Mobile IP

State of the Art Report

Abstract

Due to roaming, a mobile device may change its network attachment each time it moves to a new link. This might cause a disruption for the Internet data packets that have to reach the mobile node. Mobile IP is a protocol, developed by the Mobile IP Internet Engineering Task Force (IETF) working group, that is able to inform the network about this change in network attachment such that the Internet data packets will be delivered in a seamless way to the new point of attachment. This document presents current developments and research activities in the Mobile IP area.

Contents

1 INTRODUCTION 6

2 TERMINOLOGY 7

2.1 Terms used in Mobile IPv4 7
2.2 Terms used in Mobile IPv6 8

3 MOBILE IPV4 10

3.1 Introduction 10
3.1.1 Discovering the Care-of Address 11
3.1.2 Registering the Care-of Address 12
3.1.3 Tunnelling to the Care-of Address 13
3.1.4 Proxy and gratuitous Address Resolution Protocol (ARP) 13
3.2 Route Optimisation in Mobile IP 14
3.3 Open issues in Mobile IPv4 14
3.3.1 Inter-domain mobility (macro-mobility) 14
3.3.2 Intra-domain mobility (micro-mobility) 15
3.3.3 Quality of Service (QoS) 15
3.3.4 Simultaneous bindings 16
3.3.5 Security 16

4 MOBILE IPV6 18

4.1 Introduction 18
4.2 Comparison with Mobile IP for IPv4 18
4.3 Open issues in Mobile IPv6 20

5 INTER-DOMAIN MOBILITY (I.E., MACRO-MOBILITY); 21

5.1 Introduction 21
5.2 3G Wireless Data Provider Architecture Using Mobile IP and AAA 21
5.3 Regional Aware Foreign Agent (RAFA) for Fast Local Handoffs 22
5.4 Mobile Internet Access and QoS Guarantees Using Mobile IP 22
5.5 Handoff enhancement in Mobile-IP Environment 25
5.6 Route Optimisation in Mobile IP 25
5.7 Mobile-IP Local registration with Hierarchical Foreign Agents 26

6 INTRA-DOMAIN MOBILITY (I.E., MICRO-MOBILITY); 28

6.1 Introduction 28
6.2 Wireless network extension using Mobile IP 28
6.3 Handoffs in Cellular Wireless Networks: The Daedalus Implementation and experience 29
6.4 Reducing Router-Crossings in a Mobile Intranet 30
6.5 Cellular IP 31
6.5.1 Cellular IP functions 32
6.6 IP micro-mobility support using HAWAII 33
6.6.1 Network Architecture 33
6.7 An architecture for QoS guarantees and routing in Wireless/Mobile Networks 35

7 QUALITY OF SERVICE 37

7.1 Introduction 37
7.2 Mobility management in IP networks providing real-time services 37
7.3 Mobile Internet Access and QoS Guarantees Using Mobile IP 38
7.4 RSVP support for Mobile IP version 6 38
7.5 An architecture for QoS guarantees and routing in Wireless/Mobile Networks 39

7.6 RSVP OPERATION OVER IP TUNNELS 41

8 SIMULTANEOUS BINDINGS; 43

8.1 INTRODUCTION 43
8.2 SPECIAL TUNNELS FOR MOBILE IP 43

9 SECURITY IN MOBILE IP 44

9.1 INTRODUCTION 44
9.2 SECURITY OF CURRENT MOBILE IP SOLUTIONS 44
9.3 REVERSE TUNNELLING FOR MOBILE IP 46
9.4 MOBILE IP EXTENSION FOR PRIVATE INTERNETS SUPPORT (MPN) 47
9.5 USE OF IPSEC IN MOBILE IP 47
9.6 REGISTRATION KEYS FOR ROUTE OPTIMISATION 47
9.7 MOBILE IP CHALLENGE/RESPONSE EXTENSIONS 48
9.8 MOBILE IP PUBLIC KEY BASED AUTHENTICATION 49
9.9 MOBILE IP NETWORK ADDRESS IDENTIFIER EXTENSION 49
9.10 NAI RESOLUTION FOR WIRELESS NETWORKS 50
9.11 DIAMETER MOBILE IP EXTENSIONS 50
9.12 FIREWALL SUPPORT FOR MOBILE IP 51

10 CONCLUSIONS 52

11 REFERENCES 54

11.1 BY ALPHABET 54
11.2 BY CATEGORY 57
11.2.1 Internet drafts 57
11.2.2 RFCs 58
11.2.3 Reports and articles 59

12 APPENDIX: PATENTS ON MOBILE IP 61

12.1 SEARCH RESULTS 61

List of Abbreviations

AAA	Authentication Authorisation and Accounting
ARP	Address Resolution Protocol
CA	Certification Authority
CH	Correspondent Host
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
FA	Foreign Agent
GRE	Generic Routing Encapsulation
GPRS	General Packet Radio Service
GW	GateWay
HA	Home Agent
HAWAII	Handoff Aware Wireless Access Internet Infrastructure
HLR	Home Location Register
HO	HandOver
HDAA	Home Domain Allocation Agency
IETF	Internet Engineering Task Force
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
IMT2000	International Mobile Telecommunications 2000
IP	Internet Protocol
IPR	Intellectual Property Rights
IPv4	IP version 4
IPv6	IP version 6
ISP	Internet Service Provider
ITU	International Telecommunication Union
MD5	Message Digest 5
MN	Mobile Node
MIP-LR	Mobile IP with Location Registers
MIPv4	Mobile IP version 4
MIPv6	Mobile IP version 6
MIPv4RO	Mobile IP version 4 with Route Optimisation
MPN	Mobile IP extension for Private Internets Support
MSA	Mobility Security Associations

NAI	Network Access Identifier
PMR	Packet to Mobility Ratio
PPP	Point to Point Protocol
QoS	Quality of Service
RAFA	Regional Aware Foreign Agent
RFC	Request For Comments
RSVP	Resource Reservation Protocol
SRE	Source Route Entry
TCP	Transport Control Protocol
TIA	Telecommunications Industry Association
TS	Translation Servers
UDP	User Datagram Protocol
VLR	Visitor Location Register
W-LAN	Wireless – Local Area Network

1 Introduction

Mobile devices can be connected to the Internet by using wireless network interfaces. However, due to roaming, a mobile device may change its network attachment each time it moves to a new link. It is therefore required that efficient protocols will be able to inform the network about this change in network attachment such that the Internet data packets will be delivered in a seamless way to the new point of attachment. Such a protocol is the mobile IP protocol, that has been developed by the Mobile IP Internet Engineering Task Force (IETF) working group [MOBIP].

This document, in general, presents current developments and research activities in the Mobile IP area. In particular, the following research topics are in more detail emphasised.

- Inter-domain mobility (i.e., macro-mobility): it defines the movement of a Mobile Node from one subnetwork, i.e., wireless subnetwork, to another subnetwork;
- Intra-domain mobility (i.e., micro-mobility): it defines the movement of a Mobile Node within a subnetwork (for example, handover from cell to cell).
- Quality of Service (QoS): capabilities that guarantee the transport of real-time data in the wireless Internet;
- Simultaneous bindings: the process of registering more than one care of addresses at the same time;
- Security in Mobile IP: the basic Mobile IP protocol [RFC2002] permits mobile internetworking to be done on the network layer; however, it also introduces new vulnerabilities to the global internet. Therefore, security procedures are required.

In this document it is assumed that the reader is familiar with the TCP/IP protocol stack, IPv6, Integrated and Differentiated services.

The organisation of this document is as follows. Sections 3 and 4 describe the current status of the Mobile IPv4 and Mobile IPv6 protocols, respectively. Sections 5, 6, 7, 8, and 9 describe the current developments and the research activities on the following research topics: Inter-domain mobility (i.e., macro-mobility), Intra-domain mobility (i.e., micro-mobility), QoS, simultaneously bindings and security, respectively. Each of these sections is organised in subsections wherein each of the research work found in the literature is described. The Appendix describes the existing IPRs (Intellectual Property Rights) on Mobile IP mechanisms.

Note that, the solutions presented in this document are not ideas of the author, but are based on an overview of existing work.

2 Terminology

2.1 Terms used in Mobile IPv4

Note that, parts of this section are copied from [RFC2002].

[.. **Agent Advertisement**: An advertisement message constructed by attaching a special Extension to a router advertisement [RFC1256] message.] ([RFC2002])

Authentication: The recipient of a message should be able to determine who the actual (real) originator of the message is.

Authorisation: Provide the ability to an organisation that owns and/or operates a network to decide who may attach to the network and what network resources may be used by the attaching node.

[.. **Binding:**The association of the home address of a Mobile Node with a care-of address for that Mobile Node, along with the remaining lifetime of that association.

Care-of Address: The termination point of a tunnel toward a Mobile Node, for datagrams forwarded to the Mobile Node while it is away from home. The protocol can use two different types of care-of address: a "Foreign Agent care-of address" is an address of a Foreign Agent with which the Mobile Node is registered, and a "co-located care-of address" is an externally obtained local address which the Mobile Node has associated with one of its own network interfaces.

Correspondent Node: A peer with which a Mobile Node is communicating. A correspondent node may be either mobile or stationary.

Foreign Agent: A router on a Mobile Node’s visited network which co-operates with the Home Agent to complete the delivery of datagrams to the Mobile Node while it is away from home.

Foreign Network: Any network other than the Mobile Node's Home Network.

Home Agent: A router on a Mobile Node's home link with which the Mobile Node has registered its current care-of address. While the Mobile Node is away from home, the Home Agent intercepts packets on the home link destined to the Mobile Node's address, encapsulates them, and tunnels them to the Mobile Node's registered care-of address, i.e., to the Foreign Agent.

Home Address: An IP address that is assigned for an extended period of time to a Mobile Node. It remains unchanged regardless of where the node is attached to the Internet.

Home Network: A network, possibly virtual, having a network prefix matching that of a Mobile Node's home address. Note that standard IP routing mechanisms will deliver datagrams destined to a Mobile Node's Home Address to the Mobile Node's Home Network.

Host: Any node that is not a router.

Interface: A node's attachment to a link

Interface identifier: A number used to identify a node's interface on a link. The interface identifier is the remaining low-order bits in the node's IP address after the subnet prefix.]

Key management: The authentication, integrity and non-repudiation can only be accurately provided (inforced) by using some form of cryptography which requires the distribution/exchange of encryption key information amongst message senders and receivers. Two methods can be used for this purpose. One method for distributing the key information is to manually load it into each node. For a small number of nodes this is possible but it runs into administrative problems. Another method to distribute the key information is dynamical, using basic IETF security protocols.

[.. **Link**: A facility or medium over which nodes can communicate at the link layer. A link underlies the network layer.

Link-Layer Address: The address used to identify an endpoint of some communication over a physical link. Typically, the Link-Layer address is an interface's Media Access Control (MAC) address.] ([RFC2002])

Location Privacy: Gives the ability to a sender of a message to control which, if any, receivers know the location of the sender’s current physical attachment to the network. Location privacy is concerned with hiding the location of an MN from CN’s.

[.. **Mobile Node**: A node that can change its point of attachment from one link to another, while still being reachable via its home address.

Mobility Agent: Either a Home Agent or a Foreign Agent.

Mobility Binding: The association of a home address with a care-of address, along with the remaining lifetime of that association.

Mobility Security Association: A collection of security contexts, between a pair of nodes, which may be applied to Mobile IP protocol messages exchanged between them. Each context indicates an authentication algorithm and mode, a secret (a shared key, or appropriate public/private key pair), and a style of replay protection in use.

Node: A host or a router.

Non-repudiation: Give the opportunity to e.g., a recipient of a message, to prove that a message has been originated by a sender. In other words, the sender of a message should not be able to falsely deny that it originated a message at a later time.

Nonce: A randomly chosen value, different from previous choices, inserted in a message to protect against replays.

Router: A node that forwards IP packets not explicitly addressed to itself.

Security Parameter Index (SPI): An index identifying a security context between a pair of nodes among the contexts available in the Mobility Security Association. SPI values 0 through 255 are reserved and MUST NOT be used in any Mobility Security Association.

Subnet prefix: A bit string that consists of some number of initial bits of an IP address.

Tunnel: The path followed by a datagram while it is encapsulated. The model is that, while it is encapsulated, a datagram is routed to a knowledgeable decapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination.

Virtual Network: A network with no physical instantiation beyond a router (with a physical network interface on another network). The router (e.g., a Home Agent) generally advertises reachability to the virtual network using conventional routing protocols.

Visited Network: A network other than a Mobile Node's Home Network, to which the Mobile Node is currently connected.

Visitor List: The list of Mobile Nodes visiting a Foreign Agent.] ([RFC2002])

2.2 Terms used in Mobile IPv6

Note that, this section is copied from [draft-ietf-mobileip-optim-08.txt].

[.. **Binding:**The association of the home address of a Mobile Node with a care-of address for that Mobile Node, along with the remaining lifetime of that association.

Care-of address: An IP address associated with a Mobile Node while visiting a foreign link; the subnet prefix of this IP address is a foreign subnet prefix. Among the multiple care-of addresses that a Mobile Node may have at a time (e.g., with different subnet prefixes), the one registered with the Mobile Node's Home Agent is called its "primary" care-of address.

Foreign subnet prefix: Any IP subnet prefix other than the Mobile Node's home subnet prefix.

Foreign link: Any link other than the Mobile Node's home link.

Home address: An IP address assigned to a Mobile Node within its home link.

Home subnet prefix: The IP subnet prefix corresponding to a Mobile Node's home address.

Home link: The link on which a Mobile Node's home subnet prefix is defined. Standard IP routing mechanisms will deliver packets destined for a Mobile Node's home address to its home link.

Home Agent: A router on a Mobile Node's home link with which the Mobile Node has registered its current care-of address. While the Mobile Node is away from home, the Home Agent intercepts packets on the home link destined to the Mobile Node's address, encapsulates them, and tunnels them to the Mobile Node's registered care-of address.

Host: Any node that is not a router.

Mobile Node: A node that can change its point of attachment from one link to another, while still being reachable via its home address.

Movement: A change in a Mobile Node's point of attachment to the Internet such that it is no longer connected to the same link as it was previously. If a Mobile Node is not currently attached to its home link, the Mobile Node is said to be "away from home".] ([draft-ietf-mobileip-optim-08.txt])

3 Mobile IPv4

3.1 Introduction

The key feature of the Mobile IP (see [RFC2002], [Per98], [Per97]) design is that all required functionalities for processing and managing mobility information are embedded in well-defined entities, the Home Agent (HA), Foreign Agent (FA), and Mobile Node (MN). The current Mobile IPv4 protocol is completely transparent to the transport and higher layers and does not require any changes to existing Internet hosts and routers.

The Mobile IP protocol allows the MNs to retain their IP address regardless of their point of attachment to the network. This can be fulfilled by allowing the MN to use two IP addresses. The first one, called home address, is static and is mainly used to identify higher layer connections, e.g., TCP. The second IP address that can be used by a MN is the Care-of Address. While the mobile is roaming among different networks, the Care-of Address changes. The reason of this is that the Care-of Address has to identify the mobile's new point of attachment with respect to the network topology. In Mobile IPv4 the Care-of Address management is achieved by an entity called Foreign Agent.

The Mobile Node, using its home address is appearing to be able to receive data on its home network, through a Home Agent. In the situation that the mobile roams into a foreign region, it will need to obtain, a new Care-of Address via the Foreign Agent. Note that, in this situation the Mobile Node can also obtain a new Care-of Address by contacting the Dynamic Host Configuration Protocol (DHCP) [RFC1541] or Point-to-Point Protocol (PPP) [RFC1661]. This new Care-of Address will be registered with its Home Agent. At the moment that the Home Agent (see Figure 3-1) receives a packet that has to be send to the mobile, it delivers it from the home network to the mobile's Care-of Address. The delivery can take place only if the packet is redirected or tunneled, such that the Care-of Address appears as the destination IP address. The Home Agent tunnels the packet to the Foreign Agent. After receiving the packet, the Foreign Agent will have to apply the reverse transformation to decapsulate it, such that the packet will appear to have the mobile's home address as the destination IP address. After decapsulation, the packet is sent to the Mobile Node. Due to the fact that the packet arrives at the Mobile Node, being addressed to its home address, it will be processed properly by the upper protocol layers, e.g., TCP. The IP packets sent by the Mobile Node, are delivered by standard IP routing procedures, each to its destination (see step 4 in Figure 3-1 (i.e., home address). When the Mobile IP packet flow, follows a route similar to the one viewed in Figure 3-1, then the routing situation is typically called triangle routing, since the packet sent by the correspondent host follows the path 1,2 and 3, while the packet sent by the Mobile Node will follow routes 3 and 4.

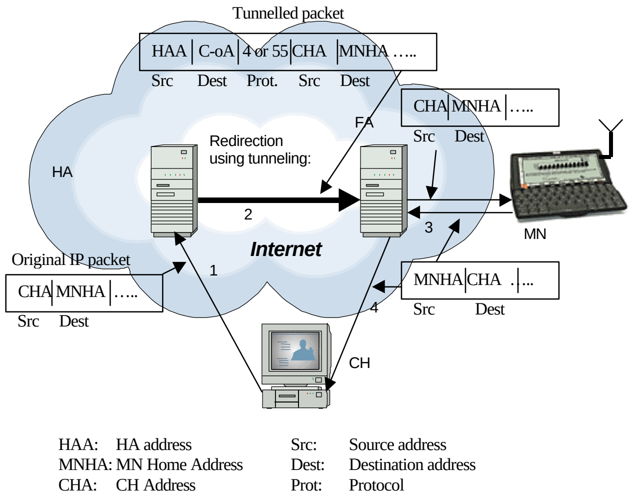

Figure 3-1: Mobile IP packet flow

The briefly explained Mobile IPv4 functionality can be realised by using three mechanisms (for a detailed description of these mechanisms see [Per98] and [Per97]):

- Discovering the Care-of Address;
- Registering the Care-of Address;
- Tunnelling to the Care-of Address;

3.1.1 Discovering the Care-of Address

The Care-of address discovery procedure used in Mobile IP is based on the ICMP (Internet Control Message Protocol) Router Advertisement standard protocol, specified in RFC 1256 [RFC1256]. In Mobile IPv4, the router advertisements are extended to also contain the required Care-of Address. These extended router advertisements are known as agent advertisements. Agent advertisements are typically broadcasted at regular intervals (e.g., once a second, or once every few seconds) and in a random fashion, by Home Agents and Foreign Agents. However, if a mobile needs to get a Care-of Address instantaneously, the Mobile Node can broadcast or multicast a solicitation that will be answered by any Foreign Agent or Home Agent that receives it.

The functions performed by an agent advertisement are the following:

- Allows the detection of Home Agents and Foreign Agents;
- Lists one (or more available) care-of addresses;
- Informs the Mobile Node about special features provided by Foreign Agents, e.g., alternative encapsulation techniques;
- Permits Mobile Nodes to determine the network number and congestion status of their link to the Internet;
- Lets the Mobile Node know, whether it is in its home network or in a foreign network by identifying whether the agent is a Home Agent, a Foreign Agent, or both.

In Mobile IP, the changes in the set of available mobility agents are detected by using ICMP router solicitations (agent solicitation) procedures defined in [RFC1256]. If the Mobile Node does not anymore receive agent solicitation advertisements from a Foreign Agent, it will presume that this Foreign Agent is not anymore within the range of its network interface.

3.1.2 Registering the Care-of Address

After the Mobile Node gets the Care-of Address it will have to inform the Home Agent about it. In Mobile IP this can be accomplished by using the registration procedure (see Figure 3-2). The Mobile Node sends a registration request (using the User Datagram Protocol (UDP)) with the Care-of Address information. This information is received by the Home Agent and normally, if the request is approved it adds the necessary information to its routing table and sends a registration reply back to the Mobile Node.

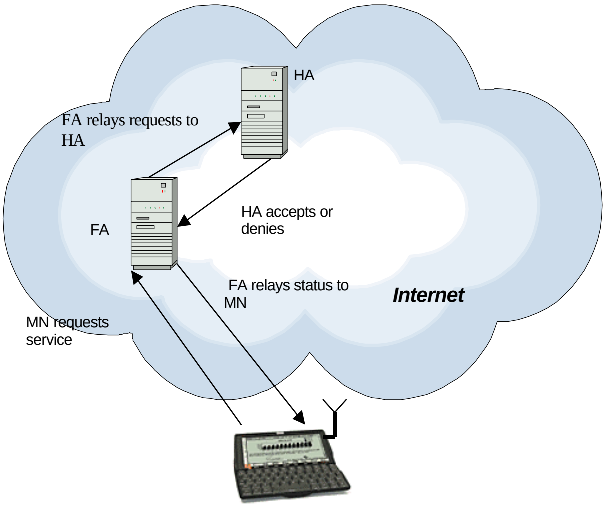

Figure 3-2: Registration in Mobile IP

The flags and parameters required to characterise the tunnel, through which the Home Agent will deliver packets to the Care-of Address, are contained in the registration request message. After accepting a registration request, the Home Agent begins to associate the home address of the Mobile Node with the Care-of Address for a pre-specified time duration, called registration lifetime. The group that contains the home address, Care-of Address, and registration lifetime is called a binding for the Mobile Node. This binding is updated by the Mobile Node at regular intervals, sending a registration request to the Home Agent.

During the registration procedure, there is a need to authenticate the registration information. The reason is that a malicious node could cause the Home Agent to alter its routing table wit erroneous Care-of Address information, and then the Mobile Node would be unreachable. Therefore, each Mobile Node and Home Agent must share a security association. During this security association it is possible to use the Message Digest 5 [RFC1321], with 128-bit keys to create unaffiliated digital signatures for registration requests.

Moreover, in the basic Mobile IPv4 protocol there are also other control message authentication methodologies, such as Secret Key, Public Key & Self-signed Certificates and Public Key & CA (Certification Authority) signed Certificates. Each of these authentication methods can use manual and/or dynamic key distribution approaches. For example, the Secret Keys may be distributed manually or dynamically, such as with the Internet Key Exchange (IKE) protocol, or DNS (Domain Name Server). Furthermore, the certificates that contain Public keys may also be distributed manually or dynamically (via e.g., X.500). For the manual key distribution approach, in order to minimise the network overhead, it is expected that the key information is distributed manually before the network deployment takes place. In contrary, the dynamic key distribution approach does not necessitate this pre-deployment key distribution phase. However this approach increases the network overhead, since these keys are established/exchanged over the network.

The computation of the signature is achieved by performing one–way hash algorithm over all data within the registration message header and the extensions that precede the signature. It is important that each request must contain unique data such that two different registrations will never have the same hash, e.g., Message Digest 5 hash. Mobile IP is assuring this by including a special identifier field within the registration message that changes with every new registration.

There are two ways to make this identification unique. One is to use a timestamp (mandatory approach); then each new registration will differ from a previous registration due to the later timestamp. The other way is to use, in the identification field (optional approach), a pseudo-random number (nonce) with enough bits of randomness.

A more detailed description of the security issues that are solved by the standard Mobile IPv4 protocol [RFC2002] is given in Section 9.2.

3.1.2.1 Automatic Home Agent discovery

In case the Mobile Node cannot contact its predefined Home Agent, it is possible that this Mobile Node will register with another unknown Home Agent on its home network. This method, called automatic Home Agent discovery, works by using a directed broadcast IP address, that reaches IP nodes on the home network, instead of the Home Agent's IP address. The IP nodes in the home network that can operate as Home Agents, will receive the directed broadcast IP packet and will send a rejection to the Mobile Node. This rejected message will among others contain the IP address of its source node. The Mobile Node will then be able to use this IP address in a new attempted registration message.

3.1.3 Tunnelling to the Care-of Address

The tunnelling to the Care-of Address is accomplished by using encapsulation mechanisms.

All mobility agents, i.e., Home Agents and Foreign Agents, using Mobile IPv4 must be able to use a default encapsulation mechanism included in the IP within IP protocol [RFC2003]. By using this protocol, the source of the tunnel, i.e., Home Agent, inserts an IP tunnel header, in front of the header of any original IP packet addressed to the Mobile Node's home address. The destination of this tunnel is the Mobile Node's Care-of Address. In IP within IP [RFC2003] there is a way to indicate that the next protocol header is again an IP header. This is accomplished by indicating in the tunnel header that the higher level protocol number is '4'. The entire original IP header is preserved as the first part of the payload of the packet. By eliminating the tunnel header the original packet can be recovered.

The tunnelling procedure can also be performed by other types of encapsulation mechanisms. These mechanisms are included in different encapsulation protocols such as the minimal encapsulation protocol [RFC2004] and the Generic Routing Encapsulation (GRE) protocol [RFC1702].

In the GRE encapsulation protocol a Source Route Entry (SRE) is provided in the tunnel header. By using the SRE, an IP source route, that includes the intermediate destinations, can be specified.

In the minimal encapsulation protocol the information from the tunnel header is combined with the information in the inner minimal encapsulation header to reconstruct the original IP header. In this manner the header overhead is reduced, but the processing of the header is slightly more complicated.

3.1.4 Proxy and gratuitous Address Resolution Protocol (ARP)

The IP nodes located in the home network of a Mobile Node are able to communicate with the Mobile Node while it is at home, by using ARP [RFC826] cache entries for this Mobile Node. When the Mobile Node moves to another subnetwork, the Home Agent will have to inform all IP nodes in the home network that the Mobile Node moved away.

This is accomplished, by sending gratuitous ARP messages. These messages will update all ARP caches of each node in the home network. After that moment the packets sent by these IP nodes, to the Mobile Node will be intercepted by the Home Agent by using proxy ARP. The intercepted packets are then tunnelled to the care of address.

3.2 Route Optimisation in Mobile IP

In [draft-ietf-mobileip-optim-08.txt] (see also [Per97] and [Per98]), the operation of the base Mobile IP protocol is extended to allow for more efficient routing procedures, such that IP packets can be routed from a correspondent host to a Mobile Node without going to the Home Agent first.

These extensions are referred to as route optimisation, wherein new methods for IP nodes, e.g., correspondent hosts, are provided. The correspondent host receives a binding update message from the mobile's node Home Agent, that contains the Mobile Node's Care-of Address. This binding is then stored by the correspondent host and is used to tunnel its own IP packets directly to the care-of address indicated in that binding, bypassing the Mobile Node's Home Agent. In this way, the triangular routing situation, explained in Section 3.1 is eliminated. However, in the initiation phase, the IP packets sent by the correspondent host still use the triangle routing until the moment that the binding update message sent by the Mobile Node's Home Agent, is received by the correspondent host.

Extensions are also provided, to allow IP packets sent by a correspondent host with an out-of-date stored binding, or in transit, to be forwarded directly to the Mobile Node's new care-of address (see Section 5.6). All operation of route optimisation that changes the routing of IP packets to the Mobile Node is authenticated using the same type of mechanisms also used in the base Mobile IP protocol. This authentication generally relies on a mobility security association established in advance between the sender and receiver of such messages.

The route optimisation protocol operates in (see also [Per97]) four steps:

- A *binding warning* control message is usually sent by a node (e.g., Mobile Node or Correspondent Host), to the Home Agent (i.e., recipient), indicating that a Correspondent Host (i.e., target) seems unaware of the Mobile Node's new Care-of Address;
- A *binding request* message is sent by a Correspondent Host to the Home Agent at the moment it determines that its binding should be refreshed;
- Typically an authenticated *binding update* message is sent by the Home Agent to all the Correspondent Hosts that need them, containing the Mobile Node's current Care-of Address;
- A *binding acknowledgement* message can be requested by a Mobile Node from a Correspondent Host that has had received the *binding update* message.

The handover procedure that can be accomplished by using the route optimisation capabilities is described in Section 5.6.

3.3 Open issues in Mobile IPv4

The Mobile IPv4 protocol can provide mobility support to portable devices that are roaming through different wireless subnetworks, but there are still several issues that have to be solved. This section gives a list with possible open issues for each of the research topics explained in Section 3.1. The discussed solutions on these issues, are presented in the sections pointed in this open issues list.

3.3.1 Inter-domain mobility (macro-mobility)

This section describes the open issues in Mobile IPv4 related to macro-mobility management.

Issue_1. *Triangle routing*: Mobile IPv4 suffers from the so called triangle routing situation (described in Section 3.1). This issue is studied in Sections 5.4, 5.6 and 5.7.

Issue_2. *Inefficient direct routing*: The routing procedure in Mobile IPv4, measured in number of hops or end to end delay, independent of the triangle routing situation, is inefficient. This issue is studied in Sections 5.2, 5.3, 5.4, 5.5, 5.6 and 5.7.

Issue_3. Inefficient Home Agent Notification: In Mobile IPv4 the Home Agent notification procedure is inefficient, since the Home Agent has to be notified during each inter-domain handover. This issue is studied in Sections 5.3, 5.5 and 5.7.

Issue_4. *Inefficient binding de-registration*: If a Mobile Node moves to another (new) Foreign Agent, then the previous Foreign Agent could release the resources used by the Mobile Node. In Mobile IPv4 this is not possible due to the fact that the previous Foreign Agent waits until a binding registration lifetime expires. This issue is studied in Sections 5.6 and 5.7.

3.3.2 Intra-domain mobility (micro-mobility)

Mobile IPv4 does not provide solutions for micro-mobility issues. However, in the near future wireless Internet, where Mobile IP will be used to integrate heterogeneous wireless subnetworks, interoperability (interworking) between macro-mobility and micro-mobility issues is quite significant. This subsection presents several micro-mobility issues that are relevant to this interoperability.

Issue_5. *Local management of micro-mobility events*: Micro-mobility events happen with relatively high frequency, therefore the handover procedures should be managed as much as possible locally. This issue is studied in Sections 6.2, 6.5, 6.6 and 6.7.

Issue_6. *Seamless intra-domain handover*: After intra-domain handover, the IP data stored into the previous entities, e.g., Base Stations (BS) should be transferred to the new BS. Similar issue have been studied in the wireless ATM area (see [MONET107]). This issue is studied in Sections 6.3 and 6.5.

Issue_7. *Mobility routing crossings in an Intranet*: During intra-domain handover the router crossings should be as much as possible avoided. This issue is studied in Section 6.4.

3.3.3 Quality of Service (QoS)

The Mobile IPv4 protocol does not specify usable features or capabilities for the provision of QoS. It is expected that the future wireless Internet networks, will provide services that require QoS guarantees, e.g., voice. Therefore, Mobile IP should be able to assist QoS algorithms or mechanisms. The relevant open issues are the following:

Issue_8. *Efficient Mobile IP aware reservation mechanisms*: Definition of reservation mechanisms that can be used to assist the QoS support. This issue is studied in Section 7.5.

Issue_9. *RSVP operation over IP tunnels*: Due to the tunnelling operation the Mobile IPv4 cannot inter-operate with the Resource Reservation Protocol (RSVP). For a detail description of the RSVP protocol see [Whi97] and [Bra96]. Routers will not be able to recognise a PATH message encapsulated while tunnelled from the Home Agent to the Mobile Node, and thus will not record the information required for reservations to be effected by the resource reservation message. This issue is studied in Sections 7.2, 7.3, 7.4 and 7.6.

Issue_10. *RSVP reservations on Mobile IP triangle route situations*: Due to the triangle route operation the Mobile IPv4 cannot inter-operate with the Resource Reservation Protocol (RSVP). The resources will only be reserved along the triangle route from the Correspondent Host to the Mobile Node. This is due to the fact that the PATH and RESV messages follow different paths and therefore operating differently than the normal RSVP operation. Therefore, the QoS guarantees desired, may not be achieved since packets sent along the triangle route receive different treatment than those sent directly. This issue is studied in Section 7.2 and 7.3.

3.3.4 Simultaneous bindings

In Mobile IPv4 it is possible that a Host registers more than one Care-of Addresses at the same time. In this way the host can register different Care-of Addresses that for example, are identifying two neighbouring subnetworks. By sending the same information to both Care-of Addresses the inter-domain handover delays can be reduced.

Issue_11. *Inefficient maintenance of simultaneous bindings*: A possible problem related to the maintenance of bindings in general, occurs when a binding indicate Care-of Addresses that are no longer valid. This occurs because of either transient or longer term effects. A Foreign Agent may receive packets tunnelled to a Mobile Node that is no longer registered with that Foreign Agent and therefore, no additional forwarding information is available. In this situation, the base Mobile IP protocol indicates that the tunnelled IP packets should be dropped. This will have negative consequences on the higher layer associations. Dropping such packets often necessitates retransmissions by higher level protocols, and such retransmissions cause significant performance degradation. This issue is studied in Section 8.2.

3.3.5 Security

Mobility introduces among others the need for enhanced security. In this section, the open issues on security are emphasised. The authentication, authorisation, non-repudiation, key management and location privacy (for terminology see Section 2.1) supported by Mobile IPv4 are explained in Section 9.2. The security open issues that are related to Mobile IPv4 are listed below. Note that these open issues are eventually solved in different contexts, but are not integrated with Mobile IPv4.

Issue_12. *Ingress filtering*: In an ISP any border router, may discard packets that contain a source IP address, that is not being configured for one of the ISP's internal network. This issue is called ingress filtering. In Mobile IPv4 the Mobile Nodes that are away from home, i.e., in a foreign ISP use their home address as the source IP address, that is different than the IP addresses configured in the ISP's internal network. This issue is studied in Sections 9.3 and 9.4.

Issue_13. *Minimise the number of required trusted entities*: Security may be enhanced, if the number of the required trusted entities, i.e., Home Agent, Foreign Agent, in a Mobile IP scenario is decreased.

Issue_14. *Authentication*: The recipient of a message should be able to determine who the actual (real) originator of the message is. Therefore authentication procedures between mobile agents and Mobile Nodes should be provided. The Mobile IPv4 authentication techniques between Mobile Nodes and Foreign Agents are not reliable enough. This issue is studied in Sections 9.2, 9.5, 9.6, 9.7, 9.8, 9.9 and 9.11.

Issue_15. *Authorisation*: An organisation that owns and/or operates a network, would need to decide who may attach to this network and what network resources may be used by the attaching node. This issue is called authorisation and is studied in Sections 9.2, 9.6, 9.7, 9.9 and 9.11.

Issue_16. *Non-repudiation*: In the future wireless Internet, a recipient of a message should have the opportunity, to prove that a message has been originated by a sender. In other words, the sender of a message should not be able to falsely deny that it originated a message at a later time. This issue is called non-repudiation and is studied in Section 9.2.

Issue_17. *Encryption key distribution*: The authentication, integrity and non-repudiation can only be accurately provided (inforced) by using some form of cryptography which requires the distribution/exchange of encryption key information amongst message senders and receivers. In other words key management procedures should be supported by Mobile IP. Two methods can be used for this purpose. One method for distributing the key information is to manually load it into each node. For a small number of nodes this is possible but it runs into administrative problems. Another method to distribute the key information is dynamical, using basic IETF security protocols. This issue is studied in Sections 9.2 and 9.8.

Issue_18. *Location privacy*: A sender of a message should able to to control which, if any, receivers know the location of the sender's current physical attachment to the network. Location privacy is concerned with hiding the location of a Mobile Node from Correspondent Hosts. This issue is studied in Section 9.2.

Issue_19. *Use one single subscription for all service types*: In RFC 2468 [RFC2468] the Network Access Identifier (NAI) is defined, it is used to identify ISP subscribers during roaming operations. Regarding second and third generation cellular networks, an interesting approach for cellular service providers would be to evolve their home cellular networks to provide second and third generation cellular services, IP packet data services and so on with a single subscription using NAIs. Mobile IPv4 does not provide solutions to this issue. This issue is discussed in Section 9.10.

Issue_20. *Firewall support in Mobile IP*: If a Mobile Node has to enter a private Internet network (i.e., Intranet) that is securely protected by a firewall, then Mobile IP aware support at this firewall is required. In Mobile IP this support is not provided. This issue is discussed in Section 9.12.

4 Mobile IPv6

4.1 Introduction

In [draft-ietf-mobileip-ipv6-07.txt] the operation of mobile computers using the Internet Protocol Version 6 (IPv6) [draft-ietf-ipngwg-ipv6-spec-v2-00.txt] is described.

IETF (Internet Engineering Task Force) expects that the IPv6 protocol will replace the IPv4 protocol in the near future. As mobile computers will probably account for a substantial fraction of the Internet population (during the lifetime of IPv6), it is particularly important to provide mobility support in IPv6. The protocol operation defined in [draft-ietf-mobileip-ipv6-07.txt], known as Mobile IPv6, provides this mobility support.

4.2 Comparison with Mobile IP for IPv4

The Mobile IPv6 uses the experiences gained from the design and development of Mobile IPv4 ([RFC2003], [RFC2002], [RFC2004]) together with the new IPv6 protocol features (see [draft-ietf-ipngwg-ipv6-spec-v2-00.txt]). Mobile IPv6 shares many features with Mobile IPv4, but the protocol is now fully integrated into IPv6 and provides many improvements over Mobile IPv4. The major differences between Mobile IPv4 and Mobile IPv6 are:

- Support for "Route Optimisation" [draft-ietf-mobileip-optim-08.txt] (see Issue_1 (*Triangle routing*) described in Section 3.3.1) This feature is now built in as a fundamental part of the Mobile IPv6 protocol. In Mobile Ipv4 the route optimisation feature is being added on as an optional set of extensions that may not be supported by all IP nodes.

- In Mobile IPv6 (also integrated in the IPv6) a new feature is specified that allows Mobile Nodes and Mobile IP to coexist efficiently with routers that perform "ingress filtering" [RFC2267] (see Issue_12 (*Ingress filtering*) described in Section 3.3.5). The packets sent by a Mobile Node can pass normally through ingress filtering (see Section 3.3) routers. This can be accomplished due to the fact that the care-of address is used as the Source Address in each packet’s IP header. Moreover, the Mobile Node’s home address is carried in the packet in a Home Address destination option. This allows the use of the care-of address in the packet to be transparent above the IP layer, e.g., TCP.

- By using the care-of address as the Source Address in each packet's IP header the routing of multicast packets sent by a Mobile Node is simplified. In Mobile IPv6 the Mobile Node will not anymore have to tunnel multicast packets, as specified in Mobile IPv4, to its Home Agent (see Issue_9 (*RSVP operation over IP tunnels*) described in Section 3.3.3). Moreover, the use of the Home Address option allows the home address to be used but still be compatible with multicast routing that is based in part, on the packet's Source Address.

- In Mobile IPv6 the functionality of the Foreign Agents can be accomplished by IPv6 enhanced features, such as Neighbour Discovery [draft-ietf-ipng-discovery-v2-00.txt], [RFC1970] and Address Autoconfiguration [draft-ietf-ipngwg-addrconf-v2-00.txt], [RFC1971]. Therefore, there is no need to deploy Foreign Agents in Mobile IPv6. This feature can provide a solution to issue_7 Issue_7 (*Mobility routing crossings in an Intranet)*, Issue_11 (*Inefficient maintenance of simultaneous bindings)* and Issue_13 (*Minimise the number of required trusted entities*) described in Section 3.3.5.

- The Mobile IPv6, unlike Mobile IPv4, uses IPsec [draft-ietf-ipsec-auth-header-02.txt], [draft-ietf-ipsec-esp-v2-01.txt], [draft-ietf-ipsec-arch-sec-02.txt] for all security requirements (see Issue_14 (*Authentication*) described in Section 3.3.5) such as sender authentication, data integrity protection, and replay protection for Binding Updates (which serve the role of both registration and Route Optimisation in Mobile IPv4). In Mobile IPv4 the security requirements are provided by its own security mechanisms for each function, based on statically configured mobility security associations.

- In mobile IPv6 a mechanism is provided to support bidirectional (i.e., packets that the router sends are reaching the Mobile Node, and packets that the Mobile Node sends are reaching the router) confirmation of a Mobile Node's ability to communicate with its default router in its current location (see Issue_12 (*Ingress filtering*) described in Section 3.3.5). This bidirectional confirmation can be used to detect the “black hole” situation, where the link to the router does not work equally well in both directions. In contrast, Mobile IPv4 does not support bidirectional confirmation, but only the forward direction (packets from the router are reaching the Mobile Node) is confirmed, and therefore the black hole situation may not be detected.

- Mobile IPv6 and IPv6 use the source routing feature. This feature makes it possible for a Correspondent Host to send packets to a Mobile Node while it is away from its home network using an IPv6 Routing header rather than IP encapsulation, whereas Mobile IPv4 must use encapsulation for all packets. In this way Issue_9 (*RSVP operation over IP tunnels*) and Issue_12 (*Ingress filtering*) described in Section 3.3.3 are partially solved. However, in Mobile IPv6 the Home Agents are allowed to use encapsulation for tunnelling. This is required, during the initiation phase of the binding update procedure (see Section 3.2).

- In Mobile IPv6 the packets which arrive at the home network and are destined for a Mobile Node that is away from home, are intercepted by the Mobile Node’s Home Agent using IPv6 Neighbour Discovery [draft-ietf-ipng-discovery-v2-00.txt], [RFC1970] rather than ARP [RFC826] (see Section 3.1.4) as is used in Mobile IPv4.

- The source routing (routing header) feature in Mobile IPv6 removes the need to manage "tunnel soft state", which was required in Mobile IPv4 due to limitations in ICMP error procedure for IPv4. In Mobile IPv4 an ICMP error message that is created due to a failure of delivering an IP packet to the Care-of Address, will be returned to the home network, but will may not contain the IP address of the original source of the tunnelled IP packet. This is solved in the Home Agent by storing the tunnelling information, i.e., which IP packets have been tunnelled to which Care-of Address, called tunnelling soft state.

- In IPv6 a new routing procedure is defined called anycast. This feature is used in Mobile IPv6 for the dynamic Home Agent address discovery mechanism. This mechanism returns one single reply to the Mobile Node, rather than the corresponding Mobile IPv4 mechanism (see Section 3.1.2.1) that used IPv4 directed broadcast and returned a separate reply from each Home Agent on the Mobile Node's home subnetwork. The Mobile IPv6 mechanism is more efficient and more reliable. This is due to the fact that only one packet need to be replied to the Mobile Node.

- In Mobile IPv6 an Advertisement Interval option on Router Advertisements (equivalent to Agent Advertisements in Mobile IPv4) is defined, that allows a Mobile Node to decide for itself how many Router Advertisements (Agent Advertisements) it is tolerating to miss before declaring its current router unreachable.

- All Mobile Ipv6 control traffic can be piggybacked on any existing IPv6 packets. This can be accomplished by using the IPv6 destination options. In contrary, for Mobile IPv4 and its Route Optimisation extensions, separate UDP packets were required for each control message.

4.3 Open issues in Mobile IPv6

In comparison to Mobile IPv4 protocol, Mobile IPv6 protocol can provide mobility support that combines the experience gained in the design of Mobile IPv4 and the new features of the IPv6 protocol. Some of the Mobile IPv4 open issues , i.e., (see Section 3.3) Issue_1 (*Triangle routing)*, Issue_7 (*Mobility routing crossings in an Intranet)*, Issue_9 (*RSVP operation over IP tunnels*), Issue_11 (*Inefficient maintenance of simultaneous bindings*), Issue_12 (*Ingress filtering)*, Issue_13 (*Minimise the number of required trusted entities)* and issue_14 (*Authentication*) are partially solved (see Section 4.2). Note that, Section 9.2 lists the security solutions provided by the Mobile IPv6 protocol. Most of the solutions provided in Sections 5 to 9, are mainly generated for Mobile IPv4. However, it is expected that some of these solutions, after some minor modifications, can also be applied for Mobile IPv6. These are:

- Issue_1 (*Triangle routing*) and Issue_2 (*Inefficient direct routing*) described in Sections 5.4 and 5.6;
- Issue_5 (*Local management of micro-mobility events)* discussed in Sections 6.5 and 6.7;
- Issue_6 (*Seamless intra-domain handover*) discussed in Sections 6.3 and 6.5;
- Issue_8 (*Efficient Mobile IP aware reservation mechanisms*) discussed in Section 7.5;
- Issue_9 (*RSVP operation over IP tunnels*) discussed in Sections 7.3 and 7.4;
- Issue_10 (*RSVP reservations on Mobile IP triangle route situations*) discussed in Section 7.3;
- Issue_19 (*Use one single subscription for all service types*) discussed in Section 9.10;
- Issue_20 (*Firewall support in Mobile IP*) discussed in Section 9.12.

5 Inter-domain mobility (i.e., macro-mobility);

5.1 Introduction

The inter-domain mobility or macro mobility defines the movement of a Mobile Node from one (wireless) subnetwork to another subnetwork. The basic Mobile-IP protocol [RFC2002] provides a scalable mechanism for node mobility within the Internet. However, there are open issues (see Section 3.3) that have to be solved. The following subsections provide solutions to these open issues:

5.2 3G Wireless Data Provider Architecture Using Mobile IP and AAA

In [draft-hiller-3gwireless-00.txt] a third generation wireless architecture that is using Mobile IPv4 to solve macro-mobility issues is specified. In particular, solutions are provided to Issue_2 (*Inefficient direct routing)* described in Section 3.3.1. However, this specification is described on a high level of abstraction, along with a set of more detailed requirements. This architecture is consistent with the requirements set by the International Telecommunications Union (ITU) for International Mobile Telecommunications 2000 (IMT-2000) systems, since it has been developed by the Telecommunications Industry Association (TIA) Standards Subcommittee TR45.6. The IMT-2000 systems will be able to provide among others, multimedia services and good quality speech services.

This architecture can, in general, be applied to interoperate between public and private networks and is designed for use with a traditional cellular network, e.g., W-LAN, GPRS, as an access medium. In particular, this architecture can assist the roaming of Mobile Nodes between different types of networks, i.e., public and private, provided by different ISP's (Internet Service Providers). Hence, a combination of Mobile IP (see Figure 5-1) and the Authentication, Authorisation and Accounting (AAA) concept is applied in order to provide the required security and accounting for its mobile users. An important handover feature supported by this architecture, is the dynamically assignment of Home Agents by a Foreign Agent (see Figure 5-1). This feature will enable the Mobile Node that roamed to a foreign ISP network to gain service with its local service provider, while avoiding unnecessarily long routing.

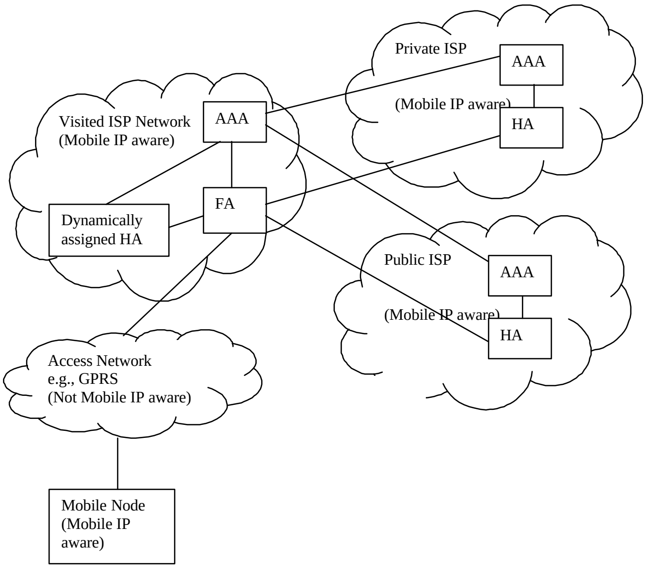

Figure 5-1: General Wireless IP architecture for service providers

5.3 Regional Aware Foreign Agent (RAFA) for Fast Local Handoffs

In [draft-chuafoo-mobileip-rafa-00.txt] an extension to the MOBILE IPv4 [MIPv4] scheme is provided, to solve Issue_2 (*Inefficient direct routing*) and Issue_3 (*Inefficient Home Agent Notification*) described in Section 3.3.1.

The network topology used to provide this solution is viewed in Figure 5-2. The main inter-domain handover feature, provided in [draft-chuafoo-mobileip-rafa-00.txt], is related to the registration process that is required during a handover procedure, accomplished between two foreign networks, i.e., FA's. By using the Regional Aware Foreign Agent (RAFA), the latency (delay) of this process is reduced, since the Mobile Node during handover will have now to register with the local RAFA node, instead with its Home Agent. Note that the Home Agent might be located far away.

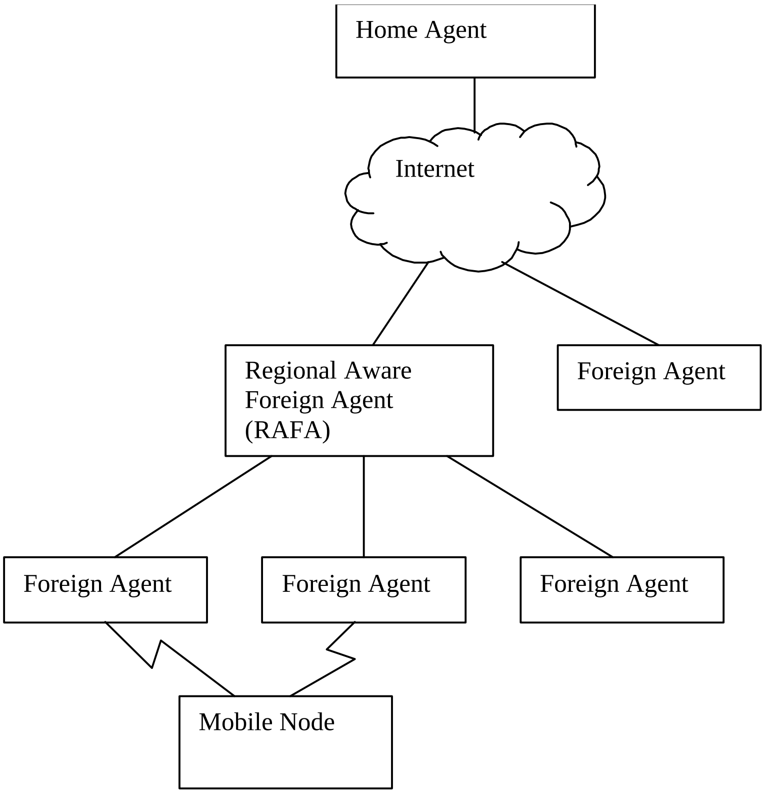

Figure 5-2: Network topology

5.4 Mobile Internet Access and QoS Guarantees Using Mobile IP

In [JaRa98] the Mobile IP with Location Registers (MIP-LR) is described that is providing improvements to the Mobile IPv4 inter-domain handover issues, Issue_1 (*Triangle routing)* and Issue_2 (*Inefficient direct routing*) described in Section 3.3.1. These improvements are mainly specified for Mobile IPv4, but it is expected that through minor modifications they can also be applied for Mobile IPv6.

Compared to the Mobile IPv4, the MIP-LR is closer to the “service node” database approach used in wireless cellular networks. The sender before sending a packet to the Mobile Node is first quering a database to obtain the recipient’s current location. MIP-LR can operate within enterprise environments or within logical administrative domains. The sending host must be aware of which hosts are potentially mobile and implement the MIP-LR protocol. The main benefits of MIP-LR are that the “triangle routes” (see Section 3.1) are avoided. Moreover, the encapsulation of packets sent to a Mobile Node is not required since Mobile Nodes and Correspondent Hosts are able to directly associate home addresses with Care-of Addresses. Furthermore, the load on the home network as well as on the home and Foreign Agents is reduced, and there is substantially improved interoperability with protocols such as RSVP for providing QoS guarantees.

MIP-LR, in general, uses a set of location registers, i.e., Visitor Location Registers (VLR) and Home Location Registers (HLR), as databases to maintain the Care-of Addresses. In particular, each subnetwork contains a VLR (Visitor Location Register), and a HLR (Home Location Register).

Each Mobile Node is served by a single HLR located in its Home Network. Similar to the Agent Advertisements messages for Mobile IPv4, each VLR and HLR advertises its presence on its local subnetwork using periodic broadcasts.

In the situation that a Mobile Node is located at its local subnetwork it is not registered at either the HLR or VLR, and originates and receives packets using normal IP routing. When the Mobile Node roams to a Foreign Network it obtains a Care-of Address. This can be done either by:

- A pool of IP addresses are owned by each VLR. The VLR can assign these IP addresses, to the visiting Mobile Nodes as Care-of Addresses and broadcasts the currently available list of Care-of Addresses periodically;
- The Care-of Address is obtained from a local DHCP [RFC1541] server.

In the foreign network the Mobile Node, via the foreign network’s VLR, chooses and registers its Care-of Address. The VLR relays this registration to the Mobile Nodes’s HLR. Similarly to Mobile IPv4, a registration reply is returned by the HLR that contains the allowed lifetime for this registration. The VLR that receives this reply, records the Mobile Nodes’s Care-of Address and its lifetime and forwards this reply back to the Mobile Node.

When a Correspondent Host is wishing to send a packet to the Mobile Node for the first time it must first discover the IP address of the Mobile Node’s HLR. There are two possible approaches to achieve this:

- *Trap query at home subnet*. Similarly to the Mobile IPv4, the Correspondent Host uses the Mobile Node’s permanent IP home address to issue this query. In the situation that, the Mobile Node is away from home and has registered to a foreign network, i.e., VLR, the query will be detected (trapped) by the HLR. The HLR will then send a reply to the Correspondent Host containing the Mobile Node’s Care-of Address.
- *Database lookup*: New database entities are introduced, called Translation Servers (TS). They are able to store the mapping from a host’s IP home address to the IP address of the HLR which serves that host. Due to the fact that the provided information does not change frequently, a Correspondent Host can cache the response for relatively long periods of time. Note that the address(es) of the TS must be fixed and well known to all hosts.

The first approach is simpler, since it is similar to the procedure followed in Mobile IPv4. However, the second approach is more efficient and it can provide better survivability and load balancing, by allowing the TS to contain a list of HLR addresses, and introducing appropriate protocols.

The Correspondent Host after finding the IP address of the HLR, issues a query to it. The HLR returns the Mobile Node's Care-of Address as well as the remaining registration lifetime. After receiving the Care-of Address, the Correspondent Host sends the IP packet to the Mobile Node's Care-of Address. Thus, the mapping from the Mobile Node's IP address to its Care-of Address is accomplished at the IP layer at the Correspondent Host. This mapping is therefore hidden from higher layer protocols (e.g., TCP) to maintain the higher layer associations, even when the Mobile Node is roaming. The IP layer at the Mobile Node does the same for the reverse mapping. The obtained Mobile Node's Care-of Address and its binding are cached by the Correspondent Host and used for subsequent packets destined to the Mobile Node. The binding cache is refreshed by the Correspondent Host, by quering the HLR before the Mobile Node's remaining registration lifetime expires. Note that contrary to Mobile IPv4, in MIP-LR the Correspondent Hosts have be aware of host mobility.

After a Mobile Node roams from a VLR to a new VLR, the new VLR has to deregister the Mobile Node at the old VLR, such that the previous reserved Care-of Address will be available for eventual reuse. If the old VLR does not manage Care-of Addresses then the new VLR has to eventually inform the local DHCP server that the Care-of Addresses can be deallocated.

After the movement of a Mobile Node, the cache at the Correspondent Host has to be updated. Two approaches can be used to accomplish this functionality:

- *Lazy caching*: after roaming, the Mobile Node informs (via the new VLR) the old VLR about it. The old VLR detects any IP packets destined to the old Care-of Address and sends a binding warning to the HLR. After receiving the binding warning message, the HLR sends a binding update message to the Correspondent Host, which contains the Mobile Node's new Care-of Address;
- *Eager caching*: a Mobile Node keeps track of all Correspondent Hosts it has connections with. This information is cached by the Mobile Node and is used during roaming, issueing a binding update to each cached host.

In this research work also a simplified average-case analysis of the costs and benefits of MIP-LR in comparison with the Mobile IPv4 "without route optimisation" and Mobile IPv4 "with the route optimisation" option included has been accomplished. The key performance measures used in this analysis are:

- Packet to Mobility Ratio (PMR): which is the number of packets received by a mobile from a Correspondent Host per movement. This number will differ per applied macro-mobility scheme, due to the varying number of sent and received control messages.
- Triangle to Direct-distance ratio (TDR), which is the ratio of the distance, i.e., number of hops, along the triangle route to the distance via the direct route.

From this analysis it can be concluded that:

MIP-LR provides performance improvements since the triangle routing (also during the initial phase of the binding procedure that is used in the route optimisation feature, see Section 3.2) and the encapsulation of packets are avoided.

Similar to Mobile IPv4 with route optimisation, MIP-LR requires Correspondent Hosts to be aware of host mobility, which Mobile IPv4 does not. However, MIP-LR avoids packet encapsulation and is able to interoperate with RSVP. Due to the fact that the packet encapsulation is avoided, the load on Foreign Agents and Home Agents is reduced. Moreover, the triangle routing issue is avoided.

5.5 Handoff enhancement in Mobile-IP Environment

In [WoLe96] a mechanism is proposed to solve the Mobile IPv4 inter-domain handover issues, Issue_2 (*Inefficient direct routing)* and Issue_3 (*Inefficient Home Agent Notification)* described in Section 3.3.1. This mechanism is an enhanced extension to the route optimisation method described in [draft-ietf-mobileip-optim-08.txt], that delivers enhanced performance at all handover rates. The inter-domain handover delay and the loss of IP packets during handover are minimised. This is accomplished by storing the incoming IP packets at the previous Foreign Agent, until the moment a new Care-of Address assigned for the roaming Mobile Node is authenticated. After that moment, the IP packets are forwarded to the new Foreign Agent.

In order to analyse and compare the performance of this mechanism, simulation experiments were accomplished. These experiments were performed for different macro-mobility schemes, i.e., the basic Mobile IP [MIPv4], the basic route optimisation method [draft-ietf-mobileip-optim-08.txt] and the new handover mechanism, described in [WoLe96]. The used performance measure is the TCP end-to-end delay. From the simulation results it can be concluded that the handover enhanced scheme (described in [WoLe96]) compared to the other two schemes, achieves the best performance under all handover rates. Furthermore, a better performance is also achieved by this scheme under increased handover registration delays.

5.6 Route Optimisation in Mobile IP

In [draft-ietf-mobileip-optim-08.txt] (see also [Per97]) a smooth Mobile IPv4 inter-domain handover procedure is described. This procedure is providing solutions to Issue_1 (*Triangle routing)*, Issue2 (*Inefficient direct routing*) and Issue_4 (*Inefficient binding de-registration)* listed in Section 3.3.1. It is expected that the solutions provided to Issue_1 (*Triangle routing)* and Issue2 (*Inefficient direct routing*) through minor modifications can also be applied for Mobile IPv6. The route optimisation mechanism has already been discussed in Section 3.2. Regarding the inter-domain handover, a mechanism is provided to enhance the handover performance. The Mobile Node' previous Foreign Agent can be reliably notified of the Mobile Node's new mobility binding. This will allow to re-direct the IP packets that arrived in transit to the Mobile Node's previous Foreign Agent, to its new Care-of Address. The same procedure can be followed, in case the sending Correspondent Host has out-of-date binding cache entries for this Mobile Node. Finally, this notification allows the previous Foreign Agent to release immediately any of its resources consumed by the Mobile Node, rather than waiting for its binding registration lifetime to expire.

Figure 5-3 views the smooth handover procedure. Essentially, after roaming to a new point of attachement, the Mobile Node instructs its new Foreign Agent to send a binding update to its previous Foreign Agent.

If the previous Foreign Agent has no fresh binding for the Mobile Node, special tunnels (i.e., treated differently then normal tunnels) (see [draft-ietf-mobileip-spectun-00.txt]) are used, which indicate to the Home Agent the need for special handling. Since the Mobile Node's cache binding is expired, the previous Foreign Agent, will not be able to find the home address in the decapsulated packet and therefore, will not be able to send an IP packet back to the Home Agent. Instead of doing that, the Foreign Agent encapsulates the IP packet to be sent to the Home Agent, using the Foreign Agent's Care-of Address as the source IP address. The Home Agent, after receiving this packet compares the source IP address with the Care-of Address known in the binding created from the last registration. In case, these addresses match, the Home Agent will not tunnel the IP packet back to the Care-of Address. If these addresses do not match, then the decapsulated IP packet is re-tunneled and send to the current Care-of Address known from the registration.

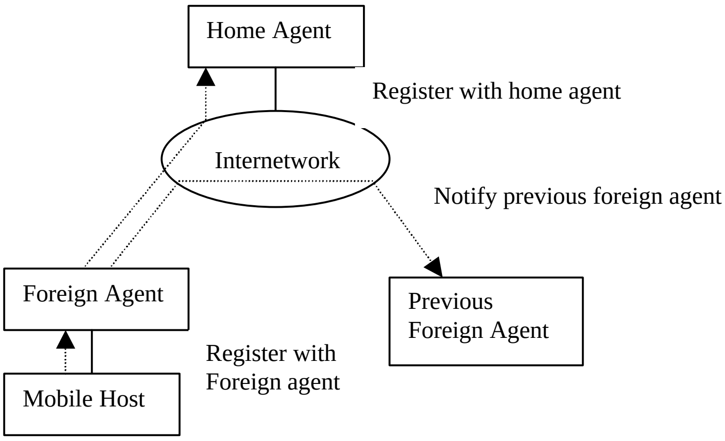

Figure 5-3: Smooth handover during registration

5.7 Mobile-IP Local registration with Hierarchical Foreign Agents

In [draft-perkins-mobileip-hierfa-00.txt] (see also [Per97]) an Mobile IPv4 inter-domain handover mechanism is described, using a hierarchy of Foreign Agents (see Figure 5-4). This mechanism is solving Issue_1 (*Triangle routing)* and Issue2 (*Inefficient direct routing)* described in Section 3.3.1. In this mechanism, during the Care-of Address discovery procedure (see Section 3.1.1) multiple Foreign Agents are advertised using the agent advertisement message. The Care-of Address registration will be provided for the Foreign Agent that is the lowest common Foreign Agent ancestor at the two points of attachment of interest. For example, in Figure 5-4, where the Mobile Node moves from FA4 to FA6 the lowest common FA ancestor for the two points of attachment, i.e., FA4 and FA6 is the FA1 node. This registration procedure can be accomplished only if the Mobile Node will be able to find out how high up the tree its registration can go. The Mobile Node will have then to transmit specialised registrations to each level of hierarchy between itself and the closest common node between its previous and new Foreign Agents. In Figure 5-4, this is accomplished by the Mobile Node that sends registration messages to FA1. By using this technique, different hop by hop tunnels are created from the FA6 to the home agent, i.e., HA to FA1 & FA1 to FA3 & FA3 to FA6. In other words, the Home Agent considers that the Mobile Node is located at Care-of Address FA1, while the Foreign Agent FA1 considers that the Mobile Node is located at FA3. Foreign Agent FA3 considers that the Mobile Node is located at FA6. Finally, FA6 actually knows the real location of the Mobile Node.

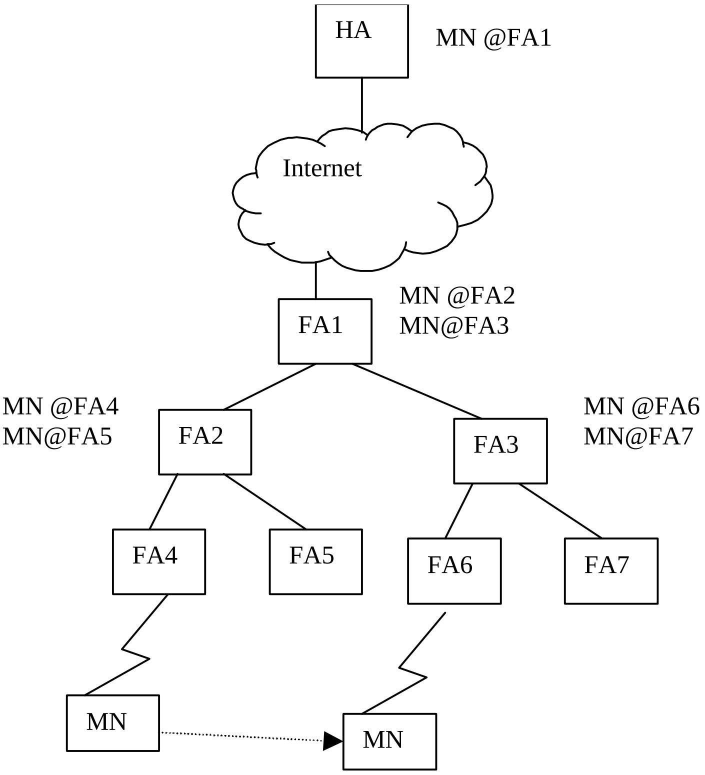

Figure 5-4: Hierarchical Foreign Agents

6 Intra-domain mobility (i.e., micro-mobility);

6.1 Introduction

The Mobile IP protocol [RFC2002] is mainly solving the macro mobility management problem. In the basic Mobile IP protocol it is considered that the (intra-domain) micro-mobility (i.e., movement of a Mobile Node within a subnetwork) management issue is solved by the link layer mobility management mechanisms of the current wireless technologies. However, there are research activities that investigate the possibility of enhancing the Mobile IP functionality to support micro-mobility.

6.2 Wireless network extension using Mobile IP

In [GeSo97] a micro-mobility management scheme in combination with Mobile IP is introduced. Using this scheme, solutions are provided to Issue_5 (*Local management of micro-mobility events)*, described in Section 3.3.2. This scheme is developed in the Motorola iDEN architecture see Figure 6-1. Due to the fact that the micro-mobility events can happen with relatively high frequency, they should be managed more efficiently than macro-mobility events. This can be accomplished by keeping the procedures and participants as local as possible. Therefore, in this system the micro-mobility procedures are managed by a data gateway. The Mobile IPv4, implemented in the Foreign Agent and Home Agent of Figure 6-1, is the technology chosen for macro-mobility between iDEN subnetworks and other subnetworks.

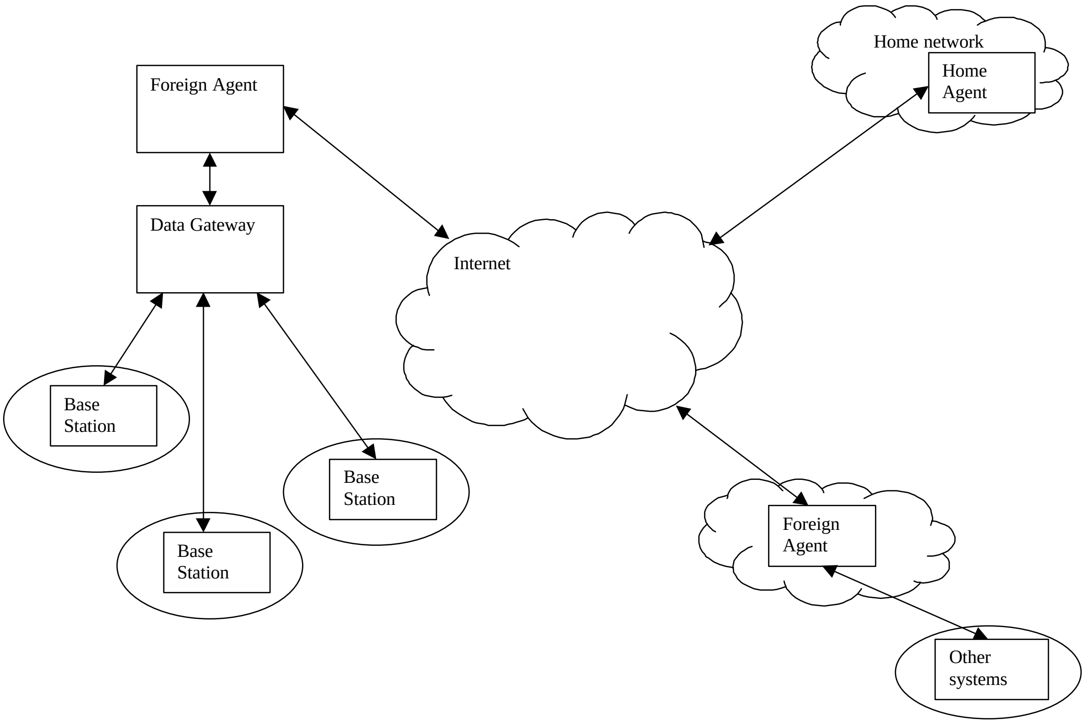

Figure 6-1: iDEN system architecture

6.3 Handoffs in Cellular Wireless Networks: The Daedalus Implementation and experience

In [SeBa97] a multicast-based Mobile IPv4 intra-handover algorithm is described that eliminates data loss and achieves negligible delays. This algorithm provides solutions to Issue_6 (*Seamless intra-domain handover)*, described in Section 3.3.2. It is expected that after some minor modifications, this algorithm could be used for Mobile IPv6. By using wireless network information in the form of received signal strengths, the nearby stations in the vicinity of the Mobile Node, can be identified. The IP data packets destined (i.e., sent) to the Mobile Node will then be multicasted to these nearby stations in advance. This multicast routing, combined with intelligent buffering techniques at the base stations, enables very rapid routing updates and eliminates data loss without the use of explicit data forwarding. However, note that the multicasting procedure will probably increase the load on the wireless sub-network.

This algorithm has been implemented and tested in the Daedalus project at Berkeley. The testbed is based on PC (i486 and Pentium) base stations and IBM ThinkPad Mobile Nodes communicating over a 2Mbit/s AT&T WaveLAN. In this implementation extra handover delays typically take between 8 and 15 ms to complete and result in no data loss.

This algorithm can be used in combination with Mobile IPv4 and is active during the procedure in which the Home Agent forwards a packet to the Mobile Node’s current Care-of Address.

In addition to the home address, the Mobile Node is also assigned a temporary IP multicast address. When a Home Agent receives IP packets that are destined (i.e., sent) for the Mobile Node, it encapsulates and forwards them to its associated multicast group (see Figure 6-2). The base stations in the vicinity of the Mobile Node are members of this multicast group and not the Mobile Node itself. The current location of the Mobile Node is determined in the following way. Periodically, each Base Station (BS) broadcasts a beacon message to all Mobile Nodes in its range. Each Mobile Node approximates its current location and motion by keeping track of the recent received beacons. By using statistics, such as the received signal strength of the beacons and communication quality, the Mobile Node is able to identify which BSs are nearby, and which wireless network cell it should join. Moreover, these statistics can also be used to estimate to which cells the Mobile Node will handover in the near future. Based on this information, the Mobile Node configures the IP multicast routing between the Home Agent and the various BSs. The BS that provides connectivity to the cell containing the Mobile Node joins the IP multicast group. Each packet, transmitted from the Home Agent is forwarded by the primary BS to the Mobile Node. At any instant in time, there is at most one primary BS in the system for a given Mobile Node. Moreover, the BSs that are identified, as likely handover targets are requested by the Mobile Node to join the multicast group. These BSs do not forward the packets from the multicast group to the wireless network, but they buffer the last few packets transmitted from the HA. Typically, handovers are to cells whose BSs have primed for a Mobile Node in this manner. At the moment a Mobile Node enters such a cell, the Mobile Node starts transmitting a set of control messages to the various BSs. These control messages will request from each BS either to begin or end forwarding and buffering of packets. The previous BS will still send packets to the Mobile Node. A list of the last packets that were received by the Mobile Node is included in the control messages that activate the forwarding on the new primary BS. This list informs the new BS about the packets that were already received by the Mobile Node.

The new primary BS begins transmitting packets (that were not yet transmitted by the previous BS) to the Mobile Node, from its stored packets in the buffer. The IP packets in transit, sent by the Correspondent Host are delivered directly to the Mobile Node, via the new BS, without having them forwarded from the previous BS. Therefore, this handover mechanism is seamless and it has minimal data loss during handover. Furthermore, it incurs no additional delays due to data transfer.

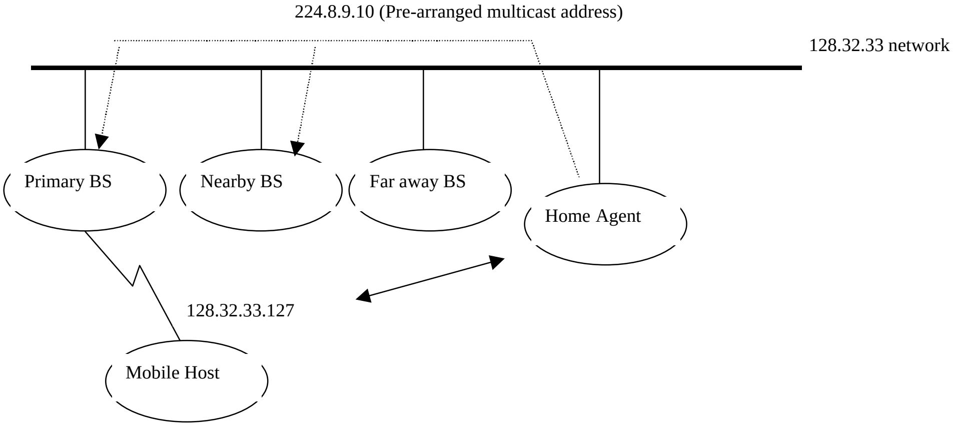

Figure 6-2: Home Agent to Mobile Node routing

6.4 Reducing Router-Crossings in a Mobile Intranet

In [KoDu98] a mechanism is presented that eliminates multiple router crossings (see Figure 6-3) in a mobile intranet by making the routers Mobile IPv4 aware, i.e., the routers can be used as Home Agents, Foreign Agents or both. By using this mechanism, a solution to Issue_7 (*Mobility routing crossings in an Intranet)*, described in Section 3.3.2 is provided. This reduces the load on the routers and minimises the handover and data delay (latency) at the Mobile Nodes.

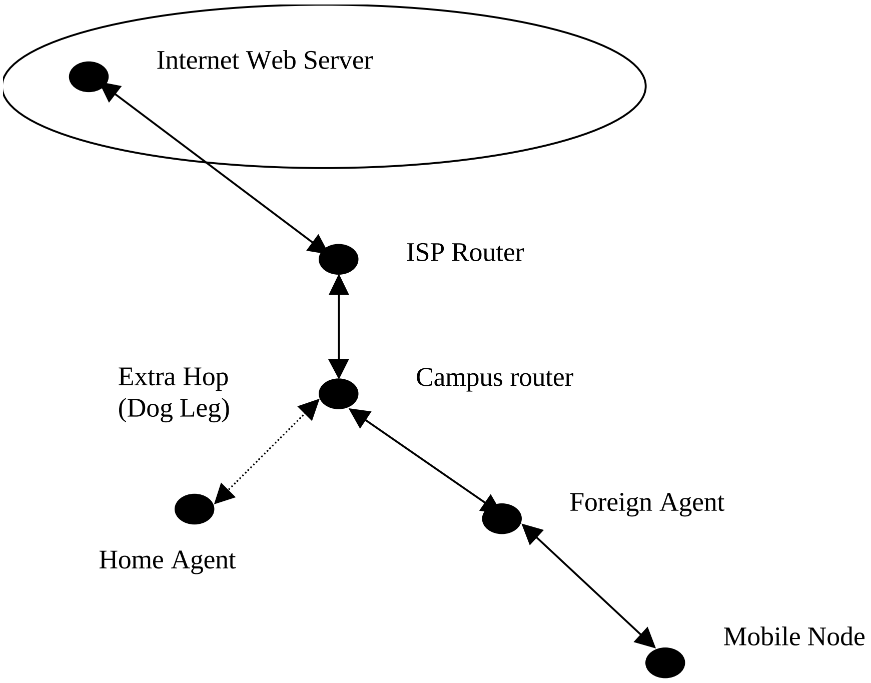

Figure 6-3: Multiple router crossings

It is very likely that the movement of Mobile Nodes in a campus or building environment, is restricted to subnetworks of a single group of routers under the control of one administrative authority. By co-locating the Home and Foreign Agents of all the subnets of a router, into a single entity, i.e., the crossing campus router (see Figure 6-3), then the stack traversals on Home Agents and Foreign Agents and the duplicate router-crossings on the campus router, are eliminated. This mechanism can be extended to multiple routers under one administrative domain (see Figure 6-4).

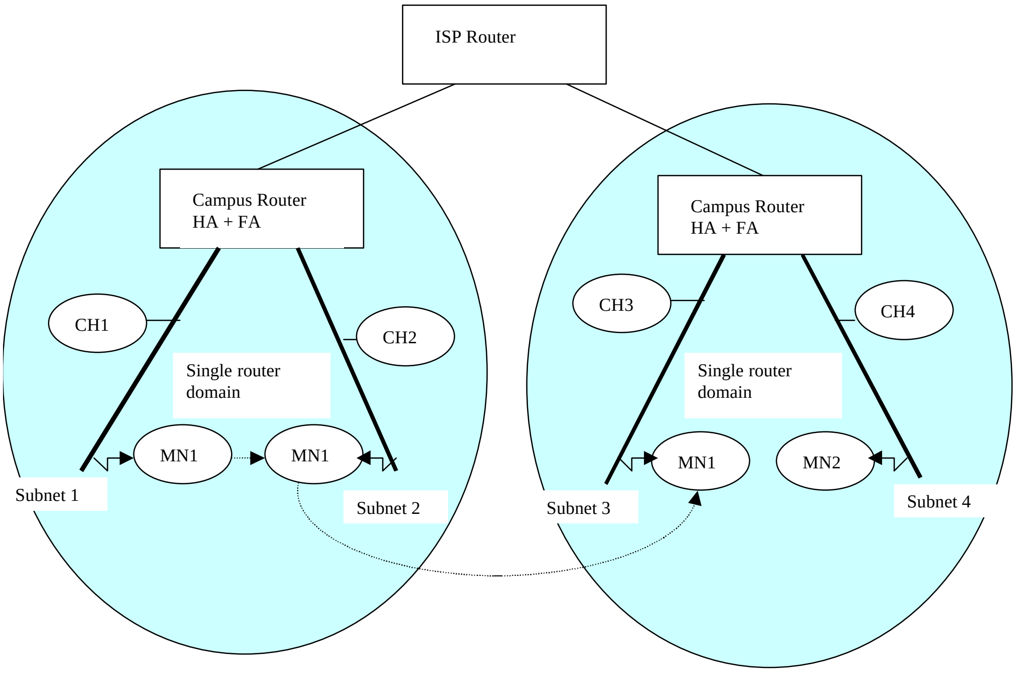

Figure 6-4: The intranet architecture

One single router domain (one campus router connecting two subnets, (see Figure 6-4) has been implemented, where the campus router is an Intel pentium machine running the 4.4 BSD IP forwarding code. The MN is an Intel 486 with an IP address on the single router domain. CH1 and CH2 are Correspondent Hosts connected on two different subnets. All hosts run BSD/OS 2.1 and are connected via 10Mbs ethernet.

This new mechanism has been compared with the basic Mobile IPv4 scheme. In this comparison the end-to-end IP packet delay is used as performance measure. The improvements achieved by the new mechanism were related to end-to-end delay drops from 12 miliseconds to 5 miliseconds for packets of 1024 bytes size.

6.5 Cellular IP

In [draft-vallko-cellularip-00.txt] a protocol is specified that provides mobility and handover support for frequently moving hosts. This protocol is called Cellular IP and is intended to be applied on a local level, e.g., in a campus or metropolitan area network. Cellular IP can interwork with Mobile IP to support wide area mobility, that is, mobility between Cellular IP Networks. By using this protocol, solutions to Issue_5 (*Local management of micro-mobility events*) and Issue_6 (*Seamless intra-domain handover*) described in Section 3.3.2 are provided. It is expected that the solutions provided to Issue_5 (*Local management of micro-mobility events*) and Issue_6 (*Seamless intra-domain handover*) through minor modifications can also be applied for Mobile IPv6.

In Figure 6-5 a schematic view of multiple Cellular IP networks that have access to the Mobile IP enabled Internet, is depicted. Periodically, each Base Station (BS) transmits beacon signals. These signals provide statistical information related to signal strength, that can be used by Mobile Nodes to locate the nearest BS. All IP packets transmitted by a Mobile Node (see Figure 6-5) are routed from the BS to the GW (gateway) by hop-by-hop shortest path routing, regardless of the destination address.

The nodes used in the Cellular IP network are called Cellular IP nodes. These nodes can route IP packets inside the Cellular IP Network and communicate with Mobile Nodes via wireless interface. Referring to the latter role, a Cellular IP Node that has a wireless interface is also called a Base Station.

The Cellular IP nodes maintain two caches, the routing and paging caches. The routing caches are used to locate an active Mobile Node that is roaming in the wireless network and it sends and receives IP packets relatively frequently. For the location of idle Mobile Nodes, that do not send or receive packets frequently, paging caches are used.

The routing caches at each node are created and updated by the packets that are transmitted by the Mobile Node. There is also an algorithm specified to map the Mobile Node's IP address to the interface through which the packet entered the node. In this way, a chain of cached mappings, referring to a single Mobile Node will be created. This chain of cached mappings will be used as a reverse path to downlink IP packets from the gateway to the Mobile Node. Any time the Mobile Node roams through different cells, the chain of cached mappings always points to its current location. This can be accomplished, since its uplink packets create new chain mappings and the old chain mappings are automatically cleared after a time out. After a successful roaming procedure, a node can temporarily have mappings for the same Mobile Node to multiple interfaces. A Mobile Node can prevent cached mappings from time out by sending periodically control packets, i.e., regular IP packets with empty payloads.

A Mobile Node can also maintain paging cache mappings. The paging caches are maintained by Paging-update packets. These packets are sent to the nearest Base Stations each time the Mobile Node moves. In this manner, the Paging Caches will be forced to point at its up-to-date location. These mappings are created by Mobile Nodes that are not actively transmitting or receiving data, but want to be reachable for incoming packets. IP packets addressed to these Mobile Nodes will be routed by paging caches. This is accomplished in a similar way as to routing caches, where the chain of cached mappings will be used as a reverse path to downlink IP packets from the gateway to the Mobile Node. Note that, the paging caches have a longer timeout value than Routing Caches and are not necessarily maintained at each node.

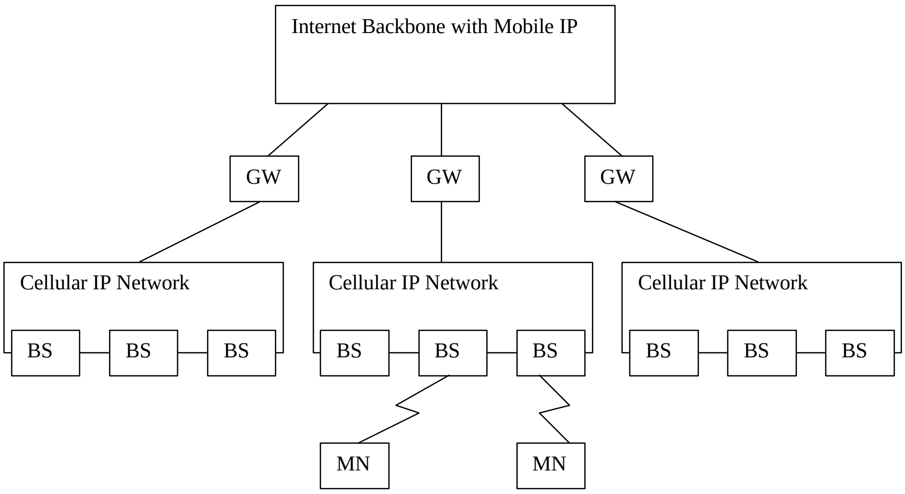

Figure 6-5: Multiple Cellular IP networks

6.5.1 Cellular IP functions

Location Management

Paging-update packets, are periodically transmitted by idle Mobile Nodes to keep Paging Cache mappings up-to-date. However, these Paging-update packets do not update Routing Cache mappings. These packets after reaching the gateway are discarded, to isolate Cellular IP specific operations from the Internet. When the Mobile Node moves, it sends its Paging-update packets to the nearest Base Station. In this way, the Paging Caches will be forced to point at its up-to-date location. After a system specific time, i.e., paging time-out, the outdated mappings are cleared. All packets that arrive at a Cellular IP node and are addressed to a Mobile Node for which no up-to-date Routing Cache mapping is available, the Paging Cache mapping is used to route these packets.

Routing

As mentioned earlier, packets that are transmitted by Mobile Nodes are routed to the Gateway using regular hop-by-hop routing. Each Cellular IP node that lies in the path of these packets, will monitor and use them to create and update Routing Cache mappings. After these Routing Cached chain mapping paths are created, they can be used to route the packets addressed to the Mobile Node along the reverse path, on a hop-by-hop basis. The structure and basic operation of routing is the same as that of location management.

Intra-domain handover

The handover in the Cellular IP network is initiated by the Mobile Node, and is accomplished in the following way. When the MN moves and approaches a new BS, it redirects its packets from the old to the new BS. However, the Routing Caches along the way from the new BS to the GW have to be reconfigured. This action is accomplished by the first packets, that are redirected from the old to the new BS. All packets addressed to the MN, for a time equal to the time out of the Routing Cache mappings, will be routed to both the old and new BSs. The Routing Cache mappings associated with the old BS will be automatically cleared at the moment the timeout elapses. The new BS will continue to receive the packets that are addressed to the MN. In order to minimise the downlink packet loss, the Route Cache mappings have to be created quickly. Therefore, when the MN has no data packets to send at the time of handover, it has to generate and transmit a Route-update packet immediately after moving to the new BS.

6.6 IP micro-mobility support using HAWAII

In [draft-ramjee-micro-mobility-hawaii-00.txt] a Mobile IPv4 intra-domain handover approach called Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) is presented. This approach provides solutions to Issue_5 (*Local management of micro-mobility events)*, described in Section 3.3.2. In this approach, host based forwarding entries are installed in specific routers to support intra-domain micro-mobility. The installation of these entries is accomplished using specialised path setup schemes. In general, by using these entries the performance is enhanced. This is due to the reduction of the mobility related disruptions to user applications and due to the reduction of the number of mobility related updates. Furthermore, in HAWAII, Mobile Nodes retain their network address while moving within the domain (subnetwork), simplifying Quality of Service support. By using the soft-state forwarding entries for Mobile Nodes, and by eliminating Foreign Agents and, in some cases, the Home Agent, better network reliability is achieved.

6.6.1 Network Architecture

The HAWAII network architecture (see Figure 6-6) is divided into hierarchies based on domains. Each domain has a gateway, called the domain root router, and each host has an IP address and a home domain.

In the situation that the Mobile Node moves within its home domain, its IP address is retained. The packets that are destined (i.e., sent) to the Mobile Node, can reach the domain root router based on the subnetwork address of the domain. The received packets are then forwarded to the Mobile Node by using special dynamically established paths.

Three different path setup schemes can be used to dynamically establish the paths followed by the IP packets from gateway to Mobile Node. In each of these schemes, the path setup update messages are sent to the gateway by the Mobile Node, to create entries (used during the reverse path) in the intermediate nodes they pass. The first setup scheme is active during power up. The other two setup schemes are active during handover. One of these is called the forwarding setup scheme and the other one is called the non-forwarding setup scheme. In the forwarding scheme, the Mobile Node can only receive/transmit from/to one Base Station at a time, e.g., Time Division Multiple Access technology, while in the non-Forwarding scheme the Mobile Node is able to receive/transmit from/to two or more Base Stations at a time, e.g., Code Division Multiple Access technology. For more details see [draft-ramjee-micro-mobility-hawaii-00.txt].

Using this approach the home domain will be able to cover a large area, made of hundreds of base stations, thereby increasing the probability that a Mobile Node is within its home domain. In the situation that the Mobile Node is roaming within its home domain, the Home Agent will not be involved in the data path. This will improve the reliability and it will enhance the routing efficiency.

In the situation that the Mobile Node moves into a foreign domain, the traditional Mobile IP mechanisms are used. The Mobile Node gets a co-located Care-of Address from a foreign domain based on HAWAII. The packets arriving at the home domain and that are destined to a Mobile Node that is away from home, are tunnelled by the Mobile Node’s Home Agent to the Care-of Address. When the Mobile Node moves within the foreign domain, it retains its Care-of Address. Due to this fact the Home Agent will not have to be notified of these movements.

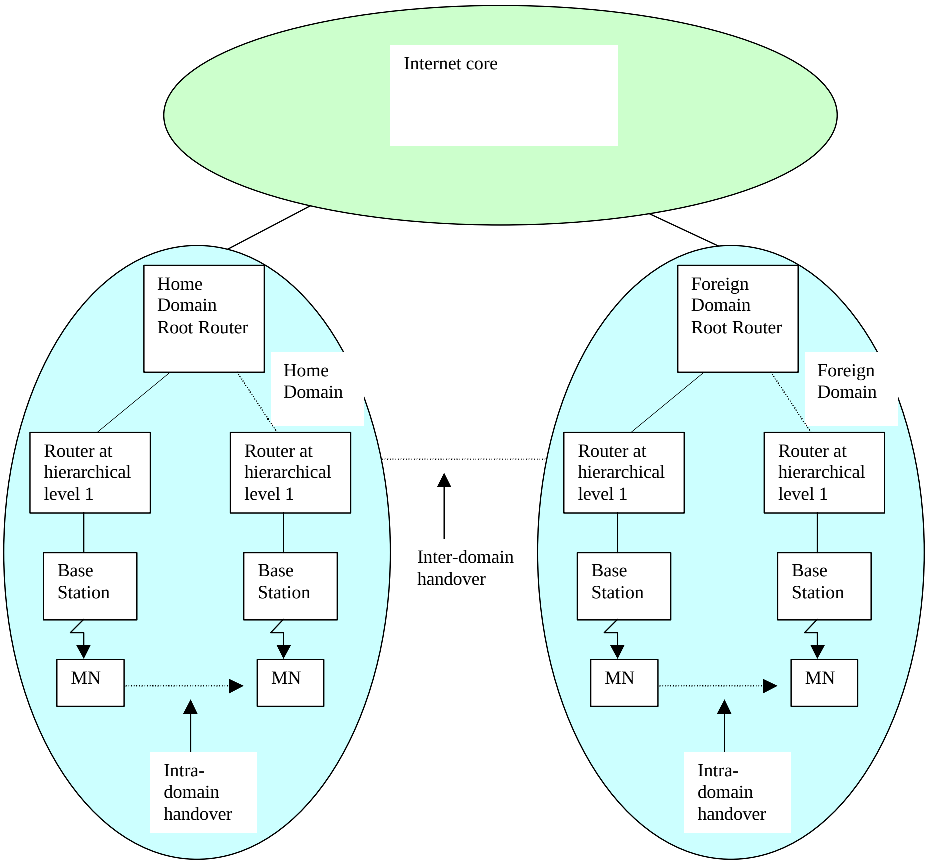

Figure 6-6: HAWAII Network Architecture

6.7 An architecture for QoS guarantees and routing in Wireless/Mobile Networks

In [MaSi98] an architecture is proposed that provides QoS support in mobile/wireless networks (see also Section 7.5) along with support for fast routing during Mobile IPv4 intra-domain handovers. This approach provides solutions to Issue_5 (*Local management of micro-mobility events)*, described in Section 3.3.2. It is expected that the solutions provided to Issue_5 (*Local management of micro-mobility events)*, through minor modifications can also be applied for Mobile IPv6. The specified and implemented architecture is hierarchical (see e.g., Figure 6-6) and is based on the concept of QoS domains and routing domains. A routing domain is the region wherein the route changes are accomplished by using local route tables, without invoking Mobile IP inter-handover functionality. A QoS domain is the region wherein the mobility resource reservations are accomplished by extending the path of the original resource reservations, without requiring partial re-routing.

Regarding the intra-domain handovers, a method is presented to overcome the delay issues involved with Mobile IPv4. If a mobile is roaming within a routing (home or foreign) domain then the Mobile Node will not have to communicate with its HA. However, due to roaming in the same routing domain, the Mobile Node may change the wireless connectivity from an old to a new BS. This change in wireless connectivity is supported by the routing domain, that itself updates the routing tables with the new location of the mobile. Note that the location of the Mobile Node is stored in the routing tables of the hosts, located within the routing domain.

The mechanism of changing routing tables in a routing domain is done as follows:

- All base stations in a routing domain, register with the routing-domain router;

- The current location of the Mobile Node is known by the routing-domain router;
- If a Mobile Node moves into another cell, then the base station that manages this new cell informs the routing-domain router about the location of the Mobile Node;
- This information is broadcasted by the routing-domain router to all systems in the routing domain. All hosts in the routing domain use this information when they want to communicate with the mobile.

In the situation that the Mobile Node roams between two different domains then the typical Mobile IP mechanisms are used.

The intra-domain handover scenarios presented in Sections 6.5, 6.6 and 6.7 have similarities and differences. The similarities are related to the achieved result, they are all solving Issue_5 (*Local management of micro-mobility events*). The differences among these scenarios are related to the mechanism used to route the packets within a local (home or foreign) domain. Cellular IP, described in Section 6.5, is using a mechanism that creates and maintains routing and paging caches, to route the packets within a local routing domain. HAWAII, described in Section 6.6, is using path setup schemes to dynamically establish the paths followed by the IP packets from the gateway to the Mobile Node. The mechanism described in Section 6.7, is using routing tables to route the packets within a local routing domain.

7 Quality of Service

7.1 Introduction

Efforts are underway to enhance the wireless Internet with Quality of Service (QoS) capabilities for transporting real-time data. The QoS capabilities required in future wireless and mobile communications can only be guaranteed if a form of resource reservation procedure is defined, that can be applied as a Mobile Node moves between wireless regions.

The found research work related to QoS, the concept of Integrated Services (see [Whi97] for more details) is applied.

7.2 Mobility management in IP networks providing real-time services

In [AnBl96] an RSVP extension is proposed to solve the Mobile IPv4 issues, Issue_9 (*RSVP operation over IP tunnels)* and Issue_10 (*RSVP reservations on Mobile IP triangle route situations)*, described in Section 3.3.3, allowing real-time communications setups between mobile and fixed hosts in TCP/IP networks. In this work, the mobility support in RSVP is achieved by providing transparent and efficient setup of a reserved data path between all kind of hosts. This is accomplished by giving the opportunity to the Home Agent to send an early notification to the sender. The current position of a Mobile Node, is included in this notifiction. This method implies that a new message (PathChange) and a new object class (MOBILITY_NOTIFICATION) has to be added to the RSVP.

The used algorithm can be summarised as follows (see . Note that in this algorithm it is assumed that the Correspondent Host is fixed.

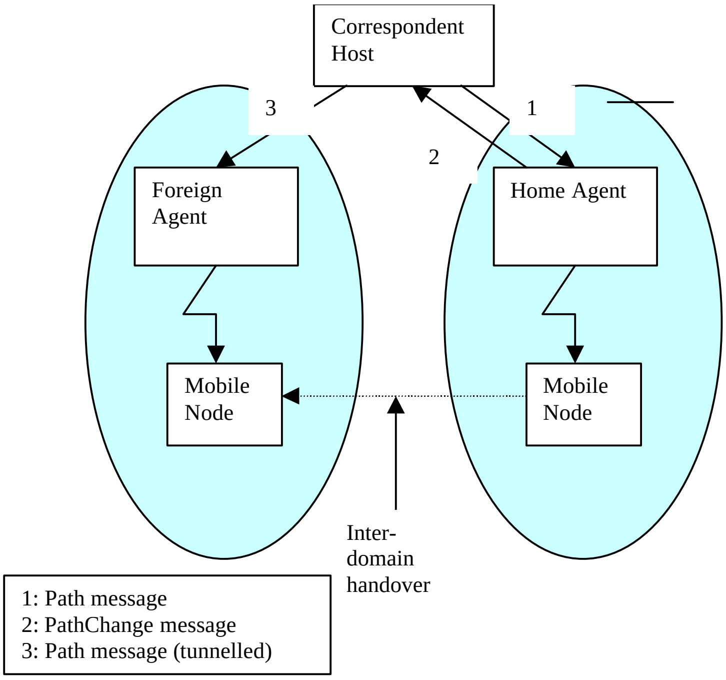

Figure 7-1: Reservation setup for mobile hosts

1. A Path message is sent by the Correspondent Host to the receiver Mobile Node.
2. If MN moves away from home, then HA captures the RSVP Path message and replies to CH with a PathChange message containing the Care-of Address of the Mobile Node and its own address (MOBILITY_NOTIFICATION Object), without tunnelling the original Path message to FA;

3. The CH after receiving the PathChange message, it caches the binding between Mobile Node's IP address and Care-of Address. After this it sends a new Path message to the Mobile Node, tunnelling it to the Care-of Address. From now on, reservation setup works in the traditional way, with the possible exception of tunnelling usage.

The proposed method has some advantages, e.g., simple, efficient and of limited impact on the actual RSVP proposal, but also disadvantages related to the unsolved security issues, i.e., the PathChange messages from Home Agents to Correspondent Hosts should be authenticated.

7.3 Mobile Internet Access and QoS Guarantees Using Mobile IP

In [JaRa98] as mentioned in Section 5.4, the Mobile IPv4 with Location Registers (MIP-LR) is described. In MIP-LR, the research issues, Issue_9 (*RSVP operation over IP tunnels)* and Issue_10 (*RSVP reservations on Mobile IP triangle route situations)* described in Section 3.3.3 are solved, since the "triangle routes" from sender to the Mobile Node and encapsulation of packets sent to a Mobile Node are not longer required. Therefore, MIP-LR is able to use the Integrated Services concept (being able to interoperate with RSVP) and provide QoS guarantees. It is expected that the solutions provided to Issue_9 (*RSVP operation over IP tunnels)* and Issue_10 (*RSVP reservations on Mobile IP triangle route situations)* through minor modifications can also be applied for Mobile IPv6.

7.4 RSVP support for Mobile IP version 6

In [draft-fhns-rsvp-support-in-mipv6-00.txt], solutions to Mobile IPv6 Issue_9 (*RSVP operation over IP tunnels*) described in Section 3.3.3, are provided.

These are:

1. Modify RSVP at both mobile and Correspondent Hosts, such that they become aware of MIPv6 addressing;

2a. Optional *triggers/objects* are added to RSVP messages, to enhance the performance and make handovers smooth and seamless. The RSVP PATH messages are triggered on bindings updates and home address objects that are contained in RSVP RESV messages. This will enable intermediate routers to recognise connections and to use resources even when the Care-of Address changes.

2b. A mechanism called *flow extension* is provided. This mechanism is able to extend the existing RSVP flows (i.e., flow_ids) that are applied on typical IP routers, to the new Mobile IP router. It is used in combination with a simultaneous binding option that has to be applied for the roaming Mobile Node. The Mobile Node receives packets on both Care-of Addresses (previous and current).

In [draft-fhns-rsvp-support-in-mipv6-00.txt] is concluded that the minimal solution (1) is a requirement in order to make Mobile IPv6 and RSVP interoperable. This requires the modification and the interfacing of the RSVP daemon and Mobile IP's binding cache at both CH's and MN's.

For advanced solutions, where performance and smooth handovers in wireless environments are required, the solutions (2a and 2b) are proposed.

A qualitative comparison (from [draft-fhns-rsvp-support-in-mipv6-00.txt]) of the latest two approaches is given in Table 7-1.

Table 7-1: Qualitative comparison of two approaches (from [draft-fhns-rsvp-support-in-mipv6-00.txt])

Criteria	(2a) Triggers/Objects	(2b) Flow extension
Changes to CH	Yes (needed for minimal solution)	Yes (needed for minimal solution)
Changes to	Yes (RSVP Mobile IP	No

intermediate routers	object extension and reuse of flow's resources)	
Changes to MIP router	No (forwarding of late packets is also an option here)	Yes (binding update interception, flow forwarding)
Changes to MN	Yes	Yes
Changes to HA	No	No
Supports multicast delivery	Yes	Yes
Bandwidth efficient	Yes	Yes (it is assumed overdimensioning in the access network)
End to end delay	Always shortest path (but re-establishment of resources requires a round trip)	Slightly increasing delay
Lossless HO	Yes (with forwarding of late packets)	Yes
HO delay	Roundrip	Faster than (2a)
Implem. complexity	Moderate	Higher than (2a)

7.5 An architecture for QoS guarantees and routing in Wireless/Mobile Networks

As mentioned in Section 6.7, [MaSi98] proposes an architecture that provides QoS support in mobile/wireless networks along with support for fast routing during intra-domain handovers. The specified and implemented architecture is hierarchical (see e.g., Figure 6-6) and is based on the concept of QoS regions and routing regions. This architecture can be used to solve the research issue, Issue_8 (*Efficient Mobile IP aware reservation mechanisms)* described in Section 3.3.3.

In [MaSi98] different resource reservation schemes (ways) used to provide QoS in mobile/wireless networks are discussed.

One way to provide QoS, is to first estimate the path(s) the mobile might follow and then reserve resources on that (these) path(s). This could be a waste of the limited wireless resources. Another proposed way is the so called, passive reservation scheme. The passive reservation schemes can make sure, that the reserved resources are not wasted when a mobile is not using them. Other applications can use the passive reservations until the moment they are claimed by the mobile for which the reservation is made. There are two architectural possibilities by which passive reservations can be accomplished.

- Passive reservations are initiated and maintained by the sender on all possible base stations in the vicinity of the mobile;
- The passive reservations are initiated and maintained by another designated node (e.g., base station) on behalf of the sender.

The specified architecture in [MaSi98] is supporting passive reservations that use a combination of the two possibilities explained above.

Furthermore, QoS domains (see Section 6.7) are defined wherein:

- Within a QoS domain, all passive reservations for mobility are done by extending the path of the original reservation;
- Between QoS domains, all passive reservations for mobility are done by partial re-routing.

In order to explain the routing and QoS based functionality of the specified architecture, the following example is provided (see Figure 7-2).

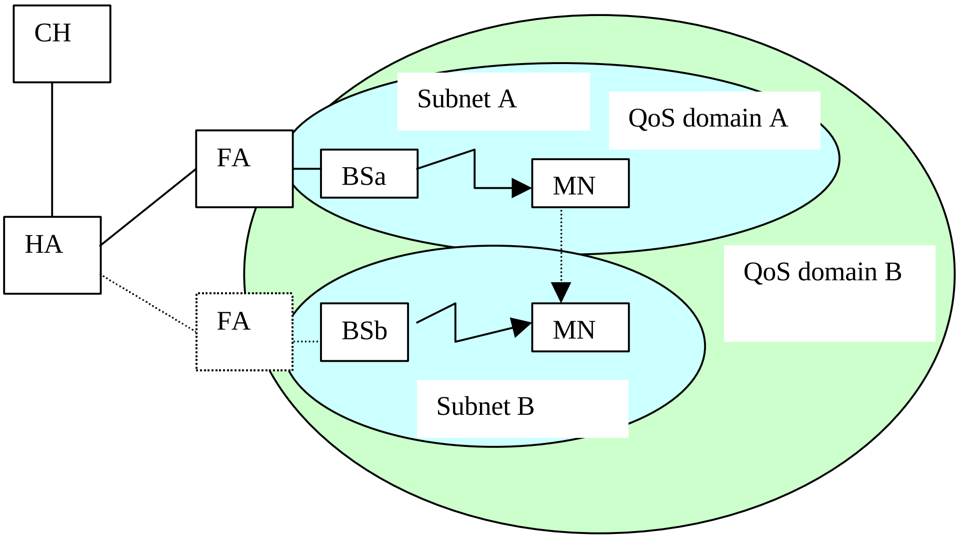

Figure 7-2: Example

- A Corrrespondent Host wishes to send data to a Mobile Node MN, which is currently located in subnet A, and is communicating with Base Station BSa. The Correspondent Host sends the request to the HA. HA will send a reservation request to the FA (that is also the routing-domain router). The path from the Correspondent Host to the FA uses the mobile IP routing protocol while the path from the FA to the mobile MN (through BSa) uses the routing table entries on hosts in the same routing-domain which reflect the current location on mobile MN.
- For the duration of time that the mobile remains in Subnet A, the passive reservations are made locally for the potential movement of the mobile. The BSa requests from the QoS –domain router to invoke all it’s neighbouring base stations in the passive reservation process. There are two possible ways of making passive reservations at this point.
  - All the neighbouring base stations are in the same QoS domain, e.g., QoS domain A. The BSa can then make passive reservations with all these neighbouring base sations.
  - Some of the neighbouring base stations are in the same QoS domain and some are in a different QoS domain. The BSa makes then passive reservation with the base stations in the same QoS domain. The QoS domain router makes passive reservation with the base stations in the neighbouring domain.
- When the mobile now moves into another region, e.g., Subnet B (managed by BSb) then, either the reservations between BSa and BSb are activated (QoS domain B) or the reservations between the QoS-domain router and BSb (QoS domain A) are activated, depending on which domain BSb resides.

- In the situation that the roaming is local, i.e., within the same routing domain, then the routing tables in the hosts in this domain are changed to indicate that the mobile is now in the location of the BSb.
- Otherwise, if the roaming is done to another routing domain, the current routing-domain router/FA informs the HA about the roaming and the HA chooses another QoS domain router to the other subnet as the FA.

The resource reservation procedure can be provided by using a modified version of RSVP. The modified version will have to contain the following changes:

- Passive reservation messages have to be incorporated;
- New QoS parameters that are specific to mobile environment have to be introduced. These are parameters such as: *loss profiles*, that give an application the opportunity to choose between distributed loss or bursty loss; *probability of seamless communication*, that defines the allowed breaks during handover; *rate reduction factor*, that is used for situations when requested passive reservations can not be provided and therefore, renegotiations on a fraction of the resources is started.
- It should be possible that the passive reservations made between base stations are used by the TCP flow that made the reservations.

7.6 RSVP operation over IP tunnels

In [draft-ietf-rsvp-tunnel-04.txt] an IP tunnelling mechanism is specified that provides a solution to Issue_9 (RSVP operation over IP tunnels) presented in Section 3.3.3. This mechanism is able to make reservations across all IP-in-IP tunnels.

In general, a tunnel is able to participate in the operation of a RSVP aware sub-network (see Figure 7-3) in one of the following ways:

- The RSVP aware sub-network does not provide QoS guarantees. This is a best effort or type 1 tunnel.
- The RSVP aware sub-network provides QoS guarantees to a group of flows (aggregates of flows). The tunnel that will participate to this operation is referred as type 2 tunnel;
- The RSVP aware network provides QoS guarantees for individual end-to-end flows. The tunnel that will participate to this operation is referred as type 3 tunnel;

The specified in [draft-ietf-rsvp-tunnel-04.txt] IP tunnel mechanisms can operate in all these three tunnel types. The RSVP operation over a tunnel can be viewed using Figure 7-3. Rentry represents the tunnel entry router, while Rexit represents the tunnel exit router.

In a type 1 tunnel the operation of the RSVP should be such that the RSVP messages traverse the sub-network correctly. Furthermore, the RSVP non-controlled sub-network has to be detected.

For type 2 and type 3 tunnels, it is assumed that reservations over IP tunnels can be guaranteed. This can only be accomplished if a mapping between end to end RSVP sessions and tunnel RSVP sessions is supported. An end to end RSVP session can for example be provided (see Figure 7-3) between M1 and M2 or between M3 and M4. A tunnel RSVP session can be provided between Rentry and Rexit.

For type 2 tunnels a static mapping from an end to end RSVP session to an existing tunnel RSVP session can be achieved.

For type 3 tunnels the mapping is dynamical, creating a new tunnel RSVP session for each end-to-end RSVP session.

After this mapping is fulfilled, some management operations on the mapped RSVP sessions have to be provided, such that the actions of the two RSVP sessions, e.g., create and torn down, can be co-ordinated. In [draft-ietf-rsvp-tunnel-04.txt] the following design decision on the above matter is made:

[.. End-to-end RSVP control messages being forwarded through a tunnel are encapsulated in the same way as normal IP packets, e.g., being wrapped with the tunnel IP header only, specifying the tunnel entry point as source and the exit point as destination.] ([draft-ietf-rsvp-tunnel-04.txt]).

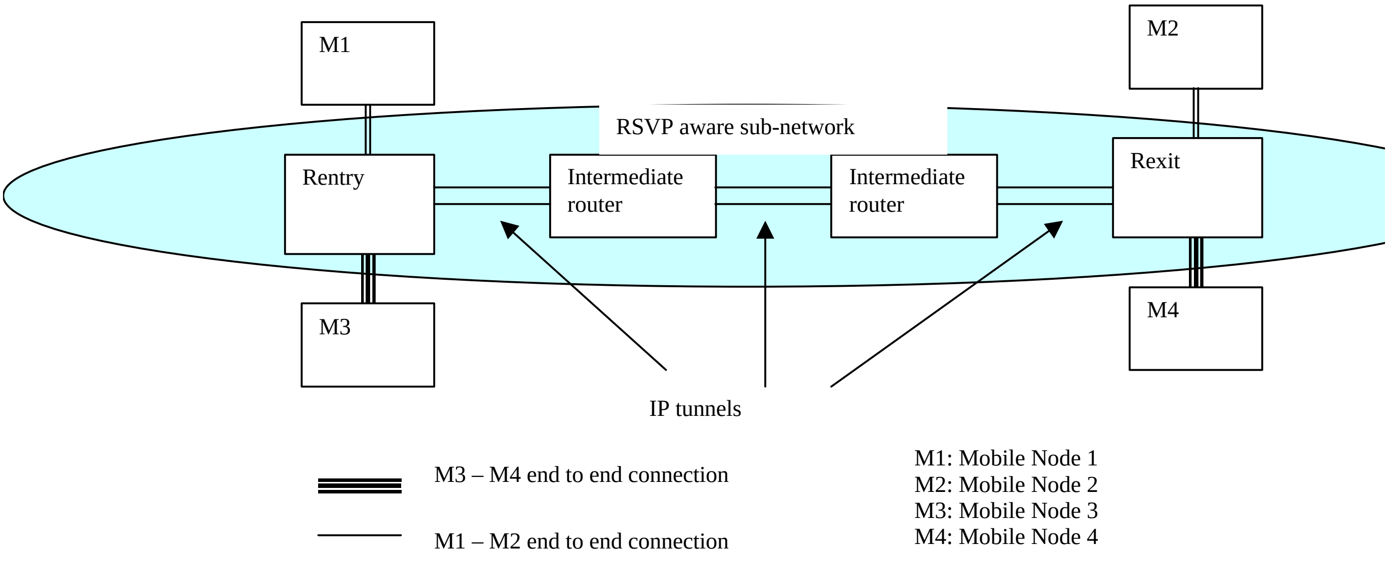

Figure 7-3: IP tunnel in an RSVP aware subnetwork

8 Simultaneous bindings;

8.1 Introduction

Simultaneous bindings refer to the possibility of a host to register more than one Care-of Addresses at the same time. The basic Mobile IPv4 protocol permits (optional feature) a Mobile Node to have simultaneously bindings, i.e., register more than one Care-of Addresses at the same time, and to deregister a specific Care-of Address as necessary. In the situation that more than one Care-of Address are active for a Mobile Node, the Home Agent is instructed to send a duplicated encapsulated IP packet to each Care-of Address. The decapsulated result will be received by the Mobile Node at each registered Care-of Address.

8.2 Special Tunnels for Mobile IP

In [draft-ietf-mobileip-spectun-00.txt] a mechanism is proposed that solves the open issue, i.e., Mobile IPv4 Issue_11 (*Inefficient maintenance of simultaneous bindings)* described in Section 3.3.4, and allows a Foreign Agent, to return IP packets to the Home Agent when these IP packets were destined to a Mobile Node that is no longer registered with this Foreign Agent. This approach after minor changes can also be applied to Mobile IPv6.

Suppose that a tunnelled packet destined to a Mobile Node, is received by a Foreign Agent that does not have a binding cache or a visitor list entry for that Mobile Node. The Foreign Agent will not be able to recognise the home address of the Mobile Node and therefore, this tunnelled IP packet will be dropped. The solution provided in [draft-ietf-mobileip-spectun-00.txt] gives the opportunity to deliver such a tunnelled IP packet. This can be accomplished by encapsulating the IP packet as a special tunnel, destined to the Mobile Node's Home Agent. The special tunnel allows the Home Agent to avoid a possible routing loop when a Foreign Agent do not anymore have an association with the Mobile Node. This special tunnel allows the Home Agent to identify the address of the node that tunnelled the IP packet, and to avoid tunnelling the IP packet back to the same node. In a special tunnel an IP packet is encapsulated in such way, that its outer destination address is set equal to its inner destination address, i.e., the original destination address of the IP packet.

9 Security in Mobile IP

9.1 Introduction

To date within the Internet, there are several authentication and authorisation approaches used for dial-up computers. Several of these approaches are provided by using AAA (Authentication Authorisation and Accounting) servers (see [draft-ietf-aaa-roamops-auth-req-00.txt], such as the (Remote Access Dialling User Service) RADIUS [RFC2138] and the DIAMETER [draft-calhoun-diameter-07.txt]. RADIUS is a protocol that carries authentication, authorisation and configuration information between a client, referred as Network Access Server, and an Authentication Server. DIAMETER, similarly to RADIUS provides Authentication Authorisation and Accounting, but in addition, it provides policy control and resource control. The DIAMETER and RADIUS protocols can co-exist and inter-work.

Such approaches can also be applied to Mobile Nodes using Mobile IP when the nodes are attempting to connect to foreign domains with AAA servers. AAA servers today identify clients by using the Network Access Identifier (NAI) [RFC2468]. The basic Mobile IP protocol [RFC2002] permits mobile internetworking to be done on the network layer; however, it also introduces new security issues that have to be solved. Note that these open issues are eventually solved in different contexts, but are not integrated with Mobile IPv4.

9.2 Security of Current Mobile IP Solutions

In [JaCi97] an evaluation is done of how the security capabilities and mechanisms of the basic Mobile IPv4 [RFC2002] (MIPv4), basic route optimisation method [draft-ietf-mobileip-optim-08.txt] (MIPv4RO) and the basic Mobile IPv6 [draft-ietf-mobileip-ipv6-07.txt] (MIPv6) map to the security requirements. This document lists the existing solutions to the issues: Issue_14 (*Authentication)*, Issue_15 (*Authorisation)*, Issue_16 (*Non-repudiation)*, Issue_17 (*Encryption key distribution)* and issue_18 (*Location privacy)* which are discussed in Section 3.3.5.

The related security issues and risks for these basic protocols are listed in Table 9-1 to Table 9-4.

Table 9-1: Authentication (from [JaCi97])

	Issue	Risk
MIPv4	Manually established Mobility Security Associations (MSAs) required between MN, FA and HA	Not described in any detail
	Optional authentication of registration messages between MN and FA	Risk of hostile FA masquerading on as a legitimate FA and present a denial-of-service threat.
	Optional authentication of registration messages between MN and FA	
	No authentication of FA Advertisement messages	
	Use of ARP and proxy ARP	No ARP authentication so Home network vulnerable to MN traffic stealing by hostile network

MIPv4RO	Manually established MSAs required between MNs, CNs, Fas and HAs	Key distribution problems (Not described in any detail)
	HA may manage its MSAs using a single “master” key by computing a node-specific key as: MD5 digest (node address || master-key || node-address) (see [RFC1321])	Hostile Node eavesdropping on communications for a period of time will see many of the node addresses used in this transform
	Use of ARP and proxy ARP	No ARP authentication so Home network vulnerable to MN traffic stealing by hostile network
MIPv6	MSAs required between MNs and Default routers, e.g. HA, defined by Security Architecture [RFC1825] and use IPv6 Authentication header [RFC1826].	Efficient key distribution/establishment between MNs and Default routers still open issue;

Table 9-2: Authorisation (from [JaCi97])

	Issue	Risk
MIPv4	Silent beyond, including an FA registration denial code of “administrated prohibited”	Fails to address how FA, or Default router, ascertains legitimacy of visiting MN. Leaves authorisation implementation up to developers without providing guidelines
MIPv4RO		
MIPv6		

Table 9-3: Non-repudiation (from [JaCi97])

	Issue	Risk
MIPv4	FA visitor list entries do not record the actual duration of the MN visit nor the amount network resources consumed.	No mechanism for logging visiting MN resource consumption therefore owner/operator of visited network unable to track network resource utilisation
	The FA must delete an MN Visitor List entry when the FA receives a valid registration reply.	Once an MN Visitor List entry is deleted there is no longer any record of an MN’s visit. No mechanism or approach, for logging MNs who have visited and left FA’s network.

MIPv4RO	FA visitor list entries do not record the actual duration of the MN visit nor the amount of network resources consumed.	No mechanism for logging visiting MN resource consumption therefore owner/operator of visited network unable to track network resource utilisation
	The FA must delete an MN Visitor List entry when the FA receives a valid registration reply.	Once an MN Visitor List entry is deleted there is no longer any record of an MN's visit. No mechanism or approach, for logging MNs who have visited and left FA's network.
MIPv6	Default router visitor list entries do not record the actual duration of the MN visit nor the amount network resources consumed	No mechanism for logging visiting MN resource consumption therefore owner/operator of visited network unable to track network resource utilisation

Table 9-4: Location Privacy (from [JaCi97])

	Issue	Risk
MIPv4	Traffic analysis on wireless links	Only viable protection against a traffic analysis attack on wireless links is use of link encryption
MIPv4RO MIPv6	Care of Address is known by the Correspondent Host	No protection

9.3 Reverse Tunnelling for Mobile IP

In [RFC2344] a solution to Mobile IPv4 Issue_12 (*Ingress filtering*) described in Section 3.3.5, is provided. A method of specifying and using a reverse tunnel is provided. A reverse tunnel is a tunnel that is established starting from the mobile node's Care-of Address (and not from the Mobile Node's home of address as defined in Mobile IPv4) up to the Home Agent. When a Mobile Node moves to a foreign network, it detects Foreign Agents that are supporting reverse tunnelling, by listening to agent advertisements. The Mobile Node selects such a Foreign Agent by registering through it. After this moment, the Mobile Node can select a packet delivery style. There are two different packet delivery styles defined in [RFC2344]. The first one is the Direct Delivery Style where the mobile sends a packet directly to the Foreign Agent without encapsulation. The Foreign Agent receives it and tunnels it to the Home Agent. The tunnelling procedure is a reverse tunnelling one, i.e., the source address of the outer header, is the Mobile Node's Care-of Address. It is considered that the Home Agent can also support the reverse tunnelling procedure.

The second delivery style is called Encapsulating Delivery Style, where the Mobile Node encapsulates the packets sent to the Foreign Agent. The Foreign Agent then decapsulates the packets, re-tunnels them by using reverse tunnelling, and sends them to the Home Agent.

9.4 Mobile IP extension for Private Internets Support (MPN)

In [draft-teoyli-mobileip-mvpn-02.txt] an extension to the Mobile IPv4 base protocol is given, that enables the mobility support to span multiple routing domains. This extension provides solutions to Issue_12 (*Ingress filtering*) described in Section 3.3.5.

In general, the base Mobile IP protocol uses IP within IP as a default encapsulation protocol to tunnel an IP packet sent by an Correspondent Host to the Care-of Address of a Mobile Node that is away from home. Due to the ingress filtering issue (see Section 3.3), this mechanism is unsuitable if the mobility agents, e.g., HA and FA, required in a transition are located in different networks, i.e., private and public. In [draft-teoyli-mobileip-mvpn-02.txt] the Generic Routing Encapsulation (GRE) protocol is used as the default tunnelling protocol. Note, that this protocol is specifying the intermediate destinations by using the combination of the source route entry and the address family option. In this way the encapsulation procedure used in Mobile IPv4 is avoided, and the tunnelling procedure can be applied on different networks, private and public.

In the situation of MPN the source route entry will include any intermediate mobility agent (in private or public domains) along the tunnel route and the tunnel endpoint.

9.5 Use of IPSec in Mobile IP

In [draft-ietf-mobileip-ipsec-use-00.txt] a solution is given to the security issue, Issue_14 (*Authentication)* described in Section 3.3.5, where a scheme is proposed to apply the IP security protocol (IPSec) [Draft-ietf-ipsec-arch-sec-02.txt] onto the IP-IP encapsulation used by Mobile IP to redirect IP packets to and from the Mobile Nodes. By using this method, authentication and confidentiality services to Mobile IP redirection traffics are provided. In this manner, these Mobile IP traffics will be protected against passive and active attacks and will give them the possibility to pass through security gateways. The proposed scheme includes:

- a mechanism for negotiating the use of IPSec protection on selected Mobile IP redirection tunnels,
- a procedure for establishing these IPSec protected tunnels;
- the formats of tunnelled packets in either full IP-IP or minimal IP-IP encapsulations.

9.6 Registration Keys for Route Optimisation

The [draft-ietf-mobileip-regkey-00.txt] is solving the security issues, Mobile IPv4 Issue_14 (*Authentication*) and Issue_15 (*Authorisation)* described in 3.3.5, where a way is introduced to provide a security association between a Mobile Node and a Foreign Agent at the moment the Mobile Node registers with this Foreign Agent.

The route optimisation messages (see [draft-ietf-mobileip-optim-08.txt] and Section3.2) that might change the routing of IP datagrams to the Mobile Node have to be authenticated. The mechanisms used to accomplish this authentication are similar to the ones used in the base Mobile IPv4 protocol. A mobility security association is established in advance between the sender and receiver of such messages. In the situation that the Mobile Node moves to a foreign network, such security association between the Mobile Node and the new Foreign Agent is difficult to be accomplished in advance (see Table 9-1). However, in order for the Foreign Agent to process future binding updates that it may receive from the Mobile Node, it needs to have such a security association. These binding updates provide a mechanism for accomplishing smooth handovers between a previous Foreign Agent to a new Foreign Agent (see Section 5.6).

The operations that are performed during the smooth handovers, i.e., handovers from the old to new Foreign Agents, should be secure. In other words, both Foreign Agents involved in this association must be sure that they are getting authentic handover information.

In [draft-ietf-mobileip-regkey-00.txt] this assurance is obtained by using messages that are applied in combination with the Mobile IP Registration Request and Registration Reply messages. Note that, the exact identity of the Foreign Agent is not crucial to the process of establishing a registration key, i.e., a secret key shared between Mobile Node and Foreign Agent that may optionally be established during the registration process. In [draft-ietf-mobileip-regkey-00.txt] several methods are specified, that are activated during the registration process, enable a Mobile Node to create a registration key with a Foreign Agent whose identity cannot be established. These methods are listed below, in order of declining preference:

1. The Foreign Agent and Mobile Node share a security association. This can be used to secure the Previous Foreign Agent Notification without need to establish a registration key.
2. When a Home Agent and a Foreign Agent share a security association, the Home Agent can choose the new registration key.
3. In the situation that the Foreign Agent has a public key, it will require from the Home Agent to supply a registration key.
4. When the Mobile Node includes its public key in its Registration Request, then the Foreign Agent can choose the new registration key.
5. The Foreign Agent and the Mobile Node can execute a Diffie-Hellman key exchange protocol [DiHe76] as part of the registration protocol.

9.7 Mobile IP Challenge/Response Extensions

In [draft-ietf-mobileip-challenge-01.txt] a number of extensions, for the Mobile IPv4 Agent Advertisements and the Registration Request are defined, allowing a Foreign Agent to use a mechanism called, challenge/response, to authenticate the Mobile Node. This mechanism provides solutions to Issue_14 (*Authorisation*) and Issue_15 (*Authorisation*) described in Section 3.3.5. Note that, the challenge is a random value of at least 128 bits and is used to compute an authentication procedure.

In this mechanism a verification infrastructure is introduced (see Figure 9-1), to create a trusted association between a Foreign Agent and a Home Agent. The Foreign Agent after receiving a Challenge response from the Mobile Node, passes it to the entity called, Verification and key Management Infrastructure, and awaits a Registration Reply. The Foreign Agent accepts the registration from the Verification and key Management Infrastructure only if the reply is positive. If the reply is negative, then the Foreign Agent assumes that the challenge did not pass the verification.

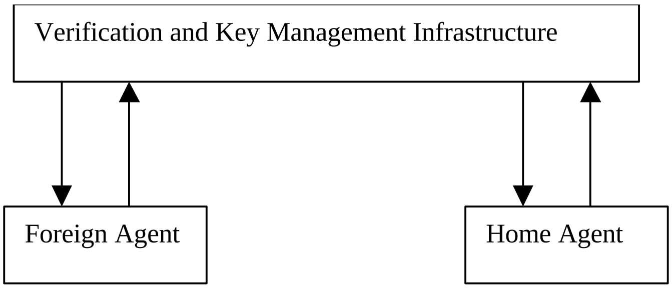

Figure 9-1: Verification Infrastructure

9.8 Mobile IP Public Key Based Authentication

In [draft-jacobs-mobileip-pki-auth-02.txt] an authentication extension, to the Mobile IP base protocol is provided, that defines how Mobile Nodes and Mobility Agents (both home network and foreign network) may use public key or secret key base authentication via digital signatures. By using this extension, solutions to Issue_14 (*Authentication*) and Issue_17 (*Encryption key distribution)* described in Section 3.3.5, are provided.

This Mobile IP authentication extension, is applying the Secure Scaleable Authentication (SSA) approach, that makes use of a few reserved fields in the existing Mobile IP message definitions. By using the increased functionality of SSA, the authentication extension used in the Mobile IPv4 protocol has been modified to accommodate different authentication types and different sizes of authenticators (digital signatures). Moreover, the use of either IP address or host name for identifying Mobile Nodes and mobility agents is achieved.

9.9 Mobile IP Network Address Identifier Extension

In [draft-ietf-mobileip-mn-nai-01.txt] the NAI extension to the Mobile IPv4 Registration Request [RFC2002] message from the Mobile Node is specified. This extension gives the possibility to a Mobile Node to authenticate itself, and be authorized to be connected to the foreign domain, without even having a home address. By using this extension, solutions to Issue_14 (*Authentication*) and Issue_15 (*Authorisation*) described in Section 3.3.5, are provided.

This solution uses a new function named the Home Domain Allocation Agency (HDAA) (see Figure 9-2) that can dynamically assign a Home Address to the Mobile Node. Any message that contain the Mobile Node NAI extension, it may have the Home Address field in the Registration Request set to zero (0). In this case the Foreign Agent must use the NAI, instead its pending registration request records. The HDAA shown in Figure 9-2 receives messages from Foreign Agents (e.g., FA) and assigns a Home Address within the Home Domain. Note that, the HDAA does not perform any Mobile IP processing on the Registration Request, but is simply forwarding the request to the Home Agent (HA) within the network that is able to handle the request.

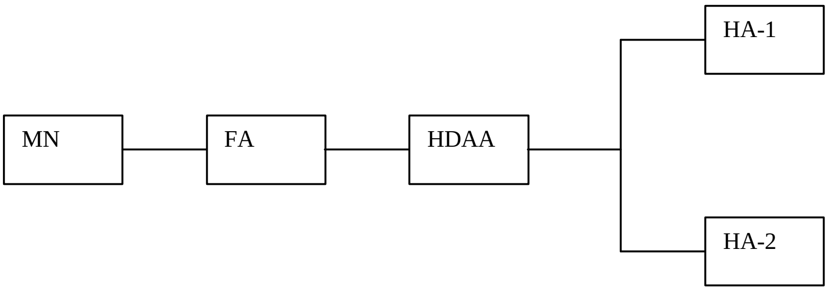

Figure 9-2: Home Domain Allocator Agency (HDAA)

When the FA receives a Registration Request from the Mobile Node (MN), it extracts the NAI and subsequently it finds the Home domain name associated with this NAI. The FA is then able to find the HDAA that processes and handles the requests for the Mobile Node's home domain.

9.10 NAI resolution for Wireless Networks

In [draft-ietf-mobileip-nai-wn-00.txt] an option is provided to match the wireless cellular subscriber identification to/from the NAI during the wireless registration and authentication process. A solution to Issue_19 (*Use one single subscription for all service types)* described in Section 3.3.5, is provided. It is expected that the solution provided to Issue_19 (*Use one single subscription for all service types)* through minor modifications can also be applied for Mobile IPv6.

The functionality of the mechanism is provided in the following steps. Note that, the cellular service for subscriber A (SUB A) depicted in Figure 9-3, is considered to be an NAI enabled Wireless Service.

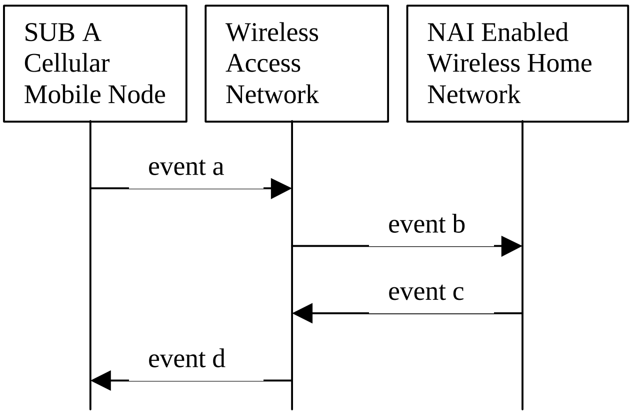

Figure 9-3: NAI resolution scenario

event a: SUB A powers-on his second or third generation cellular Mobile Node. The on powering of the Mobile Node causes it to attempt a wireless registration. The Mobile Node is identified by its Mobile Identification Number (MIN) [MoPa92].

event b: The wireless registration message is received by the wireless access network, which matches a NAI based on the MIN sent by the cellular Mobile Node. Afterwards, an appropriate registration message is sent to the NAI enabled home network.

event c: The NAI enabled home network, after receiving this registration message, it registers and authenticates the wireless SUB A. Afterwards, an appropriate registration response is sent back to the wireless access network.

event d: The wireless access network, after receiving the registration response, it sends an appropriate wireless registration return result to SUB A`s cellular Mobile Node.

9.11 DIAMETER Mobile IP Extensions

In [draft-calhoun-diameter-mobileip-01.txt] extensions to DIAMETER [draft-calhoun-diameter-07.txt] are provided that allow inter-domain (different ISP’s) authentication and authorisation. Moreover the assignment of Mobile Node Home Address, assignment of Home Agent, as well as a Key Distribution approach is specified. The provided Mobile IPv4 solutions are accomplished using associations (communications) among the AAA DIAMETER servers that have to be located in the different ISP domains. These extensions provide solutions to Issue_14 (*Authentication)* and Issue_15 (*Authorisation*) described in Section 3.3.5.

9.12 Firewall Support for Mobile IP

In [draft-montenegro-firewall-sup-03.txt] a solution is given to Mobile IPv4 Issue_20 (*Firewall support in Mobile IP*) described in Section 3.3.5. It is expected that the solution provided to Mobile IPv4 Issue_20 (*Firewall support in Mobile IP*) through minor modifications can also be applied for Mobile IPv6. At least two methods can be used to provide firewall support for mobile nodes. One is based on application proxying, where each mobile node establishes a TCP session to exchange UDP traffic with the firewall. This method can be accomplished using the SOCKS protocol (version 5) [RFC1928]. The second method is based on IP security, where the traffic from the mobile node to the firewall is using session-less IP security encryption and authentication. The mechanism that can be used to provide this type of firewall support for Mobile IP is based on SKIP [AzPa95].

10 Conclusions

Mobile IP is a protocol developed by the IETF Mobile IP Working Group, that provides mobility support to wireless Internet users. However, many issues related to topics such as, inter and intra-domain handover, QoS and security are not satisfactory solved.

This document gives in general, an overview of the current developments and research activities in the mobile IP area. In particular, the inter and intra-domain handover, QoS, simultaneously bindings and security research topics are in more detail emphasised. Moreover, a list with open issues per topic is provided and explained. These open issues are:

Inter-domain mobility (macro-mobility)

Issue_1. *Triangle routing*:.

Issue_2. *Inefficient direct routing*:.

Issue_3. *Inefficient Home Agent Notification*:.

Issue_4. *Inefficient binding de-registration*:.

Intra-domain mobility (micro-mobility)

Issue_5. *Local management of micro-mobility events*:.

Issue_6. *Seamless intra-domain handover*:.

Issue_7. *Mobility routing crossings in an Intranet*:.

Quality of Service (QoS)

Issue_8. *Efficient Mobile IP aware reservation mechanisms*:.

Issue_9. *RSVP operation over IP tunnels*:

Issue_10. *RSVP reservations on Mobile IP triangle route situations*:.

Simultaneous bindings

Issue_11. *Inefficient maintenance of simultaneous bindings*:.

Security

Issue_12. *Ingress filtering*:.

Issue_13. *Minimise the number of required trusted entities*:.

Issue_14. *Authentication*:.

Issue_15. *Authorisation*:.

Issue_16. *Non-repudiation*:

Issue_17. *Encryption key distribution*.

Issue_18. *Location privacy*:.

Issue_19. *Use one single subscription for all service types*:.

Issue_20. *Firewall support in Mobile IP*:.

In my opinion, some of these open issues are satisfactory solved, while other ones have to be resolved in the near future. The issues that in my opinion are satisfactory solved are:
Issue_1 (*Triangle routing*);
Issue_3 (*Inefficient Home Agent Notification*);
Issue_4 (*Inefficient binding de-registration*);
Issue_7 (*Mobility routing crossings in an Intranet*);
Issue_9 (*RSVP operation over IP tunnels*);
Issue_11 (*Inefficient maintenance of simultaneous bindings*);
Issue_12 (*Ingress filtering*).

Several research projects are studying the remaining open issues for Mobile IP. The Internet Next Generation (ING) [ING] research project, is such a project, that focuses on the development and introduction of Quality of Service for the fixed and wireless Internet. Ericsson Business Mobile Networks is actively involved in the ING project, where it, is investigating QoS and Mobile IP mobility management issues for the wireless Internet.

11 References

11.1 By alphabet

[AnBl96] Andreoli, G., Blefari-Melazzi, N., Listanti, M., Palermo, M., “Mobility management in IP networks providing real-time services”, Proc., Annual International Conference on Universal Personal Communications, pp. 774 – 777, 1996.

[AzPa95] Aziz, A., Patterson, M., “Design and implementation of SKIP”, available on-line at http://skip.incog.com/inet-95.ps, 1995.

[Bra96] Braden, R., et. al., “Resource reaservation Protocol (RSVP) – Version 12 Functional specification”, Aug. 12, 1996. Available via http://www.ietf.org/html.charters/intserv-charter.html.

[DiHe76] Diffie, W., Hellman, M., “New Directions in Cryptography”, IEEE Transactions on Information Theory, Vol. 22, pp.644-654, November 1976.

[draft-ietf-ipngwg-ipv6-spec-v2-00.txt] Deering, S., E., Hinden, R., M., “ Internet protocol version 6 (IPv6) specification”, Internet-Draft, draft-ietf-ipngwg-ipv6-spec-v2-00.txt, July 1997. Work in progress.

[draft-calhoun-diameter-07.txt] Calhoun, Rubens, “DIAMETER”, Internet draft, draft-calhoun-diameter-07.txt, Work in progress, November 1998.

[draft-ietf-aaa-roamops-auth-req-00.txt] Calhoun, P. R., Zorn, G., “Roamops Authentication/Authorisation Requirements”, Internet draft, draft-ietf-aaa-roamops-auth-req-00.txt, Work in progress, March 1999.

[draft-hiller-3gwireless-00.txt] Hiller, T., (editor) “3G Wireless Data Provider Using Mobile IP and AAA”, Internet draft, draft-hiller-3gwireless-00.txt, Work in progress, March 1999.

[draft-chuafoo-mobileip-rafa-00.txt] Foo, S., F., Chua, K., C., “Regional Aware Foreign Agent (RAFA) for Fast Local Handoffs”, Internet draft, draft-chuafoo-mobileip-rafa-00.txt, Work in progress, November 1998.

[draft-teoyli-mobileip-mvpn-02.txt] Teo, W., T., Li, Y., “Mobile IP extension for Private Internet Support (MPN)”, Internet draft, draft-teoyli-mobileip-mvpn-02.txt], Work in progress, 1999.

[draft-vallko-cellularip-00.txt] Valko, A., Cambell, A., Gomez, J., “Cellular IP”, Internet draft, draft-vallko-cellularip-00.txt, Work in progress, November 1998.

[draft-ramjee-micro-mobility-hawaii-00.txt] Ramjee, R., LaPorta, T., Thuel, S., Varadhan, K., “IP micro-mobility support using HAWAII”, Internet draft, draft-ramjee-micro-mobility-hawaii-00.txt, work in progress, February 1999.

[draft-ietf-mobileip-spectun-00.txt] Perkins, C., Johnson, D., B., “Special Tunnels for Mobile IP”, Internet draft, draft-ietf-mobileip-spectun-00.txt, Work in progress, November 1997.

[draft-ietf-mobileip-ipsec-use-00.txt] Zao, J., K., Condell, M., “Use of IPSec in Mobile IP”, Internet draft, draft-ietf-mobileip-ipsec-use-00.txt, Work in progress, November 1997.

[draft-ietf-mobileip-regkey-00.txt] Perkins, C., Johnson, D., B., “Registration Keys for Route Optimisation”, Internet draft, draft-ietf-mobileip-regkey-00.txt, Work in progress, November 1997.

[draft-ietf-mobileip-challenge-01.txt] Perkins, C., E., Calhoun, P., R., “Mobile IP Challenge/Response Extensions”, Internet draft, draft-ietf-mobileip-challenge-01.txt], Work in progress, May 1999.

[draft-jacobs-mobileip-pki-auth-02.txt] Jacobs, S., “Mobile IP Key Bassed Authentication”, Internet draft, draft-jacobs-mobileip-pki-auth-02.txt, Work in progress, march 1999.

[draft-ietf-mobileip-mn-nai-01.txt] Calhoun, P., R., Perkins, C., E., "Mobile IP Network Address Identifier Extension", Internet draft, draft-ietf-mobileip-mn-nai-01.txt, Work in progress, May 1999.

[draft-ietf-mobileip-nai-wn-00.txt] Aravamudhan, L., O'Brien, M., R., Patil, B., "NAI Resolution for Wireless Networks", Internet draft, draft-ietf-mobileip-nai-wn-00.txt, Work in progress, February 1999.

[draft-calhoun-diameter-mobileip-01.txt] Calhoun, P., R., Rubens, A., C., "DIAMETER Reliable Transport Extensions", Internet draft, draft-calhoun-diameter-mobileip-01.txt, Work in progress, February 1999.

[draft-fhns-rsvp-support-in-mipv6-00.txt] Fankhauser, G., Hadjiefthymiades, S., Nikaein, N., "RSVP Support for Mobile IP Version 6 in Wireless Environments", Internet draft, draft-fhns-rsvp-support-in-mipv6-00.txt, Work in progress, November 1998.

[draft-ietf-rsvp-tunnel-04.txt] Terzis, A., Krawczyk, J., Wroclawski, J., Zhang, L., "RSVP operation over IP tunnels", Internet draft, draft-ietf-rsvp-tunnel-04.txt, Work in progress, May 1999.

[draft-ietf-mobileip-ipv6-07.txt] Johnson, D., B., Perkins, C., "Mobility Support in IPv6", Internet draft, draft-ietf-mobileip-ipv6-07.txt, Work in progress, November 1998.

[draft-ietf-mobileip-optim-08.txt] Perkins, C., Johnson, B., J., "Route Optimisation in Mobile IP", Internet draft, draft-ietf-mobileip-optim-08.txt, Work in progress, February 1999.

[draft-ietf-ipsec-auth-header-02.txt] Kent, S., Atkinson, R., "IP Authentication header", Internet-Draft, draft-ietf-ipsec-auth-header-02.txt, Work in progress, October 1997.

[draft-ietf-ipsec-esp-v2-01.txt] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", Internet-Draft, draft-ietf-ipsec-esp-v2-01.txt, Work in progress, October 1997.

[draft-ietf-ipsec-arch-sec-02.txt] Kent, S., Atkinson, R., "Security architecture for the Internet Protocol", Internet-Draft, draft-ietf-ipsec-arch-sec-02.txt, Work in progress, November 1997.

[draft-ietf-ipng-discovery-v2-00.txt] Narten, T., Nordmark, E., Simpson, W., A., "Neighbour Discovery for IP version 6 (IPv6)", Internet draft, draft-ietf-ipng-discovery-v2-00.txt, July 1997. Work in progress.

[draft-ietf-ipngwg-addrconf-v2-00.txt] Thomson, S., Narten, T., "Ipv6 stateless address autoconfiguration", Internet draft, draft-ietf-ipngwg-addrconf-v2-00.txt, July 1997. Work in progress.

[draft-montenegro-firewall-sup-03.txt] Montenegro, G., Gupta, V., "Firewall support for Mobile IP", Internet draft, draft-montenegro-firewall-sup-03.txt, January 1998. Work in progress.

[GeSo97] Geiger, R., L., Solomon, J., D., Crisler, K., J., "Wireless Network Extension Using Mobile IP", IEEE Micro, Vol. 17, No. 6, pp. 63-68, 1997.

[ING] Pras, A., (editor), "Project Proposal Telematics Institute: Internet Next Generation", available at http://ing.ctit.utwente.nl/background/public.pdf, 27 January 1999.

[JaRa98] Jain, R., Raleigh, T., Graff, C., Bereschinsky, M., "Mobile Internet Access and QoS Guarantees using Mobile IP and RSVP with Location Registers", ICC International Conference on Communications, Vol. 3, pp. 1690 – 1695, 1998.

[JaSi97] Jacobs, S., Cirincione, G., "Security of current Mobile IP solutions", Proc. of MILCOM'97, Vol. 3, pp. 1122-1128, 1997.

[KoDu98] Korpeoglu, I., Dube, R., and Tripathi, S., K., "Reducing Router-Crossings in a Mobile Intranet", Journal of Network and System Management, Vol. 6, No. 1, 1998.

[MaSi98] Mahadevan, I., Sivalingham, M., "An Architecture for QoS guarantees and routing in Wireless/Mobile Networks", ACM Intl. Workshop on Wireless and Mobile Multimedia, 1998.

[MOBIP] Charter of mobile IP working group, http://www.ietf.org/html.charters/mobileip-charter.html.

[MONET107] R2066/RMR/UNA2/DS/P/107/b1, “Recommendations of UMTS Integration Scenarios in the B-ISDN Backbone”, December 1995.

[MoPa92] Mouly, M., Pautet, M. B., “The GSM system for mobile communications”, 1992.

[Per97] Perkins, C., E., “Mobile IP”, IEEE Communications Magazine, May 1997.

[Per98] Perkins, C., E., “Mobile networking through mobile IP”, IEEE Internet Computing, 1998.

[Raj97] Rajagopalan, B., “Mobility and quality of service (QoS) in the Internet”, Mobile Multimedia Communications, pp. 129 – 135, 1997.

[RFC826]. Plummer, D., C., “An Ethernet address resolution protocol: Or converting network protocol addresses to 48.bit Ethernet addresses for transmission on Ethernet hardware”, RFC 826, November 1982.

[RFC1256] Deering, S., (ed.), “ICMP Router Discovery Messages”, RFC 1256, August 1989.

[RFC1321] Rivest, R., “The MD5 Message-Digest Algorithm”, RFC 1321, April 1992.

[RFC1541] Droms, R., “Dynamic Host Configuration Protocol”, RFC 1541, October 1993.

[RFC1661] Simpson, W., (editor), “The Point-to-Point protocol (PPP)”, RFC1661, July 1994.

[RFC1702] Hanks, S., Li, T., Farinacci, D., Traina, P., “Generic Routing Encapsulation over IPv4 networks”, RFC 1702, October 1994.

[RFC1825] Atkinson, R., “Security Architecture for the Internet Protocol”, RFC 1825, August 1995.

[RFC1826] Atkinson, R., “IP Authentication Header”, RFC 1826, August 1995.

[RFC1928] Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D., and Jones, “SOCKS Protocol Version 5”, RFC 1928, March 1926.

[RFC1970] Narten, T., Nordmark, E., Simpson, W., A., “Neighbour Discovery for IP version 6 (IPv6)”, RFC 1970, August 1996.

[RFC1971] Thomson, S., Narten, T., “Ipv6 stateless address autoconfiguration”, RFC1971, August 1996.

[RFC2002] Perkins, C., E., “(ed.) “IP Mobility Support”, RFC2002, proposed standard. IETF Mobile IP Working Group, Oct., 1996.

[RFC2003] Perkins, C., “IP encapsulation within IP”, RFC2003, October 1996.

[RFC2004] Perkins, C., “Minimal encapsulation within IP”, RFC2004, October 1996.

[RFC2138] Rigney, C., Rubens, A., Simpson W., and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[RFC2267] Ferguson, P., Senie, D., “Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing”, RFC 2267, January 1998.

[RFC2344] Montenegro, G., “Reverse Tunnelling for Mobile IP”, RFC 2344, May 1998.

[RFC2468] Aboba, B., Beadles, M., “Network Access Identifier”, RFC 2486, January 1999.

[SeBa97] Seshan, S., Balakrishnan, H., Katz, R., H., “Handoffs in Cellular Wireless networks: The Daedalus Implementation and experience”, Wireless Personal Communications, Vol. 4, pp. 141 – 162, 1997.

[Whi97] White, P., P., “RSVP and Integrated Services in the Internet: A Tutorial”, IEEE Communications Magazine, May 1997.

[WoLe96] W. Woo, V.C.M. Leung, “Handoff enhancement in mobile-IP environment”, Annual International Conference on Universal Personal Communications, pp. 760 - 764, 1996.

11.2 By category

In this section the “by alphabet’ listed references are categorised into different types, i.e., Internet drafts, RFCs and reports & articles.

11.2.1 Internet drafts

[Bra96] Braden, R., et. al., “Resource reaservation Protocol (RSVP) – Version 12 Functional specification”, Aug. 12, 1996. Available via http://www.ietf.org/html.charters/intserv-charter.html.

[draft-ietf-ipngwg-ipv6-spec-v2-00.txt] Deering, S., E., Hinden, R., M., “ Internet protocol version 6 (IPv6) specification”, Internet-Draft, draft-ietf-ipngwg-ipv6-spec-v2-00.txt, July 1997. Work in progress.

[draft-calhoun-diameter-07.txt] Calhoun, Rubens, “DIAMETER”, Internet draft, draft-calhoun-diameter-07.txt, Work in progress, November 1998.

[draft-ietf-aaa-roamops-auth-req-00.txt] Calhoun, P. R., Zorn, G., “Roamops Authentication/Authorisation Requirements”, Internet draft, draft-ietf-aaa-roamops-auth-req-00.txt, Work in progress, March 1999.

[draft-hiller-3gwireless-00.txt] Hiller, T., (editor) “3G Wireless Data Provider Using Mobile IP and AAA”, Internet draft, draft-hiller-3gwireless-00.txt, Work in progress, March 1999.

[draft-chuafoo-mobileip-rafa-00.txt] Foo, S., F., Chua, K., C., “Regional Aware Foreign Agent (RAFA) for Fast Local Handoffs”, Internet draft, draft-chuafoo-mobileip-rafa-00.txt, Work in progress, November 1998.

[draft-teoyli-mobileip-mvpn-02.txt] Teo, W., T., Li, Y., “Mobile IP extension for Private Internet Support (MPN)”, Internet draft, draft-teoyli-mobileip-mvpn-02.txt], Work in progress, 1999.

[draft-vallko-cellularip-00.txt] Valko, A., Cambell, A., Gomez, J., “Cellular IP”, Internet draft, draft-vallko-cellularip-00.txt, Work in progress, November 1998.

[draft-ramjee-micro-mobility-hawaii-00.txt] Ramjee, R., LaPorta, T., Thuel, S., Varadhan, K., “IP micro-mobility support using HAWAII”, Internet draft, draft-ramjee-micro-mobility-hawaii-00.txt, work in progress, February 1999.

[draft-ietf-mobileip-spectun-00.txt] Perkins, C., Johnson, D., B., “Special Tunnels for Mobile IP”, Internet draft, draft-ietf-mobileip-spectun-00.txt, Work in progress, November 1997.

[draft-ietf-mobileip-ipsec-use-00.txt] Zao, J., K., Condell, M., “Use of IPSec in Mobile IP”, Internet draft, draft-ietf-mobileip-ipsec-use-00.txt, Work in progress, November 1997.

[draft-ietf-mobileip-regkey-00.txt] Perkins, C., Johnson, D., B., “Registration Keys for Route Optimisation”, Internet draft, draft-ietf-mobileip-regkey-00.txt, Work in progress, November 1997.

[draft-ietf-mobileip-challenge-01.txt] Perkins, C., E., Calhoun, P., R., “Mobile IP Challenge/Response Extensions”, Internet draft, draft-ietf-mobileip-challenge-01.txt], Work in progress, May 1999.

[draft-jacobs-mobileip-pki-auth-02.txt] Jacobs, S., “Mobile IP Key Bassed Authentication”, Internet draft, draft-jacobs-mobileip-pki-auth-02.txt, Work in progress, march 1999.

[draft-ietf-mobileip-mn-nai-01.txt] Calhoun, P., R., Perkins, C., E., “Mobile IP Network Address Identifier Extension”, Internet draft, draft-ietf-mobileip-mn-nai-01.txt, Work in progress, May 1999.

[draft-ietf-mobileip-nai-wn-00.txt] Aravamudhan, L., O'Brien, M., R., Patil, B., "NAI Resolution for Wireless Networks", Internet draft, draft-ietf-mobileip-nai-wn-00.txt, Work in progress, February 1999.

[draft-calhoun-diameter-mobileip-01.txt] Calhoun, P., R., Rubens, A., C., "DIAMETER Reliable Transport Extensions", Internet draft, draft-calhoun-diameter-mobileip-01.txt, Work in progress, February 1999.

[draft-fhns-rsvp-support-in-mipv6-00.txt] Fankhauser, G., Hadjiefthymiades, S., Nikaein, N., "RSVP Support for Mobile IP Version 6 in Wireless Environments", Internet draft, draft-fhns-rsvp-support-in-mipv6-00.txt, November 1998.

[draft-ietf-rsvp-tunnel-04.txt] Terzis, A., Krawczyk, J., Wroclawski, J., Zhang, L., "RSVP operation over IP tunnels", Internet draft, draft-ietf-rsvp-tunnel-04.txt, May 1999. Work in progress.

[draft-ietf-mobileip-ipv6-07.txt] Johnson, D., B., Perkins, C., "Mobility Support in IPv6", Internet draft, draft-ietf-mobileip-ipv6-07.txt, Work in progress, November 1998.

[draft-ietf-mobileip-optim-08.txt] Perkins, C., Johnson, B., J., "Route Optimisation in Mobile IP", Internet draft, draft-ietf-mobileip-optim-08.txt, Work in progress, February 1999.

[draft-ietf-ipsec-auth-header-02.txt] Kent, S., Atkinson, R., "IP Authentication header", Internet-Draft, draft-ietf-ipsec-auth-header-02.txt, Work in progress, October 1997.

[draft-ietf-ipsec-esp-v2-01.txt] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", Internet-Draft, draft-ietf-ipsec-esp-v2-01.txt, Work in progress, October 1997.

[draft-ietf-ipsec-arch-sec-02.txt] Kent, S., Atkinson, R., "Security architecture for the Internet Protocol", Internet-Draft, draft-ietf-ipsec-arch-sec-02.txt, Work in progress, November 1997.

[draft-ietf-ipng-discovery-v2-00.txt] Narten, T., Nordmark, E., Simpson, W., A., "Neighbour Discovery for IP version 6 (IPv6)", Internet draft, draft-ietf-ipng-discovery-v2-00.txt, July 1997. Work in progress.

[draft-ietf-ipngwg-addrconf-v2-00.txt] Thomson, S., Narten, T., "Ipv6 stateless address autoconfiguration", Internet draft, draft-ietf-ipngwg-addrconf-v2-00.txt, July 1997. Work in progress.

[draft-montenegro-firewall-sup-03.txt] Montenegro, G., Gupta, V., "Firewall support for Mobile IP", Internet draft, draft-montenegro-firewall-sup-03.txt, January 1998. Work in progress.

11.2.2 RFCs

[RFC826]. Plummer, D., C., "An Ethernet address resolution protocol: Or converting network protocol addresses to 48.bit Ethernet addresses for transmission on Ethernet hardware", RFC 826, November 1982.

[RFC1256] Deering, S., (ed.), "ICMP Router Discovery Messages", RFC 1256, August 1989.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[RFC1541] Droms, R., "Dynamic Host Configuration Protocol", RFC 1541, October 1993.

[RFC1661] Simpson, W., (editor), "The Point-to-Point protocol (PPP)", RFC1661, July 1994.

[RFC1702] Hanks, S., Li, T., Farinacci, D., Traina, P., "Generic Routing Encapsulation over IPv4 networks", RFC 1702, October 1994.

[RFC1825] Atkinson, R., "Security Architecture for the Internet Protocol", RFC 1825, August 1995.

[RFC1826] Atkinson, R., "IP Authentication Header", RFC 1826, August 1995.

[RFC1928] Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D., and Jones, "SOCKS Protocol Version 5", RFC 1928, March 1926.

[RFC1970] Narten, T., Nordmark, E., Simpson, W., A., "Neighbour Discovery for IP version 6 (IPv6)", RFC 1970, August 1996.

[RFC1971] Thomson, S., Narten, T., "Ipv6 stateless address autoconfiguration", RFC1971, August 1996.

[RFC2002] Perkins, C., E., "(ed.) "IP Mobility Support", RFC2002, proposed standard. IETF Mobile IP Working Group, Oct., 1996.

[RFC2003] Perkins, C., "IP encapsulation within IP", RFC2003, October 1996.

[RFC2004] Perkins, C., "Minimal encapsulation within IP", RFC2004, October 1996.

[RFC2138] Rigney, C., Rubens, A., Simpson W., and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[RFC2267] Ferguson, P., Senie, D., "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing", RFC 2267, January 1998.

[RFC2344] Montenegro, G., "Reverse Tunnelling for Mobile IP", RFC 2344, May 1998.

[RFC2468] Aboba, B., Beadles, M., "Network Access Identifier", RFC 2486, January 1999.

11.2.3 Reports and articles

[AnBl96] Andreoli, G., Blefari-Melazzi, N., Listanti, M., Palermo, M., "Mobility management in IP networks providing real-time services", Proc., Annual International Conference on Universal Personal Communications, pp. 774 – 777, 1996.

[AzPa95] Aziz, A., Patterson, M., "Design and implementation of SKIP", available on-line at http://skip.incog.com/inet-95.ps, 1995.

[DiHe76] Diffie, W., Hellman, M., "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. 22, pp.644-654, November 1976.

[GeSo97] Geiger, R., L., Solomon, J., D., Crisler, K., J., "Wireless Network Extension Using Mobile IP", IEEE Micro, Vol. 17, No. 6, pp. 63-68, 1997.

[ING] Pras, A., (editor), "Project Proposal Telematics Institute: Internet Next Generation", available at http://ing.ctit.utwente.nl/background/public.pdf, 27 January 1999.

[JaRa98] Jain, R., Raleigh, T., Graff, C., Bereschinsky, M., "Mobile Internet Access and QoS Guarantees using Mobile IP and RSVP with Location Registers", ICC International Conference on Communications, Vol. 3, pp. 1690 – 1695, 1998.

[JaSi97] Jacobs, S., Cirincione, G., "Security of current Mobile IP solutions", Proc. of MILCOM'97, Vol. 3, pp. 1122-1128, 1997.

[KoDu98] Korpeoglu, I., Dube, R., and Tripathi, S., K., "Reducing Router-Crossings in a Mobile Intranet", Journal of Network and System Management, Vol. 6, No. 1, 1998.

[MaSi98] Mahadevan, I., Sivalingham, M., "An Architecture for QoS guarantees and routing in Wireless/Mobile Networks", ACM Intl. Workshop on Wireless and Mobile Multimedia, 1998.

[MOBIP] Charter of mobile IP working group, http://www.ietf.org/html.charters/mobileip-charter.html.

[MONET107] R2066/RMR/UNA2/DS/P/107/b1, "Recommendations of UMTS Integration Scenarios in the B-ISDN Backbone", December 1995.

[MoPa92] Mouly, M., Pautet, M. B., “The GSM system for mobile communications”, 1992.

[Per97] Perkins, C., E., “Mobile IP”, IEEE Communications Magazine, May 1997.

[Per98] Perkins, C., E., “Mobile networking through mobile IP”, IEEE Internet Computing, 1998.

[Raj97] Rajagopalan, B., “Mobility and quality of service (QoS) in the Internet”, Mobile Multimedia Communications, pp. 129 – 135, 1997.

[SeBa97] Seshan, S., Balakrishnan, H., Katz, R., H., “Handoffs in Cellular Wireless networks: The Daedalus Implementation and experience”, Wireless Personal Communications, Vol. 4, pp. 141 – 162, 1997.

[Whi97] White, P., P., “RSVP and Integrated Services in the Internet: A Tutorial”, IEEE Communications Magazine, May 1997.

[WoLe96] W. Woo, V.C.M. Leung, “Handoff enhancement in mobile-IP environment”, Annual International Conference on Universal Personal Communications, pp. 760 - 764, 1996.

12 Appendix: Patents on Mobile IP

This appendix provides the found patents in the area of Mobile IP mechanisms. These patents are searched using the Ericsson database (see http://patent-search.ericsson.se) that is based upon the Derwent Information World Patent index database. The used keywords during this search were "Mobile" and "IP". In order to minimise the searching activity, a proximity operator ADJ (ADJACENCY) has been used. This operator is used to retrieve documents that contain the second query term after the first query term in the same sentence.

12.1 Search results

The following search results on the keywords (mobile ADJ IP) were found.

Document	PAN 99-060780
Earliest priority date	13-Jun-1997
Derwent Title	System for coverage area with restricted mobility within specific DECT coverage areas arranges Internet protocol to effect mobility function for handling DECT information between DECT coverage areas, handling is based on Mobile Internetprotocol and voice switching based on voice over Internet technology
Patentee details	TELIA AB;(TELI)
Inventor names	Almgren, G.; Nycander, C.
Abstract	The system at a wireless tele or data communications network including DECT terminals for coverage area restricted mobility within their specific DECT coverage areas. An Internet protocol is arranged to effect a mobility function for the handling of DECT information between the DECT coverage areas. The mobility handling is based on a Mobile Internetprotocol (**Mobile IP**) and a voice switching based on voice over Internet technology. A DECT terminal in the **Mobile IP** corresponds to a proxy which towards Internet is experienced as an Internet telephony equipped computer.
Use Advantage	For providing system at a wireless tele or data communications system including DECT terminals for coverage areas restricted mobility within their specific DECT coverage areas. Effects mobility function for simple and cheap mobility between DECT coverage areas.
Title Terms	system cover area restrict mobile specific cover area arrange protocol effect mobile function handle information cover area handle based mobile voice switch based voice technology

Document	PAN 98-532432
Earliest priority date	

Derwent Title Roaming facility enabling mobile station to operate in another packet data network with incompatible routing establishes Foreign Agent to communicate with mobile and creates IP tunnel for data exchange with Home Agent of usual network

Patentee details TELEFONAKTIEBOLAGET ERICSSON L M;(TELF)

Inventor names Andersson, D.; Axelsson, U.; Baeckstroem, M.; Frid, L.; Olsson, U.; Pehrsson, A.

Abstract The communication systems include a facility to handle packet data, e. g. for internet access. Different networks use incompatible mechanisms to handle packet data transfers, e. g. **mobile IP** method (MIM) or PMM network. A mobile associated with the first network is provided with packet data capability and roams into a MIM based network. The normal voice based methods are used to establish a voice connection by identifying a home location and visitor registers. When the mobile requests packet data permissions, a "Foreign Agent" is established in the visited network and creates an IP tunnel to the home network.

Use Advantage Cellular mobile radio network. Allows mobile to roam across networks with incompatible packet data systems.

Title Terms facility enable mobile station operate packet data network incompatible route establish Foreign Agent communicate **mobile ip** tunnel data exchange Home Agent usual network internet protocol pdc

Document PAN 94-208967

Earliest priority date 29-Sep-1993

Derwent Title Scalable and efficient intra-domain tunnelling mobile IP scheme using mobile support border routers to determine on which network destination device is located

Patentee details SUN MICROSYSTEMS INC;(SUNM)

Inventor names Aziz, A.

Abstract

The system for a data processor to communicate with a mobile host data processor once the mobile is moved to and in communication with a second network uses a mobility support border router (MSBR) and a mobility support router (MSR) coupled to the first network. A second MSBR and MSR are coupled to the second network. The first host DP device sends a data packet to the first MSR which initiates a local search on the first network to determine if the MH data processing device is coupled to it. The first MSBR notifies the first MSR that the MH data processor is not coupled to that network and instructs the first MSR to tunnel the packet to the second MSBR. The second MSBR receives the packet and initiates a search on its network to determine if the device is in communication with it, and if so, it tunnels the packet to the second MSR and which sends it to the MH data processor.

Use Advantage

Improved inter-network packet transfer.

Title Terms

efficiency intra-domain tunnel **mobile ip** scheme mobile support border router determine network destination device locate