Multihoming Mobile Computing Architecture

Kewal Krishan Sharma, Dr. Rakesh Dube

1 Ajay Kumar Garg Engineering College, Ghaziabad, UP, India
2 Department of Mathematics, Faculty of Science, Greater Noida Institute of Technology
Email: k.sharma@akgec.org

ABSTRACTS

Mobile computing has liberated users to leave their place and work while they are roaming all over the world. Multihoming is connecting the sources and destinations via various routes simultaneously. The Multihoming is used extensively in IPv4 architecture. Due to exhaustion of IPv4 and not fully implementation of IPv6 the Mobile computing has been restricted to certain domain and not reached yet to every user device. But IPv6 will create a tremendous development in Mobile Computing due ample IPv6 addresses. Due to the scarcity of IPv4, IPv4 world had adopted many methods such as NAT (Network Address Translation), Subnetting and CIDR (Classless Inter Domain Routing). Due to this mobile computing was not so much flourished. There is great requirement of Mobile Multihoming in world of dual stack world of IPv4 and IPv6. Once IPv6 fully placed the world will be of mobile devices and Multihoming, so we called it Multihoming Mobile Computing (MMC).

Keywords: Multihoming, IPv4, IPv6, Mobile computing, dual stack IP world.

1. INTRODUCTION

1.1 Mobile computing

Mobile computing [3] is a form of moving human with device such as computer, AS (Automated System) from one network to another network of computer network. Computer interaction by which an AS is expected to be connected while it is mobile (not stationary) during normal operation or in continuous use. Mobile computing has three parts: Mobile hardware, Mobile communication, and Mobile software. The first part includes communication related matter in ad-hoc and infrastructure networks in term of wireless communication, Mobile phone network communication, and as well as communication properties, protocols, data formats and concrete technologies. The second part is on the hardware, like mobile devices or device components. These devices can be laptop, tablet, mobile phone and other such device. The third is about the those s/w which are design in such way that they keep on work flawlessly while the device is keep on changing it location from one network to another network. The wireless networking had greatly enhanced the utility of a portable computing device.

1.2 Multihoming

Fig. 1 Example of Multihoming
Multihoming provides:
- Redundancy
- Load Sharing
- Enhance Performance

Multihoming can be established
- Multiple Internet Address on same NIC
- Using several ISPs
- Multiple Network Interface card

The Fig.1 depicts the Multihoming architecture, an example of multiple ISPs and Multiple interface card Multihoming. Two routs are established to reach Multihomed remote machine. IPv4 [5] has credit to development of Multihoming. The acute shortage of bandwidth and the often failure are the reasons why the multihoming is developed. In starting Multihoming was for to get access the data more speedily, but soon it become the way of increasing dependability. But as the increasing success as a tool it became popular for handling link failure mechanism also. Mobile computing has following comparison with wired network.

**Wired Networks**
- Physical wire connection
- Permanent Connection
- High bandwidth & variability
- Visible and known terminal
- Support high end machines
- High resource machines
- Low response time
- Connected operation

**Mobile Networks**
- Wireless connection within proximity
- Ad-hoc connection
- Low bandwidth & variability
- Hidden terminal problem
- Support low end machines
- Low resource normal machines
- Higher response time
- Disconnected operation

Fig. 2 Mobile and Wired network

2. PROBLEM & DISCUSSION

There are some issues which are to be discussed and to work on for future problems avoidance. As Multihoming becomes more popular it started putting additional load on the internet routers and gateways. When a single link establishment, Multihoming may creates more than 1 rout may be 4 to 5 links routs. This increases the routing table entry and creates an additional routing load [6] on routers and Gateways. Multihoming is also used to increase severity of various attacks like DOS denial of services, spamming and such others. These loads can be understood easily, but also be reasons for slow internet performance and often congestion. Mobile computing enhances the effect of Multihoming by two reasons.

1. Mobile computing provides more time to user to be remaining connected, user can be connected to the network all the time while user is not on the sitting place otherwise when user leaves the place the user put of the machine or quite the login.

2. Multihoming creates more connecting routes all the time. So the software generates more multi paths for that location. When users leave that place these routes remain active and unattended at least for sometime.

Multihoming is also be used to use channel capacity. Since single stream of data do not use full capacity of the channel. There are certain problems, faced by the current mobile network [2], such are frequent disconnections. The wireless networks are purely dependable on ad-hoc connectivity and line of site for signal strength. Mobile computing has security problem [1]. The mobility is achieved on the basis of temporary connection where ever the user moves with moving devices, the available network gives a
temporary connection which in actual remains ad-hoc and partially secure. It is not like Mobile phone where one vendor provides infrastructure to all over places. In mobile computing user has to connect to the networks which are available there. The most of the time user does not know what IP user will get and how user gets routed to internet. User works many times in a complete heterogenous network. Depending on the network the security of user computer operation highly compromised. This is bad for both client as user and as well as the network. The effects of multihoming increase the effect of the security breach and this overloads the user computer and the network itself. Suppose a user comes in the network that has double connectivity fig. 3, assuming user has a data card of mobile company and user’s device get connected with available Wi-Fi in a new place and user’s device creates multipaths using Multihoming. Since he is authorized separately for both networks a malicious program reside in the user laptop which user got infected at the previous location, and where user worked sometime before. This program will easily scan the new network available. Since such malicious program is sitting in laptop which is authorized in current network, it can take over the control of this laptop and may play malicious activities like broadcast, open port scanning of local other computers. Since this program has two networks it can bypass the securities of both network by combine two networks, behaving as router of two networks. Using multihoming it can makes fool remote machine easily and easily breach the security of remote host.

In Fig.3 the user is connected in a public network where user has access to available Wi-Fi network through its Wi-Fi Network card. User has mobile data card which provide him a 3 mbps 3G connection. Some software like torrent and other downloader are creating multi paths using multihoming.

Fig.3 User in Multihoming and Mobile Network

The IPv4 model is facing seriously following other concern:-

a). Route Congestion & network overloading

Ad-hoc network faces several types of attack such as Location Disclosure, black hole, replay, wormhole, denial of services, routing table poising, rushing attack, masquerading, virus and passive listening with traffic analysis. These are direct challenges to Mobile networks. Multihoming extended the severity and may bring down the network to standstill.

Another issue is dual stacks world fig.4. To a mobile machine, is very difficult to judge an unknown network. Whether stay on IPv4 network or shift to IPv6 in new network. These will creates a situation in which, many packets be routed from the both network because both network will be there.

The fig.4 explains how IPv6 [4] will connect the devices in future. Devices behave as Autonomous System (AS) like camera, mobile phone, Digital TV. These can be connected to internet via ISPs, one ISP is providing Internet via Mobile services while other ISP through public place Wi-Fi. These are available at airport, metro rail, hospitals, hotels and big organisations.
The fig. above depict that how Dual stack world persist now of IPv6 and IPv4.

We had created the test bed as shown in Fig. 5. One laptop used with having following type of connectivity.
1. Wi-Fi connection
2. Fiber connection (Ethernet Port)
3. Mobile phone used as Modem
4. Connection of mobile data card and,
   HTC Mobile used with following Connection.
1. Wi-Fi connection
2. Mobile phone internet connectivity

We connected these devices at work place, home, public transport systems. We used both IPV4 and IPV6 protocols. We used window 7 on laptop, IPV4 and IPV6 enabled and android 2 on HTC mobile. The following tools used.
1. DAP and torrent as downloader
2. Speed testing tools, testing website
3. Ping tools
4. Trace route tools
5. Web explorers like IE, Mozilla, and Google Chrome

We analyzed various aspect of Multihoming with mobile Computing are. We checked connectivity at various places and response times. Web browsing used at various point while moving. There were lot of disconnection and slow response times while moving. Traceroute used to see how the packets are forwarded and traveling across the network. During the transmissions using remote desktop logins we faced lot disconnection due entering in new network. At some location connected system behaved mysteriously. For example sometime packets forwarded to unknown gateways and then lost without reply or sometime the response time reaches in thousands milliseconds. Sometime browser stuck-up and it needed to reboot the system to established fresh connection. Sometime server refused to get fresh connection since the early remote login was active which we connected from early location. It has been seen that some unattended connections were still open when we returned to same locations. At overlapping zone device start change IP addresses for both overlapping networks so frequently to work properly, due auto connection condition started to connect one network than other network as the strength increases and decrease.

IPv4 use NAT [3] and subnetting and CDIR [7] to overcome shortage of IP. Multihoming will be more effective in Mobile computing since IPv6 will provide individual unique IP address to AS device. It will force
to use the IPSec, which will reduce the risk of the packet to interrupted and interpreted in the channel. Auto configuration of IPv6 greatly helps to produce proper network easily. This will support more easily implementation of Mobility without changing IP in different Networks. Due this device may able to work with it unique IP address rather than network dependent IP. But there should require more effort to implement such thing, need more open network that allow any type of IP to get connected with WAN. Proxy and NAT requirement will not be there, due to this, hopes will be reduced in each packet transmission.

Fig. 6 Use in mobile computing

Let us examine another instance as shown above. There are three locations we called it A, B and C locations. User X who is mobile and keeps on changing locations due to mobile status. Locations A and B are far away, so there is middle location where none of the two network reach. While B and C overlapped at some place and the network strengths of both varies.

One user start works at location-A user get connected to remote host RH via network. The IPv4 IP are used, due shortage of IP, everywhere the NAT is used and user works with address LAN address at different places. As fig.6 depict user get a IP of 192.168.x.x series at location A, while user moved to location B user get the IP address 10.10.x.x and in location C user gets IP series 172.16.x.x, this way, user gets a different IP at all different locations. This creates problem at remote host where user after authentication from location A and remote host authorizes the user on the basis of IP address. Since user does not have real IP, user’s router or gateway IP will be authorized at remote host. When user reaches in the no signal area user’s all connection remains open for location A. The multihoming multipaths are established will remain open. When user reaches location B user get new IP and user’s router/gateways will used as authorized computer but the remote host will treat it as unauthorized connection and abruptly force close connection. User has to relogin from new location.

While user reach at overlapping area the situation can further worsen since as the laptop keep on changing position, signals strength start changing of both network, as the strength increase of the B location, the DHCP of B location gives it LAN IP of series 10.10.x.x and user get connected that LAN. But soon C strength increase and laptop get IP of series 172.16.x.x. Such keep on changing IP, confused the network routing and the remote host and computer fails to perform and network also do unnecessary work to packet transferring unnecessary. The situation becomes more critical when both networks ask user Login/Password again and again.

The other future major problem will be that IPv6 can not be implemented in single slot by just switching off IPv4 and Change over to IPv6. When a packet leaves the source, then in-between routers rout the packets. They use lookup tables to keep routing information
such as IP address of the source, in form of routing tables. The speed of a route is effected by the speed of slowest routing point. 

Virus Attack is creating lot of traffic, virus is working maliciously. Mobile Multihoming increases effects of attacks. 

There will be a great concern how the firewall and other control will be implemented on such open network. While using Mobile computing the firewall implemented on premises LAN will not allow user to access organisation resource when he goes on WAN, by real IP in mobile Computing. Still in IPv4 all real IP are controlled by the ISP, the same may be applied in the IPv6. 

Another problem is that even all is ok the rest of websites are not IPv6 enabled. Windows like OS are using IP Teredo Tunneling Pseudo-Interface as conversion method. This tunnel creates a packet of IPv4 from IPv6 and then again IPv4 to IPv6. This conversion consumed a heavy computing resource. In our test with roaming from one place to other place we found lot of disconnection to remote machine, while doing ping and trace route such IPv6 machine. While ping such machine with stationary positions there were very lesser disconnections. 

IPv4 router has to route those packets which have less data payload and great addition packet related information. They will contain IPv6 header inside IPv4 data packet payload. So in actual they are doing data communication in very less efficient way. We see how much time is going to be consumed in IP conversion at source and destination node. If they are using Multihoming than there is huge computing resource like CPU cycle and RAM memory are going to be consumed. Due to multihoming an additional load occurs since there is further complicity is there to combine the packets of various streams a compare to a single stream.

There will be a situation when a mobile computer with multihoming will face problem when some of the packet is routed through IPv4 network and some packet will routed on IPv6. There may be situation even better rout available on either IPv4 or IPv6 network but the system will not able to use it while entering in to new unknown network. This will create under utilization condition.

3. CONCLUSION

In future the Mobile computing will heavily mixed with normal fixed networking computing in due to IPv6. It is assumed that Multihoming mobile computing has to face a critical and difficult time in the process of transition from IPv4 to IPv6 world due openness and flexibility generated by IPv6. The all websites of normal user are hosted on those computers who are installed in non movable premises. But soon each user may install website which are related to them in their own laptops and there website will move with them since they will not want to pay extra money to cloud computing and other such resources due to money reason and due security reasons. Since Multihoming with mobile computing and implementation of IPv6 will easily available the freedom to make user’s device visible to everybody on the net at any time. This will conflict the current world of firewalls and isolation mechanisms of security system. Currently we are facing such problems in our organisations, the departments want internet access also and intra-department isolations on same computer.
4. FUTURE SCOPE

Future scope of the matter discussed is very wide and lot of the work has yet to be done. The major work will come when the IPv6 will be implemented largely. At that time mobility of devices is going to be tremendous. There will be numerous and complex issues, when two heterogeneous IPv4 and IPv6 worlds will be there with mobile devices such as IP enabled camera, GPS, PDA, iPad, transport system and such others devices. The new simple, more effective and secure protocols will require. The increase dependency on computer and Internet with required availability to access information all the time, at all location of the earth, had created a lot of pressure on the computing infrastructure especially on computer network. So we see the future of Multihoming Mobile Computing Architecture.

REFERENCES


