Mobile IP

Contents

- Introduction 2
    - Basics to IP addressing 2
- The need for mobile IP. 3
    - The natural solution. 3
- Obtaining an IP address using DHCP. 3
    - Advantages and disadvantages. 4
- Obtaining an IP address using a foreign agent. 4
    - Advantages and disadvantages. 5
- Constraints on mobile IP 6
    - Registration/IP renewal and deregistration. 6
- The two crossing problem. 7
- Mobile IPv6 7
- Registration. 8
    - Deregistration 8
- Some solved problems 8
- Summary 8
- References 9

Introduction

Mobile IP is a standard that allows users to move from one network to another without loosing connectivity. Mobile devices have IP addresses that are associated with one network and moving to another network means changing IP address. Using the mobile IP system will allow users to achieve this and at the same time make the underlying process transparent for a user.

Basics o IP addressing

All computers that are connected to the Internet need to have a valid IP address. This address is usually assigned by an Internet Service Provider (ISP) which in turn has bought a block of addresses from the Internet Cooperation for Assigned Names and Numbers (ICANN). Most companies never interact with the ICANN directly. In order for a company to recieive valid IP addresses they contact a local ISP. Even local ISP:s do not interact with ICANN but in turn they contact larger ISP:s and only they contact ICANN.

IP addresses are not assigned randomly, but are carefully chosen. When a host wants to connect to the Internet he is assigned an IP address that represents the network that he is located at. This network is in turn a part of a larger network, which is then again a part of an even larger network, and in this way all networks are arranged, in a hierarchical manner. The IP address is divided into several parts where each corresponds to a given network. The rightmost part in the address always represents the host and the part to the left of it then represents the network that the host is located at and so on. In this way the leftmost part always represents the largest network. This hierarchy can be compared to a resident's home address.

Resident address:
John Smith
Arlington Road 45 3 floor
58 485 London
Great Britain

IP address:
A.B.C.D

Every letter represents a part of the address.

If we are to send a postcard from Sweden to John Smith living in London we would need to specify his resident address on the postcard. We also want to send him a message through the internet in which case we would need to specify his whole IP address. When the postcard reaches the post office they first sort it by the most significant part of the address, namely the country and forward it to that country. The same thing happens when the internet message reaches the first router on the way. The router looks at the most significant part of the address which is A and forwards the message to that network and each router on the way will do the same until it reaches a router in the network A. When the postcard reaches a post office in Great Britain they will look at the second most significant part of the address which then is London. When the message sent through the Internet has reached a router in the network A, that router will look at the second most significant part, in this case B and forward it. Forwarding is done in this way all the way until the postcard reaches John's postbox at his residence. The same scenario is repeated for the message sent through the Internet. It is routed all the way until it reaches the lowest part of the address which is D and this means that the message has reached John's computer.

The need for Mobile IP

The following sections will only consider communication using IP version four (Ipv4) and later on in the paper we will examine the coming IP version six (Ipv6) which solves some of the problems and constraints IPv4 has.

Imagine what would happen with your message if you were to move your computer (and IP address) to another network then your own. The routers would examine the address and forward it according to the previously described manner. When the message reaches the router, that you were directly connected to before you moved, it would not be able to forward the message to you since you have moved. There is no way for a router to know how to reach you and therefore the message will never arrive to you.

Having host specific routes in every router could solve the problem for routers not knowing where to find your address. This means that each router would need to have a list that tells the router where exactly your location is in the Internet. This also means that the list will be proportional to the number of all hosts connected to the Internet. This could seem like a good solution in a small private network (a network that is not connected to the Internet). When connected to the Internet this is not possible since there are extremely many hosts connected to the Internet and this means that each router would have an extremely big list of hosts. This is not scalable since every router that forwards a message needs to go through this huge list for every message which would take to long time. Another drawback is that this list would have to be kept updated when hosts moves. Propagating this information would not scale since many routers need to be notified and by the time this is done, the host maybe already has moved again.

Another solution would be to change the IP address. This on the other hand is time-consuming, especially if you are visiting a network for a short period of time. Moving a computer from one network to a neighboring network often requires the computer to reboot which will break all the existing transport layer connections.

Natural solution

The natural solution to overcome some of the limitations of the original IP addressing scheme is called Mobile IP. The basic idea behind Mobile IP is to let one host have two simultaneous addresses, one at the home network and one at the foreign network. The home network address (primary address) is never changed. This address is always used by applications and transport protocols. The address at the foreign network (secondary address) is temporary; it changes as the computer moves and is only valid at the specific foreign network.

There are two different solutions for a host to obtain a secondary address at a foreign network. Both ways have their advantages and disadvantages and we will describe them both.

Obtaining an IP address using DHCP

One of the methods involves using the Dynamic Host Configuration Protocol (DHCP) server at the foreign network. DHCP is the protocol that dynamically assigns IP-addresses to connected computers on the network. These addresses are valid and have beforehand been assigned by a network administrator to the DHCP servers. The DHCP server chooses one of the available addresses and either permanently or temporary assigns it to the computer on the network. When the mobile host arrives at the foreign network he first needs to discover a DHCP server to obtain an IP address. Discovering the server is easy since it advertises its presence every 20 seconds, but it is also possible for the host to broadcast a question if there are any DHCP servers. Each request for an IP address is required to contain a mobile-home authentication extension that allows the DHCP server to verify the mobile's identity. When the host has received a valid IP address on the foreign network he must then register this address at his home network. On the home network there is a router that is called home agent which must be located on the same physical network as the primary address of the mobile host. When the mobile host registers at home agent he notifies the agent about the newly received secondary address. The point of this is that the home agent is now obligated to intercept all messages destined for the primary address on the home network. The reason that the home agent must be located on the same physical network as the primary address is because the home agent uses proxy ARP[1]. This means that every time someone on the home network or outside the network ARP:s for the mobile host's primary address the home agent must capture the request and provide its own address pretending to be him. If the home agent was not located on the same physical network he would not be able to capture the ARP request that originated from others hosts located on the same physical network. When registration of a secondary address at the home agent has been done all messages sent to the primary address will be forwarded to the secondary address at the foreign network by the home agent. When the mobile host communicates with an arbitrary computer he specifies his primary address as the source address which means that each reply will end up at the home network where the home agent will intercepts it and forward it. The home agent intercepts the message and uses IP-in-IP encapsulation to tunnel the message to the secondary address, meaning that the message will never be altered, just put into a new IP packet. This can be compared to the post office analogy again. If a letter arrives at the post office and the receiver has moved, the address on the envelope will not be correct, the post office will put the letter into another envelope and send it to the correct address. When the new IP packet reaches the mobile host he will discard the outer packet and proceed to the inner packet which contains the message.

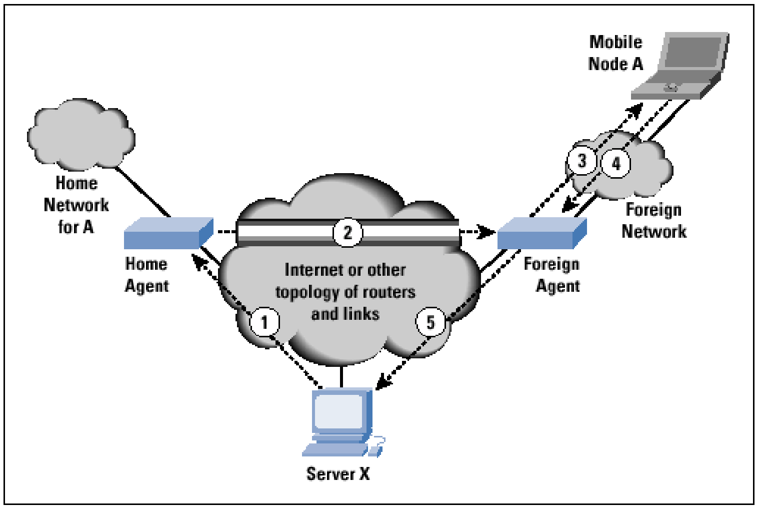
Advantages and disadvantages
The chief advantage with this method is the ability to work with existing internet infrastructure. This means that the host does not have to know anything about how the foreign network is built and know what routers exists on the foreign network since the routers do not know if a host is mobile or not. It could as likely be a stationary computer since DHCP assigns IP address in the same way to stationary computers. The chief disadvantage is that a piece of extra software is required which means that the mobile host must contain facilities to obtain an address and to communicate with the home agent.

Obtaining an IP address using foreign agent

The other method does not include the use of a DHCP server. When a mobile host arrives at a foreign network he needs to discover a foreign agent instead of discovering a DHCP server. The foreign agent is an active entity; a router as the home agent and it sends router advertisement messages telling hosts on the network that it exists. A mobile host can either wait and listen to the network to capture such a message or he can send a router solicitation, a broadcast, to prompt possible agents on the network. When a foreign agent has been discovered the mobile host obtains a valid IP address. The address in

[1] ARP stands for Address Resolution Protocol and allows a host to find the physical address of a target host on the same physical network, given only the target's IP address.

question does not have to be unique; the router acting as a foreign agent can assign it one of its own addresses. Although assigning a unique address makes communication slightly easier, using an existing address means that the visiting mobiles do not consume IP addresses. Before a mobile host can receive messages at the foreign network, he must register like in the previous method. This time the registration at the home agent goes through the foreign agent, meaning that the mobile host must first register at the foreign agent which will register the secondary address at the home agent. If a mobile host has not received a unique secondary address, a foreign agent must use the primary address as an IP destination address. This means that the foreign agent is not allowed to use ARP on the network to find out the physical address of the mobile host since it is not valid on the foreign network. To perform address binding without using ARP, a foreign agent is required to record all information about a mobile host when a registration request arrives and to keep the information during the communication. Thus a foreign agent must record the mobile host's hardware address and when the agent sends a message to the host, the agent consults its stored information to determine the appropriate hardware address and will then send the message using unicast. When someone sends a message to the mobile host, the message will go to the home network. The home agent will capture the message, just as in the previous method, using IP-in-IP encapsulation, but this time send the message to the foreign agent. The foreign agent will then discard the outer packet to be able to examine the inner packet and determine to which host on the network to send the packet using hardware unicast as described before. When a mobile host on a foreign network wants to send a message he will always use the primary address as the source IP. The message will as usual follow the shortest path to the destination, but a reply will have the primary address on the home network as destination where the home agent then will forward it to the correct network. This gives rise to a problem called the two crossing problem and we will examine it further in a later section.



1. A server X sends a message to mobile node A's primary address which is intercepted by the home agent. 2. The home agent tunnels the message to the foreign agent, 3. which forwards it to A. 4.A's reply goes to the foreign agent, 5. who forwards it directly to X.

Advantages and disadvantages

The chief advantages using this method are that there is no need for the mobile host to have any extra software on the computer since all communication with the home agent is done by the foreign agent. The disadvantage with this method is that a foreign network needs a router that will act as a foreign agent. If there is not any, the only way to obtain an IP address on a foreign network is to use the other mentioned method, which uses DHCP.

Constraints on mobile IP

There are some constraints regarding mobile IP using any of the two methods described. One constraint regards ingress filtering which is when a border router on some networks discards packets that contain a source IP that is not located at the network the packet was coming from. This sort of filtering is used to stop spoofing, impersonating someone over the internet by changing the source IP. When a mobile host visits a foreign network he specifies the source address to be the primary address which is not located on the network that he is sitting on and if there were any ingress filtering routers present on the network the packets would be discarded by them. There is a solution to this problem, but it is making the mobile IP system even more inefficient. When the mobile host is responding to a host outside the network he is located at, the ingress filtering router will discard it, unless he IP-in-IP encapsulate the message and sends it back to the home network which in turn forwards the message to the host the message was destined for. This solution is as mentioned not efficient at all since this will congest the internet with unnecessary traffic.

On some networks there are machines that are configured to warn about spoofing, when some host is trying to intercept someone else's packets. This means that two distinct IP addresses can not map to the same hardware address. What will then happen when a home agent responds to the ARP request for let say two different mobile hosts visiting other networks? The home agent will pretend to be both of the mobile hosts not present on the network, if the network has machines warning about spoofing, this would set the alarms off.

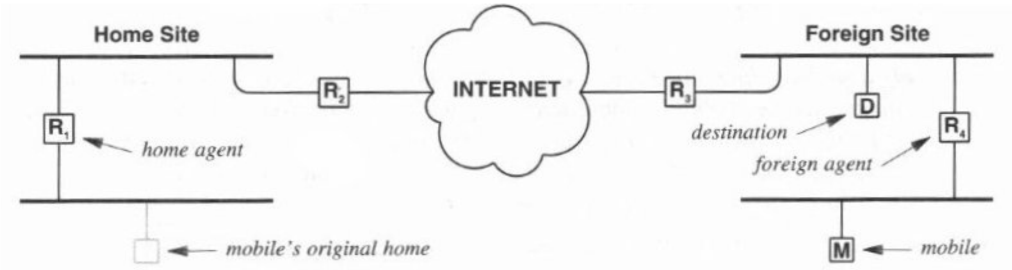
Registration/IP Renewal and Deregistration

In both methods the obtained address assigned by the DHCP or by the foreign agent may expire as well as the registration with the foreign agent. That means that a mobile host is not allowed to keep an address forever or an arbitrary long time and that the foreign agent is only willing to forward messages for a given period of time. When a host registers at the foreign agent, the agent provides the mobile host with a time for which the registration is valid, or for which the foreign agent is willing to forward the messages. When this time is coming to an end the mobile host must renew its registration at the foreign agent if he wants to stay at the foreign network. DHCP works in the same way providing a time for which the IP address is valid for. When this time expires the mobile host must renew the lease of the IP address. In some cases the DHCP server can deny the mobile host to renew the address in which case the mobile host must request a new one or move from the network.

When a mobile host decides to leave the foreign network he must notify the foreign agent and home agent. This process is called deregistration and in the case where a DHCP server is used to obtain the secondary address there is of course no need to deregister at any foreign agent. The home agent will stop intercepting messages for the mobile host since it now assumes that the host is back at the home network. In the case with the foreign agent the mobile host only needs to deregister at the foreign agent which in turn will deregister him at the home agent.

The Two-Crossing Problem

The methods described seem flawless in theory, but there exist one major problem. A visiting mobile host will tend to communicate with computers on the same network that he is currently visiting. Consider a mobile host who has received an IP address at a foreign network and has registered both at the home agent and at the foreign agent. When the host wants to send a message, the source address will like mentioned above be the primary address which is located on the home network. Consider now what happens if the receiver, a nearby computer, wants to reply to the message. The reply will have the primary address as the destination address which means that the reply will go all the way to the mobile host's home network. The home agent at the home network will then intercept the message and forward it back to the foreign network. The problem should now be obvious; the reply could have gone directly to the foreign network instead of crossing the whole internet twice. Hence the name the two crossing problem, the reply could have taken the shortest path to the destination of the secondary address, now instead it crosses the internet two times.



An example that illustrates the inefficiency of mobile IP. When the mobile M is communicating with the local destination D, messages from D will travel across the Internet to the home agent R1 and then back to the mobile host M instead of directly going from D to M.

Mobile IPv6

Mobile IP has only been an add-on, something that IPv4 has supported more or less. In the new communication protocol IPv6 support for Mobile IP is mandatory and many of the restrictions and problems are solved.

A mobile host can determine its current location by listening to the Router Advertisement messages and storing the included network prefix, just as stationary computers in IPv6 do.
When the network prefix does not match the network prefix of the mobile host's primary address, the mobile host realizes that he is on a foreign network.
In that case he selects one of the advertising routers to be his default router.

Auto configuration
To obtain a secondary address the mobile host can either use stateful or stateless address auto configuration. In the stateful auto configuration model, hosts obtain a secondary address, other parameters and configuration information from a DHCPv6 server in the same way as in the IPv4 analogy.
Stateless auto configuration requires no manual configuration of hosts, minimal (if any) configuration from routers and no need for any DHCPv6 servers. This mechanism allows a host to generate its own address using a combination of locally available information and information advertised by routers.

When a router advertises network addresses, the mobile host extracts the network prefix and adds a unique interface identifier to form a secondary address. A mobile host can also force a router to advertise its information. If there is no router present on the network, the mobile host can still generate a network valid address which would allow him to communicate only with other hosts on that link. These two methods are often combined allowing a host to generate an own secondary address and then allow a DHCPv6 server to provide the host with other information.

Using these methods the concept of a foreign agent has been eliminated. Also with the huge address space of IPv6 the Mobile IPv6 deployment is more straightforward.

Registration

When the mobile node has moved to a foreign network and has obtained an IP address it must notify the home agent which will forward messages back to the mobile host. The mobile host sends a binding update notifying the home agent of the secondary address. If the home agent is willing to accept the registration he will send back a binding acknowledgement. When a correspondent host wants to communicate with the mobile host, he will send the message to the home network not knowing that the mobile host has moved. What happens is that the home agent will intercept the message and forward it to the mobile host in the same manner as in IPv4. Once a message has been sent from one host to another, there is a great probability that there will be some further exchange between these two hosts. The mobile host sends a binding update to the correspondent node, telling the node that he has moved and also provides the new address, which is the secondary address. The correspondent host will send a binding acknowledgment and further messages exchanged between these two host will not go through the home agent, but will be sent directly between each other.

Deregistration

When the mobile host moves to a new network or moves home he has to notify the home agent and also all the corresponding nodes that were aware of the mobile host’s location. This is done be sending a binding update to each one of them. In some cases the binding has a lifetime and when that lifetime expires the binding is not valid any more.

Some solved problems

The two crossing problem will be eliminated since the correspondent node will learn the new address and will not sent messages to the home agent.

If there were an ingress filtering router on the foreign network it would not complain in this case since the mobile node would specify the source address to be the secondary address when talking to a correspondent node. In IPv4 the source address would be the home address and as mentioned before, the home address is not situated on the foreign network.

Summary

Mobile IPv4 has solved many constraints and allowed hosts to move to foreign networks without the need for changing the IP address or implementing host specific routes to all hosts. Even though mobile IPv4 has been employed for many years it has some flaws. The new IPv6 has solved many of the problems IPv4 has and in the near future the Ipv6 will take over and exchange the Ipv4 protocol.

References

- Internetworking with TCP/IP 4th ed., Douglas E. Comer.

- Introducing Mobile IPv6 in 2G and 3G mobile networks - paper, NOKIA.
  http://www.bitpipe.com/data/detail?id=1007501662_307&type=RES&x=294970019

- http://www.microsoft.com/technet/itsolutions/network/ipv6/default.mspx