IP mobility techniques compared

Joonas Kekoni
Helsinki University of Technology
Telecommunication programming and multimedia laboratory
jkekoni@cc.hut.fi

Abstract

In traditional IP network IP address has both the meaning of network locater as well as host identity. This paradigm is fundamentally incompatible with mobility, with exception of data link layer mobility, such as WLAN and GPRS.

Mobile IP, LIN6 and HIP work all work a similarly. DNS contains static identity of a host and IP of an agent or agents used for mobility. The name and form for the identity as well as name of the agent differ from protocol to another.

The mobility agent will just forward the 1st packet to the mobile host and after the reply arrives the communication continues directly. If it is not supported then tunneling is used.

Mobile IP only supports one mobility agent. LIN6 uses different identity for different interfaces. HIP uses not only numeric identity, but cryptographic one that is meant not only for mobile hosts, but others as well, for all the hosts both IPv4 and IPv6 allowing mobility between.

Mobile IP is the most established. HIP is newest, but supports features beyond just mobility. LIN6 has only one implementation.

I think HIP and mobile IP are equally strong due to the fact that mobile IP is more established and HIP is more advanced. It is also possible that no IP mobility techniques will be widely adopted.

I have also analyzed multi homing only protocols (SCTP,TCP/mh and MAST) as well as historical attempts to IP mobility (DNS, Real time extensions to DNS) and application level mobility.

KEYWORDS: Ip mobility, Mobile IP, TCP/mh, MAST, HIP, LIN6, WLAN, GPRS, MIPv4, MIPv6.

1 Introduction

In this paper I am comparing a wide range of techniques that are used to add mobility support into IP-networks. I am comparing their advantages as well as disadvantages and try to see benefits as well as weaknesses. I have divided the protocols to data link layer protocols, applications layer protocols and IP protocols with static IP addresses and IP protocols with dynamic IP addresses. The normal way to divide those protocols might have been attempt to use OSI reference model for classification of the protocols. I have by purpose not done so, because I the functionality is often similar, event they layers are not same. Therefore I do not see the benefit for such a classification.

2 What I mean by mobility

I have defined host mobility with three different terms, not all of them are important for all uses. I have not seen these described separately with their own terms in any other paper, so I had to invent my own terminology for differentiation between these different aspects of mobility.

1. Identifiability: Connecting host can be identified as itself in different network locations. In traditional IP network this is done using reverse DNS lookup. This is the least important part and is only used by access logs and host based access control.

2. Connectibility: The host is also connectible after it has been moved from network to another. In traditional IP network this has been accomplished by DNS lookup.

3. Unbreakability: Those clients and server that are located in a node must be able to keep their network servers or clients working seamlessly, even when they are moved from one network to another. In traditional IP network TCP connections are not movable, but tied into a single network address during connection negotiation.

For other terminology I have used Mobility Related Terminology by IETF.[1]

This paper I am dealing only conventional mobility, where the network is static and the hosts are mobile. I will not deal networks that are constructed from mobile nodes that also work as routers.

2.1 The basic problem

In traditional IP networks IP addresses describes both the identity of the host and the location of the host in the network[2]. Unfortunately this paradigm is fundamentally incompatible with mobility, with the exception of data link layer mobility, where the physical location is decoupled from the logical location and therefore the logical location can act only as identity, and application layer mobility, where the application software is taking care of the mobility.

In addition TCP connections are done based on IP addresses, so they cannot be migrated from a one address to another. They cannot be migrated even from one network interface of a computer to another interface in the very computer. UDP also sends datagram's to addresses that are specified by IP addresses. These addresses usually originate from DNS lookup, so even UDP is connectionless the protocols usually work more or less connection like.

This means that the IP protocol stack needs to be changed in order to support mobility independent from specific applications, or from specific networking techniques.

3 Application layer mobility

Application layer mobility means that we have applications, which are able to decouple session from TCP connections, which may be disconnected on handover from a network to another.

Example: Web browser

Web browser maintains session using cookie string that is used to mark the session. This allows the session to be independent from the TCP connection that is used to transfer the traffic.[5]

This does not allow identifiability of the mobile host, but server applications are usually more likely to identify the users, than their computers.

Like web browsers these usually allows unbreakability, but neither identifiability nor connectibility.

Connectibility could be accomplished by using a non mobile middleman such as socks proxy.

4 Data link layer mobility

Data link layer mobility means that we can keep a host logically in the same network, but still move the host physically from place to another.

This allows all the benefit of the mobility, within that network, without any ip mobility technique used.

4.1 Mobility over simple data link protocol (WLAN)

Example: If we have multiple access points on the same network segment, we can move a node from one place to another transparently, without changing it's IP address.[3] I want to put emphasis that network segment can be extended over single physical location by using some tunneling technique.

However if a host is moving from one access point in one network to another access point inside another network, this cannot be worked with WLAN mobility alone, but a higher layer technique needs to be used. [3]

WLAN handover criteria is not part of WLAN specification, but vendor dependent. [3]

4.2 Mobility using routing data link layer protocol (GPRS)

IP can be used over a mobile routing network technique, such as GPRS/GSM or GPRS/D-AMPS. If the networking technique below Datalink layer of IP, such as GPRS, provides mobile routing, it is possible to offer mobility using the mobility of the lower layer, without having mobility on the IP layer or above. [4]

5 Multi homing

Multi homing techniques allow hosts with multiple network adapters to have their connections to be independent from single network adapter, as unlike with standard TCP. This usually doubles with unbreakability, which is the ability to move connections from one network to another using the same adapter.

However it is technically possible that this is not take case, as we later see when LIN6 is introduced.

So generally these techniques offer unbreakability, but without other aspects of mobility.[21]

5.1 TCP/mh and SCTP

These protocols allow mobile host to announce new IP addresses for existing connections in case the old connections break. These extensions however make in impossible to move a connection to other network after all connections are broken and reconnected with new IP addresses. [22]

SCTP also offers a multitude of services and is intended both as carrier for PSTN signaling traffic and as generic connection oriented reliable datagram service.[22]

TCP/mh is only the multi homing part of SCTP as an extenssion to a standard TCP.[21]

These offer make before break unbreakability, when supported on both ends. In case of SCTP, SCTP needs to be known by both ends in order to communicate at all, whereas TCP/mh is backward compatible with TCP, but naturally without support for multi homing.

These could be used to supplement other mobility techniques, such as real time DNS.

SCTP makes sense also for other reasons than multi homing and multi homing is not actually even its main focus.

5.2 MAST

This does in essence the same thing than TCP/mh, but this creates it's own simple protocol, between TCP or UDP and IP.

What this does that the prior ones do not, MAST protocol supports rendezvous using DNS. So it is possible to negotiate a new connection to network after the prior break and move the existing connections to that one, whereas the prior techniques require new IP addresses to be added to existing connections, when they are still alive.

Because MAST resides above IP, so it is also possible to run UDP on top of it. [23]

6 IP mobility without fixed IP addresses

These techniques, work so that the IP address of the host are changed when host is moved from network segment to another. Therefore the identity that is used to identify computer is decoupled from IP addresses.

6.1 Limited mobility based on standard DNS

Normally DNS is used to create mapping between DNS names and IP addresses.[7] Mainly the idea is that humans remember names better than addresses and that it is possible to change move computers from physical location to another or from ISP to another and still maintain original name.

Since moving from one place to another requires computers to be powered down and moved to new location these kinds of movements require downtime so the delays caused by DNS TTL's are not entirely unacceptable.

This allows connectibility, but with downtime cause by caching. If the DNS TTL's are shortened then the down times related to connectibility are shortened, but this will increase the load caused by DNS traffic. [26]

There are services for hosts to automatically update DNS changes such as "dyndns.org", generally they are used to support some kind of connectibility to home computers that are behind DHCP pools and therefore have chancing IP addresses.

Generally these services do no have reverse mapping at all, so they do not offer indentifiability without application level protocol support, such as TLS.

DNS based mobility only allows connectibility and perhaps identifiability, but not unbreakability. Even connectibility is newer instant, but the mirragration time can be configured to be moderate.

Dyndns providers, such as "dyndns.org" do not offer reverse DNS.

Unbreakablity is not provided by this kind of service, but a multihoming protocol such as TCP/mh or SCTP or MAST could be used for that.[7]

6.2 Mobility by extended "REALTIME" DNS

Basicly this could allow the same things that normal DNS mobility, but this will allow the updates to happen more or less quickly, by actively flushing the caches. Naturally this comes with the price that the entire DNS tree needs to support this kind of extended DNS. This would also add load to the root servers, because all the moving hosts had to be updated to root-server, every time they are moved. [25]

Unbreakablity is also not provided by this kind of service, but TCP/mh or SCTP could be used for that.

According to one estimate it would take about five seconds to update the authorative DNS chain. However the price to pay is that "sophisticated name server hierarchy that can provide load balancing while minimising the amount of messaging (although there is a trade-off between these two)"[26] is needed.

According to the dates I have seen on most of these papers it looks like that the idea has already been abandoned a while ago in favor of routing based solutions.[25] I was able to find papers and proposals about this subject, but I did not find any software.

6.3 Host Identity Protocol HIP

HIP adds a new host identity layer between networking layer and session layer. This host identity layer decouples IP addresses from host identity. All applications are supposed to use host identity in place of IP addresses, that are used as host locations and have the HIP layer to take care of mapping between the host identity to IP addresses.

Host identity is realized as public/private key pairs. That host identity does not only act as decoupler between internetworking layer and transport layer, but also provides authentication of hosts. [16]

Host identity as well as information about the rendezvous server are stored into DNS, since they are static. [16]

Host identifier are newer part of transfer, but they are represented by 128 bit host identity tags that are hashes of the host identities.[16]

Now the connections are made to a host with certain identity, not to one with certain IP address. This allows static identity even with computers, that are mobile as well as those that are are hooked to the internet with dynamically changing DHCP addresses as well as those hosts that have static IP addresses. HIP even gives identity for computers that are behind NAT. Unbreakability is thus maintained by just accepting packets with correct identity regardless of their source address, and by returning packets the same address they came from. [16]

Connectibility however requires the usage of rendezvous server, since internet does not route based on host identity, but based on IP addresses. DNS contains the address of the Rendezvous server, so the first packet is sent to it. Rendezvous server then forwards that packet to the current IP address of the hosts. The mobile host can then respond the original sender directly.[16]

All mobile hosts need to keep their rendezvous server aware of their location, in order to be connectible.

HIP even allows mobility trough NAT and between IPV4 and IPV6 networks. [16]

The side effect is that IPSEC is practically mandatory and HIP rendezvous server is needed to do mapping between Host identity and IP addresses. DNS is not suitable for this due to the fact that these mapping are too dynamic for DNS.

Hip communication between HIP aware mobile node and non HIP aware node can be accomplished by tunneling or though special IP-routers that that support HIP called by rendezvous brokers. This part of the specification is in it's early state and only lists a number of techniques that could be used for such an arrangement.[19]

7 IP mobility with fixed IP addresses

The techniques still use static IP addresses to identify mobile hosts, and different IP numbers as identification of the network location of the mobile host.

7.1 Mobile IPv4

The mobile host connects to it's home network, where it has a home agent each time it moves to a new network. This is done in order to keep the home agent aware of the current position of that node in wherever it happens to be.

This home agent is then "spoofing" itself as the mobile host in the home network using gratuitious ARP.

Foreign agent is in the target network and it is receiving the traffic and delivering it to the target using a bidirectional tunnel that is used to encapsulate the traffic that is going to and from the mobile host. However if the visited network does not have foreign agent and the mobile node can get an IP address for itself using DHCP, then it can use co-located care-of address to communicate with its home network.

This triangular routing strategy is bad, because all traffic needs to flow trough the original network and then from there to where it was going. If the target is geographically close to the mobile host, while the mobile host if far away from home, this can lead to very slow long triangular routes, instead of a quick local one.

Also the home agent works as a single point of failure. Foreign agents do not work as single point of failure, if co-located care-of address can be used. [2]

Default authentication method for binding update datagrams is MD5 digest with pre shared secret used as initialization vector. IPsec is therefore not mandatory for MIPv4.

7.2 Mobile in IPv6

Can use tunneling, like MIPv4 as well as route optimization. Route optimization means that after initial connection the packets no longer need to be routed trough the home agent, but that the home agent will tell where the datagrams are rerouted to the network where the mobile host currently is.

However if the route optimization is not supported by the host that is communicating with the mobile host, the traffic will continue to flow trough the home agent.

The home agent is still needed and acts as a single point of failure, since it is needed for initialization of a new connection. Therefore any mobile host is not connectible, if there is a problem connecting to the home network of the host, since the connections are initialized first with the home agent, before they receive the route optimizations messages, after which the packets are routed directly to the target network. Foreign agent is not used in MIPv6. [10]

MIPv6 requires binding updates to be done using IPsec, so having IPsec is mandatory. [10]

7.3 LIN6

LIN6 is an IPv6 mobile networking technique that uses specific address prefix as the first 64 bits of IPV6 address. This combination is called by LIN6 generalized address. This static prefix is currently allocated from a segment that is reserved for future use in IPv6 address allocation. [12]

LIN6 also creates a layer between IP and transport layer, but unlike HIP this is just address prefix replacement. In receive the network address is just replaced by LIN6 prefix. In transmit the LIN6 layer has to use mapping agent to get the current network prefix for the host. This prefix rewriting scheme allows mobility without any packet overhead due to tunneling or extra info added to the packets.

IP address of the mapping agent or mapping agents for a host are stored in DNS. If the other end of the connection is non LIN6 host, then the mapping agent creates IP-over-IP tunnel for the traffic.

LIN6 generalized address is used in IPsec, so the changes to current location do not affect IPsec.[12]

If a host has multiple physical network interfaces, it also has multiple LIN6 generalized addresses, since LIN6 is abstracting only the 1st 64 bits that is network related, not the hardware address related part. So multi homing support in case of LIN6 is different from unbreakability in case of network handover, for example from one WLAN segment to another.

In the IPsec side LIN6 solves this by forming an IPsec connection with all of the addresses.

However transport layer must support this kind of multi homing, since it is not done by LIN6 as itself.[15] Multi homing transport layers such as TCP/mh or SCTP are suited for this. However UDP programs cannot use such extensions so in these cases special extended socket interface is needed. [15]

8 Analysis

There is no single best technique, but all have their strengths as well as weaknesses.

8.1 Data link layer mobility

Routing layer 2 mobility has already more or less established in its own field. It provides mobility without any mobility extensions to IP as long as host uses the same networking technique (or otherwise in the same logical network). It is however not the solution for all mobility problems in the IP world. For example it is not possible to move a host from gprs/GSM provided by a tele operator to corporate WLAN, while maintaining neither host identity nor connections.

Simple layer 2 techniques can be made compatible with mobility between a few locations with tunneling, this would be ok for a few offices of the same company, but I do see this as generally useful idea.

So this kind of techniques as well as connectibility using different techniques based on the availability actually add demand for IP based mobility.

8.2 IP Mobility

If one looks a bit deeper to the 4 protocols MIPv4, MIPv6, LIN6 and HIP, they all start to look the same.

Address resolution is started from DNS, then address of a mobility agent and static identity of the host is retrieved.

Mobility Agent is called by Home Agent in MIPv4 and MIPv6, Mapping Agent in LIN6 and rendezvous server in HIP. HIP and LIN6 support multiple agents.

Static identity is IP adress in case of MIPv4 and MIPv6. It is LIN6 generalized address in case of LIN6 and Host Identity in case of HIP. HIP differs from other protocols in that the host identity is not just numeric id, but a public key pair and it is not meant to mobile hosts, but static ones as well.

Then a packet is sent to mobility agent. If the connection initiator does not understand route optimization, or equal mechanism then a tunnel is built, in case of MIPv4 it always happens, since such method does not exists.

If the mobility mechanism is understood, then just the 1st packet is forwarded to its intended destination. When reply packet arrives the communication is continues directly.

If the communication breaks, then the traffic moved to Mobility agent.

8.2.1 Status of the protocols

MIPv4 has reached RFC status in the IETF and has multitude of implementations[9].

It has also requirement for home network where the host must be not only registered, but that network also needs to relay all the traffic to and from the mobile host. Due to the above reasons I do not belive that MIPv4 will newer be widely adopted, despite its status as RFC in the IETF. On the other hand it has not yet reached Internet standard status at the time of this writing.

MIPv6 as well as LIN6 and HIP are all still internet drafts. I was able to find only one LIN6 implementation[13], but for multiple operating systems[13][14] and five HIP implementations.[20] There were already multiple MIPv6 implementations 3 years ago[11].

MIPv6 adds a standard way to do the route optimization, that takes away mandatory triangular routing. This however has the requirement that the host communicating with mobile host has to support it, otherwise same kind of loop that with MIPv4 is built. Foreign agent is no longer needed, but all the mobile hosts need to have a home network with home agent. The home agent still works as single point of failure.

In my opinion this corrects the most severe faults of MIPv4 and could be adapted with same schedule that IPv6 is adapted.

The clear advantage of Mobile IP techniques are the fact that they have already been available for a while.

LIN6 is quite similar to MIPv6, but it takes away the home agent as single point of failure as it allows multiple mapping agents to be used.

The disadvantage of the LIN6 prefix rewriting technique is that a connection cannot be migrated from one network adapter to another without need for transport layer multi homing solution like TCP/mh[15].

HIP will try to do something for everybody. It will not only do mobility, but also provides hosts identity that can be used regardless of dynamically changing addresses and NAT, but also provides possibility for anonymity, through locally generated identity. HIP offers not only mobility, but ideally it would be central part of the entire internet infrastructure.

In addition to everything else, it also works with both IPv4 and IPv6 providing seamless mobility between both. It will also offer possibility of static identity for host connected over dynamic IPv4 DHCP pools.

Unfortunately there is also downside, and it is complexity. When other techniques, except IPv4 requires IPSec in order to do mapping update and such. HIP not only needs IPSec, but also extends IPSec for it's own needs. This means that the IPsec provider must participate in adding HIP support to its IPsec stack.

The 1st version of Rendezvous server has only recently been specified. [19]

IP addresses are replaced by host identity tags, so it is not impossible to use existing apis. However it is assumed that some functionality provided by HIP will require new apis.[16]

8.3 Application layer mobility

Some applications can be work with address changes by decoupling session from physical connections, such as web browser. Sometimes just the ability to open a new connection after one breaks is enough, if the protocol does not require any session.

This may be enough for many uses, but is not certainly a general solution to mobility needs.

Tunneling programs like ALaMoE can be used to create tunnels that are resistant to network breakage.[6]

I however do not see that this area will grow very much due to the fact that these features are needed for all applications separately, or the application have to be configured or adapted to support tunneling programs.[6]

8.4 Multi homing only

I think SCTP will be adopted, not because of its multi homing support, but as VOIP signaling carrier and possible as a carrier for other applications. It is also possible that it will be adopted as next generation replacement for some TCP and UDP protocols. MAST will add entirely new layer to IP just for multi homing, without providing any other functionality. It is true that this layer is simpler that the one provided by HIP, but I fail to see the logic to add such a layer just for multi homing, without any support for mobility or other major benefit.

TCP/mh promises even less that MAST, but on the other hand it is only very small extension to the TCP and no changes for the IP layer. I think it has slight changes for making it for this reason, but it won't be anything major, even if it does. It is true that it does less than MAST and even less than mobile IP techniques and, but on the other hand it does not require any infrastructure or other things from the network.

8.5 Can we actually keep living without IP mobility ?

Servers do not generally move a lot. Many of those devices that do move can take advantage of data link layer mobility. Application layer mobility is enough if the user does not have needs that go beyond what mobility compatible applications can offer.

Laptop computers that are used both in home and office can change their identity, because programs are usually using login and password combination as the identity of the user, instead of identity of the computer. Same goes with wireless devices that can connect to multitude of networks. File transfer will break on network handover, but this is not a problem if it can be started easilly or automatically again.

It is usually the identity of the user that matters, not the identity of the host, when the host is not server.

If host IP needs to be kept static, it is somtimes possible to use layer 2 tunneling for that purpose.

IP mobility would be the most useful in workplaces, where employees travel a lot. However that is also the place, where security problems will arise. An unattended laptop with connected to company network can become major problem.

The other problems are firewalls, will an uncommon mobility extensions be allowed in firewalls, even if it would add some benefit for mobile employees and will the mobility extension become commonplace, if it generally disallowed by firewalls?

9 Conclusions

It is possible, to arrange a network in wide area so that all mobility can be done on datalink layer. This is however not generally feasible, so data link layer mobility calls for upper layer mobility. If unbreakability is the only requirement then the mobility can be done with application layer alone, providing that all the needs can be met with applications that support mobility.

If connectiblity or identifiability is required, or mobility is required with applications that do not support mobility themselves, then there is not really alternative for IP mobility.

Mobile IP v4 and v6 are strong candidates for basis on future mobile internet, due to the fact that is has been around a while and has wide variety of implementations. The downsides triangular routing with IPv4 and home agent as single point of failure are however features that make room for better solutions.

HIP is clearly the most complete solution, but is several years behind mobile IP. HIP offers a consistent identity over today's fragmented internet with NATs and dynamically changing IP addresses as well as its support for mobility between IPv4 and IPv6. The downsides however are complexity as well as the fact that it is not yet as established as mobile IP.

LIN6 has only marginal advantages over MIPV6 and has also disadvantage of requiring transport layer support in order to support multi homing. It also has only one implementation and frankly is in by opinion lacking future for above reasons.

I do not see much future for multi homing only solutions. SCTP will be making it as VOIP control traffic carrier, and possible as a general purpose protocol, but not for its multi homing features. TCP/mh might have slight change for making it due to the fact that it is only small update to TCP, but won't be anything major even if it happens.

Mobility based on standard DNS work somewhat for keep home computer behind infrequently changing DHCP connectible from outside world, but not for anything else. I did not find some papers and idea, but not any real solutions based real time DNS.[26][25]

References

[1] J. Manner,M. Kojo.
Mobility Related Terminology. http://www.ietf.org/internet-drafts/ draft-ietf-seamoby-mobility-terminology-06.txt Internet Draft,February 2004. Refered 21.3.2004

[2] C. Perkins,
IP Mobility Support for IPv4 RFC3344, August 2002.

[3] LAN MAN Standards Committee of the IEEE Computer Society, USA wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications *ISO/IEC 8802-11; ANSI/IEEE Std 802.11, 1999 edn* Section 5.4

[4] Hannu Kari.
GPRS Arcitecture 18.2.1999, Helsinki Univercity of technology http://www.cs.hut.fi/ hhk/GPRS/lect/ architecture/ppframe.htm Refered 21.3.2004

[5] Kristol, Montulli
HTTP State Management Mechanism RFC2965, October 2000

[6] Ed Swierk,
ALaMoE: An Application-Layer Mobility Enabler http://www-cs-students.stanford.edu/ eswierk/cs244c/ Stanford Universiry,Spring 1998 Refered 21.3.2004

[7] P. Mockapetris
DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION RFC 1035,November 1987

[8] Vixie, P., Thomson, S., Rekhter, Y., Bound, J.,
Dynamic Updates in the Domain Name System (DNS UPDATE). RFC2136, April 1997

[9] Mip4 working group, Mobile-IP Implementations. http://www.mip4.org/2004/implementations/ Refered 21.3.2004

[10] D. Johnson,C. Perkins, J. Arkko, June 30, 2003
Mobility Support in IPv6 (Expired internet draft) http://ietfreport.isoc.org/ids/draft-ietf-mobileip-ipv6-24.txt Refered 21.3.2004

[11] Alexandru Petrescu, "Mobile IPV6" http://mailman.isi.edu/pipermail/6bone/2001-April/004140.html Refered 21.3.2004

[12] Teraoka, F., Ishiyama, M., Kunishi, M.,
"LIN6: A Solution to Mobility and Multi-Homing in IPv6", (Internet draft) http://www.ietf.org/internet-drafts/ draft-teraoka-multi6-lin6-00.txt 30 December 2003 Refered 21.3.2004

[13] Unknown,
"LIN6(Location Independent Networking for IPv6)" http://www.lin6.net/ Refered 21.3.2004

[14] Hui Tiong Khoo Load Sharing for Mobile Streaming Services using LIN6 http://www.research.att.com/ rjana/khoo.pdf Page 6 chapter5. Refered 21.3.2004

[15] Arifumi Matsumoto,Kenji Fujikawa,Yasuo Okabe.
Basic Socket API Extensions for LIN6 End-to-End Multihoming Expired Internet Draft, 23 June 2003, Chapter 3 http://www.join.uni-muenster.de/Dokumente/drafts/ draft-arifumi-lin6-multihome-api-00.txt Refered 21.3.2004

[16] Moskowitz, R. Host Identity Protocol Architecture http://www.ietf.org/internet-drafts/draft-moskowitz-hip-arch-05.txt Refered 21.3.2004

[17] Moskowitz, R. Host Identity Protocol http://www.ietf.org/internet-drafts/draft-moskowitz-hip-09.txt Internet draft Refered 21.3.2004

[18] Nikander, P. End-Host Mobility and MultiHoming with Host Identity Protocol http://www.ietf.org/internet-drafts/draft-nikander-hip-mm-01.txt Internet draft Refered 21.3.2004

[19] L. Eggert, Internet draft, Host Identity Protocol (HIP) Rendezvous Mechanisms http://www.ietf.org/internet-drafts/draft-eggert-hip-rendezvous-00.txt Refered 21.3.2004

[20] Nikander P. Introduction to HIP http://www.ietf.org/proceedings/03nov/slides/hipbof-1.pdf Refered 21.3.2004

[21] Matsumoto, A. Kozuka, M., Fujikawa, K., Okabe. Y., TCP Multi-Home Options http://www.ietf.org/internet-drafts/draft-arifumi-tcp-mh-00.txt Internet draft, 10 Sep 2003 Refered 21.3.2004

[22] L. Ong,J. Yoakum. An Introduction to the Stream Control Transmission Protocol (SCTP) RFC3286,May 2002 Refered 21.3.2004

[23] D. Crocker, MULTIPLE ADDRESS SERVICE FOR TRANSPORT (MAST): AN EXTENDED PROPOSAL Internet draft,September 16, 2003 http://www.ietf.org/internet-drafts/ draft-crocker-mast-proposal-01.txt Refered 21.3.2004

[24] D. Crocker. CHOICES FOR MULTIADDRESSESING Internet draft,October 19, 2003 http://www.ietf.org/internet-drafts/ draft-crocker-mast-analysis-01.txt Refered 21.3.2004

[25] Venkata N. PadManaphan, Randy H Katz. Using Dns to support Mobility. Univercity of Berkley, March 1996. http://research.microsoft.com/ padmanab/talks/ilp96.ps Refered 21.3.2004

[26] Andreas Pappas. Research proposal: Real time DNS 18 January 2002 http://www.ee.ucl.ac.uk/ apappas/Proposal.htm Refered 21.3.2004