IP MOBILITY SUPPORT TO MOBILE COMPUTING

Er. Navjeet Kaur

Department of Computer Science and Engineering,
IGET, Abhipur, Mohali, Punjab, India
navjeet_kharr@gmail.com

ABSTRACT - Mobile computing is all about taking a computer and all necessary files and software out into the field, using the resources regardless of the location. In this general paper we discuss about IP inter-networks in mobile computing environment and various protocols like Mobile IP, DHCP and RDP support to mobile users which make the network secure and efficient. Moreover, we focused on Mobile IP and its various issues in mobile computing environment. The paper consists of six different sections. The first section is a general discussion about mobile computing and its relationship with other computing. In the second and third section, we discuss about mobile computing environment and basic principal of designing the same. Forth section is about IP network attachment to mobile computing where we discuss in detail about Mobile IPv4 and Mobile IPv6. In the fifth and sixth section we discussed two more protocols DHCP and RDP for the sake of completeness. The paper ends with a general conclusion.

I. INTRODUCTION

Mobile computing can be defined as the environment in which user(s) has the ability to access critical data regardless of location. Data from shared file systems and databases must be made available to programs running on mobile computers. Mobile computing has become the junction of two technologies i.e. the appearance of powerful portable computers and the development of fast reliable networks [1], where portable computers includes smart phones, PDA, wearable computers, laptops etc. Here we can say that grid computing, cloud computing, utility computing, edge computing and mobile computing all are special cases of each other.

1.1. Relationship between Nomadic- Mobile Computing

Mobile computing requires wireless n/w to support outdoor mobility and handoff from one n/w to the next at a pedestrian or vehicular speed. For example, Traveler in car using laptop connected with a GSM phone is engaged in mobile computing. On the other hand, Nomadic computing refers to limited migration i.e. within a building at a pedestrian speed. For example, users carrying laptop with DIAL-UP modems are engaged in nomadic computing. Ubiquitous computing as a combination of both refers to access to computer network all the time at any location by any person and it can not be realized unless mobile computing matures.

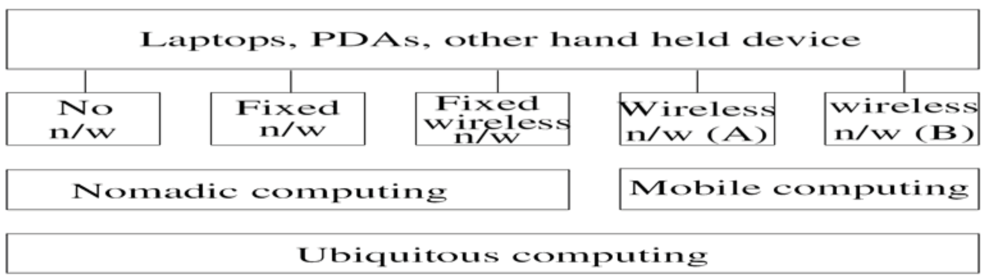

Figure 1: Relationship between Nomadic and, ubiquitous and mobile computing.

II. BASIC MOBILE COMPUTIMG ENVIRONMENT

The architecture consists of Mobile units, fixed hosts and Mobile support stations. Mobile support stations are designed to communicate with mobile units through a wireless interface. Mobile units are portable devices which are moving one location to another either in there home network or might be in another network. Home network is a limited geographical area to which the mobile agents belong also called as cell. Fixed hosts will communicate over the fixed network, while mobile units will communicate with other hosts (mobile or fixed) via a wireless channel. Each cell contains an antenna and is controlled by a solar or AC power network station, called the base station. Each base station in turn is controlled by a switching office (fixed host) called a Mobile Switching office (MSC). The MSC coordinates communication between base stations and mobile service station. It is computerized centers that keep track of user's registration, resources usage by users and billing.

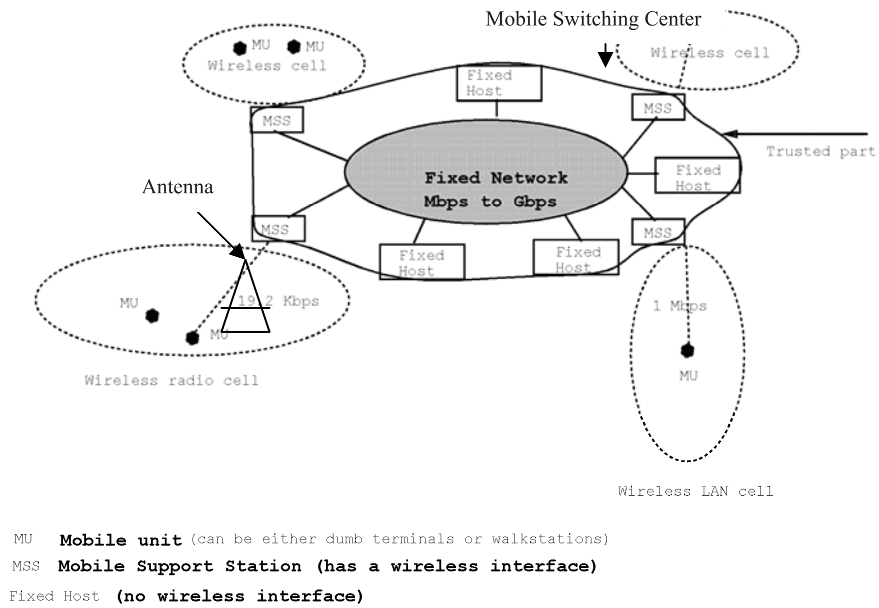

Figure 1: Mobile Architecture [1]

III. DESIGN PRINCIPAL FOR MOBILE COMPUTING

Major requirements of mobile computing are that they should be self organized and structured. By self organization we mean if it is able to manage itself by not depending upon any centralized control where on the other hand, structuring means every entity should be connected to other in a peer to peer fashion. The design paradigms that guide us in building mobile networks, as mentioned by Dr. habil. Christian Prehofer Research Leader, Nokia Research [2] is listed below:

- Design local behavior rules that should be able to achieve global properties: This design principal tries to allocate the responsibility among the individual entities. No single entity is in charge of the overall organization. In this, if the localized behavior rules are applied to all entities, these rules automatically lead to the desired global property.
- Do not aim for perfect coordination, exploit implicit coordination: mobile computing should not be designed with the goal of ideal synchronizing rather, try to achieve the level which is understood and easy to maintain or we can say robustness often more important than perfect or optimal solution [3].

- Minimize long-lived state information: keeping all the information at all the time is one of the main challenges of mobile computing. This problem should be minimized with the help of well suited routing protocols which will main only relevant information according to the communication requirement.
- Design protocols that should adapt to changes: this principal is quite related to the one we just mentioned earlier. Most of the routing protocols that we use are required to keep the entire topology for the transmission of messages but our requirement is to keep minimum and achieve maximum.

Figure 2: Summary of Principals. [3]

IV. MOBILE COMPUTING ATTACHMENT TO IP INTER-NETWORKS

4.1. Major Problem in Mobile Network

The Internet infrastructure is built on the top of Transmission Control Protocol (or TCP) and Internet Protocol (or IP). IP require the location of any host connected to the internet network to be uniquely identified by an assigned IP address. IP address (or local address) is currently in 32-bit address that consists of two parts, the higher order bits of the address determine the network on which the device resides and the remaining lower order bits determine the device number. This raises some of the most important issues in mobile computing

- When a mobile device moves to another location, it has to change its IP address.
- The mobile device has to keep its IP address the same for unique identification and also changing the IP will cause the connection to be disrupted and lost.

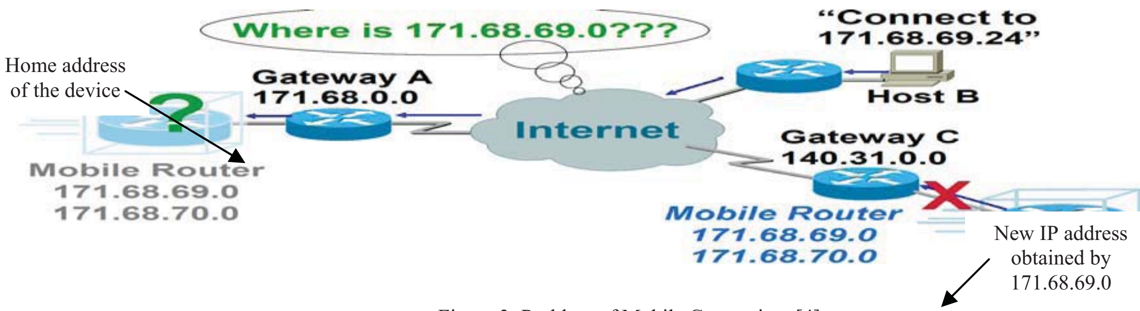

Figure 3: Problem of Mobile Computing. [4]

4.1.1. Mobile IPv4 as a Solution

In this section we discuss a special protocol developed to overcome the problems with mobile computers attaching to IP inter-networks. To support IP in a mobile environment, a new protocol called IP Mobility Support, or more simply, Mobile IP, was developed. The Mobile Internet Protocol (or Mobile IP version 4) is designed to overcome mobility shortcoming which enables devices to stay connected to the internet regardless of their location and without changing their IP address. Every device has allowed to have two IP addresses and by transparently maintaining the binding between the two addresses with the help of mobility binding table. One of the IP address is the permanent home address that is assigned by the home network which uniquely identified the device while other is a temporary care-of-address (or CoA) that represent current location of the user.

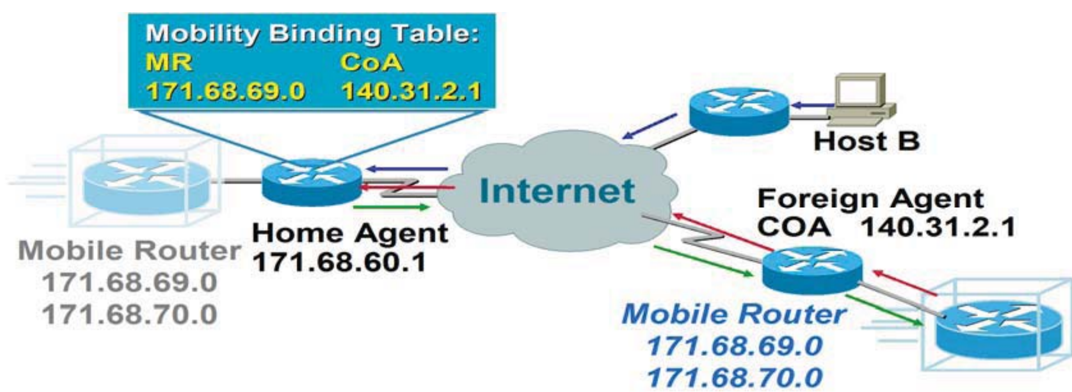

Figure 4: Mobile IP [4]

The mobility binding is maintained by some specialized routers known as mobility agents. The mobility agents are of two types

- Home agents (or HA): a designated mobile router in the home network of the mobile device which maintains the mobility binding in the "mobility binding table".
- Foreign agents (or FA): a designated mobile router in the foreign network where the mobile device is currently visiting. It maintains visitor lists which contain information about the mobile nodes currently visiting the network. Typically, the CoA of a mobile node is the foreign agent's IP address.

The whole process of Mobile IP is separates into four different stages.

1. Agent Discovery: the mobility agents advertise their presence with the help of "Agent Advertisement message" to the mobile node. A mobile node can in turn send "Agent Solicitation message" that will be responded by a mobility agent.

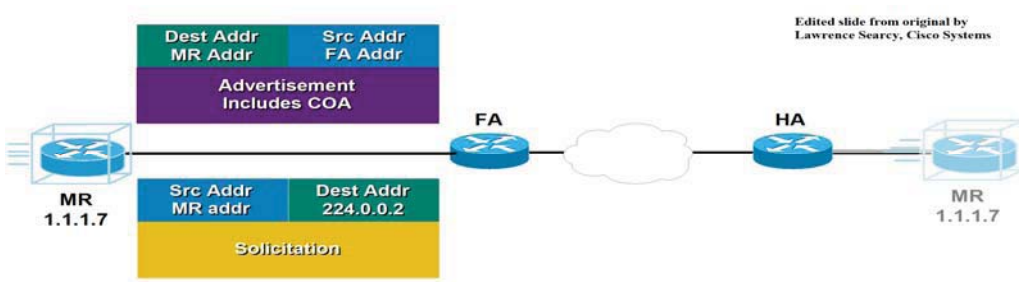

Figure 5: Agent Discovery. [4]

2. Registration: if the mobile node is on a new network, it register itself with the foreign agent by sending a "Registration Request Message"(or RRM) which includes the permanent IP address of the mobile router and the IP address of its home agent. The foreign agent in turn performs the registration process on behalf of the mobile host by sending a Registration Request containing the permanent IP address of the mobile node and IP address of the foreign agent to the home agent. The home agents update its tables after receiving request and send an acknowledgement to the foreign agent which in turn updates its visitor list.

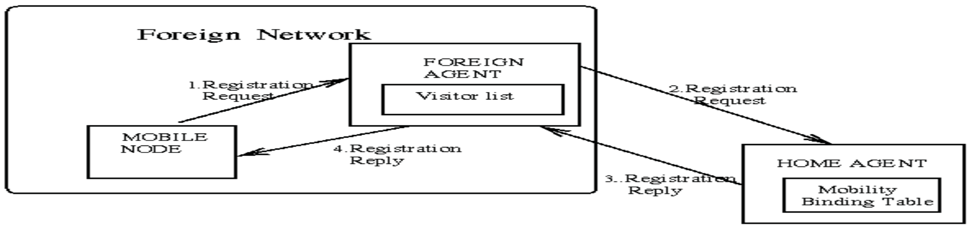

Figure 6: Registration process. [5]

3. Tunneling: whenever another device wants to send message to the mobile node. It sends a message in the form of a packet whose IP address is the permanent IP address of the mobile device. The Home agent checks the mobility binding table for the current location of the device. If the device is in another network then home agents find out the CoA of the device and construct a new IP header that contain the mobile device CoA as the destination IP address. The original packet is put into the payload of this packet and this process is known as tunneling. On the other hand, when it reaches another end, foreign agent decapsulate the original packet and sends it to the mobile node.

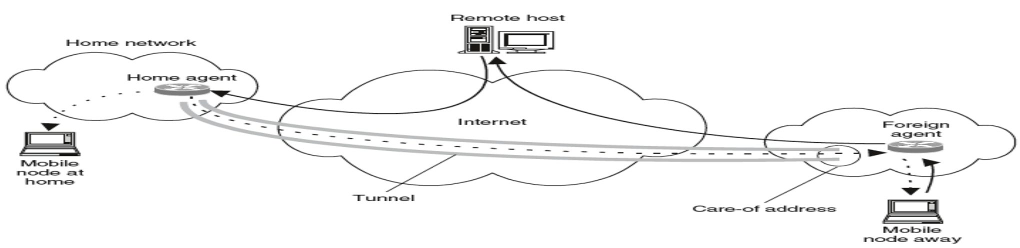

Figure 7: Tunneling in mobile IP [6].

4. Deregistration: if the mobile device want to drop its CoA, it has to deregister with its home agent. It achieves this by sending a Registration Request with the lifetime set to zero. It will automatically expire.

4.2. Issues of Mobile IPv4 and their Solutions through "Mobile IPv6"

- Problem 1: The home agent forward all packets to the mobile node wherever it may be is a convenient solution to mobility, but as the situation changes it become inefficient. Since every packet must be sent first to the home network and then be forwarded to the mobile node with the tunneling process, packet is going to travel over some part of the inter-network twice. This problem is also called triangle problem.

Some of the inefficiencies were identified in mobile internet protocol:

* Unnecessarily large end-to-end packet delay

* The HA is inevitably overloaded due to tunneling operations

* when an MH is far away from its home network, the long signaling path for CoA registration leads to a long handoff latency resulting in a high packet loss.

Let's consider the case where mobile node *M* is on a foreign network quite far from home, and a sending device, device *A*, wants to send a datagram using node *M*'s home IP address[7]. Suppose the home network is in London and the device is again in Tokyo, Japan. The following examples are arranged in order of increasing inefficiency of Mobile IP, compared to the alternative of having the mobile node just get a new temporary IP address on the foreign network and not use Mobile IP [7]:

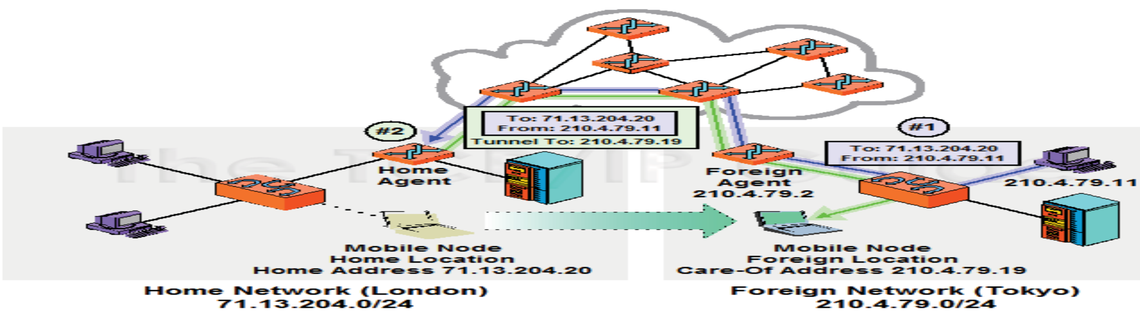

Figure 8: Inefficiency of Mobile IP [7].

This diagram show the worst possible case of Mobile IP inefficiency: when a device on the foreign network where the mobile is located tries to send to it. The sender here, 210.4.79.11, uses the mobile node's home address, so the transmission must be routed all the way back to London and then forwarded back to Tokyo, even though the two devices might be sitting on the same desk [7].

Solution: Route optimization in Mobile IPv6

Route optimization is an extension which is proposed to the mobile IP. The message from the correspondent node is directly send to the mobile node CoA rather than home address.

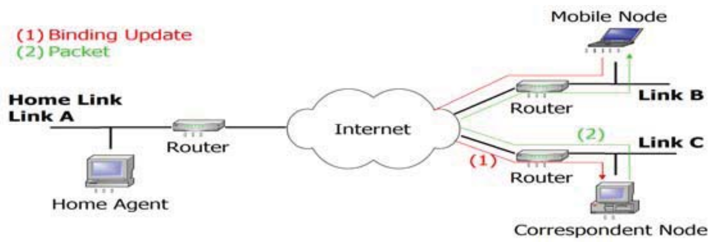

Figure 9: Route optimization principle [8]

One of the major operations of Route optimization includes updating “binding caches”. Binding caches is maintained by the correspondent node which maps mobile node home address with its current CoA. The updates have been given by the home agent by sending a Binding update message. Moreover, entries in the binding caches also associate with their lifetimes after which the entry has to be deleted from the cache. Here, lifetime is the time period for which mobile mode is registered with the foreign agent.

- Problem 2: When a mobile node register with new foreign agent, the mobile IPv4 does not specify a method to inform the previous foreign agent. Thus the packet in flight which had already tunneled to the old care-of address of the mobile node is lost.

  Solution: Handovers in Mobile IPv6

  Handovers provide a way to notify the previous foreign agent of the mobile node’s new mobility binding. If the foreign agent supports handovers, it indicates this in its Agent Advertisement message. When the mobile node moves to a new location, it requests the new foreign agent to inform its previous foreign agent about the new location as part of the registration process. The new foreign agent then construct a binding update message and sends it to the previous foreign agent of the mobile node. Thus if the previous foreign agent receive packets from a correspondent node having out-of-date binding, it forward the packets to the mobile node’s CoA.

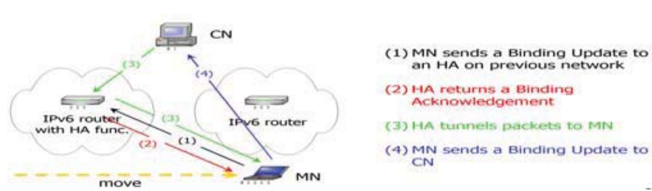

Figure 10: Handovers [8]

Handovers are the optimal solution to this problem. There are three kinds of handover designed in Mobile IPv6:

1. Smooth Handover: Minimizes data loss during the time that the Mobile Node (or MN) is establishing its link to the new access point.

2. Fast Handover: Minimizes or eliminates latency for establishing new communication paths to the MN at the new access router.

3. Seamless Handover: Both Smooth and Fast Handover

V. DHCP SUPPORT FOR MOBILE USER

5.1. Concept

DHCP (Dynamic Host Configuration Protocol) is a communications protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address, which is assigned when an Internet connection is created for a specific computer [11]. Without DHCP, the IP address must be entered manually at each computer in an organization and a new IP address must be entered each time a computer moves to a new location on the network. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network [11].

Figure 11: DHCP [12]

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses. The protocol also supports static addresses for computers that need a permanent IP address, such as Web servers.

DHCP is an extension of an earlier network IP management protocol, Bootstrap Protocol (BOOTP). DHCP is a more advanced protocol, but both configuration management protocols are commonly used and DHCP can handle BOOTP client requests. Some organizations use both protocols, but understanding how and when to use them in the same organization is important. Some operating systems, including Windows NT/2000, come with DHCP servers. A DHCP or BOOTP client is a program that is located in (and perhaps downloaded to) each computer so that it can be configured.

5.2. DHCP Process

DHCP Working in an Ethernet/IP LAN environment and assumes the client is obtaining a fresh lease without foreknowledge of the DHCP server's IP address.

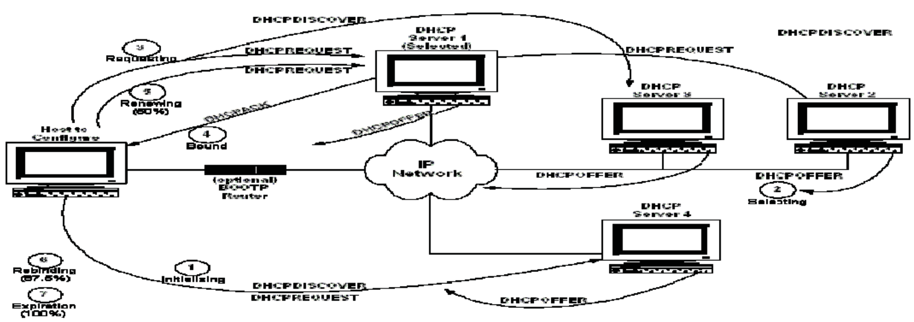

Figure 12: DHCP process in Mobile IP [13].

A. A client boots and initializes its network hardware

B. The client sends out a **DHCPDISCOVER** message formatted as follows:

- The source MAC is the client's MAC
- The destination MAC is all 1's indicating a hardware-layer broadcast (FFFFFF-FFFFFF)
- The message type is set to **DHCPDISCOVER**

C. The server hears the **DHCPDISCOVER** request and responds

- The source MAC is the server's MAC
- The destination MAC is the client's MAC
- The message type is **DHCPOFFER** containing:
    a. Server-provided IP address from pool of free addresses (the server *should* but is *not required* to check for address conflicts before offering the IP address).
    b. List of DHCP configuration parameters

D. Client responds with **DHCPREQUEST** message and does one or more of the following:

- requests values for the server-offered parameters from a single server (rejecting all offers from other servers)
- confirm the correctness of the previously allocated IP address (after the client had rebooted or lost connection to the network)
- requests extension of the lease on the specific address already supplied.

E. The server responds with

- a **DHCPACK**nowledge to confirm the server-offered options and IP previously confirmed by the client -- or-
- a **DHCPNOACK**nowledge to reject the server-offered options.
- - or -
- a **DHCPDECLINE** message to indicate to the server the address is in use.

F. The client retains the information throughout the period of its lease.

G. The client sends a **DHCPRELEASE** message to release its IP address at the DHCP server when it is leaving the network.

VI. RESOURCE DISCOVERY PROTOCOL (RDP)

6.1. Introduction

The main objective of RDP is to provide a light weight protocol which a client can use to discover network resources. It is especially targeted for mobile client whose environment may change often. In RDP the client has a mean of obtaining the address dynamically via DHCP. The basic process follows a client-server query response model. The client queries the server using a Uniform Resource Name (URN) query and server replies with one or more Uniform Resource Locator (URL) to satisfy the query. The client may then proceed to use the returned URL to access the network resources.

6.2. Resource Registration and Deregistration

RDP also support dynamic registration and deregistration of network resources which enables the server to manage the resources automatically. Mobile client use the *reg* and *dereg* request for this purpose [14]. The format of *reg/dereg* request is

<reg|dereg>:/[rp]/[na]/<url>;<desc1>[;desc2]…..

Where

rp	=	Resolution Path
na	=	naming authority
url	=	URL to be registered/deregistered
descN	=	Description of the URL

The resolution path (RP) is optionally specified by the client to direct the query to be desired RDP server [14]. In the usual cases, the resolution path is just the IP address of nearby host computer. The Naming authority (NA) specifies the organization quantity which is authorized to resolve the query and then by necessity the dictionary which is used to define the relationship between scheme and the scheme specific part of a URL [14].

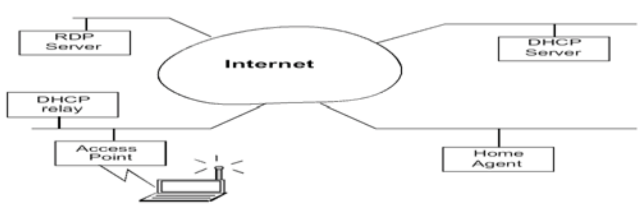

Figure 13: Mobile network and RDP [14]

Registration can be performed incrementally. The new URL will be created only if it doesn't exist in database. If the URL already exists, only the description not in the database will be added. The final URL record contains the URL and union of all descriptions.

Similarly deregistration can be performed incrementally. If no descriptions are specified, the whole URL record is deleted otherwise only the matching descriptions are added. An acknowledgement is send to the client for the successful registration and deregistration.

This completes the whole discussion about mobile computing networks.

VII. CONCLUSION

We have discussed about mobile computing and its infrastructure. The main principal of mobile computing is to distribute the load over the network and support decentralization. We discuss in briefly about DHCP [11] and RDP [14] which also plays an important role in maintaining network reliable and practical. Moreover, Mobile IP has great potential in providing trustworthy connection with mobile devices. Mobile IP is being studied in a number of research projects like Stanford University's Mosquitonet project [9] and the CMU monarch project [10].

VIII. REFERENCES

[1] Daniel Barbará "Mobile Computing and Databases¾A Survey" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING VOL. 11, NO. 1, JANUARY/FEBRUARY 1999.

[2] Nevadita Chatterjee, Anupama Potluri and Atul Negi"A Self-Organizing Approach to MANET Clustering"

[3] Dr. habil. Christian Prehofer,Research Leader,Nokia Research "Design Principles for Mobile Computing and Communication Systems Dr. habil. Christian Prehofer

[4] cicso.com

[5] http://www.coe.montana.edu/ee/rwolff/EE548/papers/MobileIP/mobileip.html

[6] http://media.techtarget.com/digitalguide/images/Misc/mobile-ip-ch10-1.gif

[7] http://www.tcpipguide.com/free/t_MobileIPEfficiencyIssues.htm

[8] IIS5711: Mobile Computing Mobile Computing and Broadband Networking Laboratory CIS, NCTU "Introduction to Mobile IPv6".

[9] Standford University, Mosquitonet Project. http:/mosquitonet.standard.edu/

[10] carnegie mellon university, monarch project. http://www. monarch.cs.cmu.edu

[11] http://searchunifiedcommunications.techtarget.com/definition/DHCP

[12] http://courseware.finntrack.eu/images/dhcp.gif

[13] http://www.multinet.process.com/ftp/docs/html/43/adminbook/figure12-1.gif

[14] charlie perkins IBM T.J. Watson Research Center ,harry harjono,Columbia University Computer Science Dept. "Resource Discovery Protocol in Mobile Computing"