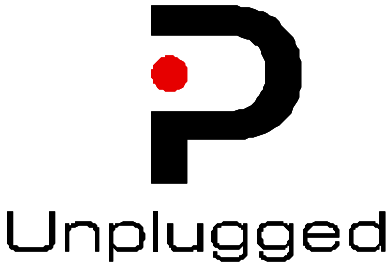


White Paper

Mobility and Mobile IP, Introduction

Abstract

This white paper introduces networking with Mobile IP and related functionality. In particular the paper describes the basic functionality of the mobility solutions included in the products from ipUnplugged.

Unplugged

Table of Contents

The Mobile Internet

While Internet technologies largely succeed in overcoming the barriers of time and distance, existing Internet technologies have yet to fully accommodate the increasing mobile computer usage. A promising technology used to eliminate this current barrier is Mobile IP. The emerging 3G mobile networks are set to make a huge difference to the international business community. 3G networks will provide sufficient bandwidth to run most of the business computer applications while still providing a reasonable user experience. However, 3G networks are not based on only one standard, but a set of radio technology standards such as cdma2000, EDGE and WCDMA. It is easy to foresee that the mobile user from time to time also would like to connect to fixed broadband networks, wireless LANs and, mixtures of new technologies such as Bluetooth associated to e.g. cable TV and DSL access points.

In this light, a common macro mobility management framework is required in order to allow mobile users to roam between different access networks with little or no manual intervention. (Micro mobility issues such as radio specific mobility enhancements are supposed to be handled within the specific radio technology.) IETF has created the Mobile IP standard for this purpose. Mobile IP is different compared to other efforts for doing mobility management in the sense that it is not tied to one specific access technology. In earlier mobile cellular standards, such as GSM, the radio resource and mobility management was integrated vertically into one system. The same is also true for mobile packet data standards such as CDPD, Cellular Digital Packet Data and the internal packet data mobility protocol (GTP/MAP) of GPRS/UMTS networks. This vertical mobility management property is also inherent for the increasingly popular 802.11 Wireless LAN standard.

Mobile IP can be seen as the least common mobility denominator - providing seamless macro mobility solutions among the diversity of accesses. Mobile IP is defining a Home Agent as an anchor point with which the mobile client always has a relationship, and a Foreign Agent, which acts as the local tunnel-endpoint at the access network where the mobile client is visiting. Depending on which network the mobile client is currently visiting; its point of attachment (Foreign Agent) may change. At each point of attachment, Mobile IP either requires the availability of a standalone Foreign Agent or the usage of a Co-located care-of address in the mobile client itself.

Unfortunately the concept “Mobile IP” today has at least two different meanings. Mobile IP is sometimes used in the general meaning of a mobilized Internet - including all different technologies and methodologies. Sometimes the name refers to the protocol of Mobile IP itself, as defined within the IETF (Internet Engineering Task Force.) In this paper, when referred to Mobile IP, we mean the IETF Mobile IP protocol.

Flavours of Mobility

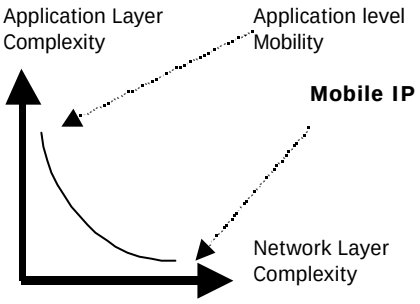
The concept of “Mobility” or “packet data mobility”, means different things depending on what context the word is used within. In a wireless or fixed environment, there are many different ways of implementing partial or full mobility and roaming services. The most common ways of implementing mobility (discrete mobility or IP roaming service) support in today’s IP networking environments includes simple “PPP dial-up” as well as company internal mobility solutions implemented by means of renewal of IP address at each new point of attachment. The most commonly deployed way of supporting remote access users in today’s Internet is to utilize the public telephone network (fixed or mobile) and to use the PPP dial-up functionality.

Another mobility scenario that is quite often used within company local area networks or even in company worldwide environments is implemented by deploying the DHCP “get and release” functions. Basically the terminal device is given a “topologically” correct IP address in every new point of attachment. This DHCP “discrete mobility” support is most often bundled with e.g. Microsoft NT back-office login procedures.

While working very well within the constraints where the discrete dial-up and "DHCP" mobility solutions are defined, both of them have severe limitations when it comes to supporting road-warriors i.e. roaming users wanting access to their home-network resources at any specific time and place, independently of access network technology.

Another feature that cannot easily be supported with the discret mobility approaches is the concept of "session continuity" among access technologies. Session continuity means that users should be able to be connected to e.g. home network resources with limited interruption while changing access network and even access technology. Users should not be forced to restart applications - or in worst case reboot their mobile devices when changing access technologies. Roaming (in an IP environment conceptually being away from the home network, but keeping the service agreement with the home network) and the change of access network (multi-access) should be as seamless as possible for the user. In the next generation IP network it should be possible to be connected all the time - possibly forever – while keeping the state of on-going user application sessions.

Keeping application state and implementing seamless mobility for the user can be done on different protocol levels. When using the Internet Protocol suite, it is possible to develop solutions implementing mobility on either the network, transport or application layers. For the purpose of this discussion, implementing the mobility support on transport or application layer is conceptually the same thing; both approaches mean that the network layer needs to be identified with a new IP address at every new point of network attachment. This means that while changing point of attachment the terminal IP address has to be released and renewed. While having the benefit of simplifying the Internet routing (no tunnels required) this mobility approach have many limitations. For example, these kinds of solutions to support session continuity – every application has to be mobility aware. Not only must the mobile terminal's running applications be updated, but also the corresponding servers in the home network – and possibly on the Internet itself.



A better and more generic way of approaching the problem of mobility - is to handle mobility-related functions in the network layer. In such a case, end user applications can be kept unaware of mobility issues, adopting a philosophy of simplified application design. This approach embrace the Internet way of thinking, developers of applications should not need to bother about lower protocol layer issues. When deploying a network layer mobility solution end-users may experience a temporary service fluctuation when changing to a new access technology or access network, but commodity applications and TCP sessions will survive. With the network (IP) layer mobility solution, the end-user will be associated with the same IP address at least during the lifetime of one IP level session (possibly "forever".) The cost, of course, is a slight increase in network layer complexity.

The work within IETF related to solving mobility issues on the network layer is handled within the "Mobile IP" working group. Mobile IP is seen as *the* "macro mobility" protocol, which as such can be combined with access specific mobility solution on the link layer for enhanced performance. Mobile IP is gradually getting market impact and one of the main drivers for the deployment is the cdma2000 community (cdma2000 is the North American version of 3G cellular systems, co-ordinated by 3GPP2.) Mobile IP is chosen as the network mobility protocol for cdma2000 packet data users. The cdma2000 community has chosen to deploy Mobile IP with a bundled IETF AAA functionality. (AAA stands for Authentication, Authorization and Accounting. Today RADIUS is used, in the next version of the cdma2000 standard, the IETF Diameter protocol will replace RADIUS). AAA provide Internet roaming services – i.e. the user is entitled the use of various access networks around the world, while keeping the users Internet service agreements with a "home Internet service provider".

AAA provides roaming services while Mobile IP adds two important concepts of mobility – namely personal mobility and terminal mobility. Personal (user) mobility makes it possible for a user to use any terminal in order to get access to IP services. The user is identified by means of a NAI,

Network Access Identifier. The user is not mandated to use a specific terminal in order to connect his/her "home" network. Instead the user may change terminal from time to time and still get access to the same network services without being required to go through annoying and troublesome configuration procedures each time he/she changes terminal equipment. Another aspect of personal mobility is reachability. When the user has established an IP level session ("attached" to the IP network and given an IP address) then there will be a relation between the IP address and the NAI. As long as the user chooses to keep a particular IP session alive, the user is reachable via this particular IP. A Company or ISP policy may tell that a particular mobile should be assigned the same IP address every time the mobile powers up. In this case this particular IP address can be used to identify the mobile for other services. However, if this static assignment cannot be guaranteed, then the mobile must register its "IP session" IP address with appropriate services at the time it powers up. An example of such a service registration may be a "SIP register". It is important to realize that when using Mobile IP, these application level registrations need only to be done at the power up (after the Mobile IP registration) of the mobile client.

When deploying Mobile IP, terminal mobility is tied to the Mobile IP protocol itself. Terminal mobility means that the terminal may change point of attachment with minimal impact on ongoing services – sessions continue in a seamless manner. Terminal mobility is implemented within Mobile IP and, it is among other things, the cornerstone for providing handover services (in a fast and loss-less manner) among access points. Since the handover is implemented on the network layer – applications will survive and session continuity is inherently provided for.

Private and Public Networks

We use the concept "public network" in the sense of meaning that a "public network" is an IP network with public IP addresses. All public networks are interconnected via routers and thereby form the Internet. A private network, on the other hand, is an IP network that is isolated from the Internet in some way. A private network may use private or public IP addresses – it may be connected to the Internet via a network address translator or a firewall. However, it is not a part of the Internet since its internal resources are protected from the Internet. Private Networks may use the Internet to interconnect a multi-site private network, a multi-site VPN solution.

The concept of "network partitioning" is used to denote that there is not a single IP network. Instead there are many IP networks with different characteristics. Each IP network constitutes its own realm, and may also reuse the same IP addresses as used in another domain. Communication between the different IP networks is established on a higher protocol level.

Originally IPv4 was designed around the concept of a transparent network layer, where each and every host had a logical address that was unique and never changed. This was the basis for a global connectivity layer where all "hosts" on the Internet where supposed to be reached via direct addressing on the IP layer. Intermediate equipment was never supposed having to change or look into the upper layers of the transmitted IP packets. Due to mainly two factors the Internet does not look like that anymore. The first factor is the shortage of IPv4 network addresses whilst the second is that network partitioning (e.g. Intranet solutions, VPNs) in many cases is regarded as a feature rather than a disadvantage. There is no distinct separation between the two drivers of network partitioning. Example mechanisms for implementing separation because of the shortage of network addresses are Dynamic IP address assignment via mechanisms such as PPP and DHCP. Another mechanism is Network Address Translators, NATs in different flavors. On the other hand when it comes to a feature driven network separation, there are mechanisms such as Firewalls, Proxy and Cache servers. The effect on the Internet is the same independently of the reasons; namely that the Internet network layer transparency has partially disappeared. It is fair to say that even though Internet technology is used today in an extremely successful way, the Internet philosophy has been gradually abandoned. The lack of end-to-end network layer transparency is sometimes referred to as the "fog" on the Internet. Sometimes we need specific techniques within Mobile IP in order to be able to establish and maintain IP communication, even though parts of the Mobile IP infrastructure resides in private networks or behind firewalls – to clear the fog.

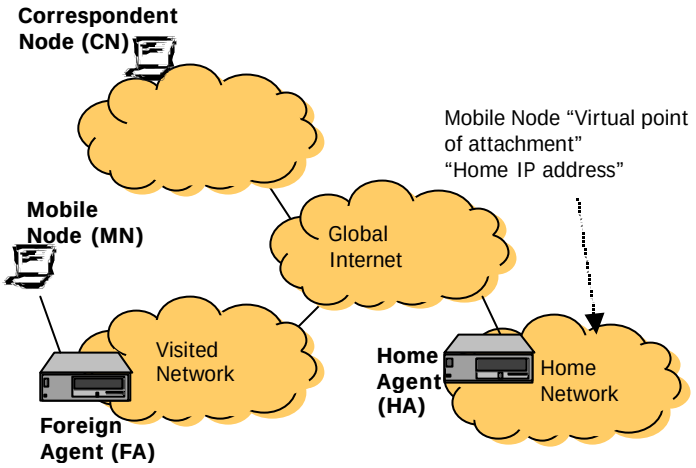
Unplugged

Mobile IP: the basics

The Basics

In general, on the Internet, IP packets are transported from their source to their destination by allowing routers to forward data packets from incoming network interfaces to outbound network interfaces according to information obtained via routing protocols. The routing information is stored in routing tables. Typically the routing tables maintain the next-hop (outbound interface) information for each destination IP network. The IP address of a packet normally specifies the IP client's point of attachment to the network. Correct delivery of IP packets to a client's point of network attachment depends on the network identifier portion contained in the client's IP address. Unfortunately, the IP address has to change at a new point of attachment.

Altering the routing of the IP packets intended for a mobile client to a new point of attachment requires a new client IP address associated with that new point of network attachment. On the other hand, to maintain existing transport protocol layer connections as the mobile client moves, the mobile client's IP address must remain the same.



In order to solve this problem, Mobile IP introduces two new functional entities within IP networks. Those are the Foreign Agent, FA and the Home Agent, HA. These two new entities together with enhancements in the mobile node (the client) are the basic building blocks for a Mobile IP enabled network. The last entity for providing a full reference for a basic Mobile IP enabled network is the Correspondent Node, CN. The Correspondent Node is another IP entity e.g. an Internet Server with which the mobile node communicates. In the basic Mobile IP scenarios the Corresponding Node does not need to have any Mobile IP knowledge at all. This is an important distinction. To require that new devices that are introduced on the Internet to have new functionality is one thing – to require that all Internet servers and fixed clients should be upgraded is completely different. A Mobile IP enabled network requires the mobile nodes to be upgraded, it also requires new functions in the visiting and home networks; however it does not require upgrading of core Internet services.

The basic entities constituting a MIP aware network are:

- The Mobile Node comprising the Terminal Equipment and the Mobile Termination
- The Foreign Agent
- The Home Agent
- The Corresponding Node

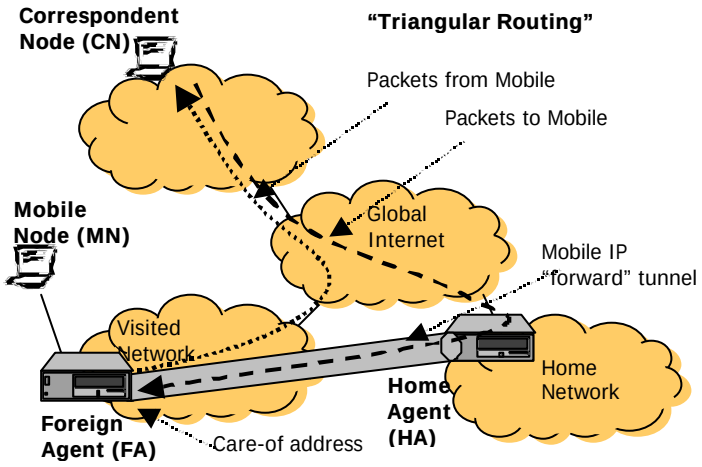
Mobile IP Operation

Mobile IP works by allowing the Mobile Node to be associated with two IP addresses: a "home" address and a dynamic, "care-of" address. While the home address is fixed, the "care-of" address changes at each new point of attachment to the Internet. The home IP address assigned to the mobile client makes it logically appear as if the Mobile Node is attached to its home network. It is

the IP address where the mobile client seems to be reachable for other Internet clients and services. For the Correspondent Node, the Mobile Node seems to be attached to the "Home Network" independently of which Network it is currently visiting.

A mobile agent (Home Agent) that is provided in a home network receives traffic directed to the mobile client's home IP address even when the mobile client is not physically attached to the home network. When the mobile node is attached to a foreign network, a Home Agent routes (tunnels) that traffic to a Foreign Agent using the mobile client's current care-of address. The care-of address, which identifies the mobile client's current, topological point of attachment (the Foreign Agent) to the Internet, is used by the Home Agent to route packets to the mobile node. If the Mobile Node is not attached to a foreign network, the Home Agent simply arranges to have the packet data traffic delivered to the mobile client's point of attachment in the home network. Whenever the Mobile Node moves its point of attachment, it registers a new care-of address with its Home Agent.

The further delivery by the Home Agent to the Foreign Agent requires that each packet intended for the mobile client be modified/extended so that the care-of address appears as the destination IP address. This modification of the packet is sometimes termed as "redirection." The Home Agent redirects packets from the home network to the care-of address by constructing a new IP header that contains the mobile client's care-of address as the packet's destination IP address. This new header "encapsulates" the original data packet causing the mobile client's home address to have no effect on the encapsulated packet's routing until it arrives at the care-of address. This encapsulation is commonly known as "tunneling" in the sense that the original data packet is hidden by the new "routing" header, while the encapsulated IP header is completely ignored during Internet transit.



When the packet arrives at the Foreign Agent the new "routing" header is removed and the original packet is sent to the mobile client for properly processing by whatever higher level protocol (layer 4) that logically receives it from the mobile client's IP (layer 3) processing layer. Tunneling between the agents can be done using IP encapsulation within IP, a mechanism specified in RFC2003 [12]. Another encapsulation mechanism is GRE, Generic Routing Encapsulation as specified in RF2784 [14].

Basic Mobile IP operation utilizes a technique called triangular routing. Triangular routing means that packets are routed in different paths depending on if the packets are directed to or from the mobile node. Packets from a corresponding node to a mobile client in a visited network are routed from the Corresponding Node to the Home Agent. The Home Agent encapsulates the packets in a Mobile IP tunnel. The tunnel is terminated in the Foreign Agent and the Foreign Agent then forwards the packet within a layer two technology to the mobile client. In the other direction, from the mobile node to the corresponding node, there is not necessarily a need for tunneling. In the basic operation packets to the Corresponding Node are sent from the mobile node (in a layer two technology) to the Foreign Agent. Since the Corresponding Node (in a basic scenario) is supposed to have a public routable address, it is possible for the Foreign Agent to directly forward the packet to the corresponding node. In this way the Home Agent is completely bypassed for corresponding node directed traffic. This technique has some inherit problems though. It cannot support private addressing in a good way since the solution requires unique IP addresses on every interface. Another problem is that many Internet Routers strictly filter out packets that are not originating from a topologically correct sub-net. The solution to these problems is a technique called "reverse tunneling". Essentially reverse tunneling means that in addition to the "forward tunnel" (from the

Home Agent to the Foreign Agent), the Foreign Agent also tunnels packets, from the mobile node, back to the Home Agent instead of directly sending them to the Corresponding Node.

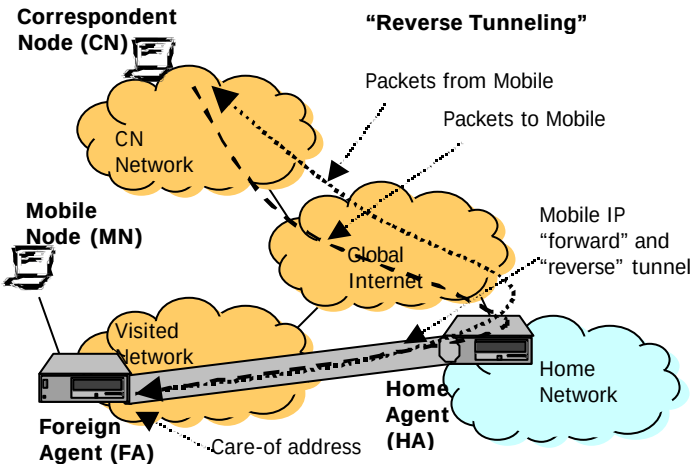
Home agents and Foreign Agents regularly broadcast agent advertisements (beacons) that include information about one or more care-of addresses. When a mobile node receives an agent advertisement, it can obtain the IP address of the beaconing Home or Foreign Agent. The mobile node may also broadcast an advertisement solicitation that will be answered by any Foreign or Home Agent that receives it. Thus, agent advertisement procedure allows for the detection of mobility agents (home or foreign), lets the mobile client determine the network number and status of its link to the Internet, and identifies whether the agent is a Home Agent or a Foreign Agent. Once a mobile client receives a care-of address, a registration process is used to inform the Home Agent of the care-of address. The registration allows the Home Agent to update its routing table to include the mobile's home address, current care-of address, and a registration lifetime.

Mobile IP: more Details

While being good enough for many deployment scenarios, mobile-IP needs specific enhancements and bundling with other technologies for supporting, among other things, personal mobility in a generic way. Other features needed are the abilities for Mobile IP to support private network interworking with e.g. home networks in private network realms. Corporate networks are most often located beyond the confines of firewalls. A Home Agent beyond a firewall in a corporate network must be able to communicate with Forign Agents in other networks i.e. the Mobile IP protocol must in certain cases be able to traverse firewalls. Another issue is charging, accounting and load-sharing. Depending of the charging policy for the access network (Visited Network) in question, the provider of the access may want to charge the mobile node. In this section we look into some specific but important additions to Mobile IP that can solve some of these problems.

More about Reverse Tunnelling and Private Networks

The concept of "reverse tunneling" introduced above is a powerful technique solving many of the shortcomings with the triangular routing approach. Such shortcomings are for example the problem with ingress filtering routers on the public Internet – but also the inability of supporting multicast as well as not supporting disparate IP address spaces. The figure describes the basic concept of reverse tunneling, where the Correspondent Node is located on the Internet.



The routing of IP packets is shown in the figure. First assuming that all of the networks in the figure belong to the same "public" IP Network, packets are routed from the Correspondent Node to the Mobile Node via the "forward tunnel" in ordinary Mobile IP manner. Packets from the Mobile Node, on the other hand, are routed via the Foreign Agent into the "reverse tunnel" back to the Home Agent. The Home Agent further routes the packets to the "Global Internet" (or the "Home Network", in case the Correspondent Node resides in the Home Network.)

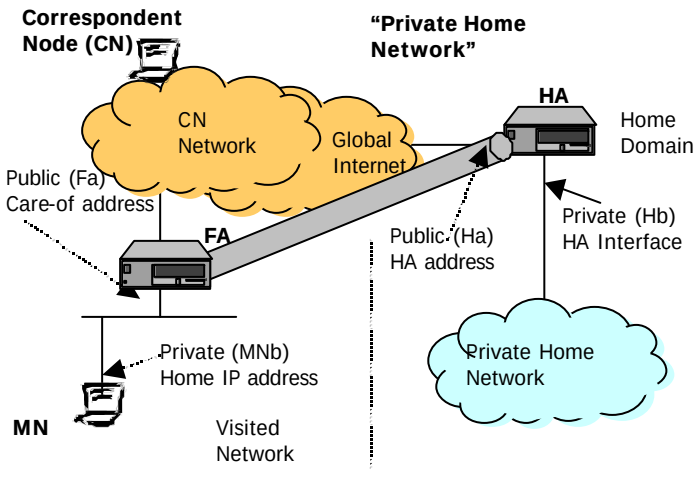
Coping with disparate address spaces is very important considering that IP networks often are built today with firewalls and, in many cases Network Address Translators, isolating private company networks from the public Internet. In the figure, for example, it is possible to overlay a scenario where the Mobile Node and the Home Network constitutes a private IP address realm. The Visited Network, the Global Internet and, the Network where the Correspondent Node reside are parts of the public IP addressing space. While being just one of many different public/private Network scenarios, the current scenario serves as a common and important internetworking example to base the further discussions around. Other common public/private internetworking scenarios may be based on the different Network concepts.

- The Correspondent Node Network is constituting a private network
- The Visited Network is a private network
- The Home Network is a private network
- The network between the Visited and the Home Network a private (basically replacing the "Global Internet" with a private network
- The network between the Correspondent Node Network and the Home Network is private.

While deploying "reverse tunneling" it should be noted that it does not really matter whether the network between the Correspondent Node Network and the Visited Network is private or public – since no IP traffic is directly routed in between them.

Basically a matrix can be generated with the mentioned five networks being either public or private. Each combination will put demands on different - sometimes specific network configurations. However, some network configuration combinations are more down to earth and, maybe therefore more interesting than others - while some combinations are utterly complex. Furthermore the different Network scenario will in most cases co-exist. For example, even though the home network might be private, it will most often be a requirement to support both private and public visited Networks. Note that the different network configurations span from the "simple" configuration where all of the networks belongs to the public addressing scheme - to a configuration where all of the networks are private network realms. In the latter case, the Networks are possibly private networks in the sense that all of the networks consist of overlapping IP addressing schemes. Here it might be the case (even though maybe not probable) that the Mobile Node, the Foreign Agent, the Home Agent as well as the Correspondent Node are assigned the same IP address number. This is of course an utterly complex network scenario – and will not be further elaborated in this paper.

Network Domain	Public/Private
Correspondent Node Network	Public
Visited Network	Public
Home Network	Private
Network between Visited and Home	Public
Network between CN network a Home network	Public



Instead we continue the analysis of the networking scenario described in the beginning of this section i.e. a scenario where the Home Network is private – but all the other networks belong to the public addressing scheme. The network address configuration for this scenario is further described in the table above. A network configuration with a private home Network and all other networks belonging to the public Network may seem simple and straightforward – but is a little bit more complex than normally

realized at a first glance. Specific handling is required in the Mobile Node, the Foreign Agent and the Home Agent. Furthermore, if the correspondent node is located in the public address space then a new network entity is needed in the border between the home Network and the "Global Internet". This network entity may either be a NAT in some flavor or a proxy server.

The figure "Private Home Network" depicts the selected network scenario. The public "visited network" can be found in the lower left corner and the "home network" is to the right. Furthermore, the global Internet and the Correspondent Node Network are drawn together in the figure. Note that the figure is still somewhat simplified. It is for example possible to foresee that either or both, the Visited and Home Network would potentially be protected by firewalls. Also, for the moment, we are ignoring the added complexity of AAA servers. Note also that there may exist "Visited Networks" within the private Home Network itself.

The IP addresses of importance for this scenario are depicted in the figure. There are two different IP address realms and specifically the Foreign Agent's public address is denoted "Fa". In the same way the mobile node's private home address is denoted "MNb". The Home Agent must have one interface in each Network. The Home Agent Interface's IP address in the public "leg" is denoted "Ha" and the corresponding interface in the private Home Network is denoted "Hb". The following is a brief analysis of the added functionality needed in the different nodes, compared to a scenario where all the Networks are public, in order to cope with private Home Networks. Starting with the Foreign (visited) Network and more specifically the Foreign Agent, the following differences can be identified:

The Foreign Agent

The Foreign Agents regularly broadcast agent advertisements that include information about one or more care-of addresses. When a mobile node receives an agent advertisement, it can obtain the IP address of the Foreign Agent. Once a mobile node receives the address of the Foreign Agent, the care-of address, a registration process is initiated to inform the Home Agent of its care-of address.

Since the Mobile Node is assigned a non-public routable IP address, reverse tunneling is required. The Foreign Agent must, in other words, support "reverse tunneling". The Foreign Agent has to build a routing entry used to route packets from the mobile into the "reverse" tunnel – and from the "forward" tunnel toward the mobile node. When supporting private home networks, one important design criteria of the Foreign Agent is that routing entry must not solely depend on the Mobile Node's IP address for the routing decision, neither for incoming (from the Internet) nor for outgoing traffic (from the mobile.) The reason for this is that the Foreign Agent cannot assume that the Mobile Node's IP address is unique. Suppose for example that the Foreign Agent hosts mobiles from two different private home networks, then it can not be guarantied that the mobiles have unique IP addresses. Two roaming mobiles may very well be assigned the same IP address.

To solve this problem, the Foreign Agent's routing entry must consist of an association of link layer specific information in the access network (visited network) – together with a combination of tunnel identification and the mobile node IP address at the tunneling interface.

The Home Agent

Home agents also broadcast agent advertisements that include information about one or more care-of addresses. When a mobile node receives an agent advertisement, it can determine if the IP address received is its Home Agent. If the Mobile Node physically attaches directly to the Home Network – no further Mobile IP specific operations are normally gone through. However, if the Mobile Node is away from the Home Network (roaming) then the Home Agent receives a registration request from the Mobile Node (via the Foreign Agent,) and the Home Agent is instructed to set up a "reverse" tunnel to the Foreign Agent in question.

One specific problem with the private Home Networks that are attached to public visited networks is that the Home Agent needs to have one interface (or "leg") in each network. It needs to have one leg in the public network and one leg in the private (home) network. More specifically the Home

Agent needs to have the "Ha" IP address allocated and routable in the public network and it needs to have the "Hb" IP address as a routable address in the private home network.

The Mobile Node

Independently of if the Mobile Node attaches to the Home Network or a Visited Network, the Mobile Node needs to be aware of its alleged Home Agent. The Mobile Node needs to include the correct IP address for its Home Agent in its registration request. Going back to the figure "Private Home Network" we can se that while out and roaming outside the Home Network, the correct Home Agent address would be the "Ha" IP address. On the other hand while in the Home Network (roaming in the Home Network), the correct Home Agent IP address would be the "Hb" IP address.

There exist a number of ways of triggering the mobile to indicate the correct Home Agent IP address. The simplest way of all is "always" to require the Mobile to use the "Hb" address as the Home Agent address. This implies, however, that the "Hb" IP address is routable within the private home network. This might be the case – but it is not generally applicable. Another way is to resolve the Home Agent IP address with an AAA protocol.

A special case worth mentioning is a roaming Mobile Node that is never attached directly to its Home Network. This may be the case for a cellular Mobile Node that always is roaming in cellular radio networks. Every network it will attach to will be a Foreign Network and its home network may be in an ISP network.

Communication with the Correspondent Node

Independently if the Mobile Node is roaming in a visited network, or a visited network in the Home Network – or even connected to the Home Network in the Home Network, the Mobile Node will always be allocated the same private IP address. Therefore the Mobile Node is assigned a private IP address and the Correspondent node, since assumed to be located on the "Global Internet", is assigned a public IP address.

Since IP packets from the public network are not for sure routable in the private network and, IP packets from the private network are not per definition allowed to be routed in the public network, some kind of translation has to take place. Normal functions to be used here are Proxy Servers and Network Address Translators. The proxy and NAT solutions are in this scenario transparent for Mobile IP.

Co-located Care-of address and Network Based Foreign Agents

At each access network a Mobile IP client normally requires a standalone Foreign Agent in the access network. However, if the access network in question does not provide for Mobile IP services then it is possible to include a Co-located care-of address in the mobile client software/hardware. The care-of address is the temporary address (foreign address) in the visited access network to which the Home Network (Home agent) forwards incoming packets and vice versa. The two different ways of getting the Mobile Clients associated with a Mobile IP care-of address (network based Foreign Agent versus Co-located care-of address) have somewhat different characteristics.

In case of a network based Foreign Agent, the Mobile IP tunnel is terminated at the Foreign Agent in the network. When using co-located care-of addresses, the tunnel is terminated in the mobile node, i.e. the tunnel is transported over the radio interface. This means that, in a radio resource perspective, network based Foreign Agents are more efficient.

A network based Foreign Agent care-of address is shared between several visiting mobile nodes. Packets to the mobile node that arrive in the home network are intercepted by the Home Agent and tunneled to the Foreign Agent in the visited network. The Foreign Agent de-capsulate the packets and forwards them to the mobile node. Since network based Foreign Agents can handle many

mobile nodes with one single care-of address, network based Foreign Agents does not require the visited network to have a large IP address space made available. Network based Foreign Agents thus facilitate optimized dimensioning of the available IP addresses, the implementation of fast handover mechanisms and the interaction with an AAA infrastructure. Furthermore, as IPv4 addresses and radio resources are scarce, Network based Foreign Agents are normally preferred.

When using a Co-located care-of-address, the mobile node is associated with a unique care-of address. The mobility tunnel from the Home Agent is extended and terminated in the mobile node itself. In this case, there is no need for a Foreign Agent in the visited network. That is, the visited network does not have to be Mobile-IP aware. Co-located care-of address requires one unique care-of address in the visited network per visited mobile node.

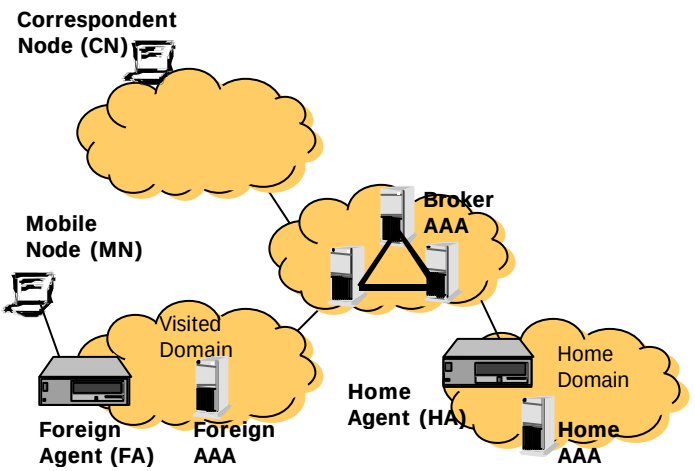
AAA and Mobile IP interworking

AAA stands for Authentication, Authorization and Accounting. RADIUS [11] is the dominating AAA protocol in IP networks today, while Diameter [3, 4] is the successor of this well-known protocol. Diameter is currently standardized within the IETF AAA working group. Both RADIUS and Diameter are flexible and extensible protocols. Additionally, Diameter is built to be interoperable (backwards compatible) with RADIUS. Both the Diameter and the RADIUS protocols are and will be used for the fixed PSTN, cellular PPP kinds of dial-up users as well as roaming Mobile IP users.

RADIUS and Diameter provide a Mobile IP based system with functionality such as:

- Simplified mobile client/user management
- NAI based user authentication
- Dynamic IP address allocation for mobiles
- Dynamic Home Agent allocation
- Flexible mechanisms for collecting accounting information
- Flexible mechanisms for creating business relations between owners of foreign networks and home networks.
- Possibilities to base the IP access reply decision on authorization information in the Home AAA server – such as e.g. time of day, weekday etc.

It is possible to foresee future evolved AAA usage in many different application areas. However, in this paper we limit ourselves to the use of AAA within Mobile IP protocol suite.



Including AAA support in mobile IP means that the reference model for the mobility architecture must be updated to also reflect the AAA infrastructure. The figure indicates a Foreign Agent, closely related to a foreign AAA server. In the same manner there exists a Home Agent closely related to one or many AAA servers. There may also exist a brokering AAA infrastructure. The AAA brokering infrastructure is to be seen as a trusted third party. It can be used and trusted to implement business agreements and act in a way that minimizes

the overall number of security associations in the network. For example, the foreign AAA and the home AAA might not have a priori knowledge, or they might not be allowed to directly talk to each other. The brokering AAA infrastructure can be deployed in a way that the foreign AAA server can "find" and set up necessary associations with the home AAA server.

Related to the figure, the important steps when it comes to the registration are as follows:

- The FA asks the AAAF (Foreign AAA) for help during the Mobile IP registration
- TH AAAF looks at the realm part of the Mobile Node NAI and deduce information on how to contact the AAAH (the Home AAA)
- The AAAH authenticates and authorizes the Mobile Node – based on the NAI in the Mobile IP registration message. Accounting starts.
- The AAAH optionally allocates a Home Agent
- The AAAH contacts and initializes the Home Agent

Conclusions

In this paper we have touched multiple areas related to mobility in IP design - such as Multi Access Network Mobility applicable for both wire-line and wireless networks. We emphasize on application independent mobility with inherent support for all IP-based applications. Mobile IP together with AAA combines personal and terminal mobility with roaming services. Personal mobility, which enables the mobile user to reach services, and be reachable for incoming service requests by holding a stable identity. Terminal mobility on the other hand enables the mobile user (and the terminal) to move while maintaining the connections to services always connected, always reachable, utilizing an IETF standard based solution.

IpUnplugged is combining the standard Mobile IP/AAA approach with state of the art security protocols such as IPSec. This solution is called a Mobile VPN. The Mobile VPN solution adds value by:

- Adding a seamless mobility experience into existing IP networks
- Adding security into existing IP networks
- Leveraging existing network investment
- Supporting current business trends (mobility, VPN, e-business, outsourcing)

Having full access to the corporate Intranet at home, in the office, in a hotel, or from within a partner's network is having access to a Mobile VPN. Utilizing the mobile VPN products from ipUnplugged means that corporate resources always are available - securely and seamlessly.

Abbreviations and Concepts

3GPP	3rd Generation Partnership project: Organization consisting of standard bodies responsible for the evolution of GSM based systems into the 3rd generation (UMTS.)
3GPP2	3rd Generation Partnership project #2: Organization consisting of standard bodies responsible for the evolution of cdmaOne based systems into the 3rd generation (cdma2000.)
AAA	Authentication, Authorization and Accounting: AAA is a common name for both RADIUS and Diameter, i.e. solutions providing customer care and billing in a large IP network.
BGP	Border Gateway Protocol: BGP is an inter-domain protocol defined by IETF for sharing routes between ISPs. A route is a collection of knowledge of a path to a destination (host).
cdma2000	Code Division Multiplexing Access 2000 is the US brand name for the 3rd generation cellular technology (IMT-2000). Cdma200 is based on a radio technology for access speeds up to 2 Mbit/s per Mobile Node.
Diameter	A later version of RADIUS with increased security and scalability features. It is standardized by IETF.
DHCP	Dynamic Host Configuration Protocol: DHCP is an Internet Engineering Task Force (IETF) standard for allocating Internet Protocol addresses to User Systems. User Systems can either be Fixed Hosts or Mobile Systems. The allocation is done when the User System is restarted. A DHCP server makes the allocation to a DHCP client. An Internet Service Provider or an IT-department controls the DHCP server. The DHCP client is a SW embedded in the User System.
DMZ	De-Militarized Zone is a zone between the Internet Service Provider router and corporate firewall where access is allowed from both the Internet and the Intranet. Normally a subset of the services available on the Intranet is mirrored on the DMZ.
FA	Foreign Agent: A tunnel agent establishing a tunnel on behalf of a mobile node in Mobile IP.
FW	Firewall: The system (or collection of systems) that enforces access control between a private network and the Internet. It may deploy mechanisms such as application gateways, packet filtering and cryptographic techniques.
HA	Home Agent: The tunnel agent which terminates the tunnel, and which encapsulates datagrams to be sent to the Mobile Node in Mobile IP.
IETF	Internet Engineering Task Force: IETF is the standardization organization for the Internet community.
IP	Internet Protocol. IP is a network layer protocol according to the ISO protocol layering. IP is the major end-to-end protocol between Mobile and Fixed End-Systems for Data Communications. It is also used in Radio Data communications Systems as an underlying transport technology for Tunneling Protocols.
IKE	Internet Key Exchange: A Key management protocol for among others the IPSec protocol.
ISP	Internet Service Provider: The ISP is a notation for the domain providing basic IP configuration services to users, i.e. servers for Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP).

LDAP Lightweight Directory Access Protocol is a slim variant of the X.500 Directory Access Protocol for accessing data storage areas such as user databases.

MANET Mobile Ad hoc Networks is a common name for a family of protocols that provide multi-hop routing in highly mobile environments.

MIB Management Information Base: IETF defines a number of MIBs for allowing management via the SNMP (Simple Network Management Protocol) of network elements. The format of a MIB is standard. The content can either be proprietary or standardized.

MIP Mobile IP: MIP is a standard being defined by IETF on making IP networks mobility aware, i.e. having knowledge on where a Mobile Node is plugged into the network. The standard includes the definition of a Foreign Agent and a Home Agent.

MC Mobile Client: The MC comprises both the Terminal (TE) and the Mobile Termination (MT).

NAT Network Address Translation:

NAPT Network Address and Port Translation:

Private Network A protected network separated from the Internet by hosts enforcing access restrictions. A private network may or may not use a private address space.

Public Network The Internet. Hosts are able to communicate with each other throughout the public network without firewall- or NAT/NAPT imposed restrictions.

RADIUS Remote Authentication Dial-In User Service: RADIUS is a protocol for carrying authentication, authorization, configuration and accounting information between a network access server and an ISP RADIUS server.

RAN Radio Access Network: RAN is the common acronym used for various types of radio access networks in 3G networks, e.g. CDMA2000 and UMTS.

SLA Service Level Agreement: SLA is the common name for a set of terms agreed with the customer on the quality of service that the ISP shall provide. The SLA can related to availability, latency and throughput of network resources.

UMTS Universal Mobile Telecommunications System: UMTS is the European name for the 3rd generation radio technology (IMT-2000).

VLAN Virtual Local Area Network is a separation of a physical Local Area Network into a set of logical subnets.

VPN Virtual Private Network is a secure overlay network on a common public infrastructure that allows a corporation to maintain its own addressing and routing between its sites.

WCDMA Wideband CDMA

WLAN Wireless Local Area Network: WLAN is a local area solution for radio access.

References and Further Reading

[1] 3GPP2 PR0001 v1.0.0/Wireless IP Network Architecture based on IETF protocols, http://www.3gpp2.org/Public_html/specs/P.R0001-0_v1.0.pdf, July, 2000.

[2] 3GPP2 PS0001-B, v1.0.0/Wireless IP Network Standard, http://www.3gpp2.org/Public_html/specs/P.S0001-B_v1.0.pdf, October 2002.

[3] Diameter Base Protocol, Calhoun, Pat et al; http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-17.txt, December 2002.

[4] Diameter Mobile IP v4 Application, Calhoun, Pat et al; http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-mobileip-13.txt, October 2002.

[5] Mobile IP Network Access Identifier Extension for IPv4, Calhoun, Pat et al; RFC2794; http://www.ietf.org/rfc/rfc2794.txt, March 2000

[6] Dynamic Host Configuration Protocol, Droms, R., RFC2131, http://www.ietf.org/rfc/rfc2131.txt, March 1997

[7] Reverse Tunnelling for Mobile IP, revised, Montenegro, G.; RFC3024; http://www.ietf.org/rfc/rfc3024.txt, January 2001

[8] IP Mobility Support, Perkins, Charlie; RFC3344 http://www.ietf.org/rfc/rfc3344.txt, August 2002

[9] Dynamic Updates in the Domain Name System (DNS UPDATE), Ed. P. Vixie, RFC 2136, http://www.ietf.org/rfc/rfc2136.txt, April 1997.

[10] The Network Access Identifier, Ed. B. Aboba, M. Beadles, RFC 2486, http://www.ietf.org/rfc/rfc2486.txt, January 1999.

[11] Remote Authentication Dial In User Service (RADIUS), Ed. C. Rigney et al., RFC 2865, http://www.ietf.org/rfc/rfc2865.txt, June 2000.

[12] Session Initiation Protocol, J. Rosenberg et al., RFC 3261, http://www.ietf.org/rfc/rfc3261.txt, June 2002.

[13] IP encapsulation within IP, C. Perkins, RFC 2003, http://www.ietf.org/rfc/rfc2003.txt, October 1996.

[14] Generic Routing Encapsulation (GRE), D. Farinacci et al., RFC 2784, http://www.ietf.org/rfc/rfc2784.txt, March 2000.