configuration running FlyingLinux (a RedHat 6.x based distribution) and Windows 98.

The basic idea was to provide the most similar set of applications for Windows and Linux users.

The standard configuration of Windows 98 was extended with StarOffice, NTP client, Kerberos POP Proxy, Acrobat Reader, Lucent Orinoco IEEE 802.11b PCMCIA support, Netscape and First Class.

FlyingLinux includes AFS client, Kerberos IV and V, Kerberos POP Proxy, Acrobat reader, StarOffice, OpenSSH, Lucent Orinoco IEEE 802.11 GPL driver, First Class client, MobileIP, Xbill and AODV.

Norton Ghost with Multicast support was used to clone 250 laptops.

4.1 FlyingLinux bootdisk

A new bootdisk image was created in order to allow Linux users to install FlyingLinux using a IEEE 802.11b Orinoco PCMCIA card. By using the new bootdisk floppy called *'flbootdisk.img'* FlyingLinux can be installed wirelessly.

Installation methods:

- FTP: Downloading the distribution from: `ftp://pluto.it.kth.se/pub/flyinglinux-6.1-1/i386`
- NFS Server: Using the RedHat Linux Kick-Start system to rapidly install large numbers of identical Linux boxes. This installation option lets us automate most/all of the FlyingLinux installation. Installing FlyingLinux *should* be as simple as inserting the boot floopy and the WaveLAN PCMCIA and rebooting.

5 Conclusions

The IT University network, the premier vintage 2000, has turned out to be a very successful network from several aspects. We will mention a few of them briefly.

5.1 A new approach to spaces

Abandoning workstation halls for laptops, lecture halls for more informal spaces, traditional laboratories for remote laboratories, offices and workplaces for meeting places will have a huge impact on how we perceive spaces.

The spacial, technical and pedagogical support systems have to be designed with regard to each other to enhance the learning experience of students.

5.2 Mobility

Currently, the wireless access network provides wireless Internet access with support for mobility to some 200 students and 50 teachers. Link level handover is available in the home network through a set of access points available in three buildings. When roaming to a foreign IP-network a set of foreign agents provide MobileIP-based connectivity.

Mobility is an extremely enabling service which has affected the way the users think about information access and started a transformation of many of the learning and work processes at the IT-university.

5.3 Security

We have managed to integrate MobileIP services in a conventional IEEE 802.11 distribution system providing high levels of security with low maitenance. We have taken care of the security issues including Kerberos support, OpenSSH and AAA services. New network monitoring tools were deployed to detect intrusions and misuse.

It is possible to provide Mobile Internet technologies and integrate them in new learning scenarios with a reasonable level of security.

6 Future work

The research issues that have emerged from our work related in this paper are abundant. We discuss a few of them here.

6.1 Distributed Interactive Learning Spaces and mobile learners.

To evaluate the effects of mobility and ubiquitous access using personal computing and communication environments on one hand and fixed interactive meeting spaces on the other, and the interaction between them, has a prominent position on our research agenda. This calls for extension of our campus network with new services and applications, e.g. with location awareness systems, ad hoc networking applications, etc.

6.2 Clients

Work is already in progress to design the Flying Linux 2001 configuration. The new Linux distribution will be based on a more recent Red Hat version while the Windows 98 will be upgraded to Windows 2000. There are also a few activities to explore how to extend the personal computing and communcation environment with handhelds, Java rings and other devices.

6.3 Networking aspects

Scalability is highly relevant also on the networking level when the number of hosts and the amount of traffic are growing exponentially.

The introduction of IPv6 to cope with the increase in the number of hosts, use of Mobile IP to faciltate roaming between different networks and link level technologies, IP over fiber based on high performance medium access and transmission technologies, support for QoS and Multicast, IX-technologies and business models are issues on our list of future work.

7 Acknowledgments

This new environment is the result of the hard work of many people around the IT University infrastructure project. We would like to thank in alphabetical order to:

Hans Berggren, <hans@ele.kth.se>
Charlotta Bååth <d99-lba@nada.kth.se>
Love Hörnquist-Åstrand, <lha@stacken.kth.se>
Fredrik Lilieblad, <fredrik@lilieblad.com>
Erik Lundesjö, <elu@it.kth.se>
Elie Salloum, <elie@admin.kth.se>
Norm Smith, <wombat@it.kth.se
Jimpa Svensson <jimpa@it.kth.se>
Henrik Svensson. <henriks@isk.kth.se>
Josev Swiatycki <josef@dsv.su.se>

About the author

Alberto Escudero is graduate student at the Institution of Microelectronics and Information Technology. (formerly Teleinformatics). KTH. Sweden.

As a researcher in IMIT, Alberto is currently focusing on "location privacy" in mobile internetworking and privacy protection of personal information and over the last year was involved in the IT University - Kista Wireless Network, FlyingLinux.NET and The Big Brother "storebror" Project. http://www.it.kth.se/~aep

References

[1] IETF Network Working Group. C. Perkins, Editor, *"RFC 2002 MobileIP"*. October 1996
`http://www.ietf.org/rfc/rfc2002.txt`

[2] J. Sorensen. *"Gigabit Ethernet Support for Linux. Alteon Acenic"*
`http://jes.home.cern.ch/jes/gige/acenic.html`

[3] MART group *"Mobile ad-hoc routing testbed - MART"* HUT Finland. 1999
`http://www.cs.hut.fi/~mart/`

[4] IETF 802.11b Standard. *"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications."*
`http://standards.ieee.org/catalog/IEEE802.11.html`

[5] The Arla project. *"Andrew Filesystem client clone"*
`http://www.stacken.kth.se/projekt/arla/`

[6] The Netfilter project *"Filtering code"*
`http://netfilter.kernelnotes.org`

[7] Dynamics *"Dynamics MobileIP implementation"*
`http://www.cs.hut.fi/Research/Dynamics`

[8] KTH Kerberos V implementation. Heimdal
`http://www.pdc.kth.se/heimdal`

[9] Arla is a free AFS implementation.
`http://www.stacken.kth.se/projekt/arla`

[10] D. Eckhardt and P. Steenkiste (Carnegie Mellon Univ.) *Measurement and Analysis of the Error Characteristics of an In Building Wireless Network*, SIGCOMM'96
`http://www.acm.org/sigcomm/sigcomm96/papers/eckhardt.html`

[11] D. Tang and M. Baker (Stanford Univ.) *Analysis of a Local-Area Wireless Network.* Proceedings of Mobicom 2000, Boston, August 2000.
`http://mosquitonet.stanford.edu/publications.html`

[12] D. Tang and M. Baker (Stanford Univ.) *Analysis of a Metropolitan-Area Wireless Network.* Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 1999), Seattle, Washington, August 1999.

http://mosquitonet.stanford.edu/
publications.html

[13] B. Pehrson, J. Odhnoff. *Sweden-Silicon Valley Link Status report.* 1997
http://ssvl.stanford.edu

[14] D. Forsgren, A. LaTorre-Yurkow, J. Willen, *Initial Evaluation of a Communication Network Infrastructure for the Student Dormitories at KistaIP*, Technical Report, KTH Teleinformatics, August 2000.
http://www.flyinglinux.net/docs

[15] A. Escudero. *Wireless Internet access: From the peruvian amazonia to the swedish silicon valley.* First International Conference of Community Networks. CNGLOBAL2000. Barcelona, June 200
http://www.cnglobal2000.org