UNIVERSITY OF VAASA

FACULTY OF TECHNOLOGY

TELECOMMUNICATION ENGINEERING

Christopher Fytousis

HETEROGENEOUS NETWORKS USING MOBILE-IP TECHNOLOGY

Master´s thesis for the degree of Master of Science in Technology submitted for inspection, Vaasa, 4th of June, 2011.

Supervisor	Mohammed Salem Elmusrati
Instructor	Kimon Kontovasilis

ACKNOWLEDGEMENTS

First I would like to express my deepest appreciation to the Supervisor of this Master's thesis Prof. Mohammed Elmusrati for his valuable course lectures during my studies and for his encouraging and inspiration to start-up this thesis topic.

I am also thankful to the Director of Research of the Institute of Informatics and Telecommunications at NCSR "Demokritos" center Dr. Kimon Kontovasilis for helping and providing the required tools of the mobile-IP test-bed implementation.

In addition, I am extremely thankful to the collaborating faculty member Lampros Sarakis for his instructions and guidance throughout this work. I want also to acknowledge my friend Vasilis for his advices and corrections concerning the language of this thesis.

Finally, I would like to thank my parents for their endless encouragement and mental support which helped me to complete this thesis.

Vaasa, Finland, 4 of June 2011

Christopher Fytousis

TABLE OF CONTENTS

ABBREVIATIONS

IP	Internet Protocol
3G	Third Generation
UMTS	Universal Mobile Telecommunication System
DNS	Domain Name Server
MN	Mobile Node
PS	Power Saving
BU	Binding Update
DHCP	Dynamic Host Configuration Protocol
HA	Home Agent
FA	Foreign Agent
CN	Correspondent Node
OSI	Open System Interconnection
WLAN	Wireless Local Area Network
WAN	Wide Area Network
RSSI	Received Signal Strength Indication
BSS	Basic Service Set
BSSID	Basic Service Set Identification
SSID	Service Set Identification
RREQ	Route Request
RREP	Route Response
MAC	Media Access Control
ARP	Address Resolution Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
RA	Route Advertisement
SPI	Security Parameter Index
CoA	Care-of-Address

MTU	Maximum Transmission Unit
SLA	Service Level Agreement
GPRS	General Packet Radio Service
QoS	Quality of Service
CA	Certificate Authority
SGSN	Serving GPRS Supported Node
GGSN	Gateway GPRS Supported Node
IPIP	Internet Protocol in Internet Protocol
WiFi	Wireless Fidelity
TCP	Transport Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
HLR	Home Location Register
WiMax	Worldwide Interoperability for Microwave Access
RTS	Request To Send
CTS	Clear To Send
ACK	Acknowledgement
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
USB	Universal Serial Bus
PC	Personal Computer
IEEE	Institute of Electronics and Electrical Engineers
UL	Up Link
DL	Down Link
VoIP	Voice over IP
ISP	Internet Service Provider
IP	Internet Protocol
TX	Transmitter
RX	Receiver
NIC	Network Interface Card

DHCPD	Dynamic Host Configuration Protocol Daemon
SIR	Signal to Interference Ratio
ISO	International Organization for Standardization
OSI	Open System Interconnection
IBSS	Independant Basic Service Set
AID	Association Identificator
IRDP	ICMP Router Discovery Protocol
AH	Authentication Header
BA	Binding Acknowledgement
OS	Operating System
SPI	Security Prefix Index
CoA	Care-of-Address
PPP	Point-to-Point Protocol
PPPD	Point-to-Point Protocol Daemon
RF	Radio Frequency

UNIVERSITY OF VAASA
Faculty of technology

Author:	Christopher Fytousis
Topic of the Thesis:	Heterogeneous networks using mobile-IP technology
Supervisor:	Mohammed Elmusrati
Instructor:	Kimon Kontovasillis
Degree:	Master of Science in Technology
Department:	Department of Computer Science
Degree Programme:	Degree Programme in Information Technology
Major of Subject:	Telecommunication Engineering
Year of Entering the University:	2007
Year of Completing the Thesis:	2011 Pages: 83

ABSTRACT:

Whenever a mobile user moves between networks a handover must occur. This basically means that a network-layer protocol must handle the moving of the mobile device. In a cellular phone a GSM/UMTS infrastructure performs horizontal handover and the user does not notices any call or ongoing session interruption while roaming. The handover procedure begins when the received signal strength identificator (RSSI) of a mobile device falls below a level, it discovers a neighbour access point with better quality of services (QoS) than its current access point. In heterogeneous wireless networks different portions of RF spectrum are used and is difficult or impossible for a mobile node to concurrently maintain its connectivity without signal interruptions. Thus, the different network environments must be integrated and support a common platform to achieve seamless handover. The seamless or vertical handover's target is to maintain the mobile user's IP address independently of user's location or of the physical parameters the current network is using. A mechanism that keeps a mobile device to an ongoing connection by maintaining its home-location IP address is the Mobile-IP protocol which operates at the network-layer of the Open System Interconnection (OSI) model.

In this M.Sc. thesis we perform heterogeneous network scenarios with the Mobile-IP technology. Moreover, we have built the system practically and assist the applicability of such heterogeneous wireless networks through real-side measurements. We used Linux operating system (Ubuntu & Debian) between different network technologies, made at the National Center for Scientific Research (NCSR) "Demokritos" institute, in Greece. The required applications for the Mobile-IP and 3G technologies were implemented and configured in a platform of fixed and mobile devices at Demokrito's departmental laboratory. The idea of using the Mobile-IP protocol was to gather information about time differences that occurred in handover delay between different networks.

KEYWORDS: Heterogeneous networks, handovers, mobile-IP.

1. INTRODUCTION

The rapid development of wireless networks target to make people's life more convienient by offering mobile device applications to the users anytime, anywhere with better Quality of Service (QoS). As the growth of the mobile internet is increasing exponentially, most organizations need to use more sophisticated networks that link their individual employees and their respective PC's and workstations. Mobile users are requiring access to the information stored on fixed or mobile computers of their private intranets and on the global network. The problem is that most network protocols are designed for computers that do not move very often, and fail to operate when computers are moving fast.

Thus, there is the need to create an heterogeneous mobile environment that provides seamless mobility to the end-user in order to notice as little changes as possible at the network level. Something similar happens in today’s cellular networks, when an end-user making a voice call on his mobile phone will not notice a network handover when the mobile user moves to another cell. The challenge is to implement the same concept across heterogeneous networks and services, in order to maintain user's applications while on the go. The Mobile-IP network protocol gives the capability to the mobile user to move seamlessly from one wireless network to another with different characteristics while its device is supported with multiple wireless network interface cards.

I concentrated on performing an heterogeneous network which is supported with mobile-IP protocol to achieve vertical handovers at the departmental laboratory of NSCR "Demokritos" Research Center, (NCSR). In my thesis, first I briefly refer to the OSI model and IPv4 protocol which was used for the testbed. Second, I describe some important signalling mechanisms about the wireless networks and I introduce the mobile-IP network features and architecture. Then, two vertical handover scenarios are described and the test-bed implementation with the mobile-IP setup are following next. Finally, the measurement results of the vertical handover scenarios are illustrated by using Matlab.

2. MOBILITY

2.1. OSI model

The International Organization for Standardization (ISO) has announced the standard Open Systems Interconnection (OSI) model, illustrated in figure 1. We describe the MAC layer (L2) processes which defines the network hardware, manages the connections, and forwards data from the physical level to the network layer.

The network layer (L3) deals with procedures related to addressing and routing IP packets. The network layer determines the path to route packets according to mobile node information processing.

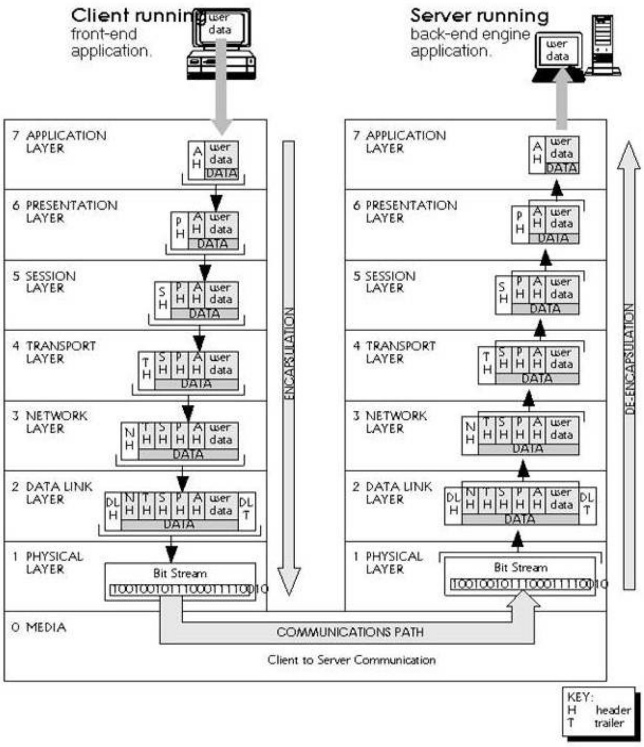


Figure 1. OSI model.

2.2. IPv4

The IP addresses are 32-bit (4-byte) numbers assigned to each network interface of fixed or mobile devices. The IP addresses consist of two main components, the network prefix portion and the host portion. The main fields that an IPv4 protocol are the following:

- Flags and Fragment Offset fields, makes fragmentation to IP packets for networks that are unable to handle large IP packets. In such a case an identification unique number is provided by the sender to allow the recepient to reassemble a packet.
- Time-To-Live (TTL) field, used to limit the number of times an individual IP packet may be forwarded from a router to another one. Without the Time-to-Live routers may caused to a packet to live for eternity.
- Protocol field, used by the IP layer to determine which higher-layer protocol created the payload within the IP packet. For example, the protocol field of 1 indicates ICMP messages, 6 indicates TCP, and 17 indicates UDP messages.
- Header check sum field, used by the receiving node to verify that there was no error in transmission of the IP-header portion of the packet.

The IPv4 addresses are separated to five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B and C are commonly used. Each class allows for a range of valid IP addresses. Below is a listing of these addresses, shown in table 1.

Table 1. IPv4 address classes.

CLASS	ADDRESS RANGE	SUPPORTS
A	1.0.0.1 to 126.255.255.254	16 million hosts on each of 127 networks
B	128.1.0.1 to 191.255.255.254	65,000 hosts on each of 16,000 networks.
C	192.0.1.1 to 223.255.254.254	254 hosts on each of 2 million networks.
D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

The loopback interface is identified by the system as lo and has a default IP address of 127.0.0.1. The ranges 127.x.x.x are reserved for loopback or localhost. Every IP address is broke down into four sets of octets that break down into binary to represent the actual IP address. For example the range 255.255.255.255 broadcasts to all hosts on the local network is shown at table 2.

Table 2. An IP address.

IP	255.	255.	255.	255
Binary value	11111111.11111111.11111111.11111111.			
Octet value	8	8	8	8

However, today there is an exhaustion of IPv4 addresses and a creation of additional IP addresses is needed. The extension of IPv4 is the IPv6 which provides wider range of IP addresses. When comparing these two addresses, the size will be the most major factor to be considered.

IPv6 has an address size of 128 bits (2^128= ~340,282,366, 920,938,463,463,374, 607,431,768,211,456) , while IPv4 maintains a 32 bits (2^32 = ~4,294,967,296) (Abdullahi A. 2010). The IPv6 addresses are classified based on their prefixes and not on the classes like in IPv4 protocol. It also provides better node classification with shorter routing tables and more efficient routing.

2.3. Network Mobility Management

In mobile communication systems, handover is a frequent procedure and the reason for handover is to keep the mobile device connected to the network. If the mobile device is moving away from its network's access point, the signal gets weaker and weaker and any real-time connection will be interrupted at last. It is important for users that owing a mobile device (PDA, cellular phone, laptop etc.) to maintain real-time connections while roaming between different wireless networks without any interuption, shown in figure 2.

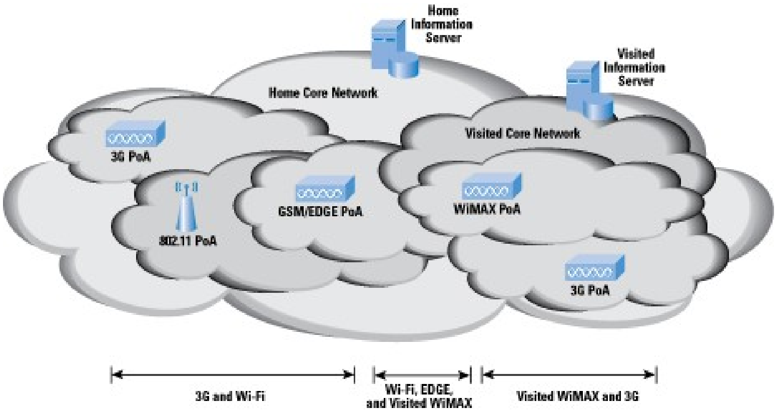


Figure 2. Different wireless networks. (Piri E. 2009)

The mobile-IP mechanism is a solution to this problem which is used to maintain the same mobile device's IP address while handover. This mechanism provides routing information to the mobile device and keeps the same IP address to a home agent on its "home" network, even if it moves to foreign links where the user may move to. This paper is strongly focused to Mobile-IP protocol which uses the IPv4 transport protocol and consists of some network features which they called home agent, mobile node and foreign agent.

3. SIGNALLING MECHANISMS

3.1. Address resolution protocol

The MAC layer uses hardware addresses to control the access of the network devices to the physical medium in ethernet or wireless infrastrucures, by using their Destination and Source Addresses, shown in figure 3.

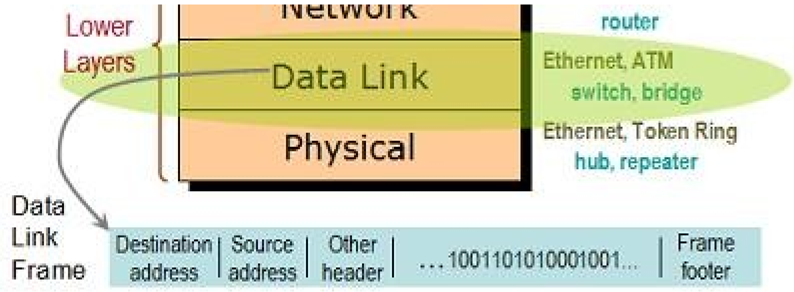


Figure 3. The Data Link Frame. (About. Com. Wireless/networking)

The device's network interface card (NIC) is identified by the 48-bit IEEE 802 MAC addresses and the frames are transfered based on the MAC addresses. The MAC addresses are unique addresses used for fixed or mobile networks, and when a mobile device is entering a network area the network first discovers the ethernet MAC address of the device in order to establish successful connection. More precisely, the mobile device before send an IP packet it broadcasts a message using Address Resolution Protocol (ARP) to discover the MAC address of the related mobile device's interface card. (About. Com. Wireless/networking)

The name interface is a generic term of software and hardware in which a user fixed or mobile attaches to a link. The nodes with multiple network interfaces, such as routers, have multiple IP addresses-one per interface. Every host must use a unique IP and MAC addresses, as it is shown in figure 4. The host A communicates with host C in the network after employing the ARP protocol.

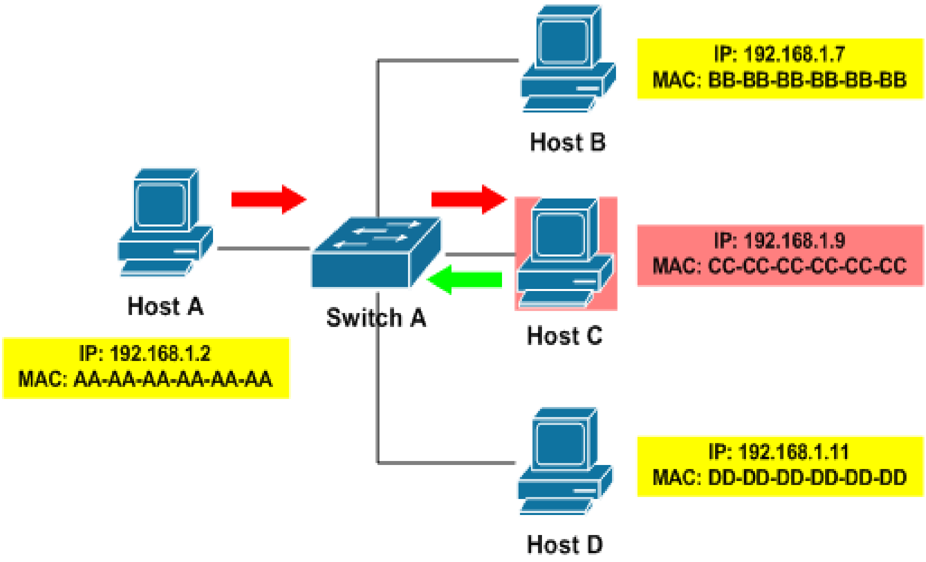


Figure 4. Unique MAC addresses.

As soon as host A finds the IP and MAC address of the destined mobile station's host C, A's operating system will store C's information in a routing table or in a cache. For example in table 3, the Wireless Local Area Network (WLAN) used the computer's device hardware address "HWaddr 90:4c:e5:ac:b4:68" with a unique IP address and MAC address in order to access the internet.

Table 3. WLAN connection reference list.

```
wlan0 Link encap:Ethernet  HWaddr 90:4c:e5:ac:b4:68
 inet addr:192.168.1.74  Bcast:192.168.1.255    Mask:255.255.255.0
       inet6 addr: fe80::924c:e5ff:feac:b468/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:36 errors:0 dropped:0 overruns:0 frame:34
       TX packets:48 errors:6 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:3440 (3.4 KB)  TX bytes:8326 (8.3 KB)
       Interrupt:17
```

By typing “`christof@ubuntu:~$ route -n`” at Linux's operating system, it provides the device's routing table, in table 4.

Table 4. Kernel IP routing table.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	2	0	0	wlan0
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	wlan0
0.0.0.0	192.168.1.254	0.0.0.0	UG	0	0	0	wlan0

The routing table maintain mappings from IPv4 addresses to MAC addresses, so the ARP discovery procedure is performed only one time. If an address from the existing routing table will be used again, it will not request new ARP protocol when a packet is sent to a 'new' destination IP address. Except the network and host routes in a routing table, the default route also exists which is an entry with zero bits prefix length and matches all IP packets.

3.2. Scanning

The authentication for a mobile station is the first step at the exchanging process for the network attachment. In wireless networks, only the authenticated mobile users are authorized to visit a secure network and associate with other hosts or users. When mobile users are joining a WLAN are authenticated by providing identification messages (ID's) before sending the payload information frames. Their device can scan for a specific network to join or for any network that are allowed to join.

The Scanning procedures may specify whether to seek out independent ad hoc networks, infrastructure networks or all type of networks. The Basic Service Set Identifier (BSSID) can be used in unicast, multicast or broadcast mode. The unicast packets target only a specific destination address, the multicast packets target multiple destinations and the broadcast packets are those destined to all hosts of the network.

When mobile devices are moving to another WLAN they may set the BSSID to broadcast mode because the scanning will include all access points of the neighbour networks. Most access points refer to the SSID as the network name because the string of bits is commonly set to a human-readable string. The 802.11 standard allows mobile devices to specify a list of channels to try and operates differently when it is in passive or active scanning mode (McCann P. 2005).

The Passive scanning saves battery power because it does not require transmitting frames as it waits. The received beacons are buffered and record information at the mobile device's cache even the mobile device moves and changes network area. In active scanning, the mobile device transmits Unicast or multicast frames to identify a network in the area. Once the network area is identified by the mobile device it gets message response with the network's SSID. The Response frames are generated by the network and authenticates all the devices into that network area by providing its SSID (McCann P. 2005).

3.3. Association

When the mobile device is being authenticated and the association request is successful, the access point responds with Association ID (AID) status code of 0. The AID is a numerical identifier used to logically identify the mobile device and issues an indication flag, `flag U` meaning that Link is UP ,shown in table 5. By using the BSSID ensures that IP packets are delivered to the correct mobile devices and ignored by mobile devices that belong to another BSSs.

Table 5. Kernel IP routing table.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	2	0	0	wlan0
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	wlan0
0.0.0.0	192.168.1.254	0.0.0.0	UG	0	0	0	wlan0

The Unsuccessful association requests include only a status code, and the procedure ends. The BSSID is advertised in the Beacon message and carry information about its power level and signal strength.

3.4. RSSI

The received signal strength identificator (RSSI) indicates the signal strength from an access point. This parameter depends on the distance between the mobile device and its access point and can be used to detect that a link is going down.
The RSSI also depends on the environment, interference, noise, channel propagation properties, and the antenna design. Thus, a degradation of the RSSI does not necessarily mean that the mobile device is about to leave its access point's network area, but it can be due to temporary interference. (Montavont etc. 2005)

The problem occurs when the mobile device is located at the edge of the coverage area and the power level of the device is decreasing. The signal strength or power level of a mobile device is measured by the amount of IP packets received. If packets received without errors are below a power level threshold, a Link Going Down event is triggered. (Murtaza A. 2010)

The power level threshold depends on the noise level of the operating environment and the receiver performance (BER as a function of E_b/N_o). In heterogeneous networks different wireless technologies exist, and the network selection for a mobile device is getting more complex. In order to schedule handover in heterogeneous environment, the decision on target network and its access router can be done by adopting triggers such Link going Down. (Lampropoulos G. 2008) When receiving this trigger the mobile device sends messages to make the decision on the target access router, presented in figure 5.

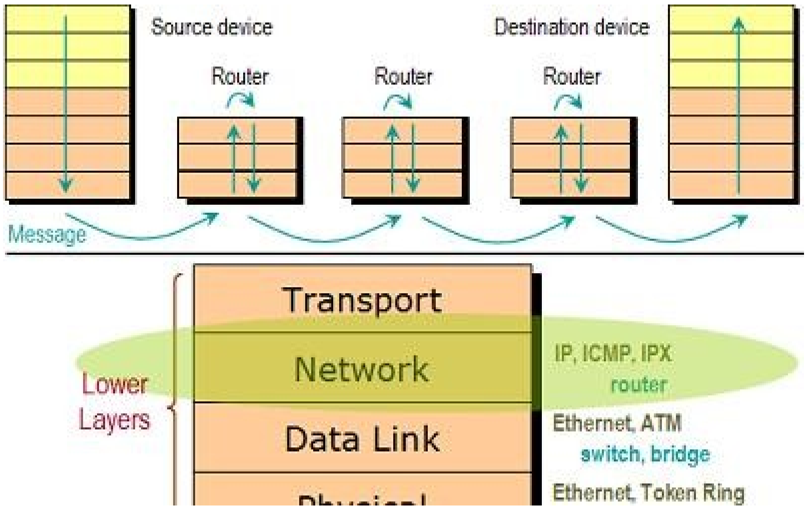


Figure 5. A message sent to a destination device. (About. Com. Wireless / networking)

When the mobile device is leaving the WLAN access point it will no longer wait for losing its connection with it, instead it generates a Link Going Down event as it gets close to the access point's network area and reassociates with a candidate access point with better Quality of Service (QoS) support. (Gupta V. 2004) The reassociation request frames contain a field with the address of the old access point.

The first step is made as the mobile device detects a candidate access point, it initiates the reassociation procedure and communicates with the old access point to determine that a previous association did exist. Then, the frames buffered at the old access point for the specific mobile user are transferred to the new access point and the old access point stops its association with the mobile user.

3.5. Registration

The registration phase in mobile-IP includes first the registration request and registration response messages, which are exchanged between the mobile device and its home agent. The registration request is sent from the mobile node to the mobile node's home agent. The home agent receives the registration request, and sends back to the mobile node a registration reply via the reverse path to tell if registration was successful. (Shaukat R. 2008) Once the mobile user enters a foreign network it listens for agent advertisements and then, it obtains a foreign address from the foreign network that it has moved to. This foreign address is a temporary address provided to visited mobile users (care-of-address), which means that the mobile user still keeps its home address. The care-of-address is better described at section 4.4.

3.6. Binding

Binding in mobile-IP is the IP packet's signal exchanging process between the mobile node's care of address that has moved to a foreign link and its home agent at the home network. When the handover is made the IP connectivity with the new access router is established and binding update between the care-of-address of the mobile node and its home agent is sent out to complete the Mobile-IP re-registration. The home agent contains a table that maps the mobile node's home addresses into the mobile node's current care-of-address(es). (Nikitopoulos D. etc. 2005)

A binding is valid for a specified Lifetime and a mobile node must re-register if this Lifetime is near to expiration. When the mobile device is located outside its home network a timer is setting up and the home agent may renew it except, if the mobile device will return to the home network and cancel the registration with the foreign network. The home address provided by the home agent to the user remains the same. Only the user's care of address (CoA) changes when he/she roaming between foreign networks. Also, when the CoA does not change either, the mobile node does not have to send a binding update to the home agent, which reduces the overall latency of the handover. (Niesink L. 2007) Sometimes, the mobile node decides to move to another network without waiting for the next periodic transmission of an agent advertisement. It will send agent solicitation to its home agent and force it to immediately transmit an agent advertisement.

It is useful when the frequency at which agents are transmitting agent advertisements is too low for a mobile node when moving rapidly from one link to another. When a foreign agent is discovered, it sends a binding update including the destination and home addresses to its home agent to announce its new location, shown in figure 6. Then, the home agent redirects the packets to the home address of the mobile device, and acknowledges the new location through a binding acknowledge message.

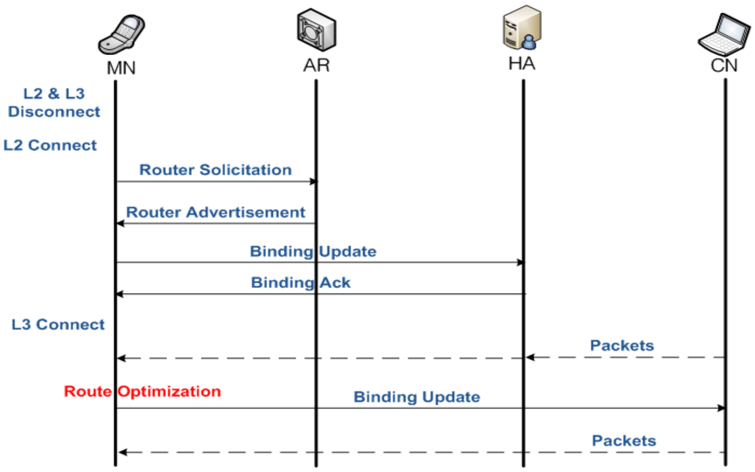


Figure 6. Mobile node's exchange messages. (Jaeho J. 2008)

After the Layer 2 connection and the link-layer procedure, the corradded node sends packets to the home address of the mobile node by using its home agent via tunnelling. The home agent sends a binding update to the user with its home IP address of the packets, back to the corradded node to inform it of its new location.

3.7. ICMP

The internet control management protocol (ICMP) defines a set of error and control messages which provide indications that errors have occured in the transmission of a packet. Other ICMP messages provide diagnostic information to a requesting node. (Solomon J. 1998) A router sends ICMP messages to its hosts to provide them optimal routes to reach a destination node. In case a host is using a non-optimal next hop, the router sends an ICMP redirect message which contains an IP address of a different router and the host will modify its routing table to the appropriate route.

If a mobile node does not listen advertisements from its home agent, it attempts to communicate by sending an ICMP Echo request message to the default router used when connected to its home link. (Solomon J. 1998) Otherwise, if there is no response from the default router the mobile node can assume that it is connected to some foreign link. In this case, the mobile node attempts to obtain an address from a Dynamic Host Configuration Protocol (DHCP) server.

3.8. Routing

The routers exchange information among themselves and inform host's location to which they are connected. The hosts IP addresses are build into routing tables, which are used to select a route for a given packet from the source to the destination. The routing table is also used by the router to make forwarding decisions for packets that are not destined to its current network. When a mobile device has an IP packet to forward it searches first its routing table to find a matching entry and forwards the packet to the destined fixed or mobile user.

The routing table includes the network-prefix, provides routes for all neighbour destinations connected to an attached link, and a default route for all other destinations. Each router keeps information at routing table about its neighbour routers which includes their IP addresses and the cost which is in terms of time and delay. (Zivkovic M. 2004) The router depending on the routing protocol it usually chooses the route with the least cost, which means that it forwards the packet to the closest or to the neighbour access router that will first discover to a particular destination.

4. MOBILE-IP NETWORK FEATURES

4.1. Mobile node network feature

A mobile user that changes its point of attachment to the Internet from one link to another while maintaining an ongoing communication must keep its IP home address. The mobile node must be configured with an IP address (IPv4) that is known to be within its home network. This allows the mobile node to know whether it is currently connected to its home network or to the public portion of the internet.

While the mobile user's device is allocated outside of its home network it listens to agent advertisements from the foreign networks to discover the destination node. The agent advertisements advertise their contents (IP address lists of their hosts) and let the mobile node to determine if it will be connected with a specific foreign link. When returns back to the home link the mobile device acts as stationary thus, is not using mobile-IP functionality.

4.2. Home Agent network feature

The home agent is a router at the mobile node's home network that keeps the mobile nodes informed of their current location when they move from the home link to a foreign link. It is also advertises reachability to the network of the mobile node's home address and exchanges IP packets that are destined to the mobile node's current location. (Sarikaya B. 2006)

Also, the home agent provides to the mobile device an IP address known to be within its home network and stays informed when the mobile device is attempting to change network. The most important function of the home agent is that it supports a tunneling mechanism in order to tunnel IP packets, in figure 7 (Netcraftsmen 2008).

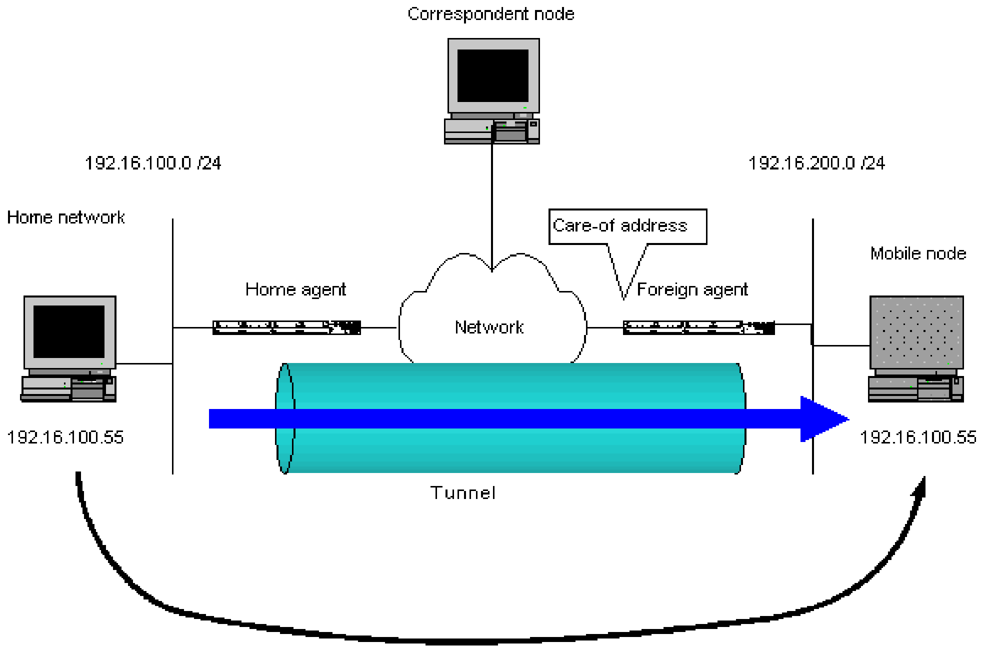


Figure 7. Tunneling mechanism. (Netcraftsmen 2008)

4.3. Foreign Agent network feature

The foreign agent is the router on the mobile node's visited network and cooperates with the mobile node's home agent in order to route packets to the mobile node. The foreign agents periodically broadcasts agent advertisements to advertise their presence to visiting mobile nodes. The mobile node's care-of-address is a temporary address and is changing every time it moves from one foreign link to another. (Chen Y. 2008)

In case that a foreign network does not support mobile-IP mechanism to visiting mobile node, it will issue temporarily IP addresses assigned to the interface of the mobile nodes using Dynamic Host Configuration Protocol (DHCP). The DHCP protocol handles the assignment of IP addresses, subnet masks, default routers, and other IP parameters to the client devices that don't have a static IP address. The client devices must have installed the DHCP daemon.

4.4. Mobile-IP architecture

In this section we describe the location of home agents and foreign agents and how mobile nodes gain access to their services. The figure 8 illustrates a departmental LAN which includes fixed or mobile hosts, home/foreign agents, and certain mobile nodes are all inside the network.

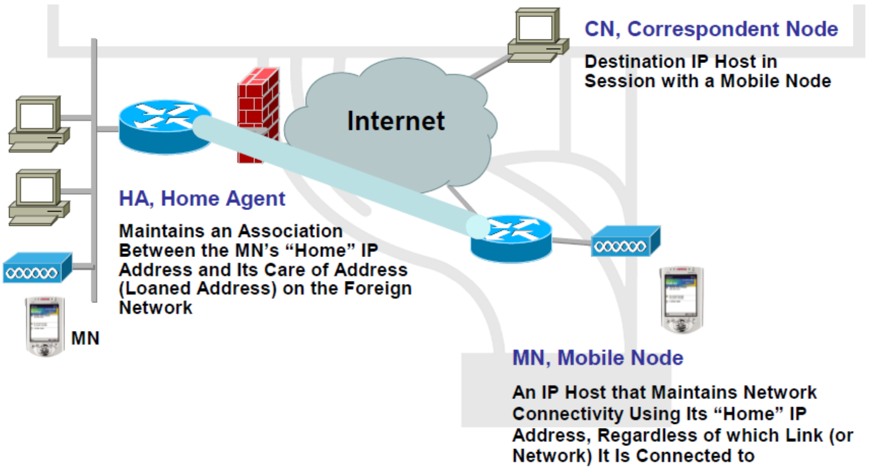

CN, Correspondent Node
Destination IP Host in Session with a Mobile Node
Internet
HA, Home Agent
Maintains an Association Between the MN's "Home" IP Address and Its Care of Address (Loaned Address) on the Foreign Network
MN
MN, Mobile Node
An IP Host that Maintains Network Connectivity Using Its "Home" IP Address, Regardless of which Link (or Network) It Is Connected to

Figure 8. Mobile-IP architecture. (Abdullahi A. 2010)

When a mobile node arrives at a foreign network listens for agent advertisements and selects a foreign agent that supports tunnelling. The mobile device encapsulates all outgoing packets and send them to the selected foreign agent. The foreign agent receives the packets, decapsulates and re-tunnels them to the home agent. On the other side, the home agent advertise its presence by periodically multicasting or broadcasting Mobile-IP agent advertisements.

The roaming mobile device maintains two addresses: a static home address and a temporary care-of address. The care-of-address encapsultes the whole IPv4 packet of the static home address within its payload and only the header size of the care-of-address is visible by other networks. With this way when the mobile user is roaming is able to keep its static home address, shown in figure 9.

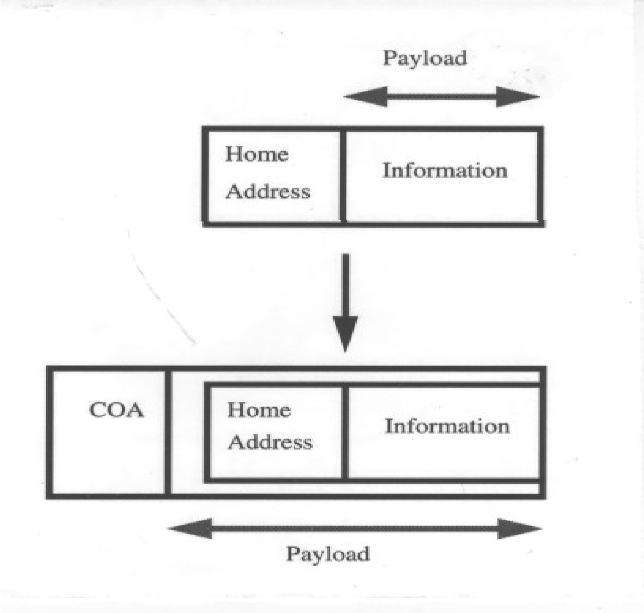


Figure 9. Care-of-Address (CoA).

The home agent maintains its routing table the mobile device's home address and when a mobile device moves to a foreign network, its home and foreign agents establish an association which is made by sending agent advertisement messages. The advertisement messages are propagated periodically in a broadcast manner by all agents. The mobile user can learn if it is located in its home network or in a foreign network depending on the type of message exchanged between the home and the foreign agent.

4.5. Triangle routing

In triangle routing the mobile user sends the packets to the correnspondent node (CN) through the foreign agent but the packets originating from the CN are sent to the home agent and then forwarded to the mobile user through the foreign agent. A registration request message is sent by the mobile node to the home agent and the home agent then replies with a registration reply message (Niesink L. 2007). The traffic between the mobile user and the correnspondent node flows is indicated by the arrows, in figure 10.

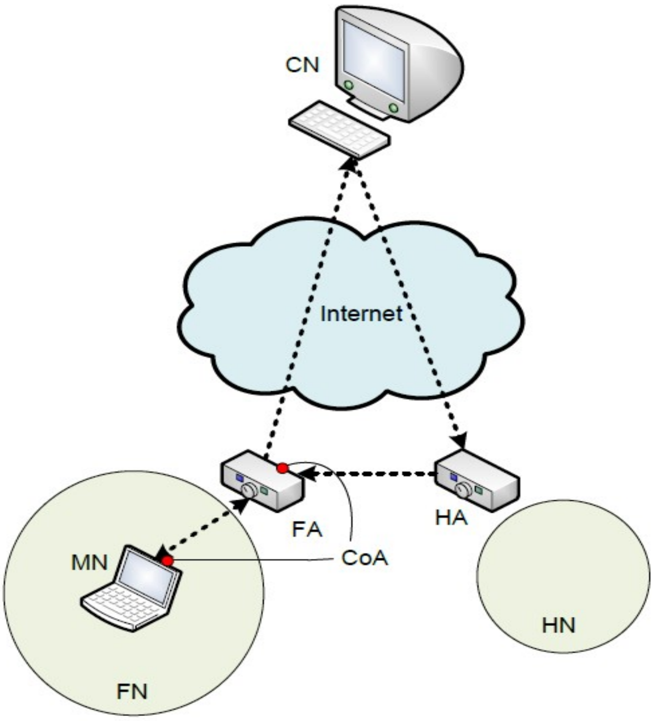


Figure 10. Triangle routing. (Niesink L. 2007)

4.6. Direct routing

As described above, in triangle routing when the correnspondent node sends a packet to the mobile node it has to travel via the home agent of the mobile node. If the mobile node is close to its home agent and the correnspondent node is far away from the mobile node this is not really a problem. However, if the mobile node and correnspondent node (CN) are close to each other and the mobile node is far away this creates a problem known as triangle routing. (Marques H. D.3.2. 2008)

This problem may cause long delays in message arriving at its destination as the message from the CN has to travel all the way to the home agent and then to the mobile node instead of travel straight to the mobile node, which would be much shorter. It is suggested that enabling a CN to have a binding for the mobile nodes current address will solve this triangle routing problem. An optimized route can be made when the correnspondent node receives a binding update and not the home agent. (Marques H. D3.1. 2008)

The mobile node can then send a binding update message containing its new CoA to the CN. The CN will then update its binding for the mobile node's address. In this way a chunk of signaling due to routing to home agent is eliminated, shown in figure 11. However, this structure leaves some security holes that potentially allow message replaying and enables someone to eavesdrop on the packets that are being sent. Thus, is the CN needs to identify and authenticate the source of the binding update message. (Niesink L. 2007)

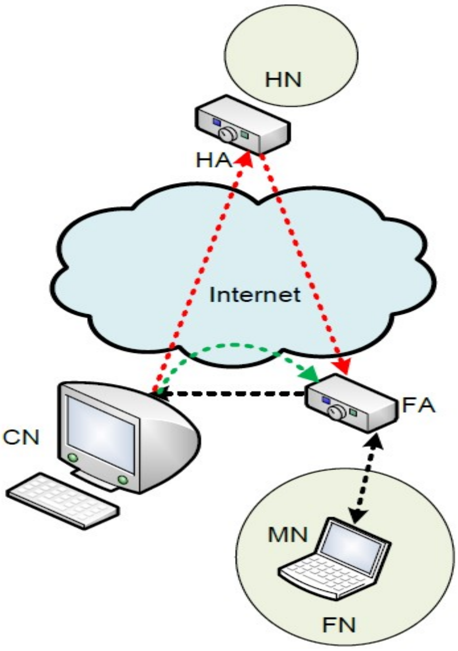


Figure 11. Direct routing.(Niesink L. 2007)

The home agent updates its mapping address between the home address of the mobile node and the updated care-of-address (CoA). The IPv4 packet format with the registration requests and message replies of the mobile node is shown in figure 12.

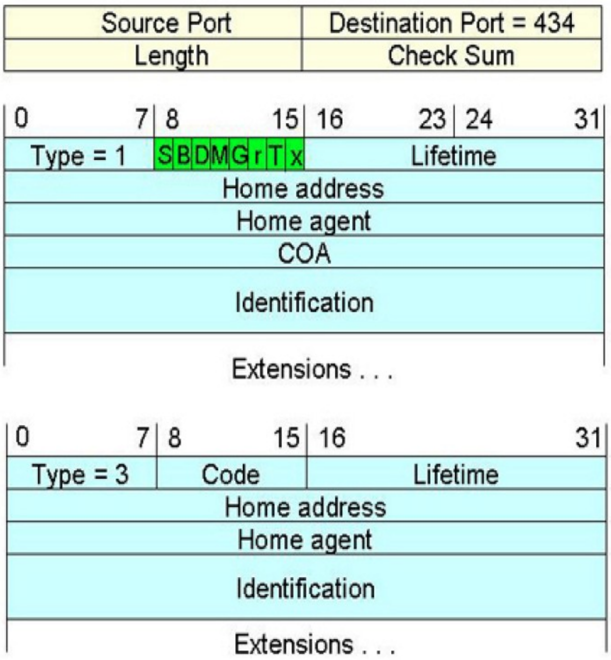


Figure 12. Registration request and Reply protocols. (Chakchai S. 2006)

The UDP packet is located on top of the figure, in the middle is located the Registration Request, and at the bottom of the figure is the Registration Reply protocol. Both registration messages use the UDP protocol in which a destination port is set to 434. In case the mobile node returns to its home network, it sends de-registration message to its home agent (Lifetime is set to 0) and mobile-IP mechanism.

5. VERTICAL HANDOVER SCENARIOS

We tested vertical handover with the mobile-IP protocol implementation between different technologies. We describe in details the handover procedures by using mobileIP. First we describe the Wimax-Wifi handover at 5.1 section and then, at 5.2 section the Wimax-UMTS handover. In Wimax-UMTS section we make a brief description of the UMTS architecture before we describe the handover. The theoritical maximum data rates and communication range of WiMax, WiFi and 3G/UMTS systems are illustrated at the following table, in table 6.

Table 6. Data rates of different wireless technologies.

Type of wireless technology	Theoretical maximum data rate	Theoretical maximum transmission range
Mobile WiMax	70 Mbps	10 km
3G cellular	3 Mbps	1 km
Wi-Fi (802.11g)	54 Mbps	100m

5.1. WiMax – WiFi vertical handover

During the vertical handover all IP packets switch from an interface to another with different physical parameters. The packets transmission between different networks causes the mobile device's IP address to be changed. In order to maintain the reachability, the mobile node should have a mechanism to inform quickly its correspondent node of its new address or it should have a permanent IP address seen by the correspondent node.

The vertical handover is the process when a mobile device moves between networks with different technology without braking the TCP/UDP connection. The Mobile-IP technology solves the problem of node mobility by redirecting packets from the mobile node's current location to its "home" network by using router advertisements. (Gondi V. 2009) The Correspondent node is any host fixed or mobile that sends packets to the mobile user’s IP address through its home agent. When the mobile user is located to a foreign network its home agent communicates with the foreign agent, and forwards data packets. (Lim W. etc. 2008)

As mentioned before, vertical handover consists of different integrated networks. In integrated 802.11/802.16e networks the mobile users may want to use the 802.11 network whenever it is accessible. The 802.11 network protocol supports smaller coverage with high data rates and 802.16 supports larger coverage with low data rates. The mobile-IP uses triggers from the MAC layer such as “link up” and “link down” although such triggers are not specified in the MIPv4 standard.(Lampropoulos G. 2010) The WLAN to WiMax vertical handover delay occurs when the mobile user moves out of the coverage of the 802.11 access point, figure 13.

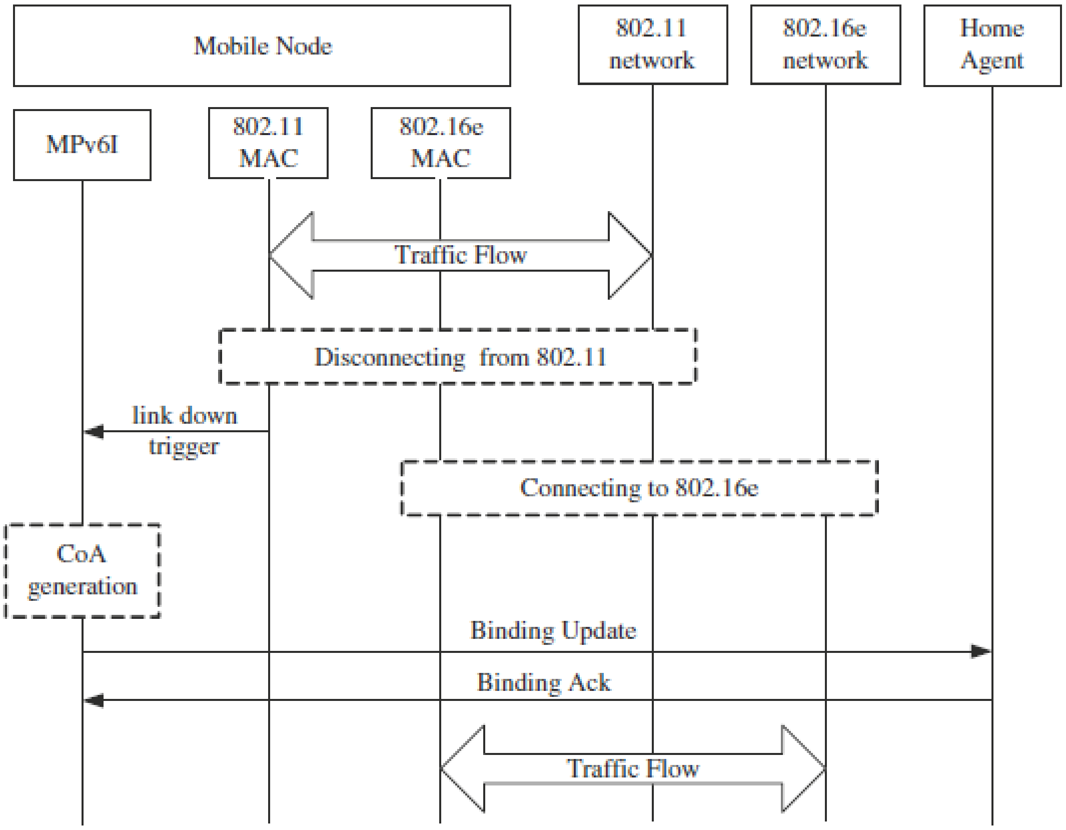


Figure 13. 802.11 to 802.16 vertical handover.

The handover procedure started when the 802.11 link was broken due to the movement of the mobile device and a “link down” trigger generated from the 802.11 MAC layer. When the mobile device detected the break of the 802.11 link through the trigger it connected to the 802.16e link. After activating the 802.16e link the mobile device generated a new care-of- address (CoA). The link connection and CoA generation maintained connectivity to the 802.16e link even when it used the 802.11 interface. (Li B. 2007) After the CoA was generated successfully the mobile device sent a binding update (BU) message to its home agent and received a biding acknowledgement (BA) message.

After exchanged binding messages the mobile device used the 802.16e interface for data communications. The link down trigger helps the MIPv4 module to detect the disconnection of the 802.11 link faster. The movement detection of the mobile device is achieved by receiving a router advertisement message periodically. (Lim W. etc. 2008) Thus, the mobile device notifies that the 802.11 link is not available when it fails to receive a new router advertisement within the lifetime of the past one. The WiMax to WLAN network vertical handover delay occurs when it moves into the coverage of an 802.11 access point, figure 14.

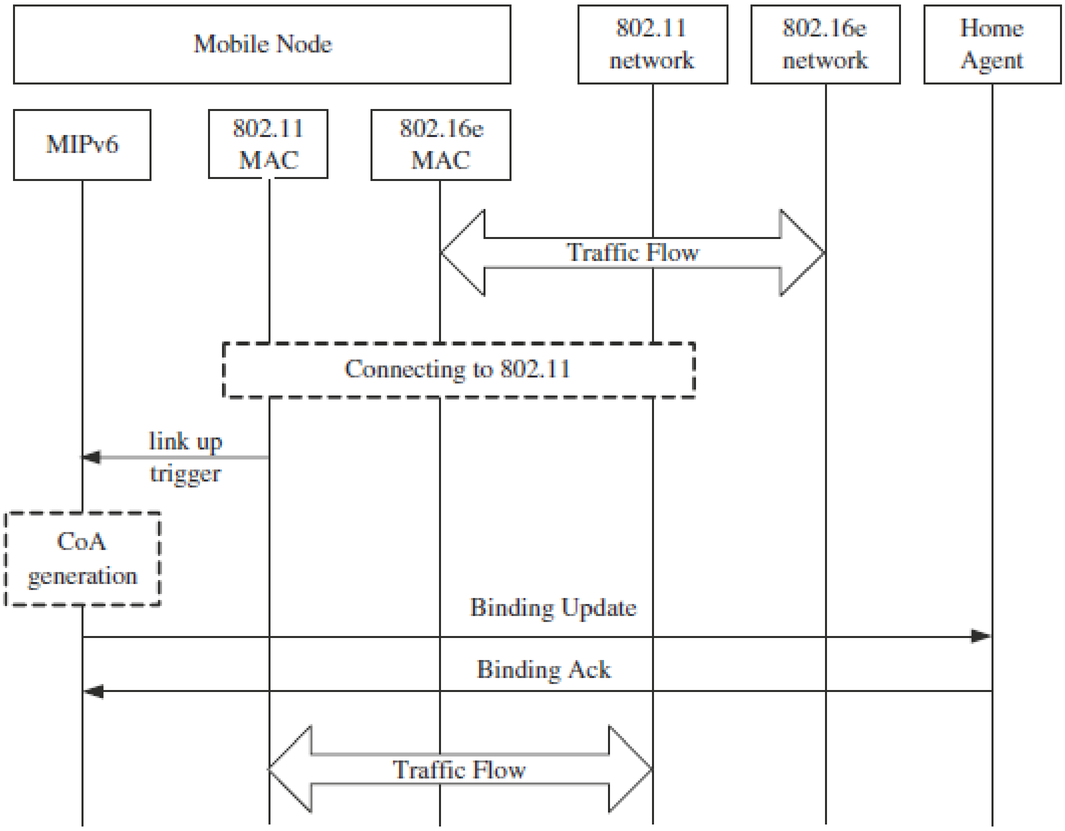


Figure 14. 802.16 to 802.11 vertical handover.

5.2. UMTS – WiMax vertical handover

The UMTS network architecture consists of the Base Station (BS), Radio Network Controller (RNC), Serving GPRS Supported Node (SGSN), Gateway GPRS Supported Node (GGSN) entities, as shown in figure 15.

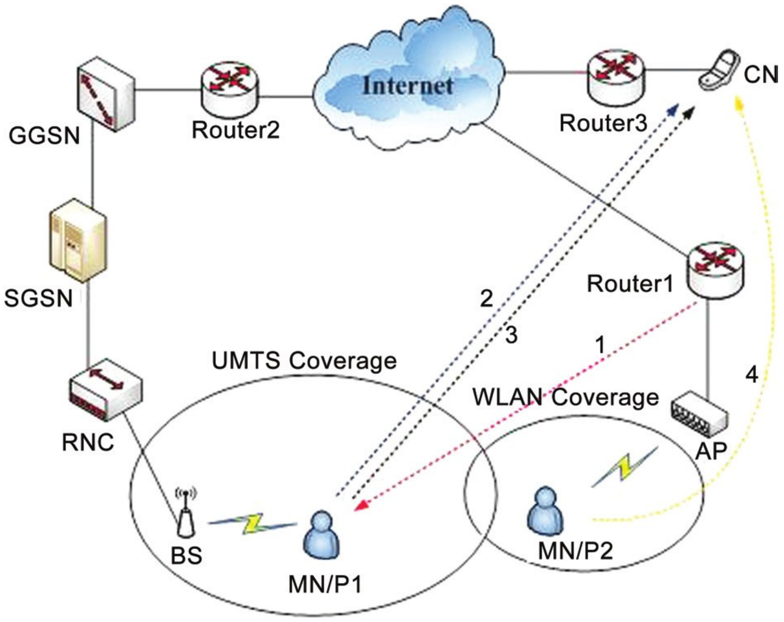


Figure 15. UMTS-WLAN signalling. (Hamza B. 2010)

The RNC performs encryption and manages connections of different areas which are in between SGSN and radio network controller. Also, it establishes the GPRS tunnel with SGSN which is a packet switched element that performs mobility management. The SGSN further creates a GPRS tunnel with GGSN and connects external packet switched networks with other UMTS or different networks.

(Gomes A. 2008) The WiMax's hardware elements consisted of the Micro Base station or input data unit and the output data unit, in figure 16.

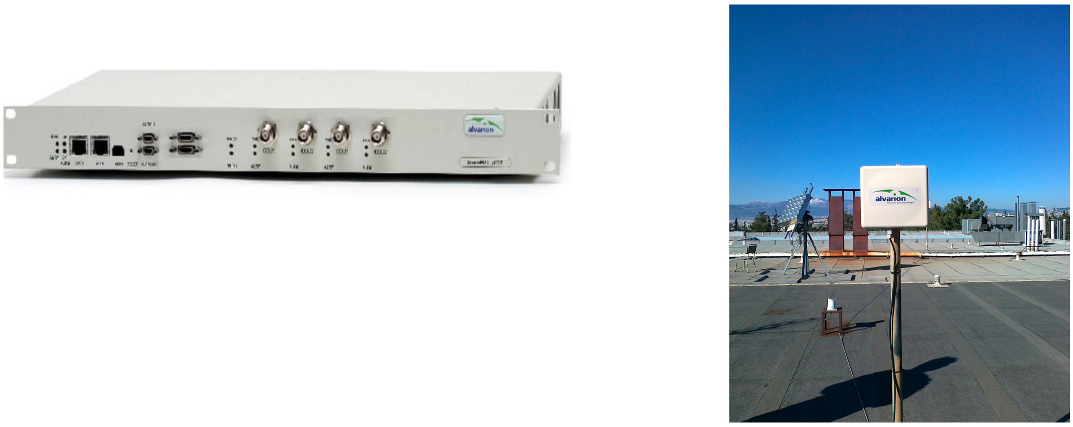


Figure 16. IDU unit (left), ODU unit (right).

The Alvarion devices are Si-V-integrated data and voice units. The ODU unit supports 3.3–3.4GHz and 3.65-3.70 GHz and maximum transmit power of 22dBm, and is intended to support mainly outdoor customers premises equipments (CPEs). This version is stable with good radio performance and focuses on all indoor and outdoor capabilities. The Micro Base station has small dimensions with all Base Station required components: Network Processing Unit (NPU), AU Power Supply and Power Interface as described in the specifications, Report UL RSSI per channel and Weighted RSSI. (Alvarion 2011)

The base station transmit the signals with high power because the coverage area is wider compared to the WLAN infrastructure which average communication distance is not further than 100m. (Taniuchi K. 2009) On the other hand, the data rates in WLAN supports a higher data rate than 3G so WLAN should be preferred if available, shown in figure 17.

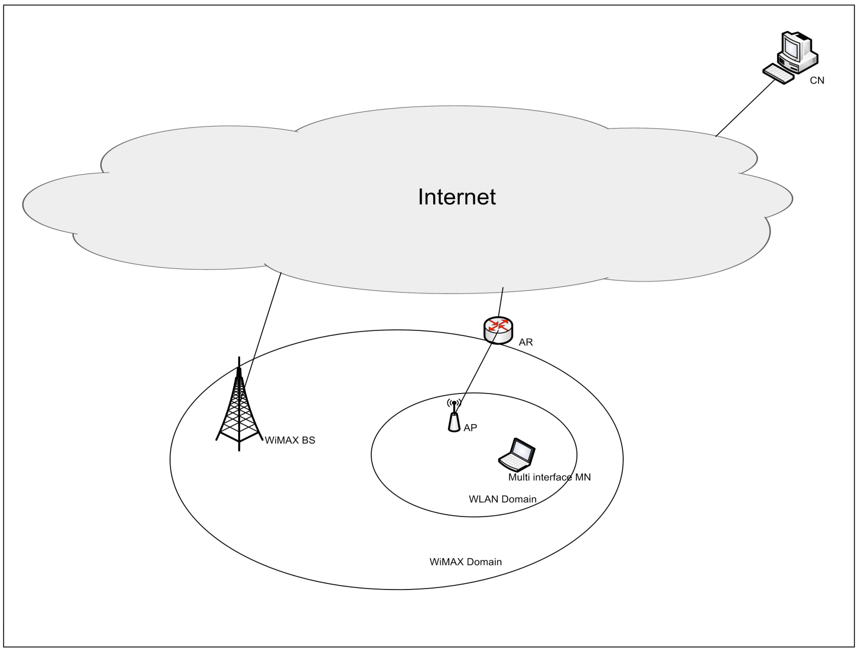


Figure 17. Wimax-WLAN integrated network (Adnan K. 2009).

In our testbed scenario the GSM/UMTS Vodafone internet service provider (ISP) does not use mobileIP technology and supports private IP addresses. The Virtual Private Network (VPN) was used to make handover from our wimax network to the Vodafone ISP. The virtual private network (VPN) uses the internet to provide remote systems or individual users with secure access to their organization's network. (Kurur N. 2008) A VPN consists of two or more physical private networks that are separated by a public network (internet) and performs as a single private network. These private networks allow only packets containing strong authentication to pass through. To achieve vertical handover from WLAN to UMTS our mobile node must be supported with no less than two access network interfaces.

In our case we had two interfaces, the wlan0 PC's interface and the ppp0 Nokia's phone interface. We installed the `wvdial` utility to our mobile node. (Softpedia - WvDial 1.61. 2011) The wvdial is a Point-to-Point protocol (PPP) dialer which dials a modem and starts a pppd daemon to connect our mobile device with Vodafone ISP (Internet). The PPP protocol is the most common link-layer protocol by which individual users connect to the Internet via their ISP's. (Schroder Carla 2008)

6. OPERATING SYSTEM & NETWORKING TOOLS

6.1. Operating system

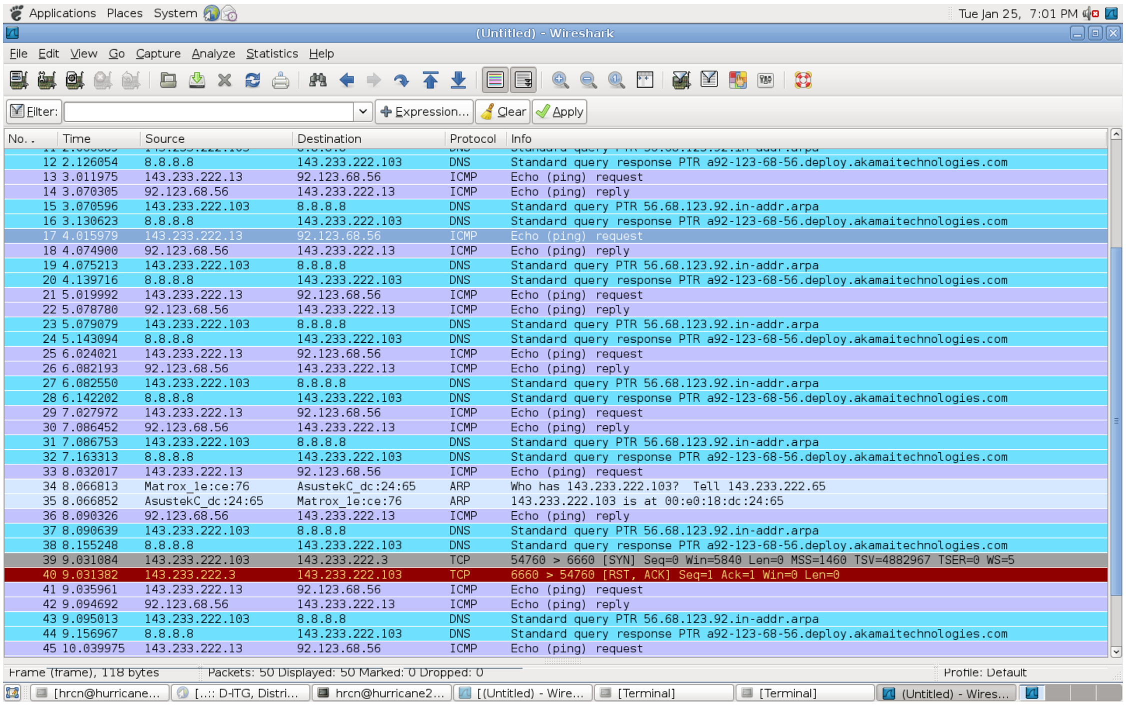
The operating systems used were Debian and Ubuntu Linux-based operating systems. Linux is a generic term referring to Unix-like computer operating systems based on the Linux kernel. The Linux kernel characterize the piece taken to handle the hardware and communication applications with it. It is responsible for memory management and file system, communication between different processes, management of system devices, etc. Usually the kernel functions are in the background and go unnoticed by the user, hiding details of the internal functioning of the computer.

Because of its nature, anyone (company or individual) can get the kernel to add the GNU tool chain and any other applications they want and create their own operating system Linux. Currently, there are over 300 + different distributions of Linux. Some of the most popular at the moment are Ubuntu, Debian, OpenSUSE, Fedora, Mandriva, Slackware etc. We used the Debian and Ubuntu operating systems and installed the Dynamic and Hierxarchical IP Tunneling System package to create our Mobile-IP Network.(Softpedia -Linux. 2010) The Ubuntu version was 9.04 with 2.6.28 Linux-kernel which includes the latest enhancements and was maintained until the beginning of 2011. (Download Ubuntu 2010)

6.2. Networking tools

To analyze the Network we used Wireshark a free and open source software computer network protocol analysis. (Lamping U. 2011) Wireshark is useful for network analysis, network monitoring, tracking and troubleshooting networks and is ideal for research and educational purposes.

The Wireshark is a packet analyzer that allows the user to intercept and display network characteristics such as UDP or TCP IP packets being transmitted or received from a network to which a fixed or mobile device is attached. It also, provides options for sorting and filtering and allows the user to monitor all traffic on the network, shown in figure 18.



```
No. .  Time       Source              Destination         Protocol  Info
    12 2.126054   8.8.8.8             143.233.222.103     DNS       Standard query response PTR a92-123-68-56.deploy.akamaitechnologies.com
    13 3.011975   143.233.222.13      92.123.68.56        ICMP      Echo (ping) request
    14 3.070305   92.123.68.56        143.233.222.13      ICMP      Echo (ping) reply
    15 3.070596   143.233.222.103     8.8.8.8             DNS       Standard query PTR 56.68.123.92.in-addr.arpa
    16 3.130623   8.8.8.8             143.233.222.103     DNS       Standard query response PTR a92-123-68-56.deploy.akamaitechnologies.com
    17 4.015979   143.233.222.13      92.123.68.56        ICMP      Echo (ping) request
    18 4.074900   92.123.68.56        143.233.222.13      ICMP      Echo (ping) reply
    19 4.075213   143.233.222.103     8.8.8.8             DNS       Standard query PTR 56.68.123.92.in-addr.arpa
    20 4.139716   8.8.8.8             143.233.222.103     DNS       Standard query response PTR a92-123-68-56.deploy.akamaitechnologies.com
    21 5.019992   143.233.222.13      92.123.68.56        ICMP      Echo (ping) request
    22 5.078780   92.123.68.56        143.233.222.13      ICMP      Echo (ping) reply
    23 5.079079   143.233.222.103     8.8.8.8             DNS       Standard query PTR 56.68.123.92.in-addr.arpa
    24 5.143094   8.8.8.8             143.233.222.103     DNS       Standard query response PTR a92-123-68-56.deploy.akamaitechnologies.com
    25 6.024021   143.233.222.13      92.123.68.56        ICMP      Echo (ping) request
    26 6.082193   92.123.68.56        143.233.222.13      ICMP      Echo (ping) reply
    27 6.082550   143.233.222.103     8.8.8.8             DNS       Standard query PTR 56.68.123.92.in-addr.arpa
    28 6.142202   8.8.8.8             143.233.222.103     DNS       Standard query response PTR a92-123-68-56.deploy.akamaitechnologies.com
    29 7.027972   143.233.222.13      92.123.68.56        ICMP      Echo (ping) request
    30 7.086452   92.123.68.56        143.233.222.13      ICMP      Echo (ping) reply
    31 7.086753   143.233.222.103     8.8.8.8             DNS       Standard query PTR 56.68.123.92.in-addr.arpa
    32 7.163313   8.8.8.8             143.233.222.103     DNS       Standard query response PTR a92-123-68-56.deploy.akamaitechnologies.com
    33 8.032017   143.233.222.13      92.123.68.56        ICMP      Echo (ping) request
    34 8.066813   Matrox_le:ce:76     AsustekC_dc:24:65   ARP       Who has 143.233.222.103?  Tell 143.233.222.65
    35 8.066852   AsustekC_dc:24:65   Matrox_le:ce:76     ARP       143.233.222.103 is at 00:e0:18:dc:24:65
    36 8.090326   92.123.68.56        143.233.222.13      ICMP      Echo (ping) reply
    37 8.090639   143.233.222.103     8.8.8.8             DNS       Standard query PTR 56.68.123.92.in-addr.arpa
    38 8.155248   8.8.8.8             143.233.222.103     DNS       Standard query response PTR a92-123-68-56.deploy.akamaitechnologies.com
    39 9.031084   143.233.222.103     143.233.222.3       TCP       54760 > 6660 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=4882967 TSER=0 WS=5
    40 9.031382   143.233.222.3       143.233.222.103     TCP       6660 > 54760 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    41 9.035961   143.233.222.13      92.123.68.56        ICMP      Echo (ping) request
    42 9.094692   92.123.68.56        143.233.222.13      ICMP      Echo (ping) reply
    43 9.095013   143.233.222.103     8.8.8.8             DNS       Standard query PTR 56.68.123.92.in-addr.arpa
    44 9.156967   8.8.8.8             143.233.222.103     DNS       Standard query response PTR a92-123-68-56.deploy.akamaitechnologies.com
    45 10.039975  143.233.222.13      92.123.68.56        ICMP      Echo (ping) request
Frame (frame), 118 bytes    Packets: 50 Displayed: 50 Marked: 0 Dropped: 0    Profile: Default
```

Figure 18. Wireshark packet analyzer.

It is also important to know that there are some other parameters that should be kept in mind when setting up a network of these characteristics, such as the transmission channel, the frequency, the transmission power, the bit-rate, etc. To set these parameters we used tools such as Iw, Iwconfig, route. Those are very useful because they allow running the network with the parameters selected by the user. Some important network tools we used at Linux OS were the following:

- `Ping:` Is a computer network administration utility used to test whether a particular host is reachable across an Internet Protocol (IP) network and to measure the round-trip time for packets send from the local host to a destination computer, including the local host's own interfaces.

- `Route:` Is a tool that manipulates the kernel's IP routing tables. Its primary use is to set up static routes to specific hosts or networks via an interface.

- `Iptables:` Provide a table-based system for defining firewall rules that can filter or transform packets. It can be also used to create static MAC address routing.

- `Iwconfig:` Used to set the parameters of the network interface which are specific to the wireless operations.

- `Ifconfig:` Is an utility that communicates with the IP configuration agent to retrieve and set IP configuration parameters.

7. TEST-BED IMPLEMENTATION

At Demokritos institute each department has its own local area network (LAN) (NCSR). There are types of media deployed throughout the campus: wired Ethernet and some type of wireless LAN products. Each department LAN is connected to a central router that provides connection to the internet. At the Department of Informatics and Telecommunications laboratory, shown in figure 19. The mobile-IP mechanism used to provide inter-system handovers between different networks such as WiMax, WiFi and UMTS/3G systems.

Figure 19. Informatics and Telecommunication's laboratory.

Our network topology included several networks using Wimax, WiFi, GSM/UMTS technologies. The network was transformed into one after we configured the Mobile-IP protocol to our platform and by installing mobile node and home agent software. (Sourceforge - Dynamics 2010) The Wifi and wimax networks connected with a wireless access point and wimax data unit respectively, are illustrated in figure 20.

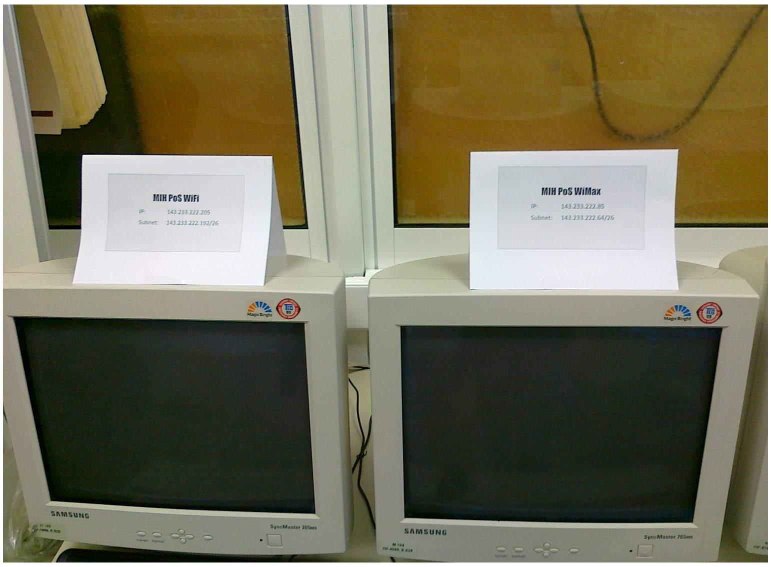


Figure 20. The wifi and wimax PC's.

Next, the testbed router and the home agent PC's are shown in figure 21.

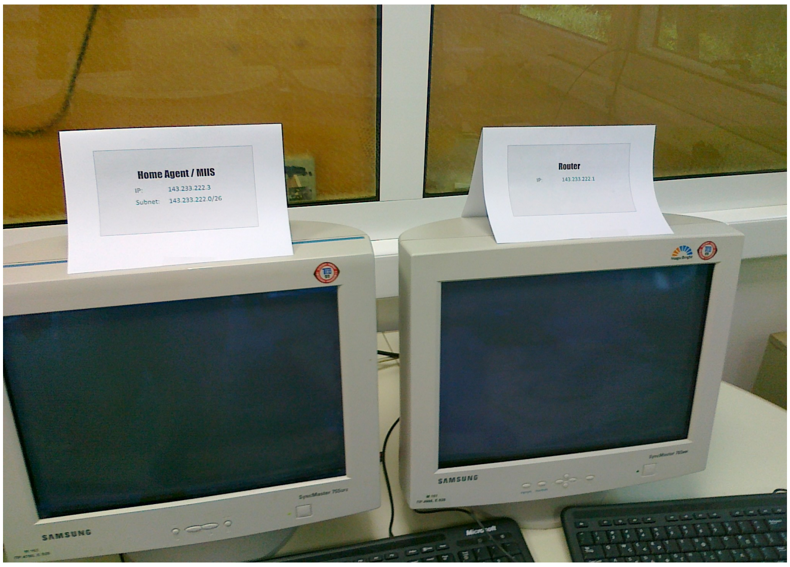


Figure 21. The home agent and testbed router PC's.

7.1. Mobile node setup-configuration file

We made the following changes at the mobile node configuration file. These changes were the Mobile Nodes's IP address in the Home Network, the Home Agent IP Address and Enable Foreign Agent Decapsulation mode. The `EnableFADecapsulation` has two modes `< TRUE | FALSE >`.

TRUE enables this mode and sets the foreign agent to decapsulate the IP-within-IP encapsulated IP packets. With the foreign agent decapsulation the mobile node uses its home address in the interface even in the foreign network . FALSE disables this mode and sets the default mode where the mobile node decapsulates the IP-within-IP encapsulated IP packets. With the mobile node decapsulation the mobile node acquires a care-of-address (CoA) from the visited network. We set `EnableFADecapsulation` to false as we did not use a foreign agent to our testbed.

In addition, we could choose the tunneling mode. The mobile-IP Authentication Authorization Accounting (AAA) supports four tunneling modes to which only one each time can be selected. The possible modes are the following are:

- 1 = automatic, prefer reverse tunnel (i.e. bi-directional tunnel)
- 2 = automatic, prefer triangle tunnel (i.e. tunnel only in CN->MN direction)
- 3 = accept only reverse tunnel
- 4 = accept only triangle tunnel

We chose `TunnelingMode 3` for our mobile node which uses reverse tunelling. When the mobile node get a care-of address and use reverse tunneling it sets the default route to the tunnel. In this way, all the IP packets are destined to the mobile node from other networks via the home agent. The following configuration option specifies the routing operation that is used with the CoA:

- 0 = set default route to the tunnel
- 1 = set only the home network route to the tunnel (the above HomeNetPrefix options must be set)
- 2 = do not change the routing entries (i.e. some external means must be used to direct traffic to the tunnel, e.g. manually adding host route to a specific host).

The Default Tunnel Lifetime is the lifetime suggested in registration. The lifetime is defined in seconds and the default value is 300, shown in table 7. The request timer will be set according to this value, and in case the foreign agent's agent advertisment has a smaller time, it is used instead. In Special cases Lifetime can be set to 65535 (or more) seconds means unlimited time and the binding will not expire. The UDP port used for sending registration requests at the `Port 434` which is allocated for Mobile-IP signaling, and this should not be changed unless the network is known to use some other port.

Also, all the foreign agents and home agents must have configured the same port. In addition, we set the Socket priority for signaling sockets (UDP) with `SO_PRIORITY` to allow easier QoS configuration. If this argument is set (value 1), the given value is used as a priority for the signaling socket and signaling is not disturbed by other traffic on a congested link.

Table 7. Mobile node configuration parameters.

```
EnableFADecapsulation FALSE

TunnelingMode 3

MNDefaultTunnelLifetime 300

UDPPort 434

SocketPriority 1
```

7.2. Home agent setup-configuration file

We configured the home agent in order to establish connection with our network and receive or send registration messages to the mobile nodes. We modified the configuration parameters such as agent discover mode, maximum lifetime, maximum bindings, and tunneling modes in registrations permitted by the home agent. The home agent's configuration parameters configured to:

- 0 = do not allow dynamic home agent discovery
- 1 = allow dynamic home agent discovery with broadcast messages `agentadv`:
- 0 = do not send agent advertisements without agent solicitation
- 1 = send agent advertisements regularly
- -1 = do not send any (even solicited) agent advertisements

We chose for home agent to provide dynamic home agent discovery with broadcast messages and the agent advertisements was set to regularly. As at the mobile configuration file the UDP port was set to the same port, to Port 434 to listen for registration requests and Socket Priority to 1. Also, we set the maximum amount of bindings to 20 times to control the amount of time that the mobile device communicates with the home agent. Then we set the default tunnel lifetime of the home agent to be 600 seconds, shown in table 8.

Table 8. Home agent configuration parameters.

```
UDPPort 434

SocketPriority 1

MaxBindings 20

HADefaultTunnelLifetime 600

EnableTriangleTunneling FALSE
```

7.3 Foreign agent setup-configuration file

The foreign agent can be configured to deny registration replies that do not have mobile node-foreign agent key from the AAA extension. We set `RequireMNFASecAssoc` to false because we did not use in our test-bed implementation foreign agent. However, if the foreign agent is used we set a maximum number of tunnels or confirmed bindings going through this foreign agent. The default value for `MaxBindings` was 20, the same amount as we set the home agent. If the mobile nodes are trying to register more than the amount of `MaxBindings` the new registrations are refused.

In addition, we configured the foreign agent to limit a maximum number of pending registration requests or unconfirmed bindings. Additional registrations will be rejected until at least one of the pending registrations has been completed or has timed out. Then we set to false the following mobile-IP mechanisms as we did at the mobile node configuration and home agent files before. Also, the foreign agent may request registration even from mobile nodes that have acquired a care-of address. This option selects whether the agent advertisements messages have 'Registration required' flag or not.

Table 9. Foreign agent configuration parameters.

```
RequireMNFASecAssoc FALSE
MaxBindings 20
MaxPending 5
DeletePendingAfter 7
EnableFADecapsulation FALSE
EnableTriangleTunneling FALSE
EnableReverseTunneling TRUE
RegistrationRequired TRUE
FADefaultTunnelLifetime 600
PacketSocketMode 1
```

The lifetime is defined in seconds and the default value is 600, illustrated in table 9. The foreign agent sets the `DefaultTunnelLifetime` which is the maximum lifetime advertised for this foreign agent. This should not be greater than any of the maximum lifetimes configured for upper foreign agents and is recommended to use the same maximum lifetime for whole foreign agents.

The foreign agent uses a packet socket for link-layer L2 header access. When sending registration messages to a mobile node it does not implement fragmentation. Thus, IP packets larger than the used maximum transfer unit (MTU) are dropped. The foreign agent can be configured not to use packet socket when sending frames, but this requires to broadcast Address Resolution Protocol (ARP) for mobile node's home address when visiting a foreign network. The possible values to set the foreign agent's packet socket mode are:

- 0 = use packet socket when sending registration replies to MN (default).
- 1 = do not use packet socket at all for sending registration messages PacketSocketMode 0.

7.4. Testbed router setup

The testbed router consisted of four interfaces where two interfaces were connected to networks with different technologies such as WiMax and WLAN. A third interface was provided for the home agent of our mobile-IP platform. The fourth interface was configured to support the 3G/UMTS infrastructure connected to the rest of the platform. We set the interfaces to the `/etc/network/interfaces` file which describes the network interfaces, shown in table 10.

Table 10. Network interfaces file.

```
#The loopback network interface

auto lo
iface lo inet loopback

# The primary network interface


allow-hotplug eth0
iface eth0 inet static
address 143.233.252.214
netmask 255.255.255.252
network 143.233.252.212
broadcast 143.233.252.215
gateway 143.233.252.213




iface eth1 inet static
address 143.233.222.1

netmask 255.255.255.192
auto eth1



iface eth3 inet static
address 143.233.222.65
netmask 255.255.255.192
auto eth3


iface eth2 inet static
address 143.233.222.129
netmask 255.255.255.192
auto eth2



iface eth4 inet static
address 143.233.222.193
netmask 255.255.255.192
auto eth4
```

The ethernet IP address was the `143.233.252.214`, the testbed router's IP address was `143.233.222.1`, the Wimax's router IP address was

143.233.222.65, the home agent's IP address was 143.233.222.129, and the Wifi router's IP address was 143.233.222.193. The IP address 143.233.252.213 was the ethernet connection to the internet. The final routing table was illustrated, shown in table 11.

Table 11. Router's Kernel IP routing table.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
143.233.252.212	0.0.0.0	255.255.255.252	U	0	0	0	eth0
143.233.222.192	0.0.0.0	255.255.255.192	U	0	0	0	eth4
143.233.222.128	0.0.0.0	255.255.255.192	U	0	0	0	eth2
143.233.222.64	0.0.0.0	255.255.255.192	U	0	0	0	eth3
143.233.222.0	0.0.0.0	255.255.255.192	U	0	0	0	eth1
0.0.0.0	143.233.252.213	0.0.0.0	UG	0	0	0	eth0

7.5. wvdial setup-configuration file

We added a new IP registration to our testbed router's routing table to forward the packets that are destined to the VPN network (Vodafone's infrastructure). It enabled us to integrate the Vodafone infrastructure system to our network. To access the internet through Vodafone's GR infrastructure the following items were required:

- a software, the wvdial running on our PC that implements TCP/IP and the PPP protocols (Softpedia - WvDial 1.61. 2011).

- a modem, our Nokia mobile device along with the software provided with it.

- a telephone line, an account (service agreement) with Vodafone's Internet Service Provider.

We used the WvDial software between the PC and the modem (Nokia mobile device) configured with the Vodafone ISP settings to dial and to established connection. When WvDial starts it first loads its configuration from the `/etc/wvdial.conf` file. The wvdialconf probes our communication ports, looking for a modem and determine its capabilities. This configuration file includes basic information about the modem port, speed, and init string, shown in table 12.

Table 12. wvdial utility installation.

```
christof@ubuntu:~$ sudo -s
[sudo] password for christof:
root@ubuntu:~# cd ..
root@ubuntu:/home# apt-get install wvdial
root@ubuntu:/home# wvdialconf
Editing `/etc/wvdial.conf'.


Scanning your serial ports for a modem.
```

```
Modem Port Scan<*1>: S0   S1   S2   S3
ttyACM0<*1>: ATQ0 V1 E1 -- OK
ttyACM0<*1>: ATQ0 V1 E1 Z -- OK
ttyACM0<*1>: ATQ0 V1 E1 S0=0 -- OK
ttyACM0<*1>: ATQ0 V1 E1 S0=0 &C1 -- OK
ttyACM0<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 -- OK
ttyACM0<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0 -- OK
ttyACM0<*1>: Modem Identifier: ATI -- Nokia
ttyACM0<*1>: Speed 4800: AT -- OK
ttyACM0<*1>: Speed 9600: AT -- OK
ttyACM0<*1>: Speed 19200: AT -- OK
ttyACM0<*1>: Speed 38400: AT -- OK
ttyACM0<*1>: Speed 57600: AT -- OK
ttyACM0<*1>: Speed 115200: AT -- OK
ttyACM0<*1>: Speed 230400: AT -- OK
ttyACM0<*1>: Speed 460800: AT -- OK
ttyACM0<*1>: Max speed is 460800; that should be safe.
ttyACM0<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0 -- OK

Found an USB modem on /dev/ttyACM0.
Modem configuration written to /etc/wvdial.conf.
ttyACM0<Info>: Speed 460800; init "ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0"
```

The `/dev/ttyACM0` is the location of the device that wvdial should use as our modem, where in our experiment was the Nokia mobile device connected with a PC into our network. After succesfull connection the PPP protocol started the link establishment phase between both ends to determine the link quality, negotiate the size of packets that can be transmitted, and if any authentication protocol would be executed.

Then, we connected to the internet and obtained an IP address in our PC and started sending IP packets over the PPP link to the internet. The dialer defaults includes information about our modem and the Vodafone internet service provider (ISP), such as the phone number, user name, and password etc., are shown in table 13.

Table 13. wvdial configuration file.

```
[Dialer Defaults]
Init1 = ATZ
Init2 = ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0
Modem Type = Analog Modem
Baud = 9600
New PPPD = yes
Modem = /dev/ttyUSB0
ISDN = 0
 Phone = *99***1#
 Password = dummy
 Username = dummy
 Stupid Mode = 1
 Dial Command = ATDT

;[Dialer pin]

;Init1 = AT+CPIN=1234

[Dialer option]

Modem = /dev/ttyUSB0
Baud = 460800
Init2 = ATZ
Init3 = ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0
ISDN = 0
Modem Type = Analog Modem

[Dialer 2gonly]

;Init4 = AT+COPS=0,0,"Vodacom-SA",0

[Dialer 3gonly]

;Init4 = AT+COPS=0,0,"Vodacom-SA",2

[Dialer internet]
```

```
;Init5 = AT+CGDCONT=1,"IP","internet";
Init5 = AT+CGDCONT=1,"IP","internet.vodafone.gr","",0,0

[Dialer internetvpn]
;Init5 = AT+CGDCONT=1,"IP","internetvpn";

[Dialer myapn]
;Init5 = AT+CGDCONT=1,"IP","myapn"

[Dialer 384k]

Init6 = AT+CGEQMIN=1,4,64,384,64,384
Init7 = AT+CGEQREQ=1,4,64,384,64,384

[Dialer 144k]
Init6 = AT+CGEQMIN=1,4,64,144,64,144
Init7 = AT+CGEQREQ=1,4,64,144,64,144

[Dialer 64k]
Init6 = AT+CGEQMIN=1,4,64,64,64,64
Init7 = AT+CGEQREQ=1,4,64,64,64,64
```

Next, we describe more precisely some of the most important parameters of the wvdial configuration file:

- `Init1 = ATZ`: This command allows wvdial to use up to seven initialization strings to set up our modem. Before dialing, these strings are sent to the modem in numerical order and are useful when specifying multiple sections.

- `Stupid Mode = 1`: When wvdial is in Stupid Mode, it does not attempt to interpret any prompts from the terminal server. When the modem runs, the wvdial file starts the pppd daemon immediately. Apparently, there are ISP's that actually give us a login prompt, but work only if we start PPP rather than logging in.

- `Dial Command = ATDT`: The wvdial used this string to tell the modem to dial.

- `Baud = 460800`: Baud specifies the speed of the wvdial when communicated with our modem (Nokia device) and the default was 460800 baud.

8. SECURITY

8.1. Mobile-IP security

The Mobile-IP requires all registration messages between the mobile node and the home agent to be authenticated. Authentication is the process by which a sending node proves its identity to a receiving node by making use of a secret key (username, password). The secret key or encryption is used to prevent session-stealing attacks. Thus, link encryption was employed between the mobile node and the agents by using secret keys to both encrypt and decrypt the payload data which they exchange.

The secret key is provided as a hexadecimal (HEX) number string. The hexadecimal has base 16 which means that it uses sixteen distinct symbols, symbols **0–9** that represent values zero to nine, and A, B, C, D, E, F to represent values ten to fifteen. Dynamics mobile-IP supports key lengths of 16 bytes or 32 hex 'characters'. This shared secret is used with the home agent is commented out as "test" when using Authentication Association Accounting (AAA) infrastructure for key generation, shown in table 14.

Table 14. Security parameters.

SECURITY_BEGIN

SPI	Auth. alg.	Replay meth.	timestamp tolerance	max lifetime	shared secret
1000	4	1	120	600	"test"

SECURITY_END

The mobile node used MD5 (Message-Digest Algorithm) authentication method to provide secret-key authentication and integrity checking to transfer IP packets. The mobile node computes an MD5 message-digest over a sequence of bytes that includes:

- shared secret-key known between the mobile node and home agent
- the fixed length portion of the Registration Request message

The output of the MD5 computation is a 16-byte message-digest located into the Registration Request message when the mobile node connects with its home agent. Then, the home agent computes its own message digest using the shared secret-key and the fields of the received Registration Request. Then, it compares the computed message-digest with the one received from the mobile node. If they are equal then the home agent knows that the mobile node sent the Registration Request and the message was not modified in transit.

A shared secret key indexed by SPI and our home agent IP address is shown in table 15. It performs a table that maps the SPI numbers and IP address ranges defined by network addresses and netmasks. The SPI is the key identificator for the rest of the security parameters on the same line. The algorithm field specifies the method used (MD5=4) for key distribution. (Chakchai S. 2006)

Table 15. Shared Secret .

HA_SECURITY_BEGIN

SPI	HA IP	Alg.	Shared Secret
1000	143.233.222.3	4	0123456789ABCDEF

HA_SECURITY_END

The Security Parameter Index (SPI) must be defined for every mobile device and is used for indexing the security association at the home agent. Thus, the home agent needs to know what kind of security parameters each authorized mobile node uses. These security parameters are determined into an authentication extension protocol, shown in figure 22.

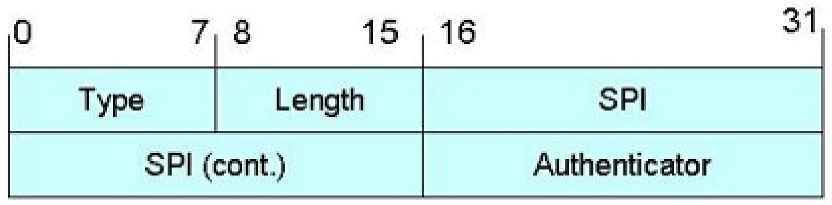


Figure 22. Authentication extension protocol. (Chakchai S. 2006)

The first 8bits refers to the type of the packet (UDP), whether the mobile node sends packets to its home network or sends packets to a foreign network. The type of a packet is also different when it is transferred from the foreign to the home network. The authenticator is a code used to authenticate the packet and the length of the packet depends on the bytes of the authenticator.

We set my-iptables-after to accept the icmp, tcp and udp protocols to operate with mobileIP protocol. The INPUT, OUTPUT and FORWARD chains refered to groups of packets that are received or destined to the fixed or mobile devices. The INPUT chain is responsible for all packets that are received by the firewall device. The OUTPUT chain is responsible for all packets leaving the firewall, and the FORWARD chain is passing packets from the INPUT to the OUTPUT chain, so basically it acts as a router. (About.com. Linux. 2011) To enable home agent to perform as a router we also set the ip_forward parameter into the iptable, in table 16. These chains includes some rules that every packet must follow in order that the packet will be transferred successfuly.

Table 16. Testbed router's firewall.

```
#*nat

#:PREROUTING ACCEPT [150:12896]

#:POSTROUTING ACCEPT [26:2088]

#:OUTPUT ACCEPT [26:2088]

#COMMIT

*mangle

:PREROUTING ACCEPT [574:76356]
```

```
:INPUT ACCEPT [426:63924]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [314:18640]

:POSTROUTING ACCEPT [314:18640]

COMMIT

*filter

:INPUT ACCEPT [426:63924]

:FORWARD ACCEPT [0:0]

:OUTPUT ACCEPT [314:18640]

:OUTBOUND - [0:0]

-A OUTPUT -o TUNLMNA -j OUTBOUND

-A OUTBOUND -p icmp -j ACCEPT

-A OUTBOUND -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT

-A OUTBOUND -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT

-A OUTBOUND -j ACCEPT

COMMIT
```

9. EXPERIMENT & RESULTS

9.1. Mobile-IP setup

The Dynamics Mobile-IP system, originally developed at Helsinki University of Technology (HUT). It is a scalable, dynamical, and hierarchical Mobile-IP software for Linux operating systems. (Sourceforge – Dynamics 2010) The Dynamics mobile ip package is partially ported for Microsoft Windows (98SE, ME, NT4, 2000) as well. The first step to setup the MobileIP test-bed was installing the dynamics package in a platform with four computer interfaces.

Once the package was installed we had to configure each computer in the network. To know how to use it we follow the steps described in the `README-CONFIGURE` file located into the package file. First, we installed the gmp library needed to build the kernel package to configure kernel options, to chose the driver options and the IEEE 802.11 settings. Then, we gave the following commands in Linux OS:

- ./configure
- make
- make install

Then we downloaded and installed the Dynamics mobile-IP. (Sourceforge – Dynamics 2010) We had to make the following changes to the mobile-IP software at mobile node machine.

- In `dynamics-0.8.1/src/mn.c` code we added the command `mn.tunnel_mode = 3` into the `find_agent` function.

- We added the `my-iptables-after` file into the file with the configuration files. The IP tables is a user space application program that allows a system administrator to set the rules of IP tables provided by the Linux kernel firewall.

- We configured a PC machine to perform as a mobile node by changing its already installed Dynamic's configuration file. The changes we made to that PC are shown in table 17.

Table 17. Our mobile node's settings.

MNHomeIPAddress	PC:143.233.222.13
HAIPAddress	143.233.222.3
HomeNetPrefix	143.233.222.192
HomeNetGateway	143.233.222.1
SPI	1000
SharedSecret	"test"
TunnelingMode	3

We located at the network 143.233.222.0 through ethernet interface and we got manually IP home address 143.233.222.13 to that network. The home IP address is visible by the mobile or fixed devices outside the network. We run the mobile-IP software through the following script (table 18):

Table 18. Script.

```
killall dynmnd

rmmod ipip

modprobe ipip

sleep 5

/usr/local/sbin/dynmnd—debug—no-wireless--config
/usr/local/etc/dynmnd.conf

sleep 20

/usr/local/sbin/dynmn_tool update

iptables-restore < /usr/local/etc/my-iptables-after

echo "preparing ha environment"

modprobe ipip

sleep 1

echo 0 >/proc/sys/net/ipv4/conf/all/rp_filter

echo 1 >/proc/sys/net/ipv4/ip_forward

echo 1 >/proc/sys/net/ipv4/conf/all/proxy_arp

echo "environment ok"
```

More precisely, in the script we set:

- `killall dynmnd`: Clear all previous operations at the mobile node's were running with the dynamic's mobile node daemon.

- `rmmod ipip`: Remove the IP-in-IP module.

- `modprobe ipip`: Set the IP-in-IP module again.

- `/usr/local/sbin/dynmnd—debug—no-wireless—config`: Run the executive file of the mobile node daemon.

- `/usr/local/etc/dynmnd.conf`: Starts the mobile node daemon.

- `/usr/local/sbin/dynmn_tool update`: Update the mobile node's executive tool.

- `iptables-restore < /usr/local/etc/my-iptables-after`: We set to the firewall the ICMP, UDP and TCP protocols to perform with the mobile-IP mechanism.

- `echo "preparing ha environment"`: Types the home agent's environment.

- `echo 1 >/proc/sys/net/ipv4/ip_forward`: Set to home agent configuration parameters to act as a router and forward IPv4 addresses.

- `echo 1 >/proc/sys/net/ipv4/conf/all/proxy_arp`: Set the Address Resolution Protocol.

- The `sleep` commands were used to give extra time to the mobile node to perform correctly without system crash.

The mobile node's tool "/usr/local/sbin/dynmn_tool" provides general information about the status of the mobile node and the home agent to ensure that both have the right settings, shown in table 19.

Table 19. Tunneling between MN and HA.

```
christof@ubuntu::/usr/local/sbin# ./dynmn_tool

Dynamics Mobile Agent Control Tool v0.8.1

Using agent path "/var/run/dynamics_mn_admin"

> status

Mobile status:

      state       Connected

      local addr  143.233.222.200

      co-addr     143.233.222.200

      FA-addr     143.233.222.3

      HA-addr     143.233.222.3

      Home addr   143.233.222.13

      tunnel is   up

      lifetime left     259s

      tunneling mode    full tunnel direct to HA

      last request      41s ago; Mon Apr 11 14:36:29 2011
      last reply  41s ago; Mon Apr 11 14:36:29 2011

      reply code  0 - registration accepted

      info text   connection established

      last warning      connected - current_adv == NULL

      active devices    3

      discarded msgs    0
```

We run the mobile node's (PC) executive tool to check the home and care-of-addresses and that the home agent was established. Then, we used the ping network utility to test if we could access the internet by using the ethernet IP home address (143.233.222.13) via the tunnel (TUNLMNA). We activated the wireless interface and made handover to an access point with IP address (143.233.222.200) and ESSID hurricane-ESS1, illustrated in table 20.

Table 20. wlan network interface activation.

```
ifconfig eth0 143.233.222.13 netmask 255.255.255.192

ping -I TUNLMNA www.nooz.gr

ifconfig wlan0 up

iwlist wlan0 scan

iwconfig wlan0 mode managed

iwconfig wlan0 essid hurricane-ESS1

dhcpcd wlan0
```

Our mobile node got the IP address 143.233.222.200 while the DHCP daemon was running. The wireless interface was set to managed in order to connect to the network provided by many access points.

While the mobile-IP protocol was running we made handover from the wimax (eth0) network to the wifi network (wlan0) `''dynmn_tool update wlan0''`, in table 21. We optionally registered the wlan interface's IP address to the home agent in case it would not be at the same network with the default gateway `(143.233.222.193)`.

Table 21. Mobile-IP handover (wimax to wifi).

```
dynmn_tool update wlan0

route add default gw 143.233.222.193

route add -host 143.233.222.3 gw 143.233.222.200 wlan0

ping -I TUNLMNA www.in.gr
```

Then, we made handover from the wifi network and to wimax (eth0) network `(143.233.222.65)` by updating the `''dynmn_tool update eth0''` tool, shown in table 22.

Table 22. Mobile-IP handover (wifi to wimax).

```
ifconfig wlan0 down
ifconfig eth0 up
dynmn_tool update eth0
route add default gw 143.233.222.65
route add -host 143.233.222.3 gw 143.233.222.65 eth0
route add default gw 143.233.222.0 dev TUNLMNA
```

We were connected to a wireless access point with network address (143.233.222.194). The home agent's address (143.233.222.3) was assigned at the mobile node's routing table. The tunnel (TUNLMNA) was established from network (143.233.222.0) to a default router (0.0.0.0.). The tunnel forwarded our IP packets to the internet via gateway (143.233.227.65), shown in table 23.

Table 23. Testbed router's routing table.

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
143.233.222.3	143.233.227.65	255.255.255.255	UGH	0	0	0	eth0
143.233.222.0	0.0.0.0	255.255.255.192	U	0	0	0	TUNLMNA
143.233.227.0	0.0.0.0	255.255.255.192	U	0	0	0	eth0
0.0.0.0	143.233.227.65	255.255.255.0	UG	0	0	0	eth0

In WiMax-WiFi handover the round trip delays for the communication between the testbed router and the mobile node were measured at approximately 4ms when the mobile used the WiFi network interface, and 35ms when the mobile switched to WiMax network interface. The results from this scenario study show that the greater part of the handover delay is due to actions that have to do with scanning of the wireless medium, dynamic network address configurations and network communication delays.

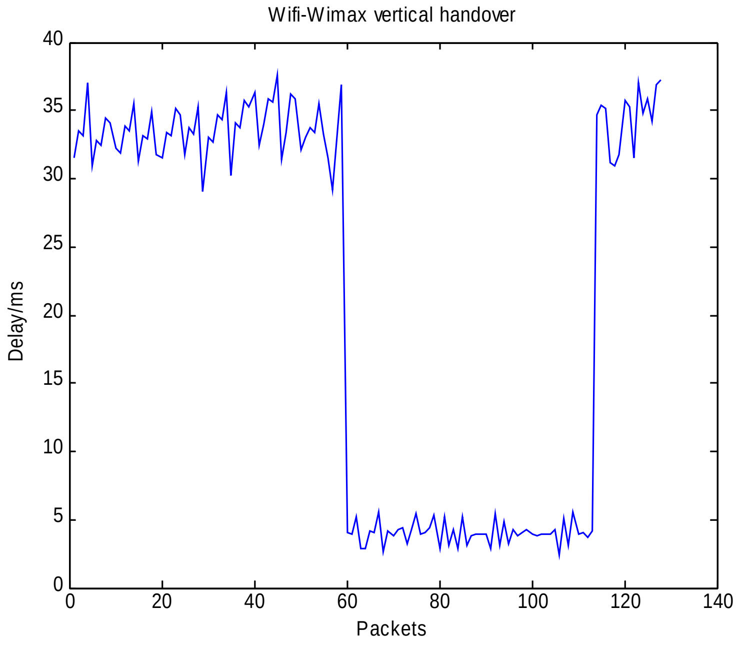
Regarding the network delay, it has impact on both the handover enable signalling and on mobility management mechanism. We chose to ping randomly from a PC located into the wifi coverage area to WiMax link to test the vertical handover. A sample of measurements of wimax-wifi vertical handover are shown, in table 24.

Table 24. Sample of measurements

```
64 bytes from 143.233.222.54: icmp_seq=6942 ttl=61 time=31.5 ms
64 bytes from 143.233.222.54: icmp_seq=6943 ttl=61 time=29.2 ms
64 bytes from 143.233.222.54: icmp_seq=6944 ttl=61 time=33.2 ms
64 bytes from 143.233.222.54: icmp_seq=6945 ttl=61 time=36.9 ms
64 bytes from 143.233.222.54: icmp_seq=6946 ttl=61 time=4.06 ms
64 bytes from 143.233.222.54: icmp_seq=6947 ttl=61 time=3.96 ms
64 bytes from 143.233.222.54: icmp_seq=6948 ttl=61 time=5.23 ms
64 bytes from 143.233.222.54: icmp_seq=6949 ttl=61 time=2.89 ms
64 bytes from 143.233.222.54: icmp_seq=6950 ttl=61 time=2.91 ms
64 bytes from 143.233.222.54: icmp_seq=6951 ttl=61 time=4.17 ms
```

We could better observe the handover delay between those technologies by using the Matlab computing language and its graph, shown in figure 23.

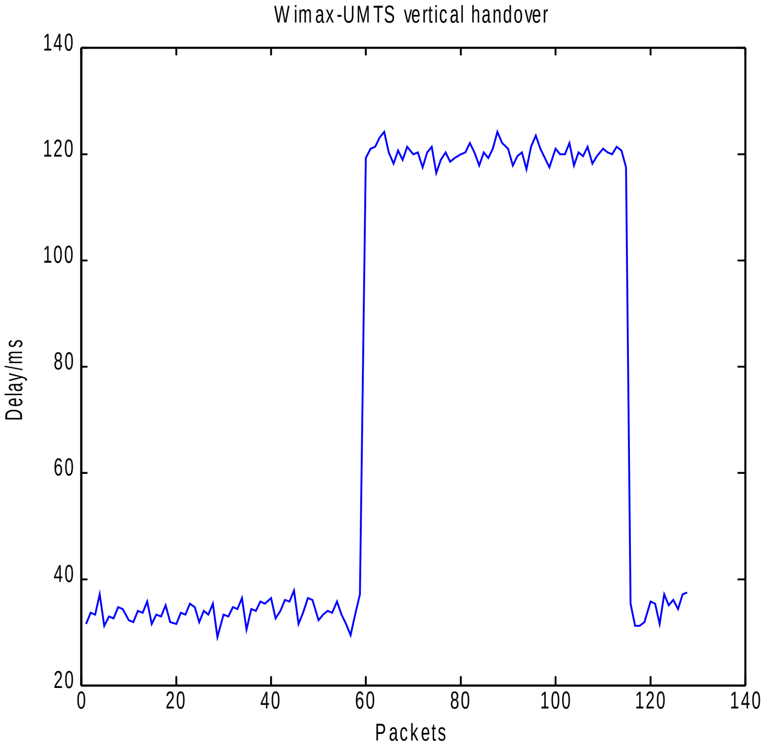
Figure 23. Wimax to Wifi vertical handover.



The figure illustrates the Mobile-IP mechanism performance. The mobile node sends IP packets (UDP-TCP) to the test-bed router for a registration request within 4ms of handover notification, while the the round trip delays to connect with the Wimax link was at approxemately 35ms.

To test the UMTS-wimax vertical handover we needed to get a connection with a telecommunication service provider, thus we chose the vodafone GR ISP. Due to the fact that the vodafone ISP allocates private network addresses and not mobile-IP, we used the Virtual Private Network (VPN). The delay over UMTS round trip times for the communication between the mobile node and the test-bed router in this case was measured approximately 120ms, shown in figure 24.

Figure 24. Wimax to UMTS vertical handover.



The main difference is that in WiMax-UMTS takes slightly more time to conclude and that UMTS-WiMax is significantly faster. These results are due to the fact that the UMTS network infrastructure introduces more communication delay than the WiMax and that the creation of a new tunnel over UMTS is slower.

The mobile-IP sends a registration request within 4ms of handover notification. The handover duration depends on the round trip delays on UMTS link. It is crucial for the decision module to anticipate the handover well in advance to mask the UMTS round trip delays. The UMTS to WLAN handover takes less than 120ms.

10. CONCLUSIONS

The telecommunication network operators must integrate their UMTS infrastructures with different infrastructure access technologies such as WiMax, WLAN etc. By performing many different networks to act as one the expensive licenses of international roaming contracts by the telecommunication network operators will be reduced. In addition, the mobile users are able to use the latest internet applications with low financial costs. The most important issue of networks integration is that the mobile users are experienced almost seamless handover when roaming.

In this paper, we introduced the mobile-IP mechanism and evaluated its performance by experiments in integrated wimax, wifi and UMTS networks. We used a centralized unit (testbed router) to experience the vertical handovers between Wimax, Wifi and UMTS infrastructures. In practise, we observed that there was no real seamless handover when we were roaming between those networks. Moreover, when our mobile node used the Wifi network the communication delay between the testbed router and our mobile node was measured at approximately 4ms. When we used the wimax network the communication delay was at approximately 35ms and when we used the 3G/UMTS network the round-trip delay was at approximately 120ms.

However, mobile-IP technology today remains a hot topic for further development by many research organizations. Researchs are focused in mobility management to achieve smoothly handover while a mobile user is roamming between different networks. A number of papers have been written on increasing the security and enhancing the overall performance of route optimization. To implement a seamless handover performance, future researches may focus to create dynamic routing algorithms and reduce as much as possible the signalism mechanisms between the different networks and make faster vertical handovers.

REFERENCES

Adnan K. (2009). Design of multihoming architecture for mobile hosts. Brunel University , School of Engineering and Design Electronic & Computer Engineering. Doctor thesis. 124-131p.

Alvarion (2011). BreezeNET® DS.11 Wireless Bridging. [Online]. Available on: <http://www.alvarion.com/index.php/en/products/productslist/breezenet/breezenetr-ds11>.

Abdullahi A., Mahadevan V. (2010). Why is IPv4 still in Existence?. Halmstad University , School of Information Science . Master's thesis. 36-45p.

About.com. Linux. (2011). Linux / Unix Command: iptables. (Referred 10.2.2011[Online]:Available<http://linux.about.com/od/commands/l/blcmdl8_iptable.htm>.

About.com.wireless/networking. (Referred 12.11.2010). [Online]: Available on:<http://compnetworking.about.com/od/basicnetworkingconcepts/l/blbasics_osi2.htm>.

Chen Y., Hsia J. & Liao Y. (2008). Advanced seamless vertical handoff architecture for WiMAX and WiFi heterogeneous networks with QoS guarantees. Science Direct, computer communications. Vol.32. 2009. Pages: 281-293.

Chakchai S. (2006). Mobile-IP Survey . 23.10.2010. [Online]. Available on:<http:// www-docs\cse574-06\ftp\mobile_ip\index.html>.

Download Ubuntu (2010). Ubuntu v10.04. (10.9.2010). [Online]. Available on: <http://www.ubuntu.com/download/ubuntu/download>.

Gomes A., et.al. (2008). Hurricane, D2.1: Handover reference scenarios, requirements specification and performance metrics. Seventh Framework Programme. no INFSO-ICT-216006 , January 2008. Pages: 43-53.

Gupta V. , Johnston D. (2004). A generalized model for Link Layer Triggers. IEEE 802.21, Intel Corporation. March 2004. Pages: 1-11.

Gondi V. (2009). Seamless Secured Roaming over Heterogeneous Wireless Networks . Université d'Evry – Val d'Essonne, Informatique. Thesis. 118-130p.

Hamza B.,et.al. (2010). Review of Minimizing a Vertical Handover in a Heterogeneous Wireless Network. Universiti Putra Malaysia , Faculty of Engineering . IETE technical review. Vol.27. ISSUE 2. Mar.-Apr. 2010. Pages: 97-104.

Jaeho J., Jinsung C. (2008). A Cross-layer Vertical Handover between Mobile WiMAX and 3G Networks. Kyung Hee University, Dept. of Computer Engineering. September 2008.

Kurur N. (2008). A secure solution for network management in heterogeneous networks. Indian Institute of technology Madras, Department of computer science and engineering. Master of Thesis. 37p.

Lampropoulos G., Salkintzis A., Passas N. (2008). Media-Independent Handover for Seamless Service Provision in Heterogeneous Networks, Mobile internet technologies and applications. IEEE Communcations Magazine. August 2008.

Lampropoulos G., et.al. (2010). Enhanced Media Independent Handover Procedure for Next Generation Networks . Future Network & MobileSummit

2010 Conference Proceedings.

Lamping U., Sharpe R. & Warnicke E. (2011). Wireshark User's Guide for Wireshark 1.5, Building and Installing Wireshark. [Online]. Available on: <http://www.wireshark.org/docs/wsug_html_chunked/index.html>

Lim W., Kim D., Suh Y., Won J. (2008). Implementation and performance study of IEEE 802.21 in integrated IEEE 802.11/802.16e networks. Science Direct, Computer Communications. Vol.32. Sempteber 2009. Pages: 134-143.

Li B.,Qin Y.,Ping C.,Gwee C. (2007). A Survey on Mobile WiMAX. IEEE communications magazine. December 2007. Pages: 70-75.

Marques H., et.al. (2008). Hurricane, D3.1: Specification of optimized handover operations for heterogeneous wireless systems. Seventh Framework Programme. no INFSO-ICT-216006, January 2008. Pages: 66-72.

Marques H., et.al. (2008). Hurricane, D3.2: Design of optimized handover operations for heterogeneous wireless systems. Seventh Framework Programme. no INFSO-ICT-216006, January 2008.

Murtaza A., Mansoor A. (2010). Decision algorithm and procedure for fast handover between 3G and WLAN. Halmstad University, School of information science. Master of Thesis. 28p.

McCann P. (2005). RFC 4260 - Mobile IPv6 Fast Handovers for 802.11 Networks. Network Working Group. Lucent Technologies. November 2005. 21.9.2010. [Online]. Available on: <http://www.faqs.org/rfcs/rfc4260.html>

Montavont N., Rouil R. & Golmie N. (2005). Effects of router configuration and link layer trigger parameters on handover performance. National Institute of Standards and Technology. IEEE 802.21. Session 10. Garden Grove, CA. September 2005.

Nikitopoulos D., et.al. (2005). Authentication platform for seamless handover in heterogeneous environments . National Technical University of Athens , School of Electrical and Computer Engineering.

NCSR - National Centre for Scientific Research "Demokritos" . Institute of Informatics and Telecommunications. [Online]. Available on: <http://www.iit.demokritos.gr/>.

Niesink L. (2007). A comparison of mobile-IP handoff mechanisms. University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science. 6th Twente Student Conference on IT , Enschede . February 2007.

Netcraftsmen-chesapeake (2008). Mobile IP Review. (Referred 2.2.2011) [Online].Available:<http://www.netcraftsmen.net/resources/archivedarticles/543.html>.

Piri E., Pentikousis K. (2009). 802.21, The internet protocol journal. Cisco.VTT Technical Research Centre of Finland. Vol.12. no.2. June 2009. [Online].
Available on:<http://www.cisco.com>.

Shaukat R. ,Cheema A. (2008). Mobile IP Based Interoperability between GSM and WiMAX. IEEE Communication Magazine. Vol.50, May 2008.

Schroder Carla (2008) Linux networking book. O'Reilly Media, USA. 500-520p.

Sarikaya B. (2006). Home agent placement and IP address management for integrating WLANs with cellular networks. IEEE Wireless communications. Huaei technologies USA. December 2006.

Solomon J. (1998). Mobile IP: The Internet Unplugged. Prentice Hall PTR, Upper Saddle River, New Jersey. p.16

Softpedia-Linux (2010). Linux distributions, Debian GNU/Linux v6.0.1. [Online]. Available on : <http:linux.softpedia.com/get/System/OperatingSystems/LinuxDistributions/Debian-GNU-Linux25655.shtml>.

Softpedia - WvDial 1.61. (2011). [Online]. Available on: <http://linux.softpedia.com/get/System/Networking/WvDial-10580.shtml>.

Sourceforge – Dynamics (2010). Mobile IP Introduction. [Online]. Available: <http://dynamics.sourceforge.net/?page=software#download>.

Taniuchi K., et.al.(2009). IEEE 802.21: Media Independent Handover: Features, Applicability, and Realization. IEEE Communications Magazine. January 2009 . Pages: 112-120.

Zivkovic M., Lagerberg K., Bemmel J. (2004). Secure Seamless Roaming over Heterogeneous Networks. Albatross, White paper. (Referred February 2011). [Online]. Available on: <http://www.ist-albatross.org/RoamingWhitePaper.pdf >