Internet Mobility Support

Teemu Rinta-aho

Helsinki 18.10.2001

Seminar on Internet Protocols

UNIVERSITY OF HELSINKI
Department of Computer Science

Contents

1 Introduction

Although networks offer access to local and global services, we usually expect to connect to the network at certain points like at office or home. The widespread use of mobile phones have changed the attitudes of people towards fixed-place working and social life. Many hand-held devices now offer Internet connectivity, and demand for mobile computing begins to rise.

If we can see that there is an analogy between the transition of the fixed telephone network to mobile phone networks and the transition of fixed Internet to mobile Internet, we can think what future consequences true mobile computing will have on working and future means of communication [Per98].

Internet is based on fixed addressing, where each host is identified and located with it's unique address. Internet Protocol (IP) is based on routing packets or datagrams independently of each other, and assuming that the host address tells in which subnetwork the host is located. This leads to the problem that the host must be in it's own subnetwork, or it can't be reached. Internet protocols have been developed during a long period of time and higher level protocols make assumptions on Internet addressing. As mobility wasn't a concern when developing the original Internet, a separate transparent mechanism for mobility support must be developed. This paper gives a brief description of mobility and the Mobile IP standard and mobility support in the next generation Internet where IP is replaced with IP version 6. Chapters 3 and 4 are mostly based on [Per99, JP00].

2 Mobility

2.1 Mobility vs. Portability

We already have portable computing and networking in widespread use today. Portability means that the host can attach to the network on multiple locations, but the difference to mobility is that possible ongoing network connections are disrupted when the host moves.

Truly mobile computing gives us the possibility to connect to the network all the time, even while moving. It can change the office work the way mobile phones have changed social lives. People no longer depend on their desktop computers – access to data and applications on the network can occur from anywhere.

2.2 Internet Addressing and Routing

Before the mobile networking can become widely used, there are still some technical problems that have to be solved. The biggest problem is the Internet Protocol itself, as it is designed for fixed networks. Internet addresses are associated with a location, and Internet routing is based on this fact. Addresses are also used for identification which is needed if the host is wanted to connect to. This scheme does not support mobility. There have been several proposals to overcome this problem. The Mobile IP standardization work has been going on at IETF and there are already several implementations of it. The next chapters will introduce this architecture and how it brings true mobility to the Internet.

3 Mobile IP

Current Internet Protocol version 4 assumes that the node's address both identifies the node and the node's attachment to Internet. Because of that, the node must be connected to the network at the point the IP address indicates. Otherwise the node can't be contacted with the regular Internet routing methods. A node can change its point of attachment but it also has to change its IP address to correspond to the network it is located to be able to communicate. Another method would be not to change the IP address but to propagate host-specific routes throughout the Internet routing fabric. If a node changes its address, all the upper layer connections have to be re-established, and the node can't be contacted with its old IP address(es) any more. If we would use host-specific routes, we would have to rebuild the whole Internet routing, and that is what nobody wants to do. Therefore a new mechanism is needed for mobile nodes to exist on the Internet.

3.1 Protocol Overview

Mobile Internet Protocol has the following requirements [Per99]:

- a mobile node must be able to move without changing its IP address,
- a mobile node must be able to communicate with hosts not implementing this protocol and
- all messages used for updates must be authenticated.

One important goal in designing of the protocol has been to minimize the amount of messages, as mobile nodes often have a wireless, error-prone link to the network and they operate on battery power.

It is also assumed that the mobile node does not generally change its point of attachment to the Internet more often than once per second. The Mobile IP protocol is designed for solving the "macro" mobility management and hand-over can be considerably longer than at the link layer. Mobile IP can handle moving across heterogenous media as well as homogeneous, for example from Ethernet to Ethernet or from Ethernet to Wireless LAN.

3.2 Terminology

3.2.1 Mobile Node

Mobile node is a host or a router that changes its point of attachment from one network to another. It can change its location without changing its IP address.

3.2.2 Home Agent

Home agent is a router on a mobile node's home network. It knows the location of the mobile nodes and captures and encapsulates the IP datagrams destined to the mobile node to the current care-of-address.

3.2.3 Foreign Agent

Foreign agent is a router on the foreign network which provides services to the visiting mobile nodes. It decapsulates the IP datagrams sent to it by the mobile node's home agent and delivers them to the mobile node. It can also act as the default gateway for the mobile node.

3.2.4 Home Address

Home address is the "permanent" IP address of an Internet host, assigned by the administration of the host's home network.

3.2.5 Care-of Address

Care-of address is the termination point of a tunnel towards a mobile node while it is away from it's home network. There can be two types of care-of addresses: a "foreign agent care-of address", which is the foreign agent's care of address the mobile node is registered to, and a "co-located care-of address", which is externally obtained, for example through DHCP.

3.3 Operation Overview

Mobile IP defines two support services: agent discovery and registration. Mobility agents (home and foreign agents) advertise their services by sending Agent Advertisement messages. A mobile node may send a Agent Solicitation message to solicit an Agent Advertisement message. When a mobile node receives an Agent Advertisement, it determines whether it is on its home network or a foreign network. If the mobile node is on its home network, it operates without mobility services, just like any other Internet host. If the mobile node still has a registration at its home agent, it de-registers by sending a Registration Request message to the home agent. If the mobile node detects that it is at a foreign network, it obtains a care-of address either from a foreign agent or externally, for example from DHCP. After that the mobile node registers its new care-of address with its home agent by sending a Registration Request, possibly via a foreign agent. After that, datagrams sent to the mobile node's home address are captured by its home agent and tunneled to its care-of address (either to the foreign agent or to the mobile node, depending on the setup), and finally to the mobile node (see Figure 1). Datagrams sent by the mobile node are delivered to their destination using standard IP routing, not necessarily passing through the home agent, but because of the ingress filtering used in almost all routers today, all the traffic goes through the home agent. Ingress filtering drops datagrams that have a source address which is not topographically correct, and no visiting node has such home address.

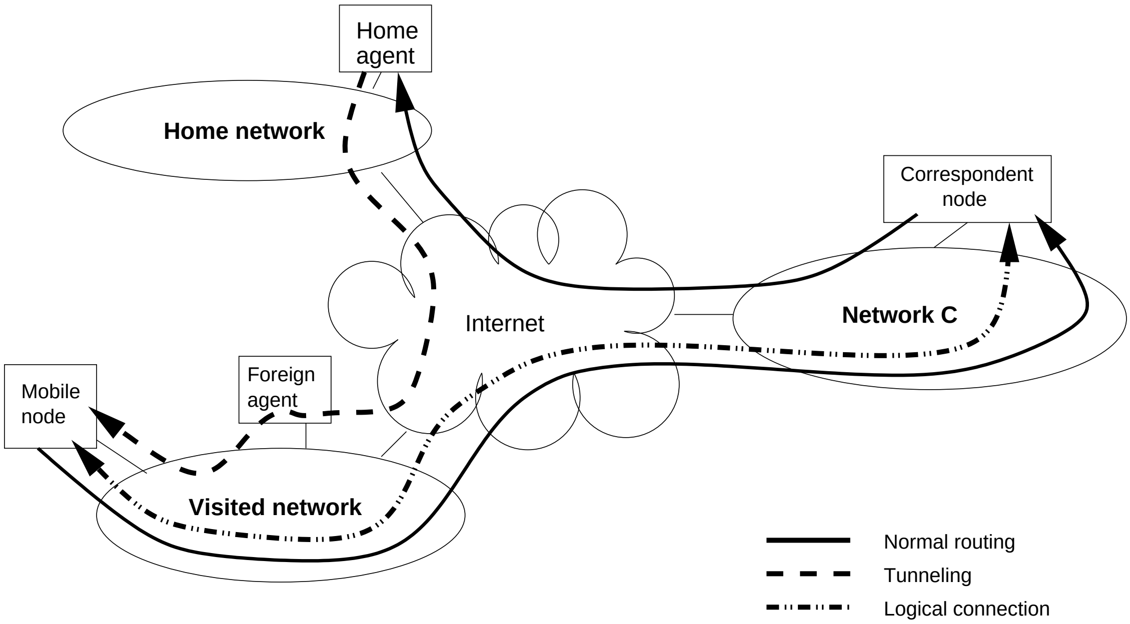

Figure 1: Mobile IP architecture

3.4 Message Format

Mobile IP defines a set of new control messages, sent with UDP, using a well-known port number 434. Currently there are two message types defined: Registration Request and Registration Reply. In addition, Mobile IP uses the existing ICMP Router Advertisement and Router Solicitation messages. Mobile IP defines a general extension mechanism to allow optional information to be carried by Mobile IP control messages or ICMP Router Discovery messages. All the extensions but one are encoded in a Type-Length-Value format. The end of the list of extensions is indicated by the total length of the IP datagram.

3.5 Agent Discovery

Agent discovery is the method by which a mobile node detects whether it is located at its home network or at a foreign network, or whether it has moved from a foreign network to another. A foreign agent care-of address can be also obtained through the agent discovery.

Mobile IP uses ICMP Router Discovery with extensions for Agent Discovery. An

Agent Advertisement is a ICMP Router Advertisement message extended with the Mobility Agent Advertisement Extension. The Agent Solicitation message is identical to the ICMP Router Solicitation except that its IP Time To Live field is set to 1.

No authentication is required for advertisement or solicitation messages although they may be authenticated by using the IP Authentication Header.

3.6 Registration

Mobile nodes use the registration mechanism to request forwarding services while at a foreign network, inform their home agent of the current location, renew a registration which is close to expiration and to de-register after returning to home network. A mobile node can also maintain multiple registrations so that each datagram is copied to each of its care-of addresses. The registration mechanism can also be used to determine the IP address of the home agent.

Registration can be done in two different ways, either via a foreign agent that forwards the registration to the home agent or directly with the home agent. If the mobile node is registering with a foreign agent care-of address, or it has a co-located care-of address, but the foreign agent informs to register via it, it must register via that foreign agent. Otherwise it can register directly to home agent.

When registering via a foreign agent the following four messages are required:

- the mobile node sends a Registration Request to a foreign agent,
- the foreign agent processes the Registration Request and then relays it to the home agent,
- the home agent sends a Registration Reply to the foreign agent to grant or deny the Request and
- the foreign agent processes the Reply and then relays it to the mobile node.

If the mobile node registers directly with its home agent, it sends a Request and receives a Reply directly from the home agent.

Each mobile node and mobility agent must support mobility security associations between the mobile entities. Registration messages between a mobile node and its home agent are authenticated with the Mobile-Home Authentication Extension.

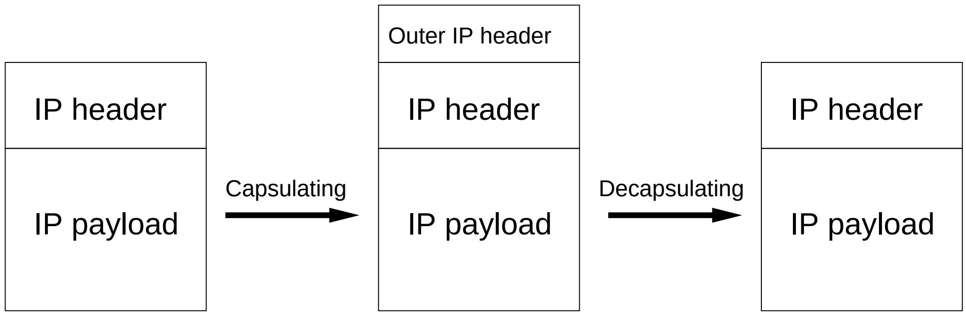

Figure 2: IP tunneling

The Authenticator field in the Authentication Extension protects the registration message. The default authentication algorithm uses keyed-MD5 in "prefix+suffix" mode to compute a 128-bit message digest of the registration message, so the default authenticator is a 128-bit MD5 checksum over the shared secret shared by the nodes, the protected fields from the registration message and the shared secret again.

The Mobile-Foreign Authentication Extension is not necessarily required in Requests and Replies between the mobile node and the foreign agent.

3.7 Routing Considerations

All mobility agents and mobile nodes using co-located care-of addresses must support IP in IP encapsulation (see Figure 2). Minimal encapsulation and GRE encapsulation may optionally be used.

A router can also be mobile. This gives a possibility for mobile networks, which in turn may also have visiting nodes. A practical implementation might be a mobile network on an airplane, a ship or a train. Mobile routers themselves are no special cases in the Mobile IP protocol, they operate the same as any mobile nodes except that they forward datagrams and may also act as foreign agents.

3.7.1 Unicast

Mobile node operates as any fixed node when it is at its home network – all datagrams are routed normally. When the mobile node is at a foreign network it chooses the default router either by using its foreign agent as a first-hop router or some other router learned from a received ICMP Router Advertisement message. Mobile nodes can not broadcast ARP packets into a foreign network. Mobile IP protocol does not specify how the mobile node can get the MAC address of a router. Similarly, a foreign agent can't use ARP for a mobile node's MAC address on a foreign network. It can obtain the MAC address for example from an Agent Solicitation or a Registration Request.

The home agent intercepts datagrams destined to the mobile node's home address while the mobile node is at a foreign network. Home agent may use proxy and gratuitous ARP for interception. Proxy ARP means an ARP reply sent by one node on behalf of another, while gratuitous ARP is a packet that updates other nodes' ARP caches. By changing the mobile node's MAC address in ARP caches to its own, the home agent will receive IP packets destined to the mobile node. This is a non Mobile IP specific security threat in all Local Area Networks. IPv6 has a better solution that replaces ARP.

Nodes implementing tunneling should also implement the "tunnel soft state" mechanism, which is used to relay the ICMP error messages coming from the tunnel to the original sender of the datagram.

3.7.2 Broadcast

The home agent only forwards broadcast datagrams if the mobile node has requested such service. Depending on the type of care-of address used, home agent uses one of the following methods to tunnel a broadcast datagram:

- If the mobile node is using a co-located care-of address, the home agent tunnels the datagram normally directly to the mobile node.
- If the mobile node is using a foreign agent care-of address, the home agent first encapsulates the broadcast datagram into a unicast datagram destined to the mobile node's home address, then it tunnels this datagram to the foreign agent. This mechanism is necessary for the foreign agent to know which mobile node it should forward the datagram. Then the mobile node must decapsulate the original broadcast datagram.

3.7.3 Multicast

A mobile node may join a multicast group via a local multicast router on the foreign network, if there is a multicast router available. If the mobile node is using a co-located care-of address, it should use that address as a source of its IGMP messages, otherwise it may use its home address.

If there is no multicast router on the visited network, the mobile node may join a multicast group with its home agent, if the home agent is a multicast router. The multicast datagram forwarding works identically with the broadcast datagram forwarding described earlier. All IGMP messages go through the home agent, and the multicast datagrams come through the same tunnel. If the mobile node wants to send a multicast datagram directly on a foreign network, it must use a co-located care-of address, and if it sends it through the home agent, it must use its home address as the source address.

3.7.4 Route optimization

Having a home agent routing datagrams destined to a mobile node presents an unoptimal routing graph between a correspondent node and a mobile node, especially if the home agent is far away from the shortest route between the communicating nodes. Consider if the mobile node wants to communicate with a node that is in the visited network. Then every packet the correspondent node sends, will go out of the network all the way to the home agent, and then back to the network to the mobile node. If the home agent is on the other side of the planet, that can become a performance bottleneck. If the correspondent node supports Mobile IP, the mobile node can send it a binding update and it can start sending packets directly to the mobile node's care-of address instead of its home address. When a mobile node moves it must send binding update messages to all nodes it is communicating with, to keep their bindings up-to-date. Route optimization is not an official part of the Mobile IP protocol, but is widely used in many implementations [PJ99].

3.8 Security Considerations

Mobile nodes are often connected to the network via wireless links, therefore threats to security are even more greater than on conventional, static, wired networks. Especially, if unauthenticated, the Mobile IP registration protocol is vulnerable to unauthorized traffic redirection. Therefore all control messages between mobile nodes and home agents are authenticated.

Mobile IP uses authentication extensions in Registration Requests and Replies between the home agents and mobile nodes. The default algorithm is MD5 with a 128-bit key in "prefix+suffix" mode (see 3.6). Although MD5 is a minimum requirement, other kind of security models may also be optionally supported.

Messages with the foreign agent are not required to be authenticated, mostly because of the lack of a network key management protocol. In commercial networks authenticating visiting users is important if anonymous access is not what is decided. Mobile IP does not itself offer a solution to this problem.

To achieve privacy, encryption has to be used. Using IPSec ESP header is one way to implement encryption. Mobile IP does not offer special support for encryption. Location privacy can be achieved by tunneling all mobile-node-originating datagrams through the home agent. That way it is difficult to observe where the mobile node is located, as all datagrams seem to originate from the home network.

Timestamp and optionally nonces are used for replay protection in Registration Requests. A nonce is a 32-bit pseudo-random number. The value of a timestamp or a nonce is copied from a Request to the Reply to avoid replay attacks.

4 Mobility in IPv6

The next version of Internet Protocol, IPv6, offers not only a larger, 128-bit address space, but also other improvements which help also in supporting mobility. All IPv6 nodes will have a built-in support for host bindings, so route optimization will work with all connections. In IPv6 source routing will be used instead of tunneling. IPv6 also has a better support for security with the AH and ESP modes [DH98].

4.1 Comparison with Mobile IPv4

The design of the Mobile IPv6 is based on experiences received from Mobile IPv4. The Mobile IPv6 design work has also affected the on-going development of IPv6 itself, making them work more seamlessly [JP00].

Mobile IPv6 is in many ways similar to the Mobile IPv4, but it is fully integrated into IPv6 and has many improvements. The major ones are:

- Support for route optimization is built into IPv6. This feature disables what was known in IPv4 as "triangle routing".
- Mobile nodes use the care-of address as a source address instead of the home address. This allows the operation in networks behind routers performing ingress filtering. It also simplifies the routing of multicast datagrams.
- Foreign agents are no longer needed, mobile nodes can operate in any network without any special support. The IPv6 address is usually obtained through Address Autoconfiguration [TN98].
- IPsec is used for security.
- The movement detection mechanism prevents a common situation in wireless networks where the router can reach the mobile but the mobile can't reach the router and the mobile node starts searching a new router without removing the registration from the old one. This is also known as the "black hole" situation.
- The IPv6 Routing Header is used instead of IP encapsulation.
- The home agent uses IPv6 Neighbor Discovery [NNS98] instead of ARP to capture packets destined to mobile node.
- Because of using the Routing Header and the ICMPv6, the "tunnel soft state" management is no longer needed.
- IPv6 anycast is used instead of the broadcast to find a home agent.
- There is a new Advertisement Interval option for the mobile nodes to decide themselves how many Router Advertisements they can miss before searching a new router.
- Using IPv6 Destination Options allows all MIPv6 control traffic to be sent along (piggypacked) with any IPv6 packets and no separate UDP packets are needed as in MIPv4.

4.2 Protocol Overview

The Mobile IPv6 protocol operation is closely related to that of Mobile IPv4. While the mobile node is at its home network, it operates as any IPv6 node. While the mobile node is away from home, it registers one of its care-of addresses with a router on its home network, and requests this router to be its home agent. A home agent keeps a list of Mobile Bindings, which relate the mobile node's home address with a care-of address. A binding registration is done by sending a packet with a Binding Update destination option, and the home agent replies by sending a packet with a Binding Acknowledgement destination option. After that, the home agent uses proxy Neighbor Discovery to capture the datagrams destined to mobile node's home address and tunnels them to the registered care-of address using IPv6 encapsulation.

If the mobile node does not know the address of its home agent or the home agent is replaced while the mobile node is at a foreign network, it uses Dynamic Home Agent Address Discovery by sending an ICMP Home Agent Address Discovery Request to the "Mobile IPv6 Home-Agents" anycast address with its own home network subnet prefix. That causes one of the home agents to reply to the mobile node with a list of home agents.

Mobile IPv6 nodes also send Binding Update destination options to the correspondent nodes to tell their new care-of address. Therefore mobile nodes keep a list of ongoing connections to other nodes with information when was the last Binding Update for this node sent and other type of management data.

4.3 New IPv6 Message Types

Mobile IPv6 defines four additional IPv6 destination options and two new ICMP message types.

Because the source addresses of datagrams a mobile node sends from a foreign network is always the care-of address, the home address is included in the *Home Address* destination option, which all IPv6 nodes place to the source address field before passing the packet to upper layer protocols to maintain mobility transparency.

The *Binding Update* option is used by a mobile node to inform a correpondent node or its home agent of its current mobility binding. If a packet includes a Binding Update option, it must also include a IPsec AH or ESP header.

The *Binding Acknowledgement* option is used as a reply to a Binding Update, if an acknowledgement was requested. The use of this option also requires the use of an AH or ESP header.

The *Binding Request* option is used to request a Binding Update from a mobile node. This can be sent when a mobility binding is close to expiration. No authentication is required for this option.

The ICMP *Home Agent Address Discovery Request* is used by a mobile node to find the addresses of home agents at its home network. The ICMP *Home Agent Address Discovery Reply* contains a list of the home agents at mobile nodes home network.

4.4 Correspondent Node

A correspondent node is any node communicating with a mobile node. It can be itself fixed or mobile, or a home agent.

Packets sent by a mobile node almost always contain a home address option. When any node receives such packet, it must copy the address from the home address option to the IPv6 header. If a packet contains a Binding Update option, it must be validated, and the Binding Cache updated by deleting any existing bindings for this mobile node and storing a new entry with the given care-of address. If the Binding Update option has the Acknowledge flag set, the correspondent node must send a Binding Acknowledgement option back to mobile node.

If an entry in the Binding Cache expires, it is removed, and further packets destined to mobile node will go through the mobile node's home network until a new Binding Update is received. A correspondent node can send a Binding Request to a mobile node of which mobile binding is to expire soon.

If the correspondent node has a mobile binding in its cache for a mobile node, any packets sent to the mobile node that cause an ICMP error message will be sent directly to the correspondent node. If the packet is sent via the home agent, and the ICMP error message is caused when the packet is in the tunnel from home agent to mobile node, the ICMP error messages are sent to the home agent which then relays certain messages to the correspondent node.

4.5 Home Agent

Each home agent on a network receive information on other home agents by receiving periodically sent Router Advertisement messages and keep their home agents lists up to date. When a home agent receives an ICMP Home Agent Address Discovery anycast message, it replies with a reply message containing the list of the home agents.

When receiving a Binding Update option requesting the router to be a home agent for the mobile node who sent the message. If the Binding Update is accepted, the home agent creates an entry to its Binding Cache, setting the mobile nodes home address from the Home Address option, and the care-of address from the Alternate Care-of Address sub-option, if present, otherwise the care-of address will be from the IPv6 header's source address field. Then the home agent will send a Binding Acknowledgement, if requested. Also when receiving a Binding Update requesting the removal of binding, the home agent must remove the entry for that mobile node in its binding cache.

When a node is serving as a home agent for a mobile node, it must intercept the packets addressed to the mobile node's home address and tunnel them to the registered care-of address. The home agent is using both proxy and gratuitous Neighbor Discovery for packet interception. The packets will be tunneled using IPv6 encapsulation.

4.6 Mobile Node

When the mobile node is away from its home and is sending IP packets, the Mobile IP modifies the packets from applications by adding a Home Address option with the home address, and putting the care-of address to the IP header's source address field. For short-term communication the mobile node can use its care-of address without the Home Address option. This gives less overhead when using for example DNS queries.

When outbound packets are processed, they are compared to the IPsec Security Policy Database to determine what processing is required for the packet. Binding Updates and Binding Acknowledgements are always protected with either AH or ESP header. IKE is used as the default key management protocol.

While away from home, a mobile node can receive packets either from a correspondent node via a home agent, directly from a correspondent node with a Binding Cache entry for the mobile node or from a correspondent node which has an outdated care-of address in its Binding Cache. If the packet goes to an old care-of address, and the default router has the mobile node's new care-of address, it tunnels the packet to the new care-of address.

When the mobile node is moving from a network to another, it detects the movement primarily from the received Agent Advertisement messages. It must sent Binding Updates to its home agent and all correspondent nodes after getting a new care-of address. It can also send a Binding Update to a home agent in its previous visited network to allow packet forwarding from old to new care-of address.

When the mobile node returns to its home network, it must send a Binding Update to its home agent requesting a deregistration and multicast a Neighbor Advertisement message to advertise its own link-layer address as the destination of its home IP address.

5 Future Work

The IETF Mobile IP working group has developed a routing support for mobile nodes in both IPv4 and IPv6 networks. Both protocols are still under development and are defined only as Internet drafts, so they are subject to change. The Mobile IP working group is focusing on deployment of Mobile IP and to find solutions to remaining problems and shortcomings. The mobile phone industry is considering to use Mobile IP for wireless data and the Mobile IP working group is developing the protocols to work with GPRS, UMTS, CDMA2000 etc. The working group identifies its short-term future work to be [IET00]:

- Use of Network Address Identifiers to identify mobile users/nodes.
- Specifying how Mobile IP should use AAA functionality to support inter-domain and intra-domain mobility.
- Evolve the security framework/trust model for mobile nodes.
- Develop solutions for IPv4 private address spaces for the scenarios needed for deployment.
- Documenting any requirements specific to cellular/wireless networks.

In the longer term, the working group needs to address:

- Additional IP-based solutions for micro mobility (movement within a subnet).
- QoS in the mobile IP environment using diff-serv and/or int-serv/RSVP.
- Location Privacy.

6 Conclusions

We can see that mobile communication is becoming more and more important. It is also important that the existing applications which don't know anything about mobility can still be used. Mobile IP and Mobile IPv6 offer a solution to the mobility problem in Internet. As Internet access is becoming necessary in almost every mobile terminal in the future, the future mobile networks may directly support Mobile IP. There are still many problems to be solved before we can globally roam from one IP network to another, especially on the security and the AAA area. Ad-hoc networking is also one important and interesting issue which brings new problems into mobility. Free implementations of Mobile IP have been done for example at Sun Microsystems [SUN00], Helsinki University of Technology [HUT00] and National University of Singapore [NUS00].

References

DH98 S. Deering and R. Hinden. Internet protocol, version 6 (ipv6). Rfc 2460, IETF, Dec 1998.

HUT00 HUT. Dynamics - hut mobile ip. WWW, Feb 2000. http://www.cs.hut.fi/Research/Dynamics/.

IET00 IETF. Ietf ip routing for wireless/mobile hosts (mobileip) www-charter. WWW, Feb 2000. http://www.ietf.org/html.charters/mobileip-charter.html.

JP00 D. Johnson and C. Perkins. Mobility support in ipv6. Internet draft, IETF, Jan 2000. draft-ietf-mobileip-ipv6-10.txt.

NNS98 T. Narten, E. Nordmark, and W. Simpson. Neighbor discovery for ip version 6. Rfc 2461, IETF, Dec 1998.

NUS00 NUS. Mobile ip at nus. WWW, Feb 2000. http://mip.ee.nus.edu.sg/.

Per98 C. Perkins. Mobile networking through mobile ip. *IEEE Internet Computing*, Jan 1998.

Per99 C. Perkins. Ip mobility support for ipv4, revised. Internet draft, IETF, Oct 1999. draft-ietf-mobileip-rfc2002-bis-00.txt.

PJ99 C. Perkins and D. Johnson. Route optimization in mobile ip. Internet draft, IETF, Feb 1999. draft-ietf-mobileip-optim-08.txt.

SUN00 SUN. Mobile ip for solaris/linux. WWW, Feb 2000. http://playground.sun.com/pub/mobile-ip/.

TN98 S. Thomson and T. Narten. Ipv6 stateless address autoconfiguration. Rfc 2462, IETF, Dec 1998.