

Mobility and the Internet

email address:

rparry@qualcomm.com

Home Web Page:

<http://people.qualcomm.com/rparry>

wireless packet address:

W9IF @ K6JCC.#SOCAL.CA.USA.NA

ABSTRACT

The explosion in demand for mobile computing, both wire and wireless based systems, places demands on the Internet Protocol (IP) that it was not originally intend to support. The protocol assumed that the point at which a computer is connected to the Internet is fixed. If a host is moved to a new network, the current routing protocol will be unable to route the datagrams to the correct destination. Mobile-IP is the new standard intended to address the mobility issue. The current standard developed by the Internet Engineering Task Force (IETF) is described in RFC 2002. This paper provides an introduction to Mobile-IP. It discusses the requirements for mobility on the Internet and how Mobile-IP provides the necessary functionality.

May 1997

Introduction

There is little doubt that the networking world's ultimate goal is *anywhere, anytime, continuous connectivity computing*. Mobility is becoming a requirement rather than an amenity. With the advent of the cellular phone, people have tasted the flexibility that roaming provides and the freedom to be untethered from the confines of a fixed network. The demand for laptop computers with connectivity to the Internet is yet another example. However, the ability to provide mobile connectivity has lagged far behind the demand. The authors of the Internet Protocol (IP) in the late 60s could not have imagined where their protocol, originally developed to allow a small number of scientists, engineers, and host computers to communicate, would lead. Certainly there was never a requirement for mobility or for automatic reconfiguration of the network when hosts were moved. In fact, IP implicitly assumes that a host is fixed and the IP address registered to the host is a direct function of the network that the host is connected to. This provides the underlying mechanism for datagrams to be properly routed.

The present process of modifying IP addresses is cumbersome and tedious, even for a computer savvy user. The process requires both know-how and coordination with a system administrator. Ideally, we would like to be able to roam from network to network seamlessly. The Mobile-IP working group of the Internet Engineering Task Force (IETF) has developed a standard to do just that. The standard, now called Mobile-IP, is an enhancement to standard IP and is described in detail in RFC 2002. There are actually two mobility standards, one to support the current IPv4 standard and another for the future Internet IPv6 (a.k.a. IPng) standard.

In this paper we will discuss the unique characteristics of Mobile-IP. As we shall see, there are many problems to address in addition to just allowing a mobile host to move seamlessly from network to network. There are issues of security, authentication, routing, delays, and more. For example, what do you do when the mobile is in transit, when it is not connected to either network. Consider also a wireless network which allows a host to be connected to two or more networks simultaneously. Each of these occurrences must be addressed and efficiently solved by Mobile-IP.

Design Requirements

IP was never intended for mobility. Nevertheless, we are faced with the need to provide this functionality without changing the underlying protocol. If we had the luxury of starting over again, hindsight would provide a wealth of wisdom in implementing a mobility protocol. However, given the installed base, the overriding design requirement must be to remain compatible with standard IP.

Mobile-IP must be able to support mobility both wired and wireless LANs. Therefore the Mobile-IP design must be able to function in the harsh wireless world where high error rates are the norm and bandwidth is limited. Taking mobility a step further, the design must accommodate a mobile host in a heterogeneous environment where a mobile host can move between wireless LANs, as well as, between a wire and wireless LAN. The wireless medium leads to unique configurations. For example, consider that a mobile host may be simultaneously connected to more than one network, a situation that would never occur in a wired LAN. However, it happens everyday in a cellular phone network where a user moves between coverage areas that overlap. In the overlapping area, data is received by more than one base station. The cellular network must be able to adapt to this environment and so must the design for Mobile-IP.

Mobile communication often implies battery powered devices, therefore the design should include a protocol with as little overhead as possible to help reduce transmissions and therefore conserve battery power.

A Mobile Supporting Network

To allow a Mobile Host (MH) to move between networks while keeping its fixed IP address, two support components are required, a Home Agent (HA) and a Foreign Agent (FA). A HA is a host on the

network were the MH normally resides. In practice, it is quite possible that the MH is never physically connected to the Home Network (HN). A FA resides on each remote network where the MH wishes to visit. A foreign agent located on a remote network acts as coordinator when the mobile host is visiting. Foreign Network “A” in Figure 1 shows this configuration.

It is interesting to note that it is possible for a FA to exist on a network other than the FN where the MH is temporarily located. In a similar manner, it is not a requirement that the HA reside on the HN. As long as there is a link, the FA and HA may be located almost anywhere. Using *proxy* or *gratuitous ARP* mechanisms it is possible that the agents not be on their respective networks.

It is also interesting to note that Mobile-IP allows a MH to move to a FN without the support of a FA. This allows the mobile host greater freedom since it implies the mobile host can move to any network. When a MH is on a foreign network without the aid of a FA, it must perform the functions of the FA. We will discuss in a subsequent section the advantages and disadvantage of this mode of operation. Foreign Network “B” in Figure 1 depicts this operating mode.

Mobile-IP Overview

The following provides a high level summary of the protocol. This scenario explains the simple case where the HA and FA are located on the HN and FN respectively.

- Mobile Agents (MA) may advertise their presence by sending *Agent Advertisement* messages.
- A MH may solicit MAs by sending *Agent Solicitation* messages.
- A MH uses the MAs advertisements to determine if it is on the HN or a FN.
- When the MH is on the HN, it acts *independent* of the HA.
- When a MH returns from a FN, it must de-register with the HA through *Registration Request* and *Registration Reply* messages.
- When a MH finds it has moved to a new FN, it obtains a care-of address from the FA or from other means such as DHCP.
- When a MH on the FN obtains its care-of address, it registers the new care-of address with the HA using a *Registration Request* and *Registration Reply*.
- Datagrams sent to the HN are intercepted by the HA and encapsulated in a new datagram which contains the care-of address and sent to the FA, or to the MH if it is acting without the aid of a FA.
- Datagrams sent by the MH on the FN need not return to the HA, they may be sent directly to the original source host.

Discovery, Advertisement, and Solicitation

Agent discovery is the method by which a MH ascertains whether it is connected to the foreign or host network. The discovery process relies on the ICMP (Internet Control Message Protocol). It also requires cooperation between the mobile agents and the mobile host. A Mobile Agent may advertise that it is available to provide mobility services or the MH may send a message to ascertain the availability of possible mobile agents, referred to as *Agent Solicitation*. If the MH is connected to a FN, it is provided with a care-of address during the discovery process.

When the MH is away from the home network, it is the responsibility of the HA to accept IP packets normally intended for the MH and forward them to the remote network. This requires the MH to keep the HA informed of its location. This is accomplished when the MH first attaches to the remote network, it uses a special registration protocol to update the HA with its location using the FA. Through the FA, the MH sends a registration message back to the HA indicating its present location. The process

is reminiscent of a child traveling to a friend's house and then calling home to inform the parent (e.g., HA) that he or she has arrived. In this way, the parent (HA) knows where the child (MH) can be contacted.

Multicasting

One might ask how an agent advertises its availability as a mobility agent efficiently? It is true that the mobility agents have a list of mobile hosts that it will support, however, this list could be long and to broadcast individual datagrams to all possible mobile hosts would be inefficient. To solve this problem Mobile-IP uses *multicasting*.

Multicasting meets the needs of Mobile-IP perfectly, since it allows a mobility agent to multicast (advertise) its availability to the local network where it can support mobility services. In addition, the multicasting scheme can limit the broadcast to the subnet. This is exactly what is required since we do not want to advertise availability off the subnet that we can provide service to.

Multicasting, as currently implemented in standard IPv4, falls into the Class E address range, 224.0.0.0 to 239.255.255.255. Messages sent in this range can be received by all machines with routing tables properly configured. However, for Mobile-IP we are interested in sending to only hosts on the local subnet. The IP range for this functionality is 224.0.0.0 to 224.0.0.255 discussed in RFC 1060 under maintenance protocols.

Tunneling (IP within IP)

When the registration process is complete, the HA has the care-of address of the MH. It is then prepared to intercept and forward packets intended for the MH on the home network, to the MH on the foreign network. The forwarding of packets is performed through a process known as *tunneling*. Tunneling is performed by *encapsulating* the original datagram in a new datagram. In this manner, routers that would normally direct the datagram to the address of the "inner" IP address, see only the "outer" IP address and pass it to the foreign agent where the MH now resides. When the FA receives the packet intended for the MH, it *de-encapsulates* the datagram and passes the original datagram to the foreign network where only the MH receives it. The MH is oblivious to the tunneling process. It is the mobility agents that perform all the work and hide the true path that the datagram has taken.

From a routing standpoint, it should be clear that this process is not optimal. For example, all packets intended for the MH are first sent to the HA which results in delays. However, this is a small price to pay for mobility in most applications. In applications that require near real time information such as voice, the additional delay may make this service unusable. Note that the delay is in one direction only. Delays occur for datagrams sent to the MH only. When datagrams from the MH are returned, they are not sent back to the HA, but are sent directly to their destination.

A few subtle points are worthy of particular attention. One should not confuse the care-of address with the IP address of the Mobile Host. The Mobile Host's IP address never changes, only the care-of address is changed to indicate to the Home Agent where the Mobile Host can be located. In addition, the care-of address is the end of the tunnel and it may or may not be the address of the FA.

Mobility without a FA

When a FA is available, it gives the HA its own IP address to use as the care-of address for the MH. This mode conserves IP addresses and places no limitations on the number of mobile hosts allowed on the network. There can be any number of MHs on a FN since they all have a single care-of address, which is the foreign agent care-of address. This is the preferred mode of operation since it conserves IP addresses and requires no IP administration. In this mode the HA tunnels datagrams to the FA by

encapsulating the true source IP address within an IP header that contains the IP address of the FA. When the datagram reaches the FA, it is de-encapsulated and sent to the MH.

A second mode supported by Mobile-IP provides the MH with a *co-located care-of address*. One mechanism for dynamically dispensing the temporary IP *co-located care-of address* is the Dynamic Host Configuration Protocol (DHCP). Under this mode of operation, there is no longer a need for the FA. This provides the MH with greater flexibility since the MH is not limited to networks that have a FA. The disadvantage is that each MH must have a unique IP address which ultimately limits the number of MHs on the network. In addition, de-encapsulation must be performed by the MH in the absence of the FA.

Conclusion

As the size and cost of computer systems continues to plummet, the interest and demand for mobility continues to soar. The use of the Internet as an information resource and vital form of communication will continue to attract new users and new applications placing further demands to support functions that the original Internet Protocol was never intended to support. The authors of the protocol could not have imagined where their idea would eventually lead. It is a tribute to their acumen that the protocol has withstood the test of time and provided sufficient flexibility so as to support an incredibly wide range of applications.

Mobile-IP is still in its infancy. Various implementations are being developed. Although there is still additional development work that needs to be done, we are well on our way to supporting innovative uses. With Mobile-IP we are one step closer to the goal of anywhere, anytime, continuous connectivity computing.

Bibliography

- Atkinson, R. "*Security Architecture for the Internet Protocol*," RFC 1825. Available at <ftp://ds.intenic.net/rfc/rfc1825.txt>.
- Badrinath, B.R., et. al, "*Handling Mobile Clients: A Case for Indirect Interaction*," 4th workshop on Workstation Operating Systems, pp. 91-97. Also available from <ftp:paul.rutgers.edu/pub/badri/wvos4>.
- Balakrishnan, Hari, et. al., "*A Comparison of Mechanisms for Improving TCP Performance over Wireless Links*," ACM SIGCOMM '96, Stanford, CA August 1996.
- Caceres, Ramon, "*Improving the Performance of Reliable Transport Protocols in Mobile Computing Environments*," IEEE Journal on Selected Areas in Communications, Vol. 13, No. 5, June 1995 pp. 850-857.
- Dixit, Abhijit, Vipul Gupta, "*Mobile-IP for Linux (ver 1.00)*," Documentation for the Linux Mobile-IP software. Available in postscript format via <http://anchor.cs.binghamton.edu/~mobile/MIPv100/Doc/mip-doc.v100.ps>.
- Droms, R. "*Dynamic Host Configuration Protocol*," RFC 1541. Available at <ftp://ds.intenic.net/rfc/rfc1541.txt>.
- Johnson, David B. and Charles Perkins, "Mobility Support in IPv6," draft-ietf-mobileip-ipv6-02.txt. November 26, 1996. Available from <http://www.ietf.org/ids.by.wg/mobileip.html>.
- Johnson, David B., "Route Optimization in Mobile IP," draft-ietf-mobileip-optim-05.txt. November 26, 1996. Available from <http://www.ietf.org/ids.by.wg/mobileip.html>.
- Lancki, Ben, et. Al., "*Mobile-IP: Transparent Host Migration on the Internet*," Linux Journal, August 1996, pp. 10-11, 65.
- Myles, Andrew, et. Al. "*A Mobile Host Protocol Supporting Route Optimization and Authentication*," IEEE Journal on Selected Areas in Communications, Vol. 13, No. 5, June 1995, pp. 839-849.

- Perkins, C. “*IP Mobility Support*,” RFC 2002. October 1996. Available at <ftp://ds.intenic.net/rfc/rfc2002.txt>.
- Perkins, Charles E, Pravin Bhagwat, “*A Mobile Networking System based on Internet Protocol*”, IEEE Personal Communications, First Quarter 1994, 99. 32-41.
- Perkins, Charles, “*Providing continuous network access to mobile hosts using TCP/IP*,” Computer Networks and ISDN Systems 26 (1993) pp. 357-369.
- Perkins, Charles, et. Al., “*IMHP: A mobile host protocol for the Internet*,” Computer Networks and ISDN Systems 27 (1994) pp. 479-491.
- Teraoka, Fumio, et. Al, “*IP: A Protocol Providing Host Mobility*,” Communications of the ACM, August 1994, Vol. 37. No. 8, pp. 67-75.
- Woodward, R. “*A Scheme for an Internet Encapsulation Protocol*”, RFC 1241. Available at <ftp://ds.intenic.net/rfc/rfc1241.txt>.

Mobile-IP Related Web Sites

Internet Engineering Task Force home page: <http://www.ietf.cnri.reston.ca.us/home.html>.

Mobile-IP for Linux home page: <http://anchor.cs.binghamton.edu/~mobileip>

Biography



Richard Parry, holds a BS in Electrical Engineering from the University of Illinois, (Urbana, Illinois), an MBA from Northern Illinois University, (DeKalb, Illinois) and a MSCS from North Central College (Naperville, Illinois). He is currently attending the University of California San Diego where he is studying computer science. He is a licensed Professional Engineer and has authored papers in various areas including: Wireless Packet Networks, Oxygen Monitoring Systems, Programmable Electronic Safety Systems, Computerized Security Systems, speech synthesis and recognition, management tools, and amateur radioteletype.

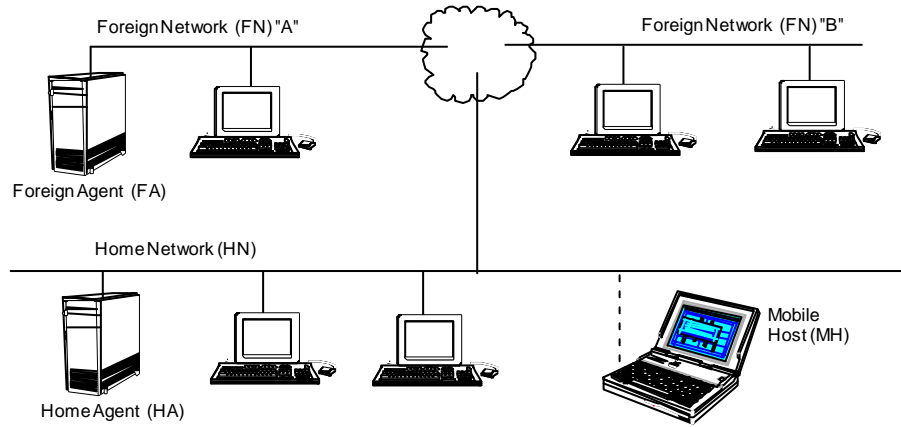


Figure 1

A Mobile Host is associated with a Home Network that is supported by a Home Agent normally connected to the Home Network. The Mobile Host may travel to a Foreign Network supported by a Foreign Agent such as network “A”. Mobile-IP also allows the Mobile Host to visit a Foreign Network that does not have a Foreign Agent such as shown in network “B”. In this latter case, the Mobile Host must provide the functionality normally provided by the Foreign Agent.