Mobile-IP: A Promising Technology for the Mobile Wireless Internet Users Fraternity

Shilpa Gambhir[1], Karishma Bajaj[2], Shashank Singh[3]
[1,2,3]Asst Prof, ECE Department ,
M.M University, Sadopur, Ambala, Haryana
shilpagambhir@ymail.com[1], vlsi.er86@gmail.com[2], shankyrock11@gmail.com[3]

Abstract:-Internet has become a most essential and irresistible part of our life. We can't even imagine a second without it. Everyone in today's world want to remain connected to the internet 24X7. And why not, as internet is the worldwide source of information that can be accessed from anywhere irrespective of the location. This paper provides an overview on the technology that is used to provide uninterrupted internet access to the mobile device users. All computers that are connected to the Internet need to have an official IP address. Mobile IP (or IP mobility) is an Internet Engineering Task Force (IETF) standard communications protocol that allows users to roam from one network to another while maintaining a permanent IP address without disconnecting from the network. Mobile IP and DHCP are two protocols that are implemented together for their usage in wireless computers. Mobile IP is the only current means that offers flawless roaming to mobile computers in the Internet.

Keywords: Mobile-IP, DHCP, IP, roaming

I. INTRODUCTION

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. When a mobile computer is not physically connected to it’s home subnet, IP is incapable of routing packets to it correctly. This then provides the motivation and the fundamental objective for Mobile IP: to allow a computer to maintain normal communications with its home network and all other nodes on the Internet regardless of its point of attachment and while it is moving. Mobile IP is an internet protocol that helps a mobile device user to remain connected with the internet without being disconnecting while moving from one network to the another network within the internet. The number of users accessing web through mobile devices is increasing tremendously and they want continuous and uninterrupted access to the internet even when they are moving from one location to another. Devices that are connected to internet have IP addresses that are associated with one network and moving between different networks requires change of IP address. Mobile IP is most often found in wired and wireless environments where users need to carry their mobile devices across multiple LAN subnets. This protocol was designed to support faultless and continuous Internet connectivity. The goal of IP Mobility is to maintain the TCP connection between a mobile host and a static host while reducing the effects of the change of the location while the mobile host is moving around, without having to change the underlying TCP/IP protocol. This protocol may be used for roaming between overlapping wireless systems, e.g., IP over DVB (Digital Video Broadcasting), WLAN, WiMAX and BWA (Broadband Wireless Access), 3G network used for mobile televisions, Internet hotspots found in cafes, airports and book stores.[2]

II. NEED OF MOBILE-IP

Traditional IP does not support mobility, which means that we have to keep our IP addresses wherever we are. We need new IP addresses whenever we change our location. Changing IP address forces TCP to establish a new connection. As a result, packets might get lost during this change. Moreover, a mobile node will be assigned a foreign IP address instead of a local IP address. A device on a network is reachable through normal IP routing by the IP address it is assigned on the network. The problem occurs when a device roams away from its home network and is no longer reachable using normal IP routing. The outcome is that the active session of the device is terminated. Mobile IP enables a user to keep the same IP address while traveling to a different network (which may even be on a different wireless operator), thus ensuring that a roaming individual could continue communication without sessions or connections being dropped. [1] A mobile node has two addresses: A permanent home address and a care of address (CoA), which is associated with the network the mobile node is visiting. Mobile IP introduces the following new functional entities

- Mobile Node (MN): It is a host or router that changes its point of connection from one network or sub network to another, without changing its IP address.
- Home Address (HA): It is the IP address assigned to a mobile node, which remains unchanged regardless of where the node is connected to the internet.

- Home agent (HA): HA is a router on a Mobile Host's (MH) home network which tunnels datagrams for delivery to the MH when it is away from home, maintains a location directory (LD) for the MH. HA stores information about mobile nodes whose permanent home address is in the home agent's network.
- Foreign Network: FN is a network other than the mobile host's home network.
- Foreign agent (FA): FA acts as a router on a MH’s visited network which provides routing services to the MH while registered FA stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP. FA de-tunnels and delivers datagrams to the MH that was tunneled by the MH’s Home Address.
- Tunnel -Tunneling is a technique use to encapsulate the data packet to reach the tunnel endpoint, and de-capsulate when the packet is delivered at that endpoint. In this case primary IP address is encapsulated in the secondary IP address.
- ARP (Address Resolution Protocol) – This network layer protocol associates an IP address with its MAC address (physical address of node) [3].

III. OBTAINING AN IP ADDRESS USING DHCP

Dynamic Host Configuration Protocol (DHCP) is a standardized protocol used on Internet Protocol that dynamically assigns IP-addresses to connected computers on the network and reclaim them when they are no longer in use. It is client-server program, that is, there is a DHCP client and a DHCP server. DHCP server chooses one of the available addresses from its pool of available addresses and either permanently or temporary assigns it to the computer (DHCP client) on the network. The whole process is initiated by the DHCP client. The client first broadcasts a DHCP discover message to locate a DHCP server on the network. The server which has available pool of IP addresses responds with a DHCP offer message, which means that the server has IP address to assign. DHCP server issues IP addresses for a specific duration of time. After that duration, the client must stop using the IP address or sends the request to the server to renew it. On receiving a valid IP address on the foreign network a host must then register this address at his home network. When the mobile host registers at home agent he notifies the agent about the newly received secondary address.

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 a random computer it specifies its 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. If the home agent is not located on the same physical network it will be impossible for it to capture the ARP request that originated from other hosts located on the same physical 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 (Address Resolution Protocol).The home agent intercepts the message intended for the primary address on the home network 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. When the new IP packet reaches the mobile host, the mobile host will discard the outer packet and proceed to the inner packet which contains the message. [5]

IV. OBTAINING AN IP ADDRESS USING FOREIGN AGENT

In this technique, a mobile host sends a router solicitation message to prompt possible foreign agents on the network. When a foreign agent has been discovered the mobile host acquires a valid IP address. It is necessary that mobile host must first register at the foreign agent which will register the secondary address at the home agent. 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. 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. For this reason, a foreign agent must record the mobile host's hardware address and when the agent sends a message to the host, the agent check its stored information to determine the appropriate hardware address and will then unicast the message. When someone sends a message to the mobile host, the message will go to the home network.

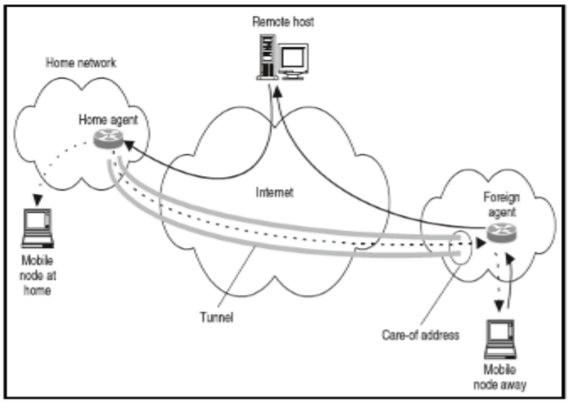

Fig.1 Mobile-IP data flow diagram [4]

The home agent will capture the message, just as in the previous method, using IP-in-IP encapsulation, but this time sends 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. When a mobile host on a foreign network wants to send a message it uses the primary address as the source IP and the reply will comprise of the primary address on the home network as destination where the home agent will forward it to the correct network [2]

V. FEATURES OF MOBILE IP

- No need to modify the current IP address of the mobile device.
- Supports authentication scheme to provide security.
- Mobile IP leaves transport and higher-level protocols unaffected.
- It overcomes the geographical limitations of the traditional IP.
- Modifications to other mobile devices/routers are not required.
- Provides global, application independent mobility to access internet
- Make mobility of a user transparent to applications and higher-level protocols such as Transfer Control Protocol.
- No special software is required.
- Provides confidentiality of the data that is, only the sender and receiver can have access to the data [6].

VI. CHALLENGES TO MOBILE IP

Mobile IP is an elegant and relatively simple solution to seamless geographically-unconstrained roaming. It is built on top of the current version of IP in a way that is transparent to the stationary nodes which want to communicate with the mobile nodes. However, as the Internet evolves and new challenges are met, Mobile IP must often include improvements to overcome changes in today’s networks.

1. Ingress filtering is related to the changes in security policies that sub networks are implementing.

2. Route Optimization creates a potentially substantial performance increase for Mobile IP at a cost of a slight increase in complexity

3. Fault Tolerance, Load Balancing and Congestion Control are very important which are required so that the system doesn’t stop working in case of any type of failure.

VII. CONCLUSION

Mobile IP has emerged as a benefit for the mobile device user as it allows a user to enjoy interrupt free internet access irrespective of the change of location. It has the potential to become an important feature of the coming era's internet. Connectivity to the Internet while in motion is becoming an enormously important part of computing research and development. Mobile IP makes boundaries between attachment points invisible, as it is able to track and deliver information to mobile devices without the requirement to change the device’s long-term Internet Protocol (IP) address.

REFERENCES

[1] en.wikipedia.org/wiki/Mobile_IP
[2] http://www.cse.wustl.edu/~jain/bnr/ftp/f33_mip.pdf
[3] http://www.cs.jhu.edu/~cs647/class- papers/Routing/mobile_ip.pdf
[4] http://cdn.ttgtmedia.com/digitalguide/images/Misc/mobile- ip-ch10-1.gif
[5] http://www.cse.chalmers.se/~tsigas/Courses/DCDSeminar/ Files/Mobile%20IP.pdf
[6] www.cs.ucy.ac.cy/courses/EPL476/slides/C07- MobileIP.ppt
[7] 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.

[8] 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.

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

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

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

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

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

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

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

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

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

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

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

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